Notes on theta series

Nicolas Simard

November 2, 2015

Contents

1 Sum of four squares: introduction to theta series

In this section, we prove the well-known four square theorem. The goal is to give a nice first encounter with theta series to the reader.

First, recall that a *modular form* of weight k for a congruence subgroup Γ is a holomorphic function $f : \mathcal{H} \to \mathbb{C}$ satisfying the following two conditions:

1. f is invariant under the slash operator defined for every γ in $\mathrm{SL}_2(\mathbb{Z})$ as

$$(f|_k \gamma)(z) = j(\gamma, z)^{-k} f(\gamma z),$$

where $j(\gamma, z) = (cz + d)$ if $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$.

2. f is holomorphic at all cusps.

The $\mathbb{C}$-vector space for weight k modular forms for Γ is denoted $\mathcal{M}_k(\Gamma)$. A modular form vanishing at all cusps is called a *cusp form*. Cusp forms of weight k for Γ form a subspace of $\mathcal{M}_K(\Gamma)$, denoted $\mathcal{S}_k(\Gamma)$. A remarkable fact in the theory is that these spaces are finite dimensional. An explicit bound can also be given ([Zag, Prop 3]).

Proposition 1. *Let Γ be a congruence subgroup of $SL_2(\mathbb{Z})$. Then*

$$\dim \mathcal{M}_k(\Gamma) \leq \frac{k \mathit{Vol}(\Gamma \backslash \mathcal{H})}{3\pi} + 1 = \frac{k[SL_2(\mathbb{Z}) : \Gamma]}{12} + 1.$$

Consider the following quadratic form in four variables:

$$Q(x) = x_1^2 + x_2^2 + x_3^2 + x_4^2$$

and define

$$r_Q(n) = \#\{x \in \mathbb{Z}^4 | Q(x) = n\}.$$

Our goal in this section is to prove the four square theorem.

Theorem 1 (Lagrange). *Let n be a positive integer. Then*

$$r_Q(n) = 8 \sum_{d|n, 4 \nmid d} d = 8\sigma_1(n) - 32\sigma_1\left(\frac{n}{4}\right),$$

where $\sigma_k(n) = \sum_{d|n} d^k$ and $\sigma_1(\frac{n}{4}) = 0$ if n is not a multiple of 4. In particular, every positive is a sum of four squares.

To prove this, first consider the *theta series* attached to the quadratic form Q:

$$\theta_Q(z) = \sum_{x \in \mathbb{Z}^4} q^{Q(x)} = \sum_{x \in \mathbb{Z}^4} r_Q(n)q^n,$$

where as usual q is defined as $e^{2\pi i z}$. This holomorphic function is in fact a modular form of weight 2 for $\Gamma_0(4)$ and so the next step is to find a basis for $\mathcal{M}_2(\Gamma_0(4))$. To do so, consider the *Eisenstein series* of weight k and level one

$$G_k(z) = \sum_{m,n \in \mathbb{Z}} \frac{1}{(mz + n)^k}.$$

For $k \geq 3$, this series converges absolutely and defines a modular form of weight k for $\mathrm{SL}_2(\mathbb{Z})$ (which is non-zero if and only if k is even). For $k = 2$, the series converges, but not absolutely. Define $\mathbb{G}_2(z)$ by fixing a specific order of summation:

$$-4\pi^2 \mathbb{G}_2 = \frac{1}{2} \sum_{n \neq 0} \frac{1}{n^2} + \frac{1}{2} \sum_{m \neq 0} \sum_{n \in \mathbb{Z}} \frac{1}{(mz + n)^2}.$$

This order is such that $\mathbb{G}_2(z)$ has the following q-expansion

$$\mathbb{G}_2(z) = -\frac{1}{24} + \sum_{n=1}^{\infty} \sigma_1(n)q^n.$$

This function is holomorphic in the upper half plane, but not slash-k invariant under $\mathrm{SL}_2(\mathbb{Z})$ (of course, since $\mathcal{M}_2(\mathrm{SL}_2(\mathbb{Z})) = 0$). One can recover the invariance by introducing a correction factor: the function

$$\mathbb{G}_2^*(z) = \mathbb{G}_2(z) + \frac{1}{8\pi \mathrm{Im}(z)}$$

transforms like a modular form of weight 2, but is not holomorphic.

With these functions, one can define

$$f_1(z) = \mathbb{G}_2^*(z) - 2\mathbb{G}_2^*(2z) = \mathbb{G}_2(z) - \mathbb{G}_2(2z) = \frac{1}{24} + q + q^2 + \dots$$

and

$$f_2(z) = \mathbb{G}_2^*(2z) - 2\mathbb{G}_2^*(4z) = \mathbb{G}_2(2z) - 2\mathbb{G}_2(4z) = \frac{1}{24} + q^2 + q^4 + \dots.$$

These functions belong to $\mathcal{M}_2(\Gamma_0(4))$ since they have the right transformation properties and are holomorphic. Since they are also linearly independent and

$$\dim \mathcal{M}_2(\Gamma(4)) \leq \frac{2[\mathrm{SL}_2(\mathbb{Z}) : \Gamma_0(4)]}{12} + 1 = 2,$$

2

they form a basis for $\mathcal{M}_2(\Gamma_0(4))$. Comparing these q-expansions with the q-expansion

$$\theta_Q(z) = 1 + 8q + \dots,$$

one sees that

$$\theta_Q(z) = 8(\mathbb{G}_2(z) - 2\mathbb{G}_2(2z)) + 16(\mathbb{G}_2(2z) - 2\mathbb{G}_2(4z)) = 8\mathbb{G}_2(z) - 32\mathbb{G}_2(z).$$

Comparing the coefficients of the q-expansions on both sides proves the theorem.

