MATHEMATICS OF COMPUTATION
Volume 83, Number 290, November 2014, Pages 2977–2999
S 0025-5718(2014)02816-0
Article electronically published on February 27, 2014

EVALUATING IGUSA FUNCTIONS

REINIER BRÖKER AND KRISTIN LAUTER

ABSTRACT. The moduli space of principally polarized abelian surfaces is parametrized by three Igusa functions. In this article we investigate a new way to evaluate these functions by using the Siegel Eisenstein series. We explain how to compute the Fourier coefficients of certain Siegel modular forms using classical modular forms of half-integral weight. One of the results in this paper is an explicit algorithm to evaluate the Igusa functions to a prescribed precision.

1. INTRODUCTION

The classical theory of complex multiplication gives an explicit description of the Hilbert class field of an imaginary quadratic field: for a fundamental discriminant $D < 0$, the Hilbert class field of $K = \mathbf{Q}(\sqrt{D})$ is obtained by adjoining the value $j((D + \sqrt{D})/2)$ to K. Here, $j : \mathbf{H} \to \mathbf{C}$ is the classical modular function with Fourier expansion $j(z) = 1/q + 744 + 196884q + \ldots$ in $q = \exp(2\pi iz)$. There are various ways to compute the minimal polynomial of $j((D + \sqrt{D})/2)$, and one of the most frequently used approaches proceeds by evaluating the j-function to high precision.

The j-function is invariant under the action of $\mathrm{SL}_2(\mathbf{Z})$ on the upper half plane $\mathbf{H}$. To evaluate $j(\tau)$, we may assume that τ is in the 'standard' fundamental domain for $\mathrm{SL}_2(\mathbf{Z})\backslash\mathbf{H}$ as described in e.g., [22, Sec. VII.1.1]. The naive approach to evaluate $j(\tau)$ is to simply compute enough Fourier coefficients using for instance the recursive formulas given in [20]. Alternatively, one can use the relation

$$j(z) = 1728\frac{g_2(z)^3}{g_2(z)^3 - 27g_3(z)^2} \tag{1.1}$$

expressing the j-function in terms of the *normalized Eisenstein* series g_2, g_3 of weight 4 and 6. Better results can be obtained [1] by using the Dedekind η-function defined by $\eta(z) = q^{1/24}\prod_{n=1}^{\infty}(1 - q^n)$, and which satisfies

$$j(z) = \left(\frac{(\eta(z/2)/\eta(z))^{24} + 16}{(\eta(z/2)/\eta(z))^8}\right)^3.$$

The sparsity of the q-expansion of the η-function makes it very efficient for explicit computations.

The j-function is intrinsically linked to the theory of elliptic curves, and the situation outlined above can be viewed as the 'one-dimensional' case of complex multiplication theory. In dimension 2, suitably chosen invariants of principally polarized abelian surfaces generate abelian extensions of degree 4 CM-fields; see

Received by the editor December 12, 2008 and, in revised form, June 28, 2012 and March 6, 2013.
2010 *Mathematics Subject Classification.* Primary 11F46; Secondary 14J15.

[23, Sec. 15] for a precise statement. A popular choice of invariants are the three *Igusa functions* j_1, j_2, j_3 defined below. Just as evaluating the elliptic j-function has applications to elliptic curve cryptography, evaluating Igusa functions is an important step in constructing genus 2 curves suitable for use in cryptography; see e.g. [26].

The explicit evaluation of Igusa functions is less developed than its dimension-1 counterpart. Most people use θ-functions to evaluate Igusa functions. The (rather unwieldy) formulas expressing Igusa functions in terms of θ-functions are given in e.g., [26, pp. 441–442]. There is also a direct analogue in dimension 2 of formula (1.1) which expresses the Igusa functions as rational functions in the *Siegel Eisenstein series* E_w. Indeed, Igusa [12, p. 195] defines the normalized cusp forms

$$\chi_{10} = -\frac{43867}{2^{12} \cdot 3^5 \cdot 5^2 \cdot 7 \cdot 53}(E_4 E_6 - E_{10})$$

and

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

With that, we have the three *Igusa functions*,

$$j_1 = 2 \cdot 3^5 \frac{\chi_{12}^5}{\chi_{10}^6}, \quad j_2 = 2^{-3} 3^3 \frac{E_4 \chi_{12}^3}{\chi_{10}^4}, \quad j_3 = 2^{-5} \cdot 3 \frac{E_6 \chi_{12}^2}{\chi_{10}^3} + 2^{-3} \cdot 3^2 \frac{E_4 \chi_{12}^3}{\chi_{10}^4}. \tag{1.2}$$

Igusa shows the equivalence with the definition of these functions in terms of theta functions in [11, p. 848]. The analogue of the denominator $\Delta = g_2^3 - 27 g_3^2$ appearing in (1.1) is the form χ_{10}. The form Δ is a classical cusp form of weight 12 and χ_{10} is a Siegel cusp form of weight 10.

A mathematically natural question is whether we can use formula (1.2) directly to evaluate the Igusa functions, thereby bypassing the θ-functions. The main focus of this paper is to give an explicit algorithm to evaluate the Siegel modular forms occuring in (1.2) to some prescribed accuracy. Our result gives a relatively easy way to analyze the precision necessary for the computation to succeed, and we give a *rigorous* complexity analysis for our method, something which has not been done for other approaches.

Although the asymptotic convergence of our algorithm is slower than the algorithm using theta functions, our approach has the advantage that there are fewer high precision multiplications required in the evaluation, and thus less precision loss and fewer rounding errors occur. Furthermore, we give a detailed analysis of the Eisenstein series and cusp forms, including an algorithm for computing them using classical modular forms of half-integral weight and explicit bounds on the size of the coefficients in their Fourier expansions. Indeed, one of the main contributions of the paper is the detailed analysis of various aspects of the computation of Siegel modular forms. Finally, our approach may lend itself to improvement in various ways and is a new direction in this area which could produce further progress.

Any degree 2 Siegel modular form f admits a Fourier expansion

$$f(\tau) = \sum_T a(T) \exp(2\pi i \operatorname{Tr}(T\tau)), \tag{1.3}$$

where T ranges over certain 2×2-matrices with coefficients in $\frac{1}{2}\mathbf{Z}$. We propose to evaluate the functions occuring in (1.2) by truncating the sum in (1.3) to only include matrices with trace below some bound. The Eisenstein series are Siegel

modular forms with a considerable amount of extra structure. We show that computing the Fourier coefficients of the Eisenstein series ultimately boils down to computing Fourier coefficients of classical modular forms of half-integral weight. One of the main results of this paper is the following theorem, proved in Section 4.

Theorem 1.1. *For $A, C \in \mathbf{Z}_{\geq 0}$ and $B \in \mathbf{Z}$ with $B^2 \leq 4AC$, the Fourier coefficients of the Siegel Eisenstein series E_w for all matrices $\left(\begin{smallmatrix} a & b/2 \\ b/2 & c \end{smallmatrix}\right)$ satisfying $0 \leq a \leq A$, $0 \leq c \leq C$, and $|b| \leq B$ can be computed in time $O((ABC)^{1+\varepsilon})$ for every $\varepsilon > 0$. The constant in the O-symbol depends on the weight w.*

By examining the *size* of the Fourier coefficients more closely, we derive the following result in Section 6.

Theorem 1.2. *Let $\tau \in \mathbf{H}_2$ be given, and let $\delta = \delta(\tau)$ be the supremum of all $\delta' \in \mathbf{R}$ such that $\mathrm{Im}(\tau) - \delta' 1_2$ is positive semi-definite. Assume that $\delta(\tau) \geq 1$. Assume $\chi_{10}(\tau)$ is non-zero and choose $n \in \mathbf{Z}_{>1}$ such that $|\chi_{10}(\tau)| \geq 10^{-n}$ holds.*

For a positive integer k, let $B \in \mathbf{Z}_{\geq 3}$ be such that

$$\sum_{t=B}^{\infty} 18 t^{18} \exp(-2\pi t \delta(\tau)) \leq 10^{-k-6n} \tag{1.4}$$

holds.

Then the following holds: if we approximate the modular forms $E_4, E_6, \chi_{10}, \chi_{12}$ using their truncated Fourier expansions consisting of all the matrices of trace at most $B-1$, then the values $j_1(\tau)$, $j_2(\tau)$, $j_3(\tau)$ computed via the formulas in (1.2) are accurate to precision 10^{-k}.

The condition $\delta(\tau) \geq 1$ is mostly for esthetic reasons. The proof of Theorem 1.2, given in Section 6, readily gives a method to find B in case $\delta(\tau) < 1$. We assume in Theorem 1.2 that we can bound $|\chi_{10}(\tau)|$ from below. This lower bound will allow us to bound the precision loss that occurs when we divide by $\chi_{10}(\tau)$. Using the explicit bounds on the Fourier coefficients of χ_{10}, proved in Section 5, we give a simple method to find a value of n in Section 6. This method works in general and does not depend on the value of $\delta(\tau)$. Hence, Theorem 1.2 gives an effective method to evaluate the three Igusa functions up to some prescribed precision.

Just as the elliptic j-function is invariant under $\mathrm{SL}_2(\mathbf{Z})$, the Igusa functions j_1, j_2, j_3 are invariant under the symplectic group $\mathrm{Sp}_4(\mathbf{Z})$. Hence, we may translate the argument τ by a matrix $M \in \mathrm{Sp}_4(\mathbf{Z})$ to obtain an $\mathrm{Sp}_4(\mathbf{Z})$-equivalent $\tau' \in \mathbf{H}_2$. The value $\delta(\tau')$ can be significantly different from $\delta(\tau)$; see e.g. Example 7.1. Before applying Theorem 1.2, we therefore move, using e.g. the method from [24], τ to the 'standard' fundamental domain for $\mathrm{Sp}_4(\mathbf{Z})\backslash\mathbf{H}_2$ described in [9].

The outline of the article is as follows. In Section 2 we recall basic facts about Siegel modular forms and their Fourier expansions. Section 3 introduces Jacobi forms and their relation to Eisenstein series. The approach we follow in this section is 'classical' and most likely well-known to experts working with Siegel modular forms. In Section 4 we go one step further, and relate Jacobi forms to classical modular forms of half-integral weight. This gives a very efficient method of computing the Fourier coefficients of the two-dimensional Eisenstein series. The functions χ_{10} and χ_{12} are Siegel cusp forms, and we explain in Section 5 how to compute the Fourier coefficients of these forms. We investigate the convergence of

the Fourier expansions of E_4, E_6, χ_{10} and χ_{12} in Section 6. This leads to the proof of Theorem 1.2. A final Section 7 contains two detailed examples.

