MODULAR FORMS TWIGS

PAUL E. GUNNELLS

1. Introduction

These are the notes from the TWIGS[1] talk on modular forms. Most of the material can be found in several places, namely [2, 4, 5] (in fact experts will be able to dissect these notes into pieces contained in *loc.cit.*). To learn more about Ramanujan graphs, one can consult [1, 3]. A copy of [5] is available from me by request.

2. Basic definitions

2.1. Let $\mathfrak{H}$ be the upper halfplane, that is the set of complex numbers with positive imaginary part, and let $k \geq 2$ be a positive integer. Let Γ be the group $SL_2(\mathbb{Z})$ of 2×2 integral matrices with determinant 1. The group Γ acts on $\mathfrak{H}$ by *fractional linear transformations*: the element $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ takes $\tau \in \mathfrak{H}$ to $\gamma(\tau) := (a\tau + b)/(c\tau + d)$.

Let $f \colon \mathfrak{H} \to \mathbb{C}$ be a holomorphic function. Then f is called a *weight k modular form* if f satisfies

- $f(\gamma(\tau)) = (c\tau + d)^k f(\tau)$ for all $\gamma \in \Gamma$, and
- f is "holomorphic at infinity."

To explain what the second condition means, we need more notation. Let $q = e^{2\pi i\tau}$. The function $\tau \mapsto e^{2\pi i\tau}$ takes $\mathfrak{H}$ onto the punctured open unit disc

$$D = \bigl\{ q \in \mathbb{C} \bigm| |q| < 1, q \neq 0 \bigr\}.$$

Since $f(\tau + 1) = f(\tau)$ (take $\gamma = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$), we can actually write f as a function of q. Since f is holomorphic on $\mathfrak{H}$, it's also holomorphic on D, and has a Laurent expansion around $q = 0$ of the form

$$f(q) = \sum_{k=-N}^{\infty} a_k q^k, \quad N \geq 0, a_k \in \mathbb{C}. \tag{1}$$

Then "holomorphic at infinity" means that f extends to be holomorphic at $q = 0$. This the case if and only if $a_k = 0$ for all $k < 0$.

We denote the space of weight k modular forms by M_k. This is a $\mathbb{C}$ vector space, *a priori* of infinite dimension. We say f is a *cuspform* if $a_0 = 0$, and let $S_k \subset M_k$ be the subspace of all cuspforms.

Date: December 12, 2003.

[1] "The What is Graduate Seminar", initiated by F. Hajir. We thank him for inviting us to speak.

2.2. Now this is a very strange collection of notions; who could possibly care about them? Why are modular forms interesting? One answer to these questions lies in (1), which is called the *q-expansion* of f. (Note that it is just the Fourier expansion of f using the periodic functions $e^{2\pi i n\tau}$.) It turns out that the a_k are usually extremely interesting numbers; in modular forms arising in nature they are usually algebraic numbers, or even (good old-fashioned) integers. The typical application is that one has a problem producing a sequence a_k, and (if one is lucky) one can show that these numbers are the coefficients of the q-expansion of a modular form. This implies many nice features of the a_k, and gives an analytic object "packaging" them together.

We can even elaborate a bit. It turns out that the space M_k is actually a *finite* dimensional vector space over $\mathbb{C}$, and in fact its dimension grows rather slowly as a function of k. Quite often one has disparate circumstances giving rise to a collection of modular forms $f_1, \ldots, f_n$, all of the same weight k. Since they all must live in M_k, if n is larger than $\dim_{\mathbb{C}}(M_k)$, we immediately get a relation satisfied by the coefficients of the q-expansions of the f_i. These relations are usually highly nontrivial when considered in the original problem domains giving rise to the f_i.

3. Examples

We only give two examples here. Many more can be found in the references.