2 Theta series and $\mathbb{L}$-functions

In this section, we explore the connection between theta series and L-functions. The goal is to give less trivial applications of theta series in mathematics. In the last subsection, we present the ideas behind an efficient algorithm that evaluates L-functions.

2.1 The Riemann zeta function

Define

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

This is a modular form of weight 1/2 for $\Gamma_0(4)$ (and a certain multiplier system, as we will see in the next section). Recall that the Poisson summation formula can be written as

$$\sum_{n\in\mathbb{Z}} f(x+n) = \sum_{n\in\mathbb{Z}} \hat{f}(n) e^{2\pi i n x},$$

where f is any continuous function on $\mathbb{R}$ which decreases rapidly as x tends to infinity and $\hat{f}$ is its Fourier transform. Applying this to $f_t(x) = e^{-\pi t x^2}$ and letting $x = 0$ we get the following transformation formula for $\theta(t)$:

$$\theta(i/t) = \sqrt{t}\theta(it) \qquad \text{for } t \in \mathbb{R}.$$

Now let

$$\phi(t) = \frac{\theta(it) - 1}{2}$$

and consider the Mellin transform of ϕ

$$\mathcal{M}(\phi)(s) = \int_0^\infty \phi(t) t^s \frac{dt}{t}.$$

On one hand, this is equal to

$$\int_0^\infty \sum_{n=1}^\infty e^{-\pi n^2 t} t^s \frac{dt}{t} = \sum_{n=1}^\infty \int_0^\infty e^{-\pi n^2 t} t^s \frac{dt}{t} = \sum_{n=1}^\infty \frac{1}{(\pi n^2)^s} \int_0^\infty e^{-t} t^s \frac{dt}{t} = \pi^{-s} \zeta(2s) \Gamma(s)$$

and on the other, using the fact that

$$\phi(1/t) = \frac{\theta(i/t) - 1}{2} = \frac{t^{1/2}\theta(it) - 1}{2} = t^{1/2}\phi(t) - \frac{1}{2} + \frac{t^{1/2}}{2},$$

it is equal to

$$\int_0^1 \phi(t) t^s \frac{dt}{t} + \int_1^\infty \phi(t) t^s \frac{dt}{t} = \int_1^\infty \phi(t)(t^s + t^{1/2-s}) \frac{dt}{t} - \frac{1}{2s} + \frac{1}{2(1/2 - s)}.$$

The equality

$$\pi^{-\frac{s}{2}} \zeta(s) \Gamma\left(\frac{s}{2}\right) = \int_1^\infty \phi(t)(t^{\frac{s}{2}} + t^{\frac{1-s}{2}}) \frac{dt}{t} - \frac{1}{s} + \frac{1}{1-s}$$

3

not only proves that $\zeta(s)$ extends to a meromorphic function on the complex plane with two simple poles at $s = 0$ and $s = 1$, it also proves that the *completed L-function*

$$\Lambda(s) = \pi^{-\frac{s}{2}} \zeta(s) \Gamma\left(\frac{s}{2}\right)$$

satisfies the functional equation

$$\Lambda(s) = \Lambda(1-s).$$

This example is an illustration of what Zagier calls "the functional equation principle" which says, roughly, that the Mellin transform of a function having a certain symmetry with respect to the transformation $t \mapsto 1/t$ (e.g. $\phi(t)$) extends meromorphically to the complex plane and has a functional equation. The next subsection gives another illustration of this principle.

A similar principle can be applied to prove that the L-function attached to a newform extends meromorphically (in fact, holomorphically) to the complex plane and satisfies a functional equation. The proof of this uses the so-called *Fricke involution*, but we won't get into this in these notes.

2.2 Non-holomorphic Eisenstein series

The *Non-holomorphic Eisenstein series* is defined as

$$G(z, s) = \frac{\operatorname{Im}(z)^s}{2} \sum_{m,n \in \mathbb{Z}} \frac{1}{|mz + n|^{2s}} = \zeta(2s) \sum_{\gamma \in \Gamma_\infty \backslash \mathrm{SL}_2(\mathbb{Z})} \operatorname{Im}(\gamma(z))^s.$$

If $Q(x, y)$ is a binary quadratic form of discriminant D and root $z \in \mathcal{H}$ (i.e. $Q(z, 1) = 0$), then

$$2^{s+1} D^{-s/2} G(z, s) = \sum_{m,n \in \mathbb{Z}} \frac{1}{Q(m, n)^s},$$

where the function on the right is called the *Epstein zeta function*.

