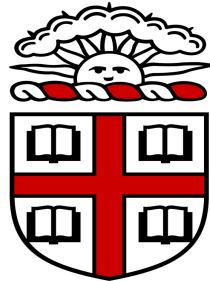


Fourier coefficients of Siegel modular forms

Reinier Bröker



BROWN

joint work with Kristin Lauter (Microsoft Research)

Complex multiplication theory, classical case

Let $K = \mathbf{Q}(\sqrt{D})$ be imaginary quadratic of discriminant D .

Let $j : \mathbf{H} \rightarrow \mathbf{C}$ be the complex analytic function with Fourier expansion $j(z) = 1/q + 744 + 196884q + \dots$ in $q = \exp(2\pi iz)$.

Theorem. *The Hilbert class field of K equals*

$$K \left(j \left(\frac{D + \sqrt{D}}{2} \right) \right).$$

This theorem forms the heart of various algorithms that compute elliptic curves with ‘cryptographic properties’.

A few ways to compute $j(z)$

- compute the Fourier coefficients of j (somehow);
- use

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

with g_i the normalized Eisenstein series of weight $2i$;

- use

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

with $\eta(z) = q^{1/24} \prod_{n=1}^{\infty} (1 - q^n)$.

The third approach is the fastest.

Complex multiplication theory, higher degree

Let K be a degree 4 CM-field, i.e., an imaginary quadratic extension of a totally real field.

Write $\mathbf{H}_2 = \{\tau \in \text{Mat}_2(\mathbf{C}) \mid \tau = \tau^T, \text{Im}(\tau) > 0\}$.

Let $j_{1,2,3} : \mathbf{H}_2 \rightarrow \mathbf{C}$ be three ‘Igusa functions’, like

$$j_2(\tau) = 2^{-3} 3^3 \frac{E_4(\tau) \chi_{12}^3(\tau)}{\chi_{10}^4(\tau)}.$$

Theorem. *Let L be a Galois closure of K . There exists $\tau \in \mathcal{O}_L$ such that $K(j_i(\tau))/K$ is unramified and abelian.*

This theorem forms the heart of various algorithms that compute principally polarized abelian surfaces with ‘cryptographic properties’.

Computing $j_i(\tau)$

- compute the Fourier coefficients of Siegel Eisenstein series somehow and use

$$j_2(\tau) = 2^{-3} 3^3 \frac{E_4(\tau) \chi_{12}^3(\tau)}{\chi_{10}^4(\tau)}.$$

- use

$$j_i(\tau) = \frac{P_i(\theta_c(\tau))}{Q_i(\theta_c(\tau))}$$

with explicit polynomials P_i, Q_i in the *theta constants* θ_c .

The theta constants are analogues of the Dedekind η , and the second method of computing $j_i(z)$ is fast.

Siegel Eisenstein series, I

Question / topic of talk. What happens if we evaluate j_i using Eisenstein series anyway?

Siegel modular forms admit a Fourier expansion

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

with $T \in \operatorname{Mat}_2(\frac{1}{2}\mathbf{Z})$ with integer diagonals.

Koecher-principle: $a(T) = 0$ if T is negative definite.

We have $a(M^T T M) = a(T)$ for $M \in \operatorname{GL}_2(\mathbf{Z})$.

Siegel Eisenstein series, II

For even $w \geq 4$, put

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

The sum ranges over all inequivalent bottom rows $(c \ d)$ of elements of $\mathrm{Sp}_4(\mathbf{Z})$ with respect to left-multiplication by $\mathrm{SL}_2(\mathbf{Z})$.

Example. The series E_4 has Fourier coefficients

$$a \left(\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \right) = 1, \quad a \left(\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \right) = 240,$$

$$a \left(\begin{pmatrix} 0 & 0 \\ 0 & 2 \end{pmatrix} \right) = 2160, \quad a \left(\begin{pmatrix} 2 & \frac{1}{2} \\ \frac{1}{2} & 3 \end{pmatrix} \right) = 2903040.$$

Structure of Siegel modular forms

Theorem I. *The graded algebra M^e of even weight Siegel modular forms equals $\mathbf{C}[E_4, E_6, E_{10}, E_{12}]$. The full algebra of all forms equals $M^e[X]/(X^2 - P(E_4, E_6, E_{10}, E_{12}))$. The element \overline{X} corresponds to a Siegel modular form of weight 35.*

A Siegel modular form is a *cuspidal form* if $a(T) = 0$ for all semi-definite T that are not definite.

Theorem II. *The ideal of cuspidal forms is generated by χ_{10} , χ_{12} and \overline{X} .*

Both results are due to Igusa.