3.1. **Eisenstein series.** Let $k \geq 4$, and define

$$G_k(\tau) = \sum_{\substack{(m,n)\in\mathbb{Z}^2 \\ (m,n)\neq(0,0)}} (m\tau + n)^{-k}.$$

It's not hard to check that G_k is a weight k modular form (you'll need to use that the series converges absolutely to verify $G_k(\gamma(\tau)) = G_k(\tau)$). Note that G_k vanishes identically if k is odd. One can compute the q-expansion and can show that

$$E_k(\tau) := \frac{1}{2\zeta(k)} G_k(\tau) = 1 + \gamma_k \sum_{n\geq 1} \sigma_{k-1}(n) q^n,$$

where

- $\zeta(s)$ is the Riemann zeta function (e.g., $\zeta(4) = \pi^4/90$, $\zeta(6) = \pi^6/945, \ldots$),
- γ_k is a certain explicitly computable rational number (e.g., $\gamma_4 = 240$, $\gamma_6 = -504, \ldots$), and
- $\sigma_{k-1}(n)$ is the sum of the $(k-1)$st powers of the divisors of n (e.g., $\sigma_{k-1}(p) = p^{k-1} + 1$ if p is prime).

The modular form E_k is called the *weight k Eisenstein series*. It is not a cuspform. The Eisenstein series are the basic building blocks of *all* modular forms in a certain sense: a basic theorem is that any modular form f can be written as a polynomial in E_4 and E_6. So for example, the space M_8 is one-dimensional and is spanned by E_8.

The modular form E_4^2 also has weight 8 and constant term 1, so it must be equal to E_8. This implies

$$\sigma_7(n) = \sigma_3(n) + 120 \sum_{m=1}^{n-1} \sigma_3(n)\sigma_3(n-m),$$

a curious identity.

3.2. **The discriminant function.** Define $\Delta(q)$ by

$$\Delta(q) = \frac{1}{1728}(E_4^3 - E_6^2). \tag{2}$$

This is a cuspform of weight 12; we divide by 1728 to make Δ have leading term q. The coefficients of the q-expansion of Δ are the values of *Ramanujan's τ-function*:

$$\Delta(q) = \sum_{n\geq 1} \tau(n)q^n.$$

Jacobi proved

$$\Delta(q) = q\prod_{n\geq 1}(1-q^n)^{24}. \tag{3}$$

Using this (or (2)) one can compute some small examples:

$$\begin{aligned}\Delta(q) = q &- 24q^2 + 252q^3 - 1472q^4 + 4830q^5 - 6048q^6 - 16744q^7 \\ &+ 84480q^8 - 113643q^9 - 115920q^{10} + 534612q^{11} - 370944q^{12} \\ &- 577738q^{13} + 401856q^{14} + 1217160q^{15} + 987136q^{16} - \cdots\end{aligned} \tag{4}$$

Note that $\tau(n) \in \mathbb{Z}$ for all n. This is clear from (3), and from (2) after a little thought. You might notice some other facts about τ from (4): for example $\tau(2)\tau(3) = \tau(6)$. If you are *really smart*, like Ramanujan was, you may notice even more properties.[2]

4. Applications of modular forms

The "standard" application of modular forms is to studying the arithmetic of elliptic curves (or more generally, certain types of motives; cf. the TWIGS by Hajir and Weston). This is undoubtedly important and beautiful, and is covered by many references (a good one is [2]). However, here we shall discuss other applications. The first is classical, and the second is quite recent.

[2]Hint: look at $\tau(2)$, $\tau(4)$, $\tau(8)$, and $\tau(16)$.

4.1. **Theta functions.** Let $L \subset \mathbb{R}^n$ be a lattice, that is a discrete subgroup such that the quotient $\mathbb{R}^n/L$ is a torus. We make some assumptions about L:

- We assume that L is *even*, which means $x \cdot x \in 2\mathbb{Z}$ for all $x \in L$ (here the dot is the usual scalar product on $\mathbb{R}^n$).
- We assume that L is *unimodular*. This is equivalent to requiring that the $n \times n$ matrix $l_i \cdot l_j$ is integral and has determinant one, where $l_1, \ldots, l_n$ is any basis for L.

These conditions imply that 8 divides n.

Define a function

$$r_L \colon \mathbb{Z} \longrightarrow \mathbb{Z}$$

by

$$r_L(N) = \#\big\{x \in L \;\big|\; (x \cdot x)/2 = N\big\}.$$

Then we have the following fact: the q-expansion

$$f_L(q) := \sum_{m \geq 0} r_L(m) q^m$$

gives a modular form of weight $n/2$. Since $r_L(0) = 1$, this is not a cuspform.

The first nontrivial case is $n = 8$. It is known that there is only one even unimodular lattice, namely the root lattice of type E_8. We denote this lattice by L_8 so that we don't confuse it with the Eisenstein series E_8. Thus f_{L_8} is a weight 4 modular form with constant term one, which means it's equal to E_4. This gives the remarkable fact that

$$r_{L_8}(N) = 240\sigma_3(N),$$

which is not that easy to establish directly even in the simplest case ($N = 2$).