Now define

$$\theta_z(t) = \sum_{m,n \in \mathbb{Z}} e^{-\pi|mz+n|^2 \operatorname{Im}(z)^{-1} t}.$$

Then using Poisson summation formula again, we see that

$$\theta_z(1/t) = t\theta_z(t)$$

and so $\phi(t) = (\theta_z(t) - 1)/2$ satisfies the following transformation formula:

$$\phi(1/t) = -\frac{1}{2} + \frac{t}{2} + t\phi(t).$$

It follows that

$$G^*(z, s) := \int_0^\infty \phi(t) t^s \frac{dt}{t} = \pi^{-s} \Gamma(s) G(z, s)$$

extends to a meromorphic on $\mathbb{C}$ with poles at $s = 0$ and $s = 1$ and satisfies the functional equation

$$G^*(z, s) = G^*(z, 1 - s).$$

This is another illustration of the functional equation principle.

The function $G(z, s)$ is used in the Rankin-Selberg method, which can be used to compute the Petersson norm of modular forms.

Note also that the leading terms of $G(z, s)$ are know by the Kronecker limit formula. This has many applications in number theory.

2.3 Numerical evaluation of L-functions

The idea behind the functional principle has other applications. They were used by Dokchister, who implemented a Pari/GP package that effectively computes the values of (nice enough) L-functions (see [Com]). The goal here is not to analyse the error term of the implementation details (for this, we refer the reader to Dokchister's article [Dok]), but only to see how one can use the ideas above in a different way.

First, we need to agree on what we mean by L-function. For us, an L-function is a Dirichlet series

$$L(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}$$

satisfying the following conditions:

1. (Ramanujan bound) The coefficients do not grow too fast, i.e.

$$a_n = O(n^\alpha)$$

   for some $\alpha > 0$. In other words, the Dirichlet series converges in some right half-plane.

2. (Meromorphy and functional equation) The function $L(s)$ extends to a meromorphic function on $\mathbb{C}$ and has a finite number of simple poles at $s = p_i$ with residues r_i. Moreover, there exists a *weigh* $w \geq 0$, a *sign* $\epsilon \in \mathbb{C}^*$, an *exponential factor* $A \in \mathbb{R}_{\geq 0}$ and a Γ-*factor*

$$\gamma(s) = \Gamma\left(\frac{s + \lambda_1}{2}\right) \Gamma\left(\frac{s + \lambda_2}{2}\right) \ldots \Gamma\left(\frac{s + \lambda_d}{2}\right)$$

   of *dimension* $d \geq 1$ and *Hodge numbers* $\lambda_1, \ldots, \lambda_d \in \mathbb{C}$ such that the completed L-function

$$L^*(s) = A^s \gamma(s) L(s)$$

   satisfies the functional equation

$$L^*(s) = \epsilon L^*(w - s).$$

Note that most of the time, $A = \frac{\sqrt{N}}{\pi^{d/2}}$, where N is a conductor.

Example: Examples of L-functions are $\zeta(s)$ (the Riemann zeta function), $\zeta_K(s)$ (the Dedekind zeta functions of number fields), $L(s, \chi)$ (the Dirichlet L-functions attached to a Dirichlet character), $L(s, \xi)$ (the Hecke L-functions attached to a Hecke character), the L-function attached to a modular form of level one, the L-function attached to a newform for $\Gamma_0(N)$, the Artin L-functions, the L-functions attached to Elliptic curves, etc.

Exercise: Pick your favourite L-function and see how it fits in the above definition, i.e. find its weight, sign, exponential factor, degree, Hodge numbers, poles(s) and residue(s) (if any). See [Dok] for a table containing this data.

Now define $\phi(t)$ as

$$\gamma(s) = \int_0^\infty \phi(t) t^s \frac{dt}{t},$$

that is ϕ is the inverse Mellin transform of the Γ-factor. Then if we let

$$\Theta(s) = \sum_{n=1}^{\infty} a_n \phi(nt/A),$$

we see that

$$\int_0^\infty \Theta(t) t^s \frac{dt}{t} = L^*(s).$$

The functional equation for $L^*(s)$ implies that $\Theta(t)$ satisfies the functional equation

$$\Theta(1/t) = \epsilon t^w \Theta(t) - \sum r_j t^{p_j}$$

for all real positive t. In fact, the converse holds: the functional equation for Θ implies the functional equation for $L^*(s)$. This gives a numerical way of verifying the functional equation of $L^*(s)$ (provided one can efficiently compute $\Theta(t)$).

Example: For $L(s) = \zeta(s)$, one has $a_n = 1$ for all $n \geq 1$, $w = 1$, $\epsilon = 1$, $A = 1/\sqrt{\pi}$, $d = 1$ and $\gamma(s) = \Gamma(s/2)$. Then

$$\phi(t) = e^{-t^2} \text{ and } \Theta(t) = 2\sum_{n=1}^{\infty} e^{-\pi n^2 t^2}.$$

We also have $p_1 = 0, r_1 = 1, p_2 = 1$ and $r_2 = -1$, so

$$\Theta(1/t) = t\Theta(t) - 1 + t,$$

which is the same formula as above, up to s simple change of variable.

Fix now $s \in \mathbb{C}$. Playing with the representation of $L^*(s)$ as an integral, one sees that

$$L^*(s) = \sum_{n=1}^{\infty} a_n G_s(n/A) + \epsilon \sum_{n=1}^{\infty} a_n G_{w-s}(n/A) + \sum_j \frac{r_j}{p_j - s},$$

where

$$G_s(t) = t^{-s} \int_0^{\infty} \phi(x) x^s \frac{dx}{x} \qquad \text{for } t > 0$$

is t^{-s} times the *incomplete Mellin transform* of ϕ.