2. Siegel modular forms

Let $\mathbf{H}_2 = \{\tau \in \mathrm{Mat}_2(\mathbf{C}) \mid \tau = \tau^T, \mathrm{Im}(\tau) > 0\}$ be the Siegel upper half plane. With $J = \left(\begin{smallmatrix} 0 & 1_2 \\ -1_2 & 0 \end{smallmatrix}\right)$, the symplectic group $\mathrm{Sp}_4(\mathbf{R})$ is defined as $\mathrm{Sp}_4(\mathbf{R}) = \{M \in \mathrm{GL}_4(\mathbf{R}) | MJM^T = J\}$. The group $\mathrm{Sp}_4(\mathbf{R})$ naturally acts on the Siegel upper half plane via

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

where dividing by $c\tau + d$ means multiplying on the right with the multiplicative inverse of the 2×2-matrix $c\tau + d$. The matrix -1_2 acts trivially, and it is well-known that the automorphism group of $\mathbf{H}_2$ equals $\mathrm{PSp}_4(\mathbf{R}) = \mathrm{Sp}_4(\mathbf{R})/\{\pm 1_2\}$.

A holomorphic function $f : \mathbf{H}_2 \to \mathbf{C}$ is called a *Siegel modular form* of weight $w \geq 0$ if it satisfies

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

for all τ and all matrices in the subgroup $\mathrm{Sp}_4(\mathbf{Z}) \subset \mathrm{Sp}_4(\mathbf{R})$. The integer w is called the *weight* of the form f. Whereas we have to demand that f is 'holomorphic at infinity' for classical modular forms $\mathbf{H} \to \mathbf{C}$, this is not necessary for Siegel modular forms. Indeed, the *Koecher principle* implies that f is bounded on sets of the form $\{\tau \in \mathbf{H}_2 \mid \mathrm{Im}(\tau) > \alpha 1_2\}$ for $\alpha > 0$; see [15].

The matrix $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ is contained in $\mathrm{Sp}_4(\mathbf{Z})$, and a Siegel modular function f is invariant under the transformation $\tau \mapsto \tau + 1$. In particular, a Siegel modular function f admits a *Fourier expansion*

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

Here, the sum ranges over all symmetric matrices $T \in \mathrm{Mat}(\frac{1}{2}\mathbf{Z})$ with integer diagonal entries. The coefficients $a(T)$ are called the *Fourier coefficients* of f. By the Koecher principle, they are zero in case T is not positive semi-definite.

We embed the group $\mathrm{GL}_2(\mathbf{Z})$ in $\mathrm{Sp}_4(\mathbf{Z})$ via $M \mapsto \left(\begin{smallmatrix} M & 0 \\ 0 & (M^T)^{-1} \end{smallmatrix}\right)$. As M^T has determinant ± 1, we see that a Siegel modular function f is invariant under the transformation $\tau \mapsto M\tau M^T$ for $M \in \mathrm{GL}_2(\mathbf{Z})$. This invariance is the key ingredient in the proof of the following well-known lemma.

Lemma 2.1. *The Fourier coefficients $a(T)$ of a Siegel modular form f satisfy $a(M^T TM) = a(T)$ for every $M \in \mathrm{GL}_2(\mathbf{Z})$.*

Proof. Writing $\tau = x + iy$ with $x, y \in \mathrm{Mat}_2(\mathbf{R})$, the Fourier coefficient $a(T)$ is given by

$$a(T) = \int f(\tau) e^{-2\pi i \mathrm{Tr}(T\tau)} \mathrm{d}x.$$

Here, $\mathrm{d}x$ means the Euclidean volume of the space of x-coordinates and the integral ranges over the 'box' $-1/2 \leq x_{ij} \leq 1/2$. Using the invariance of f we compute

$$a(M^T TM) = \int f(M\tau M^T) e^{-2\pi i \mathrm{Tr}(T\, M\tau M^T)} \mathrm{d}x,$$

and the lemma follows. $\square$

To a matrix $T = \left(\begin{smallmatrix} a & b/2 \\ b/2 & c \end{smallmatrix}\right)$ with $a, b, c \in \mathbf{Z}$ we associate the binary quadratic form $f_T = aX^2 + bXY + cY^2$ of discriminant $b^2 - 4ac = -4n$. An explicit check shows that for $M = \left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right)$ the quadratic form associated to $M^T T M$ equals

$$f_{M^T T M} = f_T(\alpha X + \beta Y, \gamma X + \delta Y),$$

which means that the $\mathrm{GL}_2(\mathbf{Z})$-action on $\mathbf{H}_2$ is compatible with the $\mathrm{GL}_2(\mathbf{Z})$-action on quadratic forms of discriminant $-4n$. In fact, the $\mathrm{GL}_2(\mathbf{Z})$-action on quadratic forms originally considered by Lagrange is not used that much, as it leads to a 'wrong' kind of equivalence. For quadratic forms, the 'correct' action is the action of the subgroup $\mathrm{SL}_2(\mathbf{Z}) \subset \mathrm{GL}_2(\mathbf{Z})$ studied by Gauß.

To illustrate the difference between these two groups, we investigate how many different values $a(T)$ attains for a fixed value of $n = \det(T) > 0$ in the following lemma. We remark that we will get a better bound in Theorem 3.4 later on.

Lemma 2.2. *Fix a Siegel modular form f and $n \in \frac{1}{4}\mathbf{Z}_{>0}$. Suppose that $-4n$ is a fundamental discriminant and let $\mathcal{O}$ be the maximal order of $\mathbf{Q}(\sqrt{-n})$. Then the set $\{a(T) \mid \det(T) = n\}$ has size at most $\frac{1}{2}(\#\mathrm{Pic}(\mathcal{O}) + \#\{\mathfrak{a} \in \mathrm{Pic}(\mathcal{O}) \mid 2\mathfrak{a} = 0\})$.*

Proof. If $-4n$ is fundamental, then any integer binary quadratic form $aX^2 + bXY + cY^2$ of discriminant $-4n$ is *primitive*. The set of $\mathrm{PSL}_2(\mathbf{Z})$-equivalence classes of positive definite primitive quadratic forms of discriminant $-4n$ is in bijection with the class group $\mathrm{Pic}(\mathcal{O})$ via $aX^2 + bXY + cY^2 \mapsto a\mathbf{Z} + \frac{-b+\sqrt{-4n}}{2}\mathbf{Z}$ by [3, Th. 5.2.8].

It remains to investigate when a $\mathrm{GL}_2(\mathbf{Z})$-equivalence class decomposes as 2 disjunct $\mathrm{SL}_2(\mathbf{Z})$-equivalence classes. If a fractional $\mathcal{O}$-ideal $\mathfrak{a}$ is $\mathrm{GL}_2(\mathbf{Z})$-equivalent but not $\mathrm{SL}_2(\mathbf{Z})$-equivalent to $\mathfrak{b}$, then $\mathfrak{b}$ equals the inverse $\mathfrak{a}^{-1}$ and we have $2\mathfrak{a} \neq 0$. The lemma follows. □

3. Eisenstein series

The purpose of this section is to give explicit, *effective*, bounds on the Fourier coefficients of the Siegel Eisenstein series. In order to do that, we rely heavily on background and results from Eichler and Zagier's book [8], which we summarize here as needed. We include a small correction (see the Remark after Theorem 3.4) and derive the explicit constant to make the bounds effective.

For $w \geq 0$, the space M_w of Siegel modular forms of weight w has a natural structure of a $\mathbf{C}$-vector space. For even $w \geq 4$, the primordial example of a degree w Siegel modular form is the Eisenstein series E_w defined by

$$E_w(\tau) = \sum_{c,d} (c\tau + d)^{-w}. \tag{3.1}$$

Here, the sum ranges over all inequivalent bottom rows $(c \quad d)$ of elements of $\mathrm{Sp}_4(\mathbf{Z})$ with respect to left-multiplication by $\mathrm{SL}(2, \mathbf{Z})$. The restriction $w \geq 4$ comes from the fact that the expression in (3.1) does not converge for $w = 2$.

The direct sum $M = \bigoplus_{w=0}^{\infty} M_w$ has a natural structure of a graded $\mathbf{C}$-algebra. By restricting the sum to *even* w, we get a graded subalgebra M^e. The following lemma gives the structure of these two algebras.

Lemma 3.1. *The Eisenstein series E_4, E_6, E_{10} and E_{12} are algebraically independent and generate M^e. There exists a polynomial P in 4 variables such that M is isomorphic to $M^e[X]/(X^2 - P(E_4, E_6, E_{10}, E_{12}))$. The element $\overline{X}$ corresponds to a Siegel modular form of weight 35.*

Proof. The first statement can be found in [12, pp. 194–195]. The second statement is proven in [11] with an explicit polynomial P on page 849. $\square$

The remainder of this section is devoted to deriving a 'formula' for the Fourier coefficient $a(T)$ of the Eisenstein series E_w. Let $f : \mathbf{H}_2 \to \mathbf{C}$ be a Siegel modular form of weight w. We write $\tau \in \mathbf{H}_2$ as $\tau = \left(\begin{smallmatrix} \tau_1 & \varepsilon \\ \varepsilon & \tau_2 \end{smallmatrix}\right)$. Because f is periodic with respect to τ_2, it admits a Fourier expansion

$$f(\tau) = \sum_{m=0}^{\infty} \varphi_m(\tau_1, \varepsilon) e^{2\pi i m \tau_2},$$

where φ_m is a function from $\mathbf{H} \times \mathbf{C}$ to $\mathbf{C}$. The functions φ_m have the following properties:

- $\varphi_m(\frac{a\tau_1+b}{c\tau_1+d}, \frac{\varepsilon}{c\tau_1+d}) = (c\tau_1+d)^{\omega} e^{2\pi i m c\varepsilon/(c\tau_1+d)} \varphi_m(\tau_1, \varepsilon), \quad \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbf{Z}),$
- $\varphi_m(\tau, \varepsilon + \lambda\tau + \mu) = e^{-2\pi i m(\lambda^2\tau_1 + 2\lambda\varepsilon)} \varphi_m(\tau_1, \varepsilon), \qquad (\lambda, \mu) \in \mathbf{Z}^2,$
- φ_m admits a Fourier expansion of the form $\displaystyle\sum_{n=0}^{\infty} \sum_{\substack{r \in \mathbf{Z} \\ r^2 \le 4nm}} c(n,r) e^{2\pi i(n\tau_1 + r\varepsilon)}$.

The first two properties follow from the transformation law of Siegel modular forms under the symplectic matrices

$$\begin{pmatrix} a & 0 & b & 0 \\ 0 & 1 & 0 & 0 \\ c & 0 & d & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \qquad \text{and} \qquad \begin{pmatrix} 1 & 0 & 0 & \mu \\ \lambda & 1 & \mu & 0 \\ 0 & 0 & 1 & -\lambda \\ 0 & 0 & 0 & 1 \end{pmatrix},$$

and the third property follows from the Koecher principle.

