Moonshine

Undergraduate Mathematics Society, Columbia University

S. M.-C.

25 March 2015

Contents

Abstract

Moonshine is a sporadic collection of mysterious connections between the algebraic world of finite groups and the number-theoretic world of modular functions. We will first introduce these worlds and discuss their independent interest. Then we will examine the moonshine that connects them, starting with its discovery and building up to some recent directions in the theory.

Good (but technical) modern survey: Moonshine, by Duncan, Griffin, Ono (arXiv:1411.6571)

1 Basics

The word "moonshine" describes a web of connections between finite groups and modular functions. The theory is quite new, beginning in the late '70s, so this connection is still quite mysterious. I'll try to give a sense of what's known at the moment. But first I want to discuss why moonshine is interesting, and to understand this we must understand the two fields that it bridges and their interest to mathematics.

1.1 Representation Theory of Finite Groups

A representation of a finite group is a "geometric" realization of the group as linear maps on a vector space. To be precise, a *representation* of a finite group G is a morphism $\rho : G \to \mathrm{GL}\, V$ to the general linear group of some (finite dimensional) vector space V.

I think representation theory of finite groups is a particularly beautiful part of math; it is one of the fields where everything works as perfectly as you could hope, perhaps even more so. Its usefulness comes from the fact that it can reduce problems in group theory to probems in linear algebra, which of course is a powerful tool.

A few more definitions essential definitions. A *subrepresentation* is a vector subspace which is invariant under the action of the group, i.e. sent into itself by every group element. A representation is *irreducible* if its only subrepresentations are the whole space and the trivial subspace.

The really magical thing about representations of finite groups is that to understand a representation it turns out you don't need to know the matrix each group element is sent to, you only need to know the trace of this matrix. Given a representation, the function that assigns to each element the trace of the corresponding matrix is called the *character* of the representation.

Let's do an example, to make these ideas more concrete and to introduce another concept we'll need. The group S_3 is the symmetry group of a triangle, and acts on itself by left multiplication. Let V be a vector space with a basis given by the elements of S_3. The action of S_3 on itself translates to an action on this vector space, so we get a representation. This construction can be performed for any group, and the resulting representation is called the *regular representation*.

Whenever you see a representation, the first thing you want to do is decompose it into irreducibles, i.e. express it as a direct sum of irreducible representations. The regular representation is special because it has a very nice decomposition in to irreducibles: the number of times each irreducible representation appears is equal to its dimension. It turns out that S_3 has three irreducible representations, which I'll call $1, 1', 2$ (the number indicating the dimension), so the decomposition of the 6-dimensional regular representation is $6 = 1 + 1' + 2 + 2$. It's convenient, especially when talking about moonshine, to refer to representations by their dimension.

The groups that appear most often in moonshine are very special: they are called *sporadic simple groups*. A simple group is a group that has no non-trivial subgroups. Simple groups can be thought of as the atoms of group theory, because any group can be "factored" in a sense into simple groups (though many different groups have the same factorization). One of the largest efforts in mathematics was the classification of finite simple groups, completed over the course of about 50 years and hundreds of journal articles.

The classification goes like this. Every finite simple group is

1. a cyclic group of prime order,
2. an alternating group of degree at least 5,

3. a group of Lie type (including about 16 families; these are mostly matrix groups over finite fields), or
4. one of 26 *others*.

These 26 *others* are the sporadic groups.

The largest sporadic group is the *monster* group $\mathbb{M}$, so named for its truly immense order $\sim 8 \times 10^{53}$. [A fun aside: 20 sporadic groups can be got from the monster by subgroups and quotients, and these are known as the *happy family*; the other six are known as the *pariahs*]. The monster group has 194 irreducible representations, of dimensions

$$\begin{array}{l} 1 \\ 196\,883 \\ 21\,296\,876 \\ 842\,609\,326 \\ \vdots \end{array}$$

1.2 Elliptic Curves and Modular Functions

Now for something completely different. An *elliptic curve* is a smooth complex curve with a group structure. They are interesting because they're super important in number theory, particularly their rational or integer points, because these are solutions to diophantine equations.