At this point, it may not be totally clear why we are doing all this work to evaluate the L-function. After all, one could simply plug a value of s in the Dirichlet L-series and add terms! The main problem is that the terms of the Dirichlet L-series tend to zero very slowly (think of how slowly the harmonic series diverges). In fact, Dirichlet series converge so slowly that it is impossible in practice to evaluate them to a great precision (see example bellow). Another problem is that the series expression for $L(s)$ is valid only in a half plane. The main advantage of the method presented here is that the function $G_s(t)$ can be efficiently computed numerically and that it tends to zero *exponentially fast* as t tends to infinity. Moreover, the formula above for $L^*(s)$ in terms of $G_s(t)$ is valid for all s and it suffices to divide its value by the exponential factor and the Γ-factor to obtain the value of $L(s)$.

Example: Take $L(s) = \zeta(s)$ for example. Using Dokchister's computel PARI/GP package, it takes 80ms to evaluate $\zeta(2)$ to 100 digits of precision. On the same computer, using the Dirichlet L-series defining $\zeta(s)$ directly, it takes a little more than 7 minutes to sum the first 500000 terms of the series to get only 6 digits of precision. Let us also mention that the computel package used only 11 terms to get the 100 digits.

In conclusion, the technique presented in this section has the advantage of being really fast in comparison with the naive approach of summing the terms in the Dirichlet series. Moreover, the computel package uses a smaller number of coefficients of the Dirichlet L-series to evaluate the L-function. Of course, the coefficients of the Riemann zeta function are easy to compute, but for more general L-functions (e.g. the L-function of an elliptic curve) it can be relatively difficult to compute large coefficients. For more details on the computational aspects of L-functions, we refer to [Dok] and [Coh].

3 Theta series in general

In this section, we introduce two kind of theta functions: the classical ones and the ones defined by Hecke. On the way, we will also need to so-called congruent theta functions. Before introducing any of these, it is necessary to define multiplier systems and spherical functions. The main reference for the material of this section is [Iwa].

3.1 Multiplier systems and automorphic forms

The main reference for this subsection is [Iwa, Sec 2.6, 2.7]. Let k be any real number and $\Gamma \leq \mathrm{SL}_2(\mathbb{Z})$ a congruence subgroup. It is not difficult to define multiplier systems when k is an integer.

Example: Let k be an integer and let

$$\chi : (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times$$

be a Dirichlet character such that $\chi(-1) = (-1)^k$. Then the map

$$\vartheta : \Gamma_0(N) \to \mathbb{C}^\times$$

which sends $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ to $\chi(d)$ is a homomorphism. ϑ is an example of a multiplier system. Without the consistency condition $\chi(-1) = (-1)^k$ there would be no modular forms of weight k for $\Gamma_0(N)$ with multiplier system ϑ.

The case where k is not an integer is more involved, but since some theta series are of half integral weight, we need to consider more general multiplier systems.

To begin, for any non-zero complex number z, fix $\arg(z) \in (-\pi, \pi]$ and denote the principal branch of log by $\log z$. Then define

$$z^s = \exp(s \log z)$$

for any $s \in \mathbb{C}$. Recall that for $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$, one defines $j_\gamma(z)$ as

$$j_\gamma(z) = cz + d.$$

For any $\gamma_1, \gamma_2 \in SL_2(\mathbb{Z})$, one defines $w(\gamma_1, \gamma_2)$ as

$$2\pi w(\gamma_1, \gamma_2) = -\arg j_{\gamma_1 \gamma_2}(z) + \arg j_{\gamma_1}(\gamma_2 z) + \arg j_{\gamma_2}(z).$$

Note that $w(\gamma_1, \gamma_2) \in \{0, \pm 1\}$. The *factor system of weight* k is defined as

$$\omega_k(\gamma_1, \gamma_2) = e(kw(\gamma_1, \gamma_2)),$$

where $e(z) = \exp(2\pi i z)$. When k is an integer, the factor system of weight k is identically one. In general,

$$\omega_k(\gamma_1, \gamma_2) j_{\gamma_1 \gamma_2}(z)^k = j_{\gamma_1}(\gamma_2 z)^k j_{\gamma_2}(z)^k$$

and

$$f|_k \gamma_1 \gamma_2 = \omega_k(\gamma_1, \gamma_2)(f|_k \gamma_1)|_k \gamma_2.$$

Definition 1. *Let Γ be a congruence subgroup of $SL_2(\mathbb{Z})$ and k a real number. A multiplier system of weight k for Γ is a map*

$$\vartheta : \Gamma \to \mathbb{C}$$

such that

$$|\vartheta(\gamma)| = 1 \qquad \text{for } \gamma \in \Gamma$$

and

$$\vartheta(\gamma_1 \gamma_2) = \omega_k(\gamma_1, \gamma_2) \vartheta(\gamma_1) \vartheta(\gamma_2).$$

Moreover, we require the following consistency condition: if $-I \in \Gamma$, then

$$\vartheta(-I) = e^{-i\pi k}$$

A holomorphic function $f : \mathcal{H} \to \mathbb{C}$ is called an *automorphic form* of weight k for Γ with multiplier system ϑ if

$$f|_k \gamma = \vartheta(\gamma) f$$

for all $\gamma \in \Gamma$ and if it is holomorphic at the cusps of Γ.