The next nontrivial case is $n = 16$. There are two even unimodular lattices here, $L = L_8 \oplus L_8$ and a new lattice $L' = L_{16}$. The space M_8 is one-dimensional, spanned by E_8, so we have

$$r_L(N) = r_{L'}(N) = 480\sigma_7(N).$$

This coincidence leads to the following remarkable fact. A famous problem in differential geometry is *Can you hear the shape of a manifold?* Precisely, the question means *Does the spectrum of the Laplacian on a Riemannian manifold uniquely determine it, up to isometry?*. The answer, as observed by Milnor, is *no*. One can take the two flat tori $\mathbb{R}^{16}/L$ and $\mathbb{R}^{16}/L'$. The equality of the functions r_L and $r_{L'}$ means that these two tori have the same spectrum, and they are non-isometric.

4.2. **Ramanujan graphs.** A *graph* G is a collection of vertices and edges; we won't be more precise here and will instead appeal to the reader's intuition and good faith. A graph is *k-regular* if every vertex meets k edges. We will only be concerned with connected k-regular graphs with no loops or multiple edges.

Graphs have many applications in computer science and engineering. For example, one can model a telecommunications network using a graph. Hence it is desirable to have explicit constructions of families of graphs with nice properties.

It turns out that many properties of a graph G are governed by its *spectrum.* To say what this means, let $A = A_G$ be the *adjacency matrix* of G. This is the $0-1$ matrix with A_{ij} equal to 1 if and only if vertex i is connected by an edge to vertex j. Then the spectrum of G is simply the set of eigenvalues of A. It is known that any eigenvalue λ satisfies $|\lambda| \leq k$; those with $|\lambda| = k$ are called *trivial.* We let $\lambda(G)$ be the maximum over the absolute values of the nontrivial eigenvalues of A_G. Then if $\lambda(G)$ is small (i.e. the spectral gap between $\lambda(G)$ and k is large), the graph will be "good." For example, a network design based on such a graph will have efficient "propagation" of transmissions in a certain sense. This leads to the problem *Construct a family of k-regular graphs G_n with the number of vertices of G_n going to ∞ as $n \to \infty$, and such that the spectral gap is as large as possible.*

This problem was solved by Lubotzky, Philips, and Sarnak for $k = p+1$, where p is an odd prime, using modular forms [1,3]. The families of graphs they construct have extremal properties for $\lambda(G)$ and are called *Ramanujan graphs.* The connection with modular forms is that if one wishes to bound $\lambda(G)$, which is an algebraic integer, one should try to make $\lambda(G)$ lie in a ready-made collection of algebraic integers satisfying a nontrivial bound. This latter collection is the set of coefficients of q-expansions of certain modular forms ("certain" means satisfying additional conditions than what we have considered here, and that we cannot explain for lack of time). In fact thanks to a theorem of Deligne we know that for these modular forms of weight w one has

$$|a(p)| \leq 2p^{(w-1)/2}.$$

This was conjectured in 1916 by Ramanujan for the τ-function, which is the origin of the name *Ramanjan graphs*; Deligne's proof uses vast technical machinery that could fill many semesters of TWIGS talks.

It is know known how to explicitly construct families of k-regular Ramanujan graphs for $k = p^\alpha + 1$, where α is a positive integer. The first k not of this form is $k = 7$. Does such a family exist?

References

1. G. Davidoff, P. Sarnak, and A. Valette, *An elementary construction of Ramanujan graphs*, Cambridge University Press, 2003.
2. A. Knapp, *Elliptic curves*, Mathematical Notes, no. 40, Princeton University Press, 1992.
3. P. Sarnak, *Some applications of modular forms*, Cambridge Tracts in Mathematics, vol. 99, Cambridge University Press, Cambridge, 1990.
4. J.-P. Serre, *A course in arithmetic*, GTM, vol. 7, Springer-Verlag, 1973.
5. D. Zagier, *Introduction to modular forms*, Number theory and physics, Springer-Verlag, 1992.

Department of Mathematics and Statistics, University of Massachusetts, Amherst, MA 01003

E-mail address: gunnells@math.umass.edu