A holomorphic function $g : \mathbf{H} \times \mathbf{C} \to \mathbf{C}$ satisfying the three properties above for some w and m is called a *Jacobi form* of weight w and index m. Jacobi forms can be seen as an 'intermediate' between Siegel modular forms and classical modular forms. Indeed, the 'Fourier coefficients' of a Siegel modular form of weight w are Jacobi forms of weight w, and for a Jacobi form g, the function $g(\tau, 0)$ is a classical modular form of weight w.

The space of all Jacobi forms of weight w and index m is denoted by $J_{w,m}$, and we have maps

$$M_w \hookrightarrow \prod_{m \ge 0} J_{w,m} \overset{\mathrm{pr}}{\twoheadrightarrow} J_{w,1},$$

where pr denotes the projection onto the first factor. For this article, the key property of Jacobi forms is that we can also construct a map $J_{w,1} \to M_w$ which will allow us to identify certain Siegel modular forms with its 'first' Jacobi form. As we have $J_{w,1} = 0$ for *odd* w by [8, Th. 2.2], we restrict to *even* weight w for the remainder of this section.

For $m \ge 0$, we define the 'Hecke operator' $V_m : J_{w,1} \to J_{w,m}$ as follows. For $g \in J_{w,1}$ with Fourier expansion $\sum_{n,r} c(n,r) e^{2\pi i(n\tau_1 + r\varepsilon)}$, we put

$$V_m(g) = \sum_{n,r} \left(\sum_{a \mid \gcd(n,r,m)} a^{w-1} c\left(\frac{nm}{a^2}, \frac{r}{a}\right) \right) e^{2\pi i(n\tau_1 + r\varepsilon)}$$

for $m > 0$. This is the natural generalization of the Hecke operators for classical modular forms; see e.g., [22, Prop. VII.12]. For $m = 0$, we put

$$V_0(g) = -\frac{B_w c(0,0)}{2w}\left(1 - \frac{2w}{B_w}\sum_{n\geq 1}\sigma_{w-1}(n)e^{2\pi i n\tau_1}\right)$$

with $\sigma_n(x)$ the sum of the nth powers of the divisors of x and B_w the wth Bernoulli number defined by $t/(e^t-1) = \sum_{n=0}^{\infty} B_n t^n/n!$. In particular, the function $V_0(g)$ is a multiple of the classical Eisenstein series of weight w. It is not hard to show that the function

$$\Psi(g) = \sum_{m\geq 0} V_m(g)(\tau_1,\varepsilon)e^{2\pi i m\tau_2}$$

defines a Siegel modular form of weight w; see [8, Th. 6.2].

Lemma 3.2. *The map $\Psi : J_{w,1} \to M_w$ is injective.*

Proof. This follows directly from the fact that the composition

$$J_{w,1} \xrightarrow{\Psi} M_w \hookrightarrow \prod_{m\geq 0} J_{w,m} \overset{\mathrm{pr}}{\twoheadrightarrow} J_{w,1}$$

is the identity. □

We stress that the map Ψ is in general *not* surjective. The image $\Psi(J_{k,1})$ is known as the *Maaß Spezialschar*. However, the Eisenstein series $E_w \in M_w$ do occur at the image of a Jacobi form. They are the images of the *Jacobi Eisenstein series* E_w^J defined by the formula

$$E_w^J(\tau,z) = \frac{1}{2}\sum_{\substack{c,d\in\mathbf{Z}\\ \gcd(c,d)=1}}\sum_{\lambda\in\mathbf{Z}}(c\tau+d)^{-w}\exp\left(2\pi i\left(\lambda^2\frac{a\tau+b}{c\tau+d} + 2\lambda\frac{z}{c\tau+d} - \frac{cz^2}{c\tau+d}\right)\right)$$

for $w \geq 4$. Here, a and b are integers such that $\left(\begin{smallmatrix} a & b\\ c & d\end{smallmatrix}\right)$ is contained in $\mathrm{SL}_2(\mathbf{Z})$. We note that E_w^J can be defined as the sum of translates of the function $1_{|w,1}$ over cosets, just like the regular Eisenstein series. We refer to [8, Sec. 2] for details.

Lemma 3.3. *We have $E_w = \Psi\left(\frac{-2w}{B_w}E_w^J\right)$.*

Proof. It follows from [8, Th. 6.3] that E_w is a multiple of $\Psi(E_w^J)$. Both the Siegel Eisenstein series E_w and the Jacobi Eisenstein series E_w^J are normalized with constant coefficient 1. The lemma follows. □

It is now a straightforward matter to compute the Fourier coefficients of the Siegel Eisenstein series. The result is the following theorem.

Theorem 3.4. *Let E_w be the Siegel Eisenstein series of weight w, and let $T = \left(\begin{smallmatrix} a & b/2\\ b/2 & c\end{smallmatrix}\right) \in \mathrm{Mat}(\frac{1}{2}\mathbf{Z})$ be a positive semi-definite matrix with integer entries on the diagonal. Write $D = b^2 - 4ac \leq 0$ and let D_0 be the discriminant of $\mathbf{Q}(\sqrt{D})$. Then the Fourier coefficient $a(T)$ equals 1 for $a = b = c = 0$ and*

$$\frac{-2w}{B_w}\sum_{d|\gcd(a,b,c)} d^{w-1}\alpha(D/d^2)$$

otherwise. Here, B_k is the kth Bernoulli number and α is defined by $\alpha(0) = 1$, $\alpha(D) = 0$ if $D < 0$ is not a discriminant and

$$\alpha(D) = \frac{1}{\zeta(3-2w)} H(w-1, D)$$

otherwise. Here, H is Cohen's function defined by

$$H(s-1, D) = L_{D_0}(2-s) \sum_{d|f} \mu(d) \left(\frac{D_0}{d}\right) d^{s-2} \sigma_{2s-3}(f/d), \qquad D = D_0 f^2.$$

In this formula, ζ denotes the Dedekind ζ-function, L_{D_0} is the quadratic Dirichlet L-series, μ is the Möbius function, $\left(\frac{\cdot}{\cdot}\right)$ is the Kronecker symbol and $\sigma_n(x)$ denotes the sum of the nth powers of the divisors of x.

Proof. By [8, Th. 2.1], the term $\alpha(D/d^2)$ equals the Fourier coefficient $c(n, r)$ of the Jacobi Eisenstein series E_w^J with $D/d^2 = r^2 - 4n$. By Lemma 3.3, we have to apply the Hecke operators V_m to these coefficients. The theorem follows. □

Remark. A formula for $a(T)$ is also given in Corollary 2 of [8, Th. 6.3]. In this formula, the Bernoulli numbers and the ζ-function from Theorem 3.4 are missing.

Remark. In the case $D = 0$, we have $\mathbf{Q}(\sqrt{D}) = \mathbf{Q}$, and Theorem 3.4 reads that we have

$$a(T) = \frac{-2w}{B_w} \sum_{d|\gcd(a,b,c)} d^{w-1}$$

for $\mathrm{Tr}(T) \neq 0$.

Theorem 3.4 implies that for fundamental discriminants $-4n$, we have only *one* Fourier coefficient, $a(T)$. In general, the number of coefficients is bounded by the number of square divisors of $-4n$, which in turn is bounded by $O(n^\varepsilon)$ for all $\varepsilon > 0$. These bounds hold in general for functions in the Spezialschar $\Psi(J_{w,1}) \subset M_w$. Indeed, the Fourier coefficients $c(n, r)$ of a function $g \in J_{w,1}$ only depend on the value $4n - r^2$; cf. [8, Th. 2.2].

Corollary 3.5. *Let n_k be the numerator of the kth Bernoulli number B_k. Then the Fourier coefficient $a(T)$ of the Siegel Eisenstein series E_w for the matrix $T = \left(\begin{smallmatrix} a & b/2 \\ b/2 & c \end{smallmatrix}\right)$ is contained in the set $1/(n_w n_{2w-2})\mathbf{Z} \subset \mathbf{Q}$.*

Proof. As we have $\zeta(3-2w) = -B_{2w-2}/(2w-2)$, all we have to do is examine the denominator of the value $L_{D_0}(2-w)$ occuring in Theorem 3.4. This is most easily done using the p-adic L-series as in [4, Ch. 11]. The corollary follows from [4, Cor. 11.4.3] except in the following case: the discriminant of $\mathbf{Q}(\sqrt{b^2-4ac})$ equals $-p$ for an odd prime p with $w - 1 \equiv (p-1)/2 \bmod (p-1)$. If this is the case, we a priori find that the denominator of the L-value could be divisible by $p(w-1)$. However, the prime p then satisfies $(p-1) \mid (2w-2)$ and by the Clausen-von Staudt theorem [4, Cor. 9.5.15] the prime p also occurs in the denominator of B_{2w-2}. Finally, $w-1$ is a divisor of the denominator of $\zeta(3-2w)$. □

Corollary 3.6. *The Fourier coefficient $a(T)$ of the Siegel Eisenstein series E_w for the matrix $T = \left(\begin{smallmatrix} a & b/2 \\ b/2 & c \end{smallmatrix}\right)$ satisfies $|a(T)| = O((4ac-b^2)^{w-3/2})$ if $b^2 - 4ac$ is non-zero.*

Proof. Using the functional equation for Dirichlet L-series, see e.g., [4, Th. 10.2.6], we bound $L_{D_0}(2-w) = O(D_0^{w-3/2})$. The inequalities

$$\frac{\sigma_n(x)}{x^n} = \sum_{d|x} \frac{1}{d^n} \leq \sum_{d=1}^{\infty} \frac{1}{d^n} = \zeta(n) < \infty$$

give $\sigma_n(x) = O(x^n)$ for $n > 1$. It follows that the $c(D')$ in Theorem 3.4 is of size $O(D'^{w-3/2})$. As $\sum_{d|n} d^{w-1}/d^{2w-3}$ is finite for $w \geq 4$ and $n \to \infty$, the corollary follows. □

Remark 3.7. It is not hard to make the constant in the O-symbol explicit. One can take

$$\left| \frac{4w(w-2)!\,\zeta(w-1)^2\zeta(2w-3)\zeta(w-2)}{\pi^{w-1}\zeta(3-2w)B_w} \right|.$$

4. Computing special values of the L-series

The hard part in computing Fourier coefficients of the Siegel Eisenstein series is computing the special values of the L-series occuring in Theorem 3.4. If the discriminant of the quadratic field $\mathbf{Q}(\sqrt{b^2-4ac})$, corresponding to the matrix $\left(\begin{smallmatrix} a & b/2 \\ b/2 & c \end{smallmatrix}\right)$, is small these computations can be efficiently done, by employing generalized Bernoulli numbers as we now explain.

For $n \geq 1$, we let χ_n be the quadratic Dirichlet character modulo n and define the χ_n-*Bernoulli numbers* $B_k(\chi_n)$ by the expansion

$$\frac{\sum_{r=1}^{n} \chi_n(r) t e^{rt}}{e^{nt}-1} = \sum_{k \geq 0} \frac{B_k(\chi_n)}{k!} t^k \in \mathbf{Q}[t]. \tag{4.1}$$

The generalized Bernoulli numbers $B_k(\chi_n)$ equal the ordinary Bernoulli numbers B_k for $n = 1$ and $k \geq 2$.