We will see many examples of automorphic forms of half integral weight with various multiplier systems. Before that, we briefly introduce spherical functions.

3.2 Spherical functions

For the rest of these notes, $A = (a_{ij})$ will be an integral symmetric positive definite matrix of rank r. The Laplace operator attached to A is

$$\Delta_A = \sum_{i,j} a_{ij}^* \frac{\partial^2}{\partial x_i \partial x_j} \qquad \text{where } (a_{ij}^*) = A^{-1}.$$

A *spherical function* of degree ν for A is a homogeneous polynomial P in r variables of degree ν such that

$$\Delta_A P = 0.$$

Equivalently, P is constant if $\nu = 0$, P is a linear form if $\nu = 1$ and

$$P(x) = \sum_{i=1}^{d} c_i (\ell^t A x)^\nu,$$

where $\ell \in \mathbb{C}^r$ is isotropic (i.e. $\ell^t A \ell = 0$) and $c_i \in \mathbb{C}$, if $\nu \geq 2$.

3.3 Classical theta functions

Let A be a matrix as above and let P be a spherical function of degree ν for A. The matrix A is called even if its diagonal entries are even. Equivalently, $x^t A x$ is even for all $x \in \mathbb{Z}^r$. The *theta series* attached to A and P is defined as

$$\Theta_{A,P}(z) = \sum_{m \in \mathbb{Z}^r} P(m) e\left(\frac{1}{2} A[m] z \right),$$

where $A[m] = m^t A m$. Now fix an integer $N > 0$ such that $N A^{-1}$ has integral entries (e.g. $N = |A|$). For any vector $h \pmod{N}$, the *congruent theta series* is defined as

$$\Theta_{A,P,h}(z) = \sum_{\substack{m \in \mathbb{Z}^r \\ m \equiv h \pmod{N}}} P(m) e\left(\frac{A[m] z}{2N^2} \right).$$

Note that if $h = 0$, then $\Theta_{A,P,0}(z) = N^\nu \Theta_{A,P}(z)$.

    Example: The following series are example of theta series. Note that the matrix of the first series is not even.

$$\Theta_{(1),1}(z) = \sum_{n \in \mathbb{Z}} e(n^2 z/2) = \sum_{n \in \mathbb{Z}} e^{i\pi n^2 z},$$

$$\Theta_{(2),1}(z) = \sum_{n \in \mathbb{Z}} e(n^2 z) = \sum_{n \in \mathbb{Z}} q^{n^2},$$

where as usual $q = e^{2\pi i z}$ and

$$\Theta_{2I_4,1}(z) = \sum_{m \in \mathbb{Z}^4} q^{m_1^2 + \cdots + m_4^2}$$

are examples of theta series that we have seen before.

    Our goal in this section is to see that theta functions are modular forms and find the corresponding weight, level and multiplier system. The first step towards this is to prove the following inversion formula.

Theorem 2. *Let A be a symmetric, positive definite integral matrix of dimension r and let P be a spherical function with respect to A of degree ν. Then for any $z \in \mathcal{H}$ and $x \in \mathbb{C}^r$ we have*

$$\sum_{m \in \mathbb{Z}^r} P(m+x) e\left(\frac{A[m+x] z}{2} \right) = \frac{i^{-\nu}}{\sqrt{|A|}} \left(\frac{i}{z} \right)^k \sum_{m \in \mathbb{Z}^r} P^*(m) e\left(\frac{-A^{-1}[m]}{2z} + m^t x \right).$$

In particular, for $x = 0$,

$$\Theta_{A,P}(z) = \frac{i^{-\nu}}{\sqrt{|A|}} \left(\frac{i}{z} \right)^k \Theta_{A^{-1},P^*}(-1/z),$$

where $P^*(m) = P(A^{-1}m)$.

Sketch of proof. The first step is to apply the Poisson summation formula to the function

$$f(x) = e\left(\frac{A[x]z}{2}\right).$$

Now suppose, without loss of generality, that $P(x) = (\ell^t A x)^\nu$, where ℓ is isotropic if $\nu \geq 2$ and $\ell \in \mathbb{C}$ if $\nu = 0, 1$. Then define the differential operator

$$L = \sum_{j=1}^{r} \ell_j \frac{\partial}{\partial x_j}$$

and apply L^ν to the equation obtained above via Poisson summation formula to get the result.

For more details, see [Iwa, Sec 10.2]. □

Corollary 1. *If $|A| = 1$, then*

$$\Theta_{A,P}(-1/z) = i^{-\nu}(-1/z)^{\nu + r/2}\Theta_{A,P}(z).$$

A matrix satisfying the condition of the corollary is called unimodular. It turns out that the dimension of such a matrix is a multiple of 8. If the dimension is not a multiple of 8, the inversion formula in the theorem above does not relate the theta function of the matrix to itself.