Modular functions, which are the things we're really going to be concerned with, are functions on the moduli space of elliptic curves. Let me explain a little more what this means. There is a group $\mathrm{SL}_2\,\mathbb{Z}$ of 2×2 integer matrices with determinant 1 which acts on the upper half of the complex plane $\mathfrak{H}$. This action is nice, so the quotient $\mathrm{SL}_2\,\mathbb{Z}\backslash\mathfrak{H}$ (identifying points in the same orbit) is a complex manifold. It turns out that the points of this manifold correspond naturally with (isomorphism classes of) elliptic curves—I would love to explain why this is, but I haven't got the time.

A modular function is a holomorphic function on this space; or equivalently, a holomorphic function on the upper half-plane invariant under the action of $\mathrm{SL}_2\,\mathbb{Z}$.

There is also a more general notion of modular function, which comes about like so. Other groups, in particular subgroup of $\Gamma \subset \mathrm{SL}_2\,\mathbb{Z}$, also acts on $\mathfrak{H}$, and we again get a complex manifold by taking the quotient $\Gamma\backslash\mathfrak{H}$. For certain subgroups this produces a moduli space of objects of interest, "decorated" elliptic curves. For example, for each natural number N there is a subgroup

$$\Gamma_0(N) = \{\text{matrices upper triangular mod } n\} \subset \mathrm{SL}_2\,\mathbb{Z},$$

and $\Gamma_0(N)\backslash\mathfrak{H}$ parametrizes isomorphism classes of an elliptic curve together with a specified cyclic subgroup of order N. The functions on $\mathfrak{H}$ invariant under a group Γ, i.e. functions on the space $\Gamma\backslash\mathfrak{H}$, are called *modular functions for* Γ.

The geometry of the curve $\Gamma\backslash\mathfrak{H}$ is closely related to the structure of functions on it. In particular, the field of functions on a complex curve is generated (over

$\mathbb{C}$) by a single element precisely when the curve is topologically a sphere (perhaps with some points removed). When a group Γ has this property it is said to be a *genus zero group*, and a generator for the field of modular functions is called a *principal modulus for* Γ. A principal modulus for Γ, regarded as a function $\Gamma\backslash\mathfrak{H} \to \mathbb{C}$, gives an isomorphism between their compactifications $\Gamma\backslash\hat{\mathfrak{H}} \xrightarrow{\sim} \hat{\mathbb{C}}$ (i.e. is a uniformizing function for $\Gamma\backslash\hat{\mathfrak{H}}$).

All of the groups Γ acting on $\mathfrak{H}$ that we're interested in include the transformation $\tau \mapsto \tau + 1$. So a modular function f for Γ, regarded as a function on $\mathfrak{H}$, is periodic: $f(\tau) = f(\tau+1)$. This means that f admits a Fourier expansion; we can write

$$f(\tau) = \sum_{n \geq N} a_n q^n,$$

where $q = e^{2\pi i \tau}$. This is how we'll actually work with modular functions, as functions of q (for $q = e^{2\pi i\tau}$ in the open unit disk).

The standard example of all this is the j-function, which has featured in some previous UMS talks. The j-function is a principal modulus for $\mathrm{SL}_2\,\mathbb{Z}$, and its (normalized) Fourier expansion is

$$j(\tau) = q^{-1} + 0 + 196\,884q + 21\,493\,760q^2 + 864\,299\,970q^3 + \cdots$$

(note that adding or subtracting a constant has no effect on its uniformizing property, so we can set the constant term to 0). As another example, the subgroup $\Gamma_0(2) \subset \mathrm{SL}_2\,\mathbb{Z}$ of matrices upper triangular mod 2 has genus 0, and its normalized principal modulus is

$$q^{-1} + 0 + 276q - 2048q^2 + 11202q^3 + \cdots .$$

2 Moonshine

We're finally ready for the observation that forms the basis for moonshine.

$$\begin{aligned} 1 &= 1 \\ 196\,884 &= 1 + 196\,883 \\ 21\,493\,760 &= 1 + 196\,883 + 21\,296\,876 \\ 864\,299\,970 &= 2 \times 1 + 2 \times 196\,883 + 21\,296\,876 + 842\,609\,326 \\ &\vdots \end{aligned}$$

The numbers on the left are coefficients of the j-function, and the numbers on the right are dimensions of representations of the monster.

Let's stop already and ask: who cares? The point is that this appears too good to be a coincidence. And if it's not a coincidence, then it's happening because of some big mathematical "thing" that we don't understand. And we want to understand it, because it might lead us interesting places … and so it does.