Lemma 4.1. *For $n \geq 1$ and $w \geq 2$, we have $L_n(2-w) = -B_{w-1}(\chi_n)/(w-1)$.*

Proof. See [25, Th. 4.2]. □

The values $B_{w-1}(\chi_n)$ can easily be computed using the definition (4.1) for small w and n. For evaluating the Igusa functions, we are only interested in the values $w = 4, 6, 10, 12$, and by computing $B_{11}(\chi_n)$ we get the other values $B_9(\chi_n), B_5(\chi_n)$ and $B_3(\chi_n)$ 'for free'.

To compute the Fourier coefficients of the Eisenstein series E_w for *large* values of $D = b^2 - 4ac$, we clearly need another method. It is a relatively well-known fact that Jacobi forms of even weight and index 1 'correspond to' classical modular forms of half-integral weight. Explicitly, for a discriminant $D \leq 0$, we define $\alpha_w(D)$ as in Theorem 3.4. Following Cohen, we define the function $C_w : \mathbf{H} \to \mathbf{C}$ by

$$C_w(z) = \sum_{n=0}^{\infty} \alpha_w(-n) q^n \qquad (q = \exp(2\pi i z)).$$

Lemma 4.2. *Let C_w be defined as above. Then C_w is a modular form of weight $w - 1/2$ for the congruence subgroup $\Gamma_0(4)$.*

Proof. See [5, Th. 3.1], or an alternate proof in [14, Prop. IV.6]. □

Remark. The bound $\alpha_w(n) = O(n^{w-3/2})$ from the proof of Corollary 3.6 is in nice accordance with the general result that the Fourier coefficients of a modular form of weight k are of size $O(n^{k-1})$.

As the $\mathbf{C}$-vector space of modular forms of fixed (half-integral) weight is finite dimensional, we can easily compute coefficients of C_w given a basis for the vector space. It is not hard to show that the function

$$\theta(z) = \sum_{n\in\mathbf{Z}} q^{n^2} = 1 + 2\sum_{n=1}^{\infty} q^{n^2} \qquad (q = e^{2\pi i z})$$

is a modular form of weight 1/2 for $\Gamma_0(4)$. The function

$$\widetilde{\theta}(z) = \theta^4(z+1/2) = \Big(1 + 2\sum_{n=1}^{\infty}(-1)^n q^{n^2}\Big)^4 \qquad (q = e^{2\pi i z})$$

is therefore a modular form of weight 2. Analogous to the proof of [14, Prop. IV.4], it follows that θ and $\widetilde{\theta}$ generate the $\mathbf{C}$-*algebra* of all level 4 half-integral weight forms.

Proposition 4.3. *The following equalities hold:*

$$\begin{aligned}
C_4 &= \frac{\theta^7 + 7\theta^3\widetilde{\theta}}{8},\\
C_6 &= \frac{-\theta^{11} + 22\theta^7\widetilde{\theta} + 11\theta^3\widetilde{\theta}^2}{32},\\
C_{10} &= \frac{-43867\theta^{19} + 725876\theta^{15}\widetilde{\theta} + 12824886\theta^{11}\widetilde{\theta}^2 + 8845412\theta^7\widetilde{\theta}^3 + 107597\theta^3\widetilde{\theta}^4}{22459904},\\
C_{12} &= \frac{77683\theta^{23} + 212405\theta^{19}\widetilde{\theta} + 38627902\theta^{15}\widetilde{\theta}^2 + 100820362\theta^{11}\widetilde{\theta}^3}{159094784}\\
&\quad + \frac{193139951\theta^7\widetilde{\theta}^4 + 42481\theta^3\widetilde{\theta}^5}{159094784}.
\end{aligned}$$

Proof. Using Lemma 4.1, we compute the first few Fourier coefficients of C_w for $w = 4, 6, 10, 12$. With the obervation that C_w equals an *isobaric* polynomial in θ and $\widetilde{\theta}$, we have to solve a system of $w/2$ equations in $w/2$ unknowns. The proposition follows. □

The main reason that we chose $\theta, \widetilde{\theta}$ as a basis is that these two functions have a very lacunary Fourier expansion. Indeed, Proposition 4.3 now allows us to compute the first N coefficients of C_w in time $O(N^{1+o(1)})$ using fast multiplication techniques. This leads to the theorem stated in the introduction. An important conclusion is that it is much faster to compute L-values *simultaneously* than to compute them individually.

Corollary 4.4. *For $A, C \in \mathbf{Z}_{\geq 0}$ and $B \in \mathbf{Z}$ with $B^2 \leq 4AC$, the Fourier coefficients of the Siegel Eisenstein series E_w for all matrices $\left(\begin{smallmatrix} a & b/2 \\ b/2 & c \end{smallmatrix}\right)$ satisfying $0 \leq a \leq A$, $0 \leq c \leq C$, $|b| \leq B$ can be computed in time $O((ABC)^{1+\varepsilon})$ for every $\varepsilon > 0$. The constant in the O-symbol depends on the weight w.*

5. Cusp forms

5.1. **Siegel cusp forms in the Spezialschar.** The techniques explained in Sections 3 and 4 allow us to efficiently compute the Fourier coefficients of the Siegel Eisenstein series. This suffices for evaluating Igusa functions, since these functions are rational expressions in E_w for $w = 4, 6, 10, 12$. However, the denominators of the Igusa functions have more structure: they are Siegel cusp forms. It is a natural question to ask if we can compute the Fourier coefficients of χ_{10} *directly* via Jacobi forms. We explain this method in this section.

Let M_w^1 be the vector space of classical modular forms of integral weight w, and let $M^1 = \bigoplus_{w\geq 0} M_w^1$ be the space of all classical modular forms. It is well known that we have $M^1 \cong \mathbf{C}[E_4^1, E_6^1]$, with E_w^1 the classical Eisenstein series of weight w; see [22, Cor. 2 to Th. VII.4]. We define the *Siegel operator* $S : M \to M^1$ as follows. For a Siegel modular form $f : \mathbf{H}_2 \to \mathbf{C}$ with Fourier expansion $f(\tau) = \sum_T a(T)\exp(2\pi i \mathrm{Tr}(T\tau))$, we put

$$S(f) = \sum_{n\geq 0} a\left(\begin{pmatrix} n & 0 \\ 0 & 0 \end{pmatrix}\right) e^{2\pi i n \tau_1}, \qquad \text{with } \tau = \begin{pmatrix} \tau_1 & \varepsilon \\ \varepsilon & \tau_2 \end{pmatrix}.$$

The Siegel operator is a ring homomorphism $M \to M^1$, and it maps Eisenstein series to Eisenstein series. In fact, for the Eisenstein series E_w, it is the composition of the maps

$$M_w \longrightarrow \prod_{m\geq 0} J_{w,m} \overset{\mathrm{pr}}{\twoheadrightarrow} J_{w,0} \longrightarrow M_w^1,$$

introduced in Section 2.

A Siegel modular form f is called a *cusp form* if it satisfies $S(f) = 0$. Equivalently, f is a cusp form if and only if the Fourier coefficients $a(T)$ are zero for all semi-definite T that are not definite. It follows from well-known identities between the classical Eisenstein series that

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

and

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

are cusp forms. The constants in χ_{10} and χ_{12} should be regarded as 'normalization factors'.

Lemma 5.1. *The ideal of cusp forms in M^e is generated by χ_{10} and χ_{12}. The ideal of cusp forms in M is generated by χ_{10}, χ_{12} and a modular form χ_{35} of weight 35 corresponding to $\overline{X}$ in Lemma 3.1*

Proof. See [13, Th. 3]. □

It is well-known that the cusp forms χ_{10} and χ_{12} are contained in the Maaß Spezialschar $\Psi(J_{k,1})$, the gist of the proof being [8, Th. 6.3]. A Jacobi form $g \in J_{w,m}$ is called a *cusp form* if its Fourier coefficients $c(n, r)$ are zero for $4nm - r^2 = 0$. In particular, the map

$$M_w \to \prod_{m\geq 0} J_{w,m} \overset{\mathrm{pr}}{\twoheadrightarrow} J_{w,1}$$

maps Siegel cusp forms to Jacobi cusp forms. In weight 10 and 12 we have the Jacobi cusp forms

$$\varphi_{10,1} = \frac{1}{144}(E_6^1 E_{4,1} - E_4^1 E_{6,1}) \qquad \text{and} \qquad \varphi_{12,1} = \frac{1}{144}((E_4^1)^2 E_{4,1} - E_6 E_{6,1}),$$

with $E_4^1 = 1+240\sum_{n>0}\sigma_3(n)q^n$ and $E_6^1 = 1-504\sum_{n>0}\sigma_5(n)q^n$ being the classical Eisenstein series. The factor 144 should again be regarded as a normalization factor.

Lemma 5.2. *We have* $\chi_{10} = \Psi(-\varphi_{10,1}/4)$ *and* $\chi_{12} = \Psi(\varphi_{12,1}/12)$.

Proof. The cusp forms χ_{10} and χ_{12} are contained in the Spezialschar and therefore occur as images of Jacobi cusp forms. The spaces of Jacobi cusp forms of weight 10 and 12 are one-dimensional by [8, Th. 3.5]. Using Theorem 3.4, we compute

$$a\left(\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}\right) = \frac{1}{2}$$

for a Fourier coefficient of χ_{10} and

$$c(1,0) = -2$$

for the corresponding coefficient of $\varphi_{10,1}$. The result for χ_{10} follows. The computation for χ_{12} yields

$$a\left(\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}\right) = \frac{5}{6} \qquad \text{and} \qquad c(1,0) = 10.$$

The lemma follows. □

To compute the Fourier coefficients of $\varphi_{10,1}$ and $\varphi_{12,1}$ we note that the coefficients $c_{\varphi_{10,1}}(n,r)$ and $c_{\varphi_{12,1}}(n,r)$ only depend on the value of $4n - r^2 \geq 0$. Furthermore, the functions

$$K_{10} = \sum_{k\geq 0} c_{\varphi_{10,1}}(k)q^k \qquad \text{and} \qquad K_{12} = \sum_{k\geq 0} c_{\varphi_{12,1}}(k)q^k$$

are classical modular *cusp forms*, for the group $\Gamma_0(4)$, of weight $9\frac{1}{2}$ and $11\frac{1}{2}$ respectively, by [8, Th. 5.4].