Fourier coefficients of special Siegel modular forms

Let $f : \mathbf{H}_2 \rightarrow \mathbf{C}$ be a Siegel modular form of weight w . We have

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

with $\varphi_m : \mathbf{H} \times \mathbf{C} \rightarrow \mathbf{C}$ satisfying

A. $\varphi_m\left(\frac{a\tau_1+b}{c\tau_1+d}, \frac{\varepsilon}{c\tau_1+d}\right) = (c\tau_1+d)^w e^{\frac{2\pi i m c \varepsilon}{c\tau_1+d}} \varphi_m(\tau_1, \varepsilon), \quad \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbf{Z})$

B. $\varphi_m(\tau_1, \varepsilon + \lambda\tau + \mu) = e^{-2\pi i m(\lambda^2\tau_1 + 2\lambda\varepsilon)} \varphi_m(\tau_1, \varepsilon), \quad (\lambda, \mu) \in \mathbf{Z}^2$

C. $\varphi_m(\tau_1, \varepsilon) = \sum_{n=0}^{\infty} \sum_{\substack{r \in \mathbf{Z} \\ r^2 \leq 4nm}} c(n, r) e^{2\pi i(n\tau_1 + r\varepsilon)}.$

Jacobi forms

A holomorphic function $g : \mathbf{H} \times \mathbf{C} \rightarrow \mathbf{C}$ satisfying **A–C** is called a *Jacobi form*. It has a *weight* w and an *index* m .

- $J_{w,m}$ is finite-dimensional.
- w odd $\implies J_{w,1} = 0$.
- previous slide gives a map

$$M_w \hookrightarrow \prod_{m \geq 0} J_{w,m} \xrightarrow{\text{pr}} J_{w,1}.$$

- using *Hecke operators* we can define an injective map

$$s : J_{w,1} \rightarrow M_w.$$

Image of s

The image of $s : J_{w,1} \rightarrow M_w$ is called the *Maaß Spezialschar*.

The Fourier coefficient $a(T)$ of $f \in \text{Im}(s)$ only depends on $\det(T)$ if $\det(T)$ is square-free.

The map s is completely *explicit*. Hence, we can compute $a(T)$ of $s(f)$ by computing the Fourier coefficients of $f \in J_{w,1}$.

Classical result. *The Siegel Eisenstein series are contained in $\text{Im}(s)$.*

Fourier coefficients of Siegel Eisenstein series

Theorem. For E_w , the Fourier coefficient of $T = \begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix} \neq 0 \in \text{Mat}(\frac{1}{2}\mathbf{Z})$ equals

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

with $\alpha(0) = 1$ and for $b^2 - 4ac = D = D_0 f^2 < 0$ we have

$$\alpha(D) = \frac{1}{\zeta(3-2w)} L_{D_0}(2-w) \sum_{d \mid f} \mu(d) \left(\frac{D_0}{d}\right) d^{w-2} \sigma_{2w-3}(f/d).$$

Computing Fourier coefficients

We have isomorphisms

$$\begin{aligned} \text{Ma\ss Spezialschar} \subset M_w &\xrightarrow{\sim} J_{w,1} \xrightarrow{\sim} \\ &\xrightarrow{\sim} \text{Kohnen's "+"-space} \subset M_{w-1/2}^1(\Gamma_0(4)). \end{aligned}$$

The +-space contains those forms with Fourier coefficient $c(N) = 0$ for $(-1)^{w-1}N \equiv 2, 3 \pmod{4}$.

The Eisenstein series E_w corresponds to

$$H_w(z) = \sum_{n=0}^{\infty} \alpha_w(-n) \exp(2\pi iz) \in M_{w-1/2}^1.$$

Computing Fourier coefficients

The algebra of all half-integral weight forms is generated by

$$\theta(z) = \sum_{n \in \mathbf{Z}} q^{n^2} = 1 + 2 \sum_{n=1}^{\infty} q^{n^2} \quad \text{and} \quad \tilde{\theta}(z) = \theta^4(z + 1/2).$$

Linear algebra: *We have*

$$H_4 = \frac{\theta^7 + 7\theta^3\tilde{\theta}}{8}$$

$$H_6 = \frac{-\theta^{11} + 22\theta^7\tilde{\theta} + 11\theta^3\tilde{\theta}^2}{32}.$$

Examples

The quotient $\Gamma_0(4)\backslash\mathbf{H}$ has three cusps. Around ∞ we have

$$\begin{aligned}\frac{-8}{B_4}H_4 &= 240 + 13440q^3 + 30240q^4 + 138240q^7 \\ &\quad + 181440q^8 + 362880q^{11} + O(q^{12})\end{aligned}$$

$$\begin{aligned}\frac{-12}{B_6}H_6 &= -504 + 44352q^3 + 166320q^4 + 2128896q^7 \\ &\quad + 3792096q^8 + O(q^{11})\end{aligned}$$

in $q = \exp(2\pi iz)$.

The coefficient of q^n is zero for $n = 1, 2 \pmod{4}$.

Back to Igusa functions

Recall: we are evaluating Igusa functions like

$$j_2(\tau) = 2^{-3} 3^3 \frac{E_4(\tau) \chi_{12}^3(\tau)}{\chi_{10}^4(\tau)}.$$

We only need the Eisenstein series E_4, E_6 and the *cusp forms* χ_{10}, χ_{12} .

For a real algorithm, we also need *explicit* sizes of the Fourier coefficients. No problem for E_w .