To proceed further in the analysis of theta functions, it is convenient to study the space spanned by a specific family of congruent theta functions. First, define

$$H = \{h \pmod{N} | Ah \equiv 0 \pmod{N}\},$$

where, as above, N is any integer such that NA^{-1} is integral. The following result is not hard to establish.

Proposition 2. *For any $h \in H$,*

$$\Theta_{A,P,h}(z+2) = e\left(\frac{A[h]}{N^2}\right)\Theta_{A,P,h}(z)$$

and if A is even,

$$\Theta_{A,P,h}(z+1) = e\left(\frac{A[h]}{2N^2}\right)\Theta_{A,P,h}(z)$$

Proof. Simply note that

$$A[m] \equiv A[h] \pmod{N^2}.$$

□

The next proposition follows from an application of the inversion formula.

Proposition 3. *For any $h \in H$,*

$$\Theta_{A,P,h}(-1/z) = i^{-\nu}|A|^{-1/2}(-iz)^{\nu+r/2}\sum_{\ell \in H} e\left(\frac{h^t A \ell}{N^2}\right)\Theta_{A,P,\ell}(z)$$

Sketch of proof. Apply the transformation formula of Theorem 2 with $x = h/N$. Then the left hand side is $N^{-\nu}\Theta_{A,P,h}(z)$. On the right hand side, change m to $NA^{-1}m$ to get

$$\Theta_{A,P,h}(-1/z) = i^{-\nu}|A|^{-1/2}(-iz)^{\nu+r/2}\sum_{Am \equiv 0 \pmod{N}} P(m)e\left(\frac{A[m]z}{2N^2} + \frac{m^t Ah}{N^2}\right).$$

Rearranging the sum gives the result. □

This proposition says that the space spanned by congruent theta functions with $h \in H$ is stable under $z \mapsto z+2$ and $z \mapsto -1/z$. With some work, one can then prove the following general theorem about the transformation properties of congruent theta functions.

Theorem 3. *Let* $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$ *with* $d \equiv 1 \pmod 2$ *and suppose that at least one of the following three conditions hold:*

- $c \equiv 0 \pmod{2N}$ *and* $b \equiv 0 \pmod 2$.

- $c \equiv 0 \pmod{2N}$ *and* A *is even.*

- $c \equiv 0 \pmod N$ *and* A *and* $N^{-1}A$ *are even.*

Then for any $h \in H$,

$$\Theta_{A,P,h}(\gamma z) = e\left(\frac{A[h]}{2N^2}\right)^{ab} \vartheta(\gamma)(cz+d)^{\nu+r/2}\Theta_{A,P,ah}(z),$$

where

$$\vartheta(\gamma) = \left(\frac{|A|}{d}\right)\left(\bar{\epsilon}_d\left(\frac{2c}{d}\right)\right)^r,$$

with

$$\epsilon_d = \begin{cases} 1 & \text{if } d \equiv 1 \pmod 4 \\ i & \text{if } d \equiv -1 \pmod 4 \end{cases}$$

and $\left(\frac{|A|}{d}\right)$ *is the Jacobi symbol.*

Proof. See [Iwa, Prop 10.6]. □

Corollary 2. *We have*

$$\Theta_{A,P,h}(z) \in \mathcal{M}_{\nu+r/2}\left(\Gamma(4N), \left(\frac{2c}{d}\right)^r\right)$$

and if $\nu > 0$, $\Theta_{A,P,h}(z)$ *is a cusp form.*

Using this general result about congruent theta functions, one can prove the following theorem.

Theorem 4. *Let* A *be a symmetric, positive definite, integral and even matrix of even rank* r. *Let* N *be such that* NA^{-1} *has the same properties. Let* P *be a spherical function of degree* ν *for* A. *Then*

$$\Theta_{A,P}(z) \in \mathcal{M}_{\nu+r/2}(\Gamma_0(N), \chi_D),$$

where $D = (-1)^{r/2}|A|$ *and* $\chi_D(\gamma) = \left(\frac{D}{d}\right)$ *is the Kronecker symbol. If* $\nu > 0$, *then* $\Theta_{A,P}(z)$ *is a cusp form.*

Proof. See [Iwa, Thm 10.9]. □

Example: Let $Q(x,y) = ax^2 + bxy + cy^2$ be an integral binary quadratic form. Then the theta series

$$\sum_{m,n\in\mathbb{Z}^2} q^{Q(m,n)}$$

is a modular form of weight one for the congruence subgroup $\Gamma_0(-D)$ with character (multiplier system) χ_D, where $D = b^2 - 4ac$. To see this, it suffices to take $P = 1$ and

$$A = \begin{pmatrix} 2a & b \\ b & 2c \end{pmatrix}.$$

Example: The theta series

$$\sum_{x\in\mathbb{Z}^4} q^{x_1^2+\cdots+x_4^2}$$

that was used in the proof of the four square theorem is a modular form of weight 2 for the congruence subgroup $\Gamma_0(4)$ with trivial character. This is because the determinant of the matrix

$$A = \begin{pmatrix} 2 & & & \\ & 2 & & \\ & & 2 & \\ & & & 2 \end{pmatrix}$$

is 16 and so the character χ_{16} is trivial in this case.