Proposition 5.3. *Let* θ *and* $\widetilde{\theta}$ *be as in Section 4. Then we have*

$$\begin{aligned} K_{10} &= \frac{\theta^{15}\widetilde{\theta} - 3\theta^{11}\widetilde{\theta}^2 + 3\theta^7\widetilde{\theta}^3 - \theta^3\widetilde{\theta}^4}{4096},\\ K_{12} &= \frac{5\theta^{19}\widetilde{\theta} - 16\theta^{15}\widetilde{\theta}^2 + 18\theta^{11}\widetilde{\theta}^3 - 8\theta^7\widetilde{\theta}^4 + \theta^3\widetilde{\theta}^5}{16384}. \end{aligned}$$

Proof. Analogous to the proof of Proposition 4.3. □

Proposition 5.3 allows us to compute the Fourier coefficients of χ_{10} and χ_{12}, which in turn enables us to evaluate the Siegel cusp forms χ_{10} and χ_{12} at arbitrary points $\tau \in \mathbf{H}_2$. For the proof of Theorem 1.2, we need a bound on the size of the Fourier coefficients of χ_{10} and χ_{12} as well. We need an *explicit* bound, like the bound in Remark 3.7.

For the remainder of Section 5.1 we let T be positive definite. Then the 'Resnikoff-Saldaña conjecture' ([21])

$$|a(T)| = O((\det T)^{w/2-3/4+\varepsilon})$$

for the size of a Fourier coefficient $a(T)$ of a Siegel modular cusp form of weight w is known to be false in general. Counterexamples are for instance provided by Siegel cusp forms that are *lifts* of classical modular cusp forms; see [2, Example 2.2]. In particular, the modular forms χ_{10}, χ_{12} that we are interested in do not satisfy the Reskinoff-Saldaña conjecture.

At this moment, the best known general result is

$$|a(T)| = O((\det T)^{w/2-13/36+\varepsilon})$$

for every $\varepsilon > 0$; see [16]. We will prove in Section 5.2 that the Fourier coefficients of χ_{10} and χ_{12} satisfy

$$|a(T)| = O((\det T)^{w/2-1/2+\varepsilon}),$$

and we will make the constant in the O-symbol explicit. The reason that our bound is better than the bound in [16] is that our Siegel modular forms lie in the Maaß Spezialschar, and this allows us to give a stronger bound. In fact, we will show that if the Lindelöf-hypothesis is true, the Fourier coefficients *for squarefree* $\det(T)$ satisfy the Reskinoff-Saldaña conjecture. This shows that the obstruction to the Reskinoff-Saldaña conjecture comes from the case that $\det(T)$ is non-squarefree, and the obstruction is of size $O((\det T)^{1/4+\varepsilon})$.

5.2. **Bounding Fourier coefficients.** First we will bound the Fourier coefficients of K_{10} and K_{12} explicitly. One approach would be to adapt 'Hecke's proof' [22, Th. VII.5] for cusp forms. This technique would yield a bound of $O(n^{4.75})$ for K_{10}, where we can make the constant in the O-symbol explicit. However, our modular forms have considerably more structure and we will use a variant of Waldspurger's formula to obtain a better bound.

The modular forms K_{10} and K_{12} have the property that their Fourier coefficients $c(n)$ are zero for $n \equiv 1, 2 \bmod 4$. As a consequence, they are contained in a *subspace*, known as Kohnen's plus space, of the space of all weight $w-1/2$ forms; see [8, Sec. 6]. As Kohnen's plus space is one-dimensional for $w = 10, 12$, both K_{10} and K_{12} are Hecke eigenforms. For every Hecke eigenform f of weight $w - 1/2$, Shimura constructs, see e.g., [8, Sec. 5], an integral weight cuspform g of weight $2w - 2$ with the property that

$$c(|D|)^2 = \frac{\langle f, f\rangle}{\langle g, g\rangle} \frac{(w-2)!}{\pi^{w-1}} L(g, \chi_D, w-1)|D|^{w-3/2} \tag{5.1}$$

holds for the Fourier coefficient $c(|D|)$ of f. In formula (5.1), known as Waldspurger's formula, $\langle \cdot, \cdot \rangle$ denotes the usual Petersson inner product, and $L(g, \chi_D, s)$ is the L-series associated to g, twisted by the quadratic Dirichlet character χ_D. For a non-fundamental D one should be careful how to define the L-series; we refer to [17] for details.

First we reduce the question of bounding $c(D)$ to the case that D is fundamental. Let f be either K_{10} or K_{12} of weight $w - 1/2$. It is well-known (one carefully goes through the Shimura correspondence) that the Fourier coefficients $c(n^2|D|)$ and $c(|D|)$ of f are related by

$$c(n^2|D|) = c(|D|) \cdot \sum_{d|n} \mu(d) \left(\frac{D}{d}\right) d^{w-2} b(n/d),$$

where b is the Fourier coefficient of the corresponding integral weight form $g = \sum b(n)q^n$. We can easily estimate the sum on the right-hand side; the result is the following lemma.

Lemma 5.4. *For $D < 0$, the Fourier coefficient $c(n^2|D|)$ of $f = K_{10}, K_{12}$ satisfies*

$$c(n^2|D|) \leq C(\varepsilon)^2 n^{w-3/2+2\varepsilon} c(|D|)$$

for every $\varepsilon > 0$. Here, C is defined by $C(x) = \exp(2^{1/x}/(x \log 2))$.

Proof. We bound

$$\sum_{d|n} \mu(d) \left(\frac{D}{d}\right) d^{w-2} b(n/d) \leq \sum_{d|n} d^{w-2} b(n/d) \leq \sum_{d|n} \left(d^{w-2} (n/d)^{w-3/2} \sum_{f|(n/d)} 1 \right),$$

where the last inequality is due to Deligne [7, Thm. 8.2]. The lemma now follows from the bound $\sum_{d|n} 1 \leq C(\varepsilon) n^{\varepsilon}$ from e.g., [10, Sec. 18.1]. □

We continue with bounding the Fourier coefficient $c(|D|)$ for a fundamental discriminant $D < 0$. First we bound the quotient of the Petersson inner products occuring in (5.1).

Lemma 5.5. *Let g_{18}, g_{22} be the modular forms associated to K_{10}, K_{12} respectively under Shimura's construction. Then we have*

$$75633 \leq \frac{\langle g_{18}, g_{18} \rangle}{\langle K_{10}, K_{10} \rangle} \leq 75634 \qquad \textit{and} \qquad 1197338 \leq \frac{\langle g_{22}, g_{22} \rangle}{\langle K_{12}, K_{12} \rangle} \leq 1197339.$$

Proof. As the space of weight 18 cusp forms is one-dimensional, we have $g_{18} = \Delta E_6^1$. Likewise, $g_{22} = \Delta E_{10}^1$. By formula (5.1) we have

$$\frac{\langle g_{18}, g_{18} \rangle}{\langle K_{10}, K_{10} \rangle} = \frac{L(g_{18}, \chi_D, 9)}{c(|D|)^2} \cdot \frac{8!}{\pi^9} |D|^{8.5}$$

for every discriminant $D < 0$ for which the Fourier coefficient $c(|D|)$ of K_{10} is non-zero. Since we can compute the Fourier coefficients of K_{10}, it suffices to explicitly evaluate the L-series at the center of the critical strip.

Since g_{18} is a Hecke eigenform, the formula

$$(2\pi)^{-s} \Gamma(s) L(g_{18}, \chi_D, s) = \int_0^\infty g_{18}(iy) y^s dy/y$$

is valid for all $s \in \mathbf{C}$. Analogous to the example in [17], we derive the relation

$$L(g_{18}, \chi_D, 9) = \frac{2}{\Gamma(9)} (2\pi/|D|)^9 \sum_{n=1}^{\infty} \left(\frac{D}{n}\right) b(n) \phi_8(2\pi n/|D|) \tag{5.2}$$

for $g_{18} = \sum_n b(n) n^{-s}$. Here, we write

$$\phi_8(x) = \int_1^\infty y^8 \exp(-xy) dy = \frac{8!}{x^9} \exp(-x) \left(1 + x + x^2/2! + \ldots + x^8/8!\right).$$

The right-hand side of (5.2) converges exponentially fast, and since we know the Fourier coefficients of g_{18} we easily compute the first bound of the lemma.

Since the space of weight 22 cusp forms is also one-dimensional, the bound for K_{12} follows analogously. □

Lemma 5.6. *For every $\varepsilon > 0$, the twisted L-series associated to the cusp forms g_{18} and g_{22} satisfy*

$$|L(g_{18}, \chi_D, 9)| \leq B(\varepsilon, 9)|D|^{0.5+\varepsilon}, \qquad |L(g_{22}, \chi_D, 11)| \leq B(\varepsilon, 11)|D|^{0.5+\varepsilon}$$

for all fundamental discriminants $D < 0$. Here, B is defined by

$$B(\varepsilon, n) = \frac{1}{\sqrt{2\pi}} \max\left\{\zeta(1+\varepsilon)^2, \zeta(1+\varepsilon)^2 \frac{\Gamma(n+1/2+\varepsilon)}{\Gamma(n-1/2-\varepsilon)}\right\}.$$

Proof. Let $g = \sum_m b(m)q^m$ be either g_{18} or g_{22}, and let $2w$ be the weight of g. With $\Lambda(s, \chi_D) = \left(\frac{D}{2\pi}\right)^s \Gamma(s+w-1/2)L(g, \chi_D, s+w-1/2)$, the twisted L-series for g satisfies the functional equation

$$\Lambda(s, \chi_D) = \Lambda(1-s, \chi_D)$$

for all $s \in \mathbf{C}$. We will bound $L(g, \chi_D, s)$ on a vertical line to the right of the critical strip, which by the functional equation gives a bound on a vertical line to the left of the critical strip. A variant of the Phragmen-Lindelöf theorem will then give the result.

We put $P(s) = \left(\frac{D}{2\pi}\right)^s L(g, \chi_D, s+w-1/2)$ and $A(m) = b(m)/m^{w-1/2}$. We have $L(g_{18}, \chi_D, s+w-1/2) = \sum_m \frac{A(m)\chi_D(m)}{m^s}$, and the coefficients $A(m)$ are bounded by $\sigma_0(m) = \sum_{d|m} 1$ by Deligne's theorem [7, Th. 8.2]. For any $\varepsilon > 0$ and any $t \in \mathbf{R}$, we bound

$$|L(g_{18}, \chi_D, 1+\varepsilon+w-1/2)| \leq \sum_m \frac{|A(m)|}{m^{1+\varepsilon}} \leq \sum_m \frac{\sigma_0(m)}{m^{1+\varepsilon}} = \zeta(1+\varepsilon)^2.$$

We get $|P(1+\varepsilon+it)| \leq \frac{|D|^{1+\varepsilon}\zeta(1+\varepsilon)^2}{2\pi} = U_1(\varepsilon)|D|^{1+\varepsilon}$, with $U_1(\varepsilon) = \frac{\zeta(1+\varepsilon)^2}{2\pi}$. Using the functional equation, we bound

$$|P(-\varepsilon+it)| \leq \left|\frac{|D|^{1+2\varepsilon}}{2\pi} \frac{\Gamma(1+\varepsilon-it+w-1/2)}{\Gamma(-\varepsilon+it+w-1/2)} \zeta(1+\varepsilon-it)^2\right|$$

$$\leq U_2(\varepsilon)(1+|t|)^{1+2\varepsilon} U_1(\varepsilon)|D|^{1+2\varepsilon},$$

where we can use $U_2(\varepsilon) = \frac{\Gamma(w+1/2+\varepsilon)}{\Gamma(w-1/2-\varepsilon)}$ by Stirling's formula.