The first step in understanding this is to regard the right hand side as a single representation (just as the left hand side is a single function), by introducing the notion of a grading. A *graded* representation is representation V that can be written as a direct sum, e.g.

$$V = V_{-1} \oplus V_0 \oplus V_1 \oplus V_2 \oplus \cdots ,$$

where each V_i is a finite-dimensional subrepresentation. We'd like to talk about its dimension; the whole representation may be infinite-dimensional, but we can record the *graded dimension*, a sort of generating function for the dimensions of the pieces.

$$\operatorname{gdim} V = \sum_{n \geq -1} \dim V_n \, q^n$$

With this idea, we can rephrase our idea that "j-coefficients should come from representations" as

Conjecture 1. *There is a graded representation* $V^\natural$ *of* $\mathbb{M}$ *such that* $\operatorname{gdim} V^\natural = j$.

Here is another piece of inspiration: the trace of the identity on a vector space is the dimension of the space, so we can rewrite the graded dimension as

$$\operatorname{gdim} V = \sum_{n \geq -1} \operatorname{tr}_{V_n}(e) q^n.$$

Writing it like this, we can replace the identity with any other group element to get a *graded character*.

$$\operatorname{gtr}_V(g) = \sum_{n \geq -1} \operatorname{tr}_{V_n}(g) q^n$$

If the graded character of the identity is the j-function, then perhaps it's worth looking into the graded characters of other monster elements.

Now remember our discussion of principal moduli from earlier: a principal modulus for a genus-zero group is a function that gives an isomorphism with the canonical genus-zero surface, the Riemann sphere. Amazingly, after computing the first few coefficients of these graded characters, it appears that every graded character is the normalized principal modulus for a genus-zero group!

$$\begin{aligned} 1 &= 1 \\ 276 &= 1 + 275 \\ -2\,048 &= 1 + 275 - 2\,324 \\ 11\,202 &= 2 \times 1 + 2 \times 275 - 2\,324 + 12\,974 \\ &\vdots \end{aligned}$$

Conway, the first person to make this observation, described it as one of the most exciting moments of his life:

> after computing several coefficients of these series using information from the character table of $\mathbb{M}$, he went down to the mathematical library and found some of the series in the classical book by Jacobi, with the same coefficients down to the last decimal digit!

This led Conway and Norton to the following conjecture.

Monstrous Moonshine Conjecture. *There is a graded representation $V^\natural$ of $\mathbb{M}$ such that for every element $g \in \mathbb{M}$, the graded character $\mathrm{gtr}_{V^\natural}(g)$ is a normalized principal modulus for some genus zero group Γ_g.*

Let's pause and emphasize this for a minute. This is the main purely mathematical content of moonshine, in all its flavors. Moonshine is not a phenomenon limited to the monster group; there are many examples, and they all consist mainly of this connection: a graded representation of a finite group whose graded characters are special, a priori unrelated, functions.

How can one prove such a conjecture? Here is the first attack. By making guesses for the first few representations (there is only one reasonable guess for a while), we can use the representation theory of the monster to write down the first few terms of each graded character. This way we figure out which principal modulus had ought to be associated to each group element.

Then using representation theory, prove that for the coefficients of these principal moduli to be (virtual) characters it is enough to check that they satisfy finitely many congruence relations. Finally, these finitely many relations may be checked by computer.

However, this is somewhat unsatisfactory because it "just barely" resolves the conjecture; that is, it doesn't make any progress toward understanding a conceptual connection between the monster and principal moduli. A better way would be to construct the representation explicitly, and this was done shortly after.

The construction is rather difficult (and I don't know anything about it), so I won't go into it. However, I will try to convey its importance. Remember that what we want is to understand why there is this connection between the monster and principal moduli. To have any hope of this understanding, the representation we find has to be more than just a representation; it should connect the monster to principal moduli, but it should also connect to other things, which may explain its existence.

The representation constructed does indeed have some extra structure. A mathematician would call it a "vertex algebra", and a physicist would call it a "conformal field theory" (or perhaps its symmetry algebra). In fact this structure is exactly preserved by the action of the monster, i.e. the automorphism group of this structure is $\mathbb{M}$.

3 Physics

4 Questions

What do modular functions tell us about elliptic curves, or anything else?
What do Jacobi forms tell us about things?
What is a vertex algebra to physicists?