3.4 Hecke's theta series

Throughout this subsection, fix an K imaginary quadratic field, $\mathfrak{m}$ a modulus of K, $I_{\mathfrak{m}}$ the multiplicative group of fractional ideals coprime to $\mathfrak{m}$ and

$$K_{\mathfrak{m},1} = \{(\mathfrak{a})|\mathfrak{a} \equiv 1 \pmod{\mathfrak{m}}\}.$$

The congruence condition in the definition of $K_{\mathfrak{m},1}$ means that for all integral prime ideals $\mathfrak{p}$ of $\mathcal{O}_K$ dividing $\mathfrak{m}$, we have $\mathrm{ord}_{\mathfrak{p}}(\mathfrak{a} - 1) \geq \mathrm{ord}_{\mathfrak{p}}(\mathfrak{m})$. Note that the ideals of $K_{\mathfrak{m},1}$ belongs to $I_{\mathfrak{m}}$.

Fix now an embedding of K in $\mathbb{C}$ and an integer u and define a map

$$\xi_{\infty}^{u} : K^{*} \longrightarrow \mathbb{C}^{*}$$

$$\mathfrak{a} \longmapsto \left(\frac{\mathfrak{a}}{|\mathfrak{a}|}\right)^{u}.$$

For $\mathfrak{m}$ small enough $U_{\mathfrak{m},1} \subseteq \ker \xi_{\infty}^{u}$, where $U_{\mathfrak{m},1} = U_K \cap K_{\mathfrak{m},1}$. It follows that for such a modulus $\mathfrak{m}$, ξ_{∞}^{u} induces a well-defined map

$$\xi_{\infty}^{u} : K_{\mathfrak{m},1} \longrightarrow \mathbb{C}^{*}.$$

We define a *Hecke character* for K as a (unitary) character

$$\xi : I_{\mathfrak{m}} \longrightarrow \mathbb{C}^{*}$$

such that $\xi|_{K_{\mathfrak{m},1}} = \xi_{\infty}^{u}$ for some integer u. Note that if $u = 0$, then ξ induces a character on the ray class group modulo $\mathfrak{m}$, $C_{\mathfrak{m}} = I_{\mathfrak{m}}/K_{\mathfrak{m},1}$, and that conversely any unitary character of the ray class group can be seen as a Hecke character with $u = 0$.

The main result in this subsection is the following theorem.

Theorem 5. *Let* $K = \mathbb{Q}(\sqrt{D})$ *be an imaginary quadratic field and* ξ *a Hecke character modulo* $\mathfrak{m}$ *such that*

$$\xi((\mathfrak{a})) = \left(\frac{\mathfrak{a}}{|\mathfrak{a}|}\right)^{u} \qquad \text{if } \mathfrak{a} \equiv 1 \pmod{\mathfrak{m}},$$

where $u \in \mathbb{Z}_{\geq 0}$. *Then*

$$\theta_{\xi}(z) = \sum_{\mathfrak{a}} \xi(\mathfrak{a}) \mathbb{N}(\mathfrak{a})^{\frac{u}{2}} q^{\mathbb{N}\mathfrak{a}},$$

where the sum runs over all integral ideals of K, is a modular form of weight $u + 1$ *for* $\Gamma_0(|D|\mathbb{N}\mathfrak{m})$ *with character (multiplier system)* ϑ *defined as*

$$\vartheta(\gamma) = \chi_D(d)\xi((d)) \qquad \text{for } \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}).$$

If $u > 0$, $\theta_{\xi}(z)$ *is a cusp form.*

Proof. See [Iwa, Prop 12.5] for a sketch of the proof. □

Let us mention that the proof of this theorem uses techniques that are different than the ones used before (Poisson summation, in particular). In fact, Hecke used his theory of L-functions to prove it.

Example: In [Wei, Sec 4.2], the author mentions the fact that if χ is a character

$$\chi : (\mathbb{Z}[i]/(\alpha))^{*} \longrightarrow \mathbb{C}^{*}$$

such that $\chi(i) = 1$, where $\alpha \in \mathbb{Z}[i]$, then the function

$$\theta_{\chi}(z) = \frac{1}{4} \sum_{a,b \in \mathbb{Z}} \chi(a + bi) q^{a^2 + b^2}$$

is a modular form of weight one for $\Gamma_1(4|\alpha|^2)$ (and trivial multiplier system). This follows directly from the theorem above. The idea is that for any field K and any modulus $\mathfrak{m}$ of K, one has the following exact sequence

$$1 \to U_K/U_{\mathfrak{m},1} \to K_{\mathfrak{m}}/K_{\mathfrak{m},1} \to C_{\mathfrak{m}} \to C \to 1,$$

where C is the class group of K (see [Mil, Ch.V, Thm 1.7]). Moreover,

$$K_{\mathfrak{m}}/K_{\mathfrak{m},1} \cong \prod_{\substack{\mathfrak{p}|\mathfrak{m} \\ \mathfrak{p} \text{ real}}} \{\pm 1\} \times (\mathcal{O}_K/\mathfrak{m})^*.$$

For $K = \mathbb{Q}(i)$, one has $U_K = \{\pm 1, \pm i\}$. Taking $\mathfrak{m} = (\alpha)$ and remembering that $\chi(U_K) = 1$ by assumption, we see that χ induces a character of the ray class group modulo (α), hence a Hecke character with $u = 0$. Finally, note that every ideal of $\mathbb{Z}[i]$ is principal and note that the multiplier system of the theorem is trivial on $\Gamma_1(4|\alpha|^2)$.