By the Phragmen-Lindelöf theorem, see e.g. [6, Sec. VI.4], we can bound

$$|P(\sigma+it)| \leq U(\varepsilon)(1+|t|)^{M(\sigma)}|D|^{M(\sigma)} \qquad \text{for all } \sigma \in [-\varepsilon, 1+\varepsilon],$$

where $U(\varepsilon) = \max\{U_1(\varepsilon), U_2(\varepsilon)U_1(\varepsilon)\}$ is the maximum of the two ε-dependent bounds on the vertical lines, and $M(\sigma) = 1+\varepsilon-\sigma$ takes the values $M(-\varepsilon) = 1+2\varepsilon$ and $M(1+\varepsilon) = 0$. Taking $\sigma = 1/2$ and $t = 0$, we derive

$$|L(g, \chi_D, w)| \leq \sqrt{2\pi}U(\varepsilon)|D|^{1/2+\varepsilon},$$

which yields the lemma. □

Remark 5.7. It is possible to improve the exponent $1/2+\varepsilon$ occuring in Lemma 5.6. For instance, if the Lindelöf hypothesis is true, then we can replace $1/2+\varepsilon$ by ε. Using more advanced techniques than the Phragmen-Lindelöf theorem, we can reduce the $1/2$ unconditionally as well. Lemma 5.6 will suffice for our applications.

Corollary 5.8. *Let the notation be as in Lemmas 5.4 and 5.6 and write $n = f^2 n_0 \geq 0$ with $-n_0$ fundamental. Then, for every $\eta, \varepsilon > 0$, the coefficients $c_{10,1}(n)$ and $c_{12,1}(n)$ of K_{10} and K_{12} satisfy*

$$c_{10,1}(n) \leq \frac{1}{236}\sqrt{B(\varepsilon,9)}C(\eta)^2 f^{8.5+2\eta} n_0^{4.5+1/2\varepsilon} \qquad \text{and}$$

$$c_{12,1}(n) \leq \frac{1}{311}\sqrt{B(\varepsilon,11)}C(\eta)^2 f^{10.5+2\eta} n_0^{5.5+1/2\varepsilon}$$

for all $n \geq 1$.

Proof. Substitute Lemmas 5.4–5.6 into Waldspurger's formula (5.1). □

Remark 5.9. As we have $f = (n/n_0)^{1/2}$, the size of $c_{w,1}(n)$ in Corollary 5.8 is $O(n^{w/2-1/2+\varepsilon})$, where the constant in the O-symbol is explicit. If the Lindelöf hypothesis is true, then we immediately get $c_{w,1}(n) = O(n^{w/2-3/4+\varepsilon})$ (possibly with an ineffective constant). This last estimate is known as the Petersson-Ramanujan conjecture for half-integral weight cusp forms.

We are now in the position to give an estimate for the Fourier coefficients of the cusp forms χ_{10}, χ_{12}.

Theorem 5.10. *Let the functions B, C be as in Lemmas 5.4 and 5.6 and write $(4\det T) = n = f^2 n_0$. Then, for every $\varepsilon, \eta, \gamma > 0$, the Fourier coefficients $a_{10}(T)$ and $a_{12}(T)$ of χ_{10} and χ_{12} satisfy*

$$|a_{10}(T)| \leq \tfrac{1}{236}C(\eta)^2 C(\gamma)\sqrt{B(\varepsilon,9)} f^{9+\gamma+2\eta} n_0^{4.5+1/2\varepsilon} = O((\det T)^{4.5+\varepsilon}),$$
$$|a_{12}(T)| \leq \tfrac{1}{311}C(\eta)^2 C(\gamma)\sqrt{B(\varepsilon,11)} f^{11+\gamma+2\eta} n_0^{5.5+1/2\varepsilon} = O((\det T)^{5.5+\varepsilon}).$$

Proof. The Fourier coefficient of χ_{10} for the matrix T is bounded by

$$\sum_{d^2|n} d^9 c_{10,1}\left(\frac{n}{d^2}\right) \leq \frac{1}{236}\sqrt{B(\varepsilon,9)}C(\eta)^2 n_0^{4.5+\varepsilon/2} \sum_{d|f} d^9 (f/d)^{8.5+2\eta}$$

$$\leq \frac{1}{236}\sqrt{B(\varepsilon,9)}C(\eta)^2 f^{9+2\eta} n_0^{4.5+\varepsilon/2} \sum_{d|f} \frac{1}{d^{2\eta}}.$$

The sum on the right-hand side is bounded by

$$\sum_{d|f} 1 \leq C(\gamma) f^{\gamma};$$

see e.g., [10, Sec. 18.1.]. The proof for χ_{12} is similar. □

Corollary 5.11. *Assume that the Lindelöf-hypothesis is true. Then for the Fourier coefficients $a_w(T)$ of χ_{10}, χ_{12} we have*

$$|a_w(T)| = O((\det T)^{w/2-3/4+\varepsilon})$$

for every $\varepsilon > 0$ if $\det(T)$ is squarefree. In general, we have

$$|a_w(T)| = O\left((\det T)^{w/2-3/4+\varepsilon} \sum_{d^2|(4\det T)} \sqrt{d}\right) = O((\det(T))^{w/2-1/2+\varepsilon})$$

for every $\varepsilon > 0$.

6. Speed of convergence

In this section we carefully analyse the speed of convergence of the Siegel Eisenstein series occuring in (1.2), and this will yield Theorem 1.2 without too much effort. To analyse the convergence of a Siegel modular function we a priori have to consider *three* variables. We begin by showing that it suffices to look at a 'one-dimensional' convergence problem.

The imaginary part $\mathrm{Im}(\tau)$ of a matrix $\tau \in \mathbf{H}_2$ is positive definite. Hence, there exists $\delta \in \mathbf{R}_{>0}$ with $\mathrm{Im}(\tau) \geq \delta 1_2$, meaning that $\mathrm{Im}(\tau) - \delta 1_2$ is positive semi-definite. We define

$$\delta(\tau) = \sup\{\delta' \in \mathbf{R} \mid \mathrm{Im}(\tau) \geq \delta' 1_2\}$$

to be the 'largest' of all these values. With this notation, we have the following lemma.

Lemma 6.1. *Let* $T = \left(\begin{smallmatrix} a & b/2 \\ b/2 & c \end{smallmatrix}\right) \in \mathrm{Mat}_2(\frac{1}{4}\mathbf{Z})$ *be positive semi-definite and let* $\tau \in \mathbf{H}_2$. *Then the inequality*

$$|\exp(2\pi i \mathrm{Tr}(T\tau))| \leq \exp(-2\pi \mathrm{Tr}(T)\delta(\tau))$$

holds.

Proof. We have an equality $|\exp(2\pi i \mathrm{Tr}(T\tau))| = \exp(-2\pi \mathrm{Tr}(T\mathrm{Im}(\tau)))$. Since T is positive semi-definite, we have $T\mathrm{Im}(\tau) \geq T\delta(\tau)$. The lemma follows. □

We have

$$E_w(\tau) = \sum_T a(T)\exp(2\pi i \mathrm{Tr}(T\tau)) = \sum_{t=0}^{\infty} \sum_{T \in S(t)} a(T)\exp(2\pi i \mathrm{Tr}(T\tau), \tag{6.1}$$

where $S(t)$ is the set of all 2×2 positive semi-definite symmetric matrices of trace t with non-negative integer entries on the diagonal and half-integer entries on the off-diagonal. The set $S(t)$ clearly has at most $2(t+1)^2$ elements for which $a(T)$ is non-zero.

The technique of 'splitting up' the evaluation of a Siegel modular form as in equation (6.1) enables us to find a lower bound for $|\chi_{10}(\tau)|$. The idea is that if we have

$$\left| \sum_{\substack{T \in S(t) \\ t \leq B}} a(T)\exp(2\pi i \mathrm{Tr}(T\tau)) \right| > 10 \left| \sum_{\substack{T \in S(t) \\ t > B}} a(T)\exp(2\pi i \mathrm{Tr}(T\tau)) \right|, \tag{6.2}$$

then the value of $|\chi_{10}(\tau)|$ is roughly equal to the left-hand side of (6.2). Furthermore, we can apply the upper bound for the Fourier coefficients of χ_{10} given by Theorem 5.8 to bound the right-hand side of (6.2). Taking $B = 2$ yields the following lemma.

Lemma 6.2. *Let*

$$M_1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \qquad M_2 = \begin{pmatrix} 1 & \frac{1}{2} \\ \frac{1}{2} & 1 \end{pmatrix}, \qquad M_3 = \begin{pmatrix} 1 & -\frac{1}{2} \\ -\frac{1}{2} & 1 \end{pmatrix},$$

and for $\varepsilon, \eta, \gamma > 0$, *put* $M(\varepsilon, \eta, \gamma) = \frac{1}{236} C(\eta)^2 C(\gamma)\sqrt{B(\varepsilon, 9)}$, *where the notation is as in Lemmas 5.4 and 5.6. If, for any* $\varepsilon, \eta, \gamma > 0$, *we have*

$$|c| \geq 10 \sum_{t=3}^{\infty} 2M(\varepsilon, \eta, \gamma) t^{11+\varepsilon+2\eta} \exp(-2\pi t \delta(\tau))$$

for

$$c = \frac{1}{2}\exp(2\pi i \mathrm{Tr}(M_1\tau)) - \frac{1}{4}\exp(2\pi i \mathrm{Tr}(M_2\tau)) - \frac{1}{4}\exp(2\pi i \mathrm{Tr}(M_3\tau)),$$

then we have $|\chi_{10}(\tau)| \geq 9/10|c|$.

Proof. Since χ_{10} is a cusp form, there are no matrices $T \in S(0) \cup S(1)$ for which the Fourier coefficient $a(T)$ of χ_{10} is non-zero. In particular, the set $S(t)$ has at most $2t^2$ elements for which $a(T)$ is non-zero.

The only $T \in S(2)$ for which $a(T)$ is non-zero are the matrices $T = M_1, M_2, M_3$. These matrices have Fourier coefficients $1/2, -1/4, -1/4$ respectively. Hence, c equals the left-hand side of (6.2) with $B = 2$.