Siegel cusp forms

The cusp forms

$$\chi_{10} = c_1(E_4E_6 - E_{10}) \quad \text{and} \quad \chi_{12} = c_2(3^2 \cdot 7^2 E_4^3 - 2 \cdot 5^3 E_6^2 - 691E_{12})$$

generate the ideal of all even weight cusp forms. They lie in the Spezialschar.

Linear algebra: *The corresponding weight $9\frac{1}{2}$, $11\frac{1}{2}$ forms K_{10}, K_{12} satisfy*

$$K_{10} = \frac{\theta^{15}\tilde{\theta} - 3\theta^{11}\tilde{\theta}^2 + 3\theta^7\tilde{\theta}^3 - \theta^3\tilde{\theta}^4}{4096}$$
$$K_{12} = \frac{5\theta^{19}\tilde{\theta} - 16\theta^{15}\tilde{\theta}^2 + 18\theta^{11}\tilde{\theta}^3 - 8\theta^7\tilde{\theta}^4 + \theta^3\tilde{\theta}^5}{16384}.$$

Examples

Around ∞ we have

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

in $q = \exp(2\pi iz)$.

The coefficient of q^n is zero for $n = 1, 2 \pmod{4}$.

Estimating sizes

The ‘linear algebra’ result does not help us to estimate the size of $a(T)$ for χ_{10}, χ_{12} .

Theorem (Shimura, Kohnen) *Kohnen’s $+-$ -space $\subset M_{w-1/2}^1(\Gamma_0(4))$ is isomorphic to $M_{2w-2}^1(\mathrm{SL}_2(\mathbf{Z}))$ under the Shimura correspondence.*

The spaces S_{18}^1, S_{22}^1 of classical cusp forms are one-dimensional. We have

$$\chi_{10} \longleftrightarrow \Delta E_6^1 \quad \chi_{12} \longleftrightarrow \Delta E_{10}^1.$$

Philosophy. *Deligne’s bound for S_w^1 governs the size of the Fourier coefficients of χ_{10}, χ_{12} .*

Waldspurger's formula

Let $f = \sum_D a(D)q^D$ be in the $+$ -space corresponding to $g \in M_{2w-2}^1$.

Then:

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

holds for any $D = f^2 D_0$. (Waldspurger, Kohnen, Zagier).

Here:

$$L(g, \chi_D, w-1) = L_{D_0}(g, \chi, w-1) \sum_{d|f} \mu(d) \left(\frac{D_0}{d}\right) d^{w-2} \sigma_{2w-3}(f/d)$$

is a 'completed' Dirichlet L -series.

For simplicity: only squarefree D in this talk.

Estimating Petersson products

Lemma. We have $\frac{\langle g_{18}, g_{18} \rangle}{\langle K_{10}, K_{10} \rangle} \leq 75634$.

Proof. We know that

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

holds for *any* D . Since we can compute any Fourier coefficient of K_{10} ... take $D = 3$.

It remains to estimate the L -series at the center of the critical strip.

L-series in critical strip

One proves

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

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

$$\phi_8(x) = \int_1^{\infty} y^8 \exp(-xy) dy.$$

This ‘series expansion’ converges exponentially fast. We only need the first few terms of

$$g_{18} = \Delta E_6^1 = q - 528q^2 - 4284q^3 + 147712q^4 + \dots \quad \square$$

Asymptotic L -series estimate

Recall: we are using

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

Lemma. *For every $\varepsilon > 0$, we have*

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

for all squarefree discriminants $D < 0$ with

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

Asymptotic L -series estimate

Proof of lemma. Rescale the L -series to have the critical strip between 0 and 1.

Use Deligne's bound to bound the L -series on a vertical line to the right of the critical strip. The functional equation gives a bound on a line to the left of the critical strip.

The *Phragmen-Lindelöf* theorem gives a bound inside the strip. \square

Remark. Bound can be improved by assuming Lindelöf-hypothesis.

Combining the bounds

Theorem. Define $B_2(x) = \exp(2^{1/x}/(x \log 2))$. Then, for every $\varepsilon > 0$ and any $\eta > 0$, the Fourier coefficients $a_{10}(T)$ and $a_{12}(T)$ of χ_{10} and χ_{12} satisfy

$$|a_{10}(T)| \leq 320B_2(\eta)\sqrt{B(\varepsilon, 9)}(4 \det T)^{4.5+1/2\varepsilon+\eta}$$

$$|a_{12}(T)| \leq 3843B_2(\eta)\sqrt{B(\varepsilon, 11)}(4 \det T)^{5.5+1/2\varepsilon+\eta}$$

in case $\det(T)$ is square-free.

Remark. Under the Lindelöf-hypothesis, the coefficients for square-free $\det(T)$ satisfy the Reskinoff-Saldaña conjecture. They do *not* satisfy this conjecture for all T .

Summary

- The Eisenstein series and χ_{10}, χ_{12} lie in the Maaß Spezialschar.
- Functions in the Schar correspond to Jacobi forms / special half-integral weight forms / classical integral weight forms.
- Use knowlegde of classical modular forms to derive results on Siegel modular forms.
- Make the correspondence *completely explicit* to perform actual computations and prove size bounds.