4 Modular forms of weight one

Modular forms of weight one are very interesting. For example, one can attach a 2-dimensional representation of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ to them (a theorem of Deligne and Serre). This gives a way to prove the Artin conjecture in certain cases. Following an example of Serre (see [Ser, Note on 5.3]), we will see how modular forms of weight one appear naturally.

Let $f(x) = x^3 - x - 1$, let $E = \mathbb{Q}[x]/(f)$ and let L be the Galois closure of E. Then $\mathrm{Gal}(L/\mathbb{Q}) \cong S_3$. Since f has discriminant -23, $K := \mathbb{Q}(\sqrt{-23}) \subseteq L$. Since L/K is unramified everywhere (verify this!) and K has class number 3 (verify this too!), L is the Hilbert class field of K. Our goal is to compute

$$N_p = \text{number of roots of } f \mod p.$$

In fact, for $p \neq 23$, N_p is the number of fixed point of $\sigma_p \in \mathrm{Gal}(L/\mathbb{Q})$ (the Frobenius at p) as a permutation in S_3 (see [Ser]). It is not too difficult to prove that for $p \neq 23$

$$N_p = \begin{cases} 0 \text{ or } 3 & \text{if } \left(\frac{-23}{p}\right) = 1 \\ 1 & \text{if } \left(\frac{-23}{p}\right) = -1 \end{cases}.$$

To distinguish between the two cases when $\left(\frac{-23}{p}\right) = 1$, first write $p\mathcal{O}_K = \mathfrak{p}\bar{\mathfrak{p}}$. Then

$$
\begin{aligned}
N_p = 3 &\Leftrightarrow \sigma_{\mathfrak{p}} = 1 \\
&\Leftrightarrow \sigma_{\mathfrak{p}} = 1 \\
&\Leftrightarrow \mathfrak{p} \text{ is principal} \\
&\Leftrightarrow p = m^2 + mn + 6n^2 \text{ for some } m, n \in \mathbb{Z}
\end{aligned}
$$

where we used the fact that $\mathrm{Gal}(L/K)$ is isomorphic to the class group of K to pass from the second to the third row. This proves that for $p \neq 23$

$$N_p = \begin{cases} 3 & \text{if } p \text{ is representable by } x^2 + xy + 6y^2 \\ 0 & \text{if } p \text{ is representable by } 2x^2 + xy + 3y^2 \\ 1 & \text{if } \left(\frac{-23}{p}\right) = -1 \end{cases}.$$

This example leads to the consideration of the following function

$$\frac{1}{2}\left(\sum_{m,n\in\mathbb{Z}} q^{m^2+mn+6n^2} - \sum_{m,n\in\mathbb{Z}} q^{2m^2+mn+3n^2} \right) = \sum_{n=1}^{\infty} a_n q^n.$$

Then $N_p = a_p + 1$ and using the results of the previous section, we see that it is a cusp form of weight one for the congruence subgroup $\Gamma_0(23)$ with character χ_{-23} (the Kronecker symbol). It is natural to ask if we can use the same technique as in the four square theorem to completely solve the problem, i.e. to find conditions on p to determine by which quadratic form it is represented when $\left(\frac{-23}{p}\right) = 1$. Unfortunately, the space of modular forms of weight one is more difficult to study. Note however that with some work, one can define Eisenstein series of weight one.

An explicit basis of these spaces would lead to interesting results on the representation of primes by quadratic forms. A few things are known in this subject, but there are still interesting problems. For example, since the class group of $K = \mathbb{Q}(\sqrt{-23})$ has only one genus with three classes in it, it is not possible to determine which quadratic form represents p based on congruence conditions. For $K = \mathbb{Q}(i)$, this is possible, since Fermat showed that an odd prime p is a sum of two squares if and only if $p \equiv 1 \pmod 4$. Those results come from the genus theory of quadratic forms, which was developed by Gauss.

References

[Coh]   Cohen, H., *Computational Number Theory in relation with L-functions*.

[Com]   Dokchister, T., *ComputeL - Computing special values of L-functions, version 1.3.3*, PARI/GP package available at `http://www.maths.bris.ac.uk/ matyd/computel/index.html`.

[Dok]   Dokchister, T., *Computing special values of L-functions*, `arXiv:math/0207280v1 [math.NT]`, 2002.

[Iwa]   Iwaniec, H., *Topics in Classical Automorphic Forms*, Graduate Studies in Mathematics, Volume 17, American Mathematical Society, Providence, 1991.

[Mil]   Milne, J. S., *Class Field Theory (v4.02)*, Available at www.jmilne.org/math/, 2013.

[Ser]   Serre, J.-P., *On a theorem of Jordan*, Bull. Amer. Math. Soc. 40 (2003), no. 4, 429-440.

[Wei]   Weinstein, J., *Reciprocity laws and Galois representations: recent breakthroughs*.

[Zag]   Zagier, D., *Elliptic modular forms and their applications* in *1-2-3 of Modular Forms*, Universitext, Springer-Verlag Berlin Heidelberg, 2008.