From Theorem 5.10 and the 'AGM-inequality' $n = f^2 n_0 = 4\det(T) \leq \mathrm{Tr}(T)^2$ we bound

$$|a(T)| \leq M(\varepsilon,\eta,\gamma) f^{9+\gamma+2\eta} n_0^{4.5+1/2\varepsilon} \leq M(\varepsilon,\eta,\gamma)\mathrm{Tr}(T)^{9+\varepsilon+2\eta+\gamma}. \tag{6.3}$$

The right-hand side of (6.2) is now bounded from above by

$$10\sum_{t=3}^{\infty} 2t^2 \Big| \max_{T\in S(t)} \big\{a(T)\exp(-2\pi\mathrm{Tr}(T)\delta(\tau))\big\}\Big|$$

$$\leq 20\sum_{t=3}^{\infty} M(\varepsilon,\eta,\gamma) t^{11+\varepsilon+2\eta+\gamma}\exp(-2\pi t\delta(\tau)),$$

and the lemma follows. □

Remark 6.3. In Lemma 6.2, we can choose any $\varepsilon, \eta, \gamma$. The optimal choice depends on the value of $\delta(\tau)$.

Remark 6.4. If the condition in Lemma 6.2 does not hold for any $\varepsilon, \eta, \gamma$, we can look at the contribution of all matrices of trace 2 and 3. If that majorates the contribution coming from all matrices of trace 4 and higher, we have found a lower bound on $|\chi_{10}(\tau)|$.

Proof of Theorem 1.2. The Igusa functions are rational expressions in the Eisenstein series E_4, E_6 and the cusp forms χ_{10} and χ_{12}. The proof consists of 2 parts: first we analyse the 'loss of precision' that occurs when applying the formulas in (1.2). Knowing the precision in which to evaluate the four Siegel modular forms, we then carefully analyse the speed of convergence of these series.

Using Corollary 3.6 with the constant from Remark 3.7, we bound

$$|a(T)| \leq 19230\,\mathrm{Tr}(T)^5 \tag{6.4}$$

for a Fourier coefficient of E_4 in case $\det(T)$ is non-zero. For $\det(T) = 0$ and $\mathrm{Tr}(T) \neq 0$, we use Theorem 3.4 directly: the rough bound

$$\frac{-8}{B_4}\sum_{d|\gcd(a,b,c)} d^4 \cdot 1 \leq 240 \sum_{d|\mathrm{Tr}(T)} \mathrm{Tr}(T)^4 \leq 240\mathrm{Tr}(T)^5$$

implies that inequality (5.2) holds in this case as well. We conclude that $|E_4(\tau)|$ is bounded by

$$1 + \sum_{t=0}^{\infty} 2\cdot 19230 t^5 (t+1)^2 \exp(-2\pi t\delta(\tau)) \leq 328,$$

where we have used the assumption $\delta(\tau) \geq 1$. For $E_6(\tau)$ we get the bound $|E_6(\tau)| \leq 285$. Using equation (6.2) with $\eta = 1.5, \varepsilon = 0.2, \gamma = 1.8$, we derive the bounds $|\chi_{10}(\tau)| \leq 3$ and $|\chi_{12}(\tau)| \leq 18$ for the cusp forms.

Using these four upper bounds, it is straightforward to check that if we evaluate all four Siegel modular forms up to $k+9$ decimal digits, then we know the products $\chi_{12}(\tau)^5$, $E_4(\tau)\chi_{12}(\tau)^3$ and $E_6(\tau)\chi_{12}(\tau)^2$ occuring in formula (1.2) up to k decimal digits of precision. Furthermore, we know by assumption that $\chi_{10}(\tau)$ does not equal zero. Let $n \in \mathbf{Z}_{>1}$ be the smallest n such that $|\chi_{10}(\tau)| \geq 10^{-n}$ holds. By dividing by $\chi_{10}(\tau)^6$, we lose $\max\{0, 6n\}$ digits of precision. Hence, if we evaluate all the Siegel modular forms occuring in (1.2) up to $l = k + \max\{7, 6n\} = k + 6n$ digits of precision, we know the Igusa values $j_1(\tau), j_2(\tau), j_3(\tau)$ up to k decimal digits of precision.

We evaluate the Siegel modular functions $E_4, E_6, \chi_{10}, \chi_{12}$ using the sum (6.1), truncated to only include matrices whose trace is below some bound B. It remains to give a value for B such that the function values are accurate up to l decimal digits. For $B \geq 3$, the speed of convergence of the four series involved is slowest for χ_{12}, and it suffices to look at this function. Taking $\eta = 1.5, \varepsilon = 0.2, \gamma = 1.8$, we have

$$\sum_{\substack{T \in S(t) \\ t \geq B}} a_{12}(T) \exp(2\pi i \mathrm{Tr}(T\tau)) \leq \sum_{t=B}^{\infty} 18 t^{18} \exp(-2\pi t \delta(\tau)),$$

and if the sum on the right-hand side is less than 10^{-l}, then the contribution coming from the matrices of trace larger than B does not alter the first l decimal digits. The theorem follows. □

7. Examples

In this section we illustrate the techniques developed in this paper by evaluating $j_1(\tau)$ for two choices of τ.

7.1. **Example.** We detail the evaluation of the Igusa functions j_1, j_2, j_3 at

$$\tau = \begin{pmatrix} 2+5i & 13+26i \\ 13+26i & 83+141i \end{pmatrix} \in \mathbf{H}_2$$

to 500 decimal digits of precision. The Igusa functions are rational expressions in the Siegel modular forms E_4, E_6, χ_{10} and χ_{12}; cf. Section 1. The idea is to simply evaluate these series at τ to high enough precision and then apply the formulas in (1.2).

We have the rather low bound $\delta(\tau) \geq 0.15$ in this case. However, for the purpose of evaluating Igusa functions, we may replace τ by an $\mathrm{Sp}_4(\mathbf{Z})$-equivalent matrix τ'. It is straightforward to check that the matrix

$$\tau' = \begin{pmatrix} 5i & i \\ i & 6i \end{pmatrix} = \begin{pmatrix} 1 & 0 & -2 & -13 \\ -5 & 1 & -3 & -18 \\ 0 & 0 & 1 & 5 \\ 0 & 0 & 0 & 1 \end{pmatrix} (\tau)$$

lies in the fundamental domain for $\mathrm{Sp}_4(\mathbf{Z})\backslash\mathbf{H}_2$ as e.g. described in [9]. We have $\delta(\tau') \geq 4.3$.

To bound $|\chi_{10}(\tau')|$ from below, we apply Lemma 6.2. With the notation of this lemma, we compute $c \approx -1.28 \cdot 10^{-28}$, and the value of the sum is roughly equal

to $6.3 \cdot 10^{-27}$ for $(\eta, \varepsilon, \gamma) = (1.5, 0.2, 1.8)$. We see that Lemma 6.2 does not apply directly. However, if we compute the contribution c' coming from all matrices of at most 3, then we get $c' \approx -1.28 \cdot 10^{-28} \approx c$, but we now have

$$20 \sum_{t=4}^{\infty} M(1.5, 0.2, 1.8) t^{16} \exp(-2\pi t \cdot 4.3) \approx 2.3 \cdot 10^{-37}.$$

We conclude that $|\chi_{10}(\tau')|$ is bounded from below by $1.28 \cdot 10^{-28}$.

The lower bound on $|\chi_{10}(\tau')|$ yields that we lose $6 \cdot 28 = 168$ decimal digits of precision in the computation of $j_1(\tau')$. However, we also easily bound $|\chi_{12}(\tau')| \leq 4.37 \cdot 10^{-29}$. Hence, we gain $5 \cdot 29 = 145$ decimal digits of precision by multiplying by $\chi_{12}(\tau')^5$. The 'net loss' of precision is therefore only $168 - 145 = 23$ decimal digits of precision.

Putting everything together, we need to evaluate the Siegel modular forms $E_4, E_6, \chi_{10}, \chi_{12}$ up to 524 decimal digits of precision to know the values of the Igusa functions up to 500 decimal digits of precision. The sum

$$\sum_{t=B}^{\infty} 18 t^{18} \exp(-8.6\pi t)$$

is less than 10^{-524} for $B = 48$ and we hence have to consider all matrices of trace up to 47.

To compute the Fourier coefficients for all matrices $\left(\begin{smallmatrix} a & b/2 \\ b/2 & c \end{smallmatrix}\right)$ of *trace* at most 47, we compute the Fourier coefficients of all matrices satisfying $4ac - b^2 \leq 2209 = 47^2$, with the convention that we only take the matrices of trace at most 47 in the case of determinant 0. To compute all the coefficients $a(T)$ for E_4, E_6, χ_{10} and χ_{12} we compute the first 2209 terms of the power series

$$\theta = 1 + 2 \sum_{n=1}^{\infty} q^{n^2} \qquad \text{and} \qquad \widetilde{\theta} = \Big(1 + 2 \sum_{n=1}^{\infty} (-1)^n q^{n^2}\Big)^4.$$

Using Proposition 4.3, we compute the first 2209 coefficients of the modular forms C_4 and C_6:

$$\frac{-8}{B_4} C_4 = 240 + 13440 q^3 + 30240 q^4 + 138240 q^7 + 181440 q^8 + 362880 q^{11} + O(q^{12}),$$
$$\frac{-12}{B_6} C_6 = -504 + 44352 q^3 + 166320 q^4 + 2128896 q^7 + 3792096 q^8 + O(q^{11}).$$

The coefficients of the forms C_i are the Fourier coefficients of the Jacobi Eisenstein series E_i^J. Using Proposition 5.3 we compute the first 2209 coefficients of the modular forms K_{10} and K_{12}:

$$\begin{aligned} \tfrac{-1}{4} K_{10} &= -1/4 q^3 + 1/2 q^4 + 4 q^7 - 9 q^8 - 99/4 q^{11} + O(q^{12}), \\ \tfrac{1}{12} K_{12} &= 1/12 q^3 + 5/6 q^4 - 22/3 q^7 - 11 q^8 + 425/4 q^{11} + O(q^{12}). \end{aligned}$$

The coefficients of K_{10} and K_{12} are the Fourier coefficients of the Jacobi cusp forms $\varphi_{10,1}$ and $\varphi_{12,1}$.

Since the four Siegel modular forms we are interested in all lie in the Maaß Spezialschar, the Fourier coefficient $a(T)$ of one of them only depends on the determinant of T and the greatest common divisor of the entries of T. We make an array 'encoding' these Fourier coefficients as follows. For every positive integer $N \leq 2209$, we compute its squarefree part N_0 and write $N = N_0 f^2$. For every

divisor $d \mid f$, we compute and store the Fourier coefficient belonging to a matrix $T = \left(\begin{smallmatrix} a & b/2 \\ b/2 & c \end{smallmatrix}\right)$ with $4ac - b^2 = N$ and $\gcd(a,b,c) = d$. For E_4 and $N = 16$ we get

$$[997920, 1239840, 0, 1239840]$$

for instance. For $N = 0$ we make a list of all positive integers $d \leq X$ and store the coefficients for the determinant zero matrices with trace d.

The computations so far were independent of the choice of $\tau = \left(\begin{smallmatrix} \tau_1 & z \\ z & \tau_2 \end{smallmatrix}\right) \in \mathbf{H}_2$. We let $q_1 = \exp(2\pi i \tau_1)$, $q_2 = \exp(2\pi i \tau_2)$ and $q_3 = \exp(2\pi i z)$ be the 'Fourier variables' of the entries of τ. We compute and store the values $q_1^0 = 1, q_1, q_1^2, \ldots, q_1^X$ and likewise for q_2. For ζ we need to compute both the first X powers of ζ and ζ^{-1} because the off-diagonal entries of the matrices can be negative.

The precision needed for this computation is easily computed. Indeed, the maximum bound for a Fourier coefficient is roughly 10^{31} and occurs for χ_{12} and a trace 47 matrix. As we need to recognize the values $a(T)\exp(2\pi i \mathrm{Tr}(T\tau))$ up to 524 decimal digits of precision, we need to compute q_1, q_2 and q_3 with $524 + 31 = 555$ decimal digits of precision.

After making these 4 lists, we now simply loop over $a = 0, \ldots, X$, $c = 0, \ldots, X$ and $b = 0, \ldots, \lfloor \sqrt{4ac} \rfloor$ and for the triples (a,b,c) with $b^2 - 4ac \leq X$ we compute $\gcd(a,b,c)$ and look up the Fourier coefficient in the stored array.

We implemented this algorithm in the computer algebra package Magma. We did not attempt to be as efficient as possible in our implementation. On our 64-bit, 2.1 Ghz computer it took roughly 1 second to compute $j_1(\tau), j_2(\tau), j_3(\tau)$ up to 500 decimal digits of precision. We have

$$j_1(\tau) = 1739974391457516743024648218 3.29799\ldots$$

for instance. The computation of the Fourier coefficients of the Eisenstein series is negligible: the bottleneck is the 'loop' over all matrices $\left(\begin{smallmatrix} a & b/2 \\ b/2 & c \end{smallmatrix}\right)$ satisfying $0 \leq a \leq X$, $0 \leq c \leq X$, $|b| \leq \lfloor \sqrt{4ac} \rfloor$.

7.2. **CM-example.** The evaluation of Igusa functions is a main ingredient in the computation of Igusa class polynomials, which is in turn used to construct e.g. hyperelliptic curves with cryptographic properties. We illustrate our algorithm by computing $j_1(\tau)$ for a small CM-point τ.

Let $K = \mathbf{Q}(\sqrt{-5+\sqrt{5}})$ be a quartic CM field. The extension $K/\mathbf{Q}$ is cyclic and K has class number two. Using [24, Algorithm 1], see also [26, Thm. 3.1], we compute that

$$\tau' = \begin{pmatrix} 2.4060038200i & 0.4595058410i \\ 0.4595058410i & 1.9464979789i \end{pmatrix}$$

is an approximation to the matrix τ representing the abelian surface $\mathbf{C}^2/\Phi(\mathcal{O}_K)$, where Φ is a CM-type for K. We will work with a 50 digit approximation to τ.

As shown in [24], the values $j_i(\tau)$ are in fact integers. Hence, we only need one digit past the decimal place to recognize them, and we take $k = 1$ in Theorem 1.2. The matrix τ already lies in the fundamental domain for $\mathrm{Sp}_4(\mathbf{Z})\backslash\mathbf{H}_2$, and we have $\delta(\tau) \geq 1.66$. Just as in the previous example, Lemma 6.2 does not apply directly. Using Remark 6.4, we compute $c \approx -5.3 \cdot 10^{-12}$, where we include all matrices of trace up to and including 5. The corresponding sum is roughly equal to $9 \cdot 10^{-15}$ for $\eta = 1.5, \varepsilon = 0.2, \gamma = 1.8$. We conclude that we may take $n = 12$ in Theorem 1.2.

Just as in Example 7.1, we bound $|\chi_{12}(\tau)| \leq 3.1 \cdot 10^{-12}$. We lose at most $1 + 6 \cdot 12 - 5 \cdot 12 = 13$ digits of precision, and we need to know the evaluations of the four Siegel modular forms up to precision 10^{-14}. The sum

$$\sum_{t=B}^{\infty} 18t^{18} \exp(-3.32\pi t)$$

is less than 10^{-14} for $B = 7$. To get all matrices of trace at most 6, we take all matrices $\left(\begin{smallmatrix} a & b/2 \\ b/2 & c \end{smallmatrix}\right)$ satisfying $4ac - b^2 \leq 9^2 = 36$. We compute

$$j_1(\tau) = 6202728393749.9999\ldots,$$

which is accurate enough to derive $j_1(\tau) = 6202728393750$.

In this example, it turns out that we only needed to look at the matrices with $4ac - b^2 \leq 6$. The fact that our bound of 36 was much higher can be explained as follows. First, our analysis for the precision loss is for a worst case scenario and we actually do not lose 14 digits of precision in this example. Second, we use the *same bound* for all the Fourier coefficients of the matrices of a given trace t, whereas these coefficients actually vary quite a lot.

Acknowledgements

We thank the referee for detailed comments on an earlier draft of this paper, and Jeff Hoffstein for helpful discussions.

References

[1] Harald Baier, *Efficient computation of singular moduli with application in cryptography*, Fundamentals of computation theory (Riga, 2001), Lecture Notes in Comput. Sci., vol. 2138, Springer, Berlin, 2001, pp. 71–82, DOI 10.1007/3-540-44669-9_9. MR1914098 (2003e:94062)

[2] S. Böcherer and S. Raghavan, *On Fourier coefficients of Siegel modular forms*, J. Reine Angew. Math. **384** (1988), 80–101, DOI 10.1515/crll.1988.384.80. MR929979 (89c:11068)

[3] Henri Cohen, *A course in computational algebraic number theory*, Graduate Texts in Mathematics, vol. 138, Springer-Verlag, Berlin, 1993. MR1228206 (94i:11105)

[4] H. Cohen, *Number Theory, volume II: analytic and modern tools*, Springer Graduate Texts in Mathematics, vol. 240, 2007.

[5] Henri Cohen, *Sums involving the values at negative integers of L-functions of quadratic characters*, Math. Ann. **217** (1975), no. 3, 271–285. MR0382192 (52 #3080)

[6] John B. Conway, *Functions of one complex variable*, 2nd ed., Graduate Texts in Mathematics, vol. 11, Springer-Verlag, New York, 1978. MR503901 (80c:30003)

[7] Pierre Deligne, *La conjecture de Weil. I* (French), Inst. Hautes Études Sci. Publ. Math. **43** (1974), 273–307. MR0340258 (49 #5013)

[8] Martin Eichler and Don Zagier, *The theory of Jacobi forms*, Progress in Mathematics, vol. 55, Birkhäuser Boston Inc., Boston, MA, 1985. MR781735 (86j:11043)

[9] Erhard Gottschling, *Explizite Bestimmung der Randflächen des Fundamentalbereiches der Modulgruppe zweiten Grades* (German), Math. Ann. **138** (1959), 103–124. MR0107020 (21 #5748)

[10] G. H. Hardy, E. M. Wright, *An introduction to the theory of numbers*, Oxford University Press, 1938.

[11] Jun-ichi Igusa, *Modular forms and projective invariants*, Amer. J. Math. **89** (1967), 817–855. MR0229643 (37 #5217)

[12] Jun-ichi Igusa, *On Siegel modular forms of genus two*, Amer. J. Math. **84** (1962), 175–200. MR0141643 (25 #5040)

[13] Jun-ichi Igusa, *On Siegel modular forms genus two. II*, Amer. J. Math. **86** (1964), 392–412. MR0168805 (29 #6061)

[14] Neal Koblitz, *Introduction to elliptic curves and modular forms*, 2nd ed., Graduate Texts in Mathematics, vol. 97, Springer-Verlag, New York, 1993. MR1216136 (94a:11078)

[15] Max Koecher, *Zur Theorie der Modulformen n-ten Grades. I* (German), Math. Z. **59** (1954), 399–416. MR0059946 (15,603e)

[16] Winfried Kohnen, *Estimates for Fourier coefficients of Siegel cusp forms of degree two. II*, Nagoya Math. J. **128** (1992), 171–176. MR1197036 (94f:11032b)

[17] W. Kohnen and D. Zagier, *Values of L-series of modular forms at the center of the critical strip*, Invent. Math. **64** (1981), no. 2, 175–198, DOI 10.1007/BF01389166. MR629468 (83b:10029)

[18] H. W. Lenstra Jr., *Factoring integers with elliptic curves*, Ann. of Math. (2) **126** (1987), no. 3, 649–673, DOI 10.2307/1971363. MR916721 (89g:11125)

[19] H. W. Lenstra Jr. and Carl Pomerance, *A rigorous time bound for factoring integers*, J. Amer. Math. Soc. **5** (1992), no. 3, 483–516, DOI 10.2307/2152702. MR1137100 (92m:11145)

[20] K. Mahler, *On a class of non-linear functional equations connected with modular functions*, J. Austral. Math. Soc. Ser. A **22** (1976), no. 1, 65–118. MR0441867 (56 #258)

[21] H. L. Resnikoff and R. L. Saldaña, *Some properties of Fourier coefficients of Eisenstein series of degree two*, J. Reine Angew. Math. **265** (1974), 90–109. MR0352009 (50 #4497)

[22] J.-P. Serre, *A course in arithmetic*, Springer-Verlag, New York, 1973. Translated from the French; Graduate Texts in Mathematics, No. 7. MR0344216 (49 #8956)

[23] Goro Shimura, *Abelian varieties with complex multiplication and modular functions*, Princeton Mathematical Series, vol. 46, Princeton University Press, Princeton, NJ, 1998. MR1492449 (99e:11076)

[24] Paul van Wamelen, *Examples of genus two CM curves defined over the rationals*, Math. Comp. **68** (1999), no. 225, 307–320, DOI 10.1090/S0025-5718-99-01020-0. MR1609658 (99c:11079)

[25] Lawrence C. Washington, *Introduction to cyclotomic fields*, 2nd ed., Graduate Texts in Mathematics, vol. 83, Springer-Verlag, New York, 1997. MR1421575 (97h:11130)

[26] Annegret Weng, *Constructing hyperelliptic curves of genus 2 suitable for cryptography*, Math. Comp. **72** (2003), no. 241, 435–458 (electronic), DOI 10.1090/S0025-5718-02-01422-9. MR1933830 (2003i:14029)

Brown University, Box 1917, 151 Thayer Street, Providence, Rhode Island 02912
E-mail address: `reinier@math.brown.edu`

Microsoft Research, One Microsoft Way, Redmond, Washington 98052
E-mail address: `klauter@microsoft.com`