A short introduction to Monstrous Moonshine

Valdo Tatitscheff
valdo.tatitscheff@normalesup.org
IRMA, 7 rue René Descartes, 67084 Strasbourg Cedex

January 24, 2019

arXiv:1902.03118v2 [math.NT] 18 Feb 2019

Abstract

This paper is an introduction to the Monstrous Moonshine correspondence aiming at an undergraduate level. We review first the classification of finite simple groups and some properties of the monster $\mathbb{M}$, and then the theory of classical modular functions and modular forms, in order to define Klein's J-invariant. Eventually we turn to the correspondence itself, the historical framework in which it appeared, the ideas that were developped in its proof, and its status nowadays. I'm very thankful to A. Thomas and S. Tornier for their useful feedback.

1 Finite simple groups and the monster

Why finite simple groups ? Let's recall some general definitions and facts about groups.

A *group* G is a set endowed with an associative inner law that has a neutral element $e \in G$, and such that every element of G has an inverse. A *subgroup* H of G is a non-empty subset that is closed under multiplication and inverses. In that case one writes $H \leq G$. Any subgroup H of G defines a partition of G into left and right H-orbits; the left (resp., right) H-orbit of a $g \in G$ is denoted gH (resp. Hg). The set of left (resp., right) orbits is written G/H (resp., $H\backslash G$). A priori, the left and right orbits for a $g \in G$ do not coincide. However, there are as many left H-orbits in G as right H-orbits. This number is called the *index* of H in G.

A subgroup H of G is said to be *normal* (one writes $H \trianglelefteq G$) if the following holds:

$$\forall g \in G,\ gH = Hg.$$

In that case, the sets $G/H \simeq H\backslash G$ can be endowed with a group structure. The *group* G/H is called the *quotient group* of G by H. A group G always have two normal subgroups that are said to be *trivial*: the singleton $\{e\}$, and G itself. They respectively yield the quotient groups $G/\{e\} = G$ and $G/G = \{e\}$.

In the cases where G has a non-trivial normal subgroup H, the knowledge of the latter can be useful to study the structure of G since some of it can be retrieved from the structure of H and G/H, which are two "smaller" groups. We're led to the definition of *simple groups*, as the ones that have no non-trivial normal subgroups, and thus cannot be broken into smaller pieces, in the following sense.

A *composition series* for a group G is a finite sequence

$$\{e\} = G_0 \trianglelefteq G_1 \trianglelefteq \cdots \trianglelefteq G_n = G$$

for $n \geq 1$ an integer, such that for any $1 \leq i \leq n$, one has $G_{i-1} \trianglelefteq G_i$ and such that each *factor* G_i/G_{i-1} is simple. Groups do not always admit composition series ($\mathbb{Z}$ is an easy example), however *every finite group admits a composition series.*

Besides, a group G, even finite, may have more than one composition series. For instance, the cyclic group C_{12} fits whithin:

$$\{e\} \trianglelefteq C_3 \trianglelefteq C_6 \trianglelefteq C_{12}\ ,$$
$$\{e\} \trianglelefteq C_2 \trianglelefteq C_6 \trianglelefteq C_{12}\ ,$$
$$\text{and } \{e\} \trianglelefteq C_2 \trianglelefteq C_4 \trianglelefteq C_{12}\ .$$

Fortunately, the *Jordan-Hölder theorem* states that any two composition series for a finite group G have the same factors, up to permutation. The set of factors for C_{12}, for example, is always $\{C_2, C_2, C_3\}$.

Two non-isomorphic groups may have the same factors though. For instance, and for p a prime, the dihedral group D_p (the group of symmetries of a regular p-gon) and the cyclic group C_{2p} both have $\{C_2, C_p\}$ as factors.

This situation is similar in many ways to the pursuit of building structures with small plastic bricks. Given a single set of bricks of different shapes and different colours, one can built many objects by assembling them together differently. This is the brick-interpretation of the fact that the factors do not characterise a single group.

The Jordan-Hölder Theorem also admits a brick-counterpart, as the fact that even if there are many ways to build the same object, all the possible methods use the same initial set of elementary bricks.

Any such game always has some catalogue that lists the existing elementary bricks, hence extending the metaphor one may wonder if it is possible to do the same with finite simple groups. It turns out that it is possible, and this catalogue is one of the greatest mathematical achievements of the last century.

The classification of finite simple groups The origins of group theory go back to 1832, as Galois introduces *permutation groups* and *normal subgroups*, and proves that the groups A_n (of even permutations on a set of n elements (for $n \geq 5$)) and $\mathrm{PSL}_2(\mathbb{F}_p)$ (for $p \geq 5$) are simple. However, the notion of abstract group as the one we gave above was only formulated by Cayley around 1854. The *Sylow theorems*, that are cornerstones of the theory of finite groups, were published in 1872. Twenty years later, as Hölder proves a theorem constraining the order of non-abelian finite simple groups, he asks for a classification of the latter.

The first half of the 20th century sees the development of a bunch of new concepts in finite group theory. Then the *Feit-Thompson theorem* (announced in 1963) gives deep information on the generic structure of any non-abelian finite simple group, and allows the exploration of new landscapes to study and classify finite simple groups. For the first time in the theory of finite groups, the proof needs much more than a few pages to be written down, and the ideas developed within it revealed themselves to be very useful as such. In 1972, Gorenstein proposed a program to *achieve the classification of finite simple groups*. The classification was completed in 2004 with a publication of a long paper by Aschbacher and Smith (even if in fact, a small oversight elsewhere in the classification was corrected in 2008). Of course, one can find much more detailed accounts of the history of the classification of finite simple groups, see [Sol01] for example.

Theorem 1 (Classification of the finite simple group)**.** *Let G be a finite simple group. Then G is either:*

- *a member of one of 18 infinite families.*
- *one of the 26 sporadic groups.*

Amongst the infinite families, two of them are elementary: the sequences $(C_p)_{p \text{ prime}}$ of cyclic groups of prime order, and $(A_n)_{n\geq 5}$ of alternating permutation groups. The 16 other families are said to be *of Lie type*, and are grouped together according to their structure. For example, there are the *Chevalley groups* that form a set of nine infinite families carrying fancy names such as $(B_n(q))$ (for $n > 1$ and $q = p^\alpha$, for p a primer number), or $E_7(q)$ (again for $q = p^\alpha$, for p a primer number). Four more families are gathered together as the *Steinberg groups*, and there is one family of *Suzuki groups* and two of *Ree groups* (plus the *Tits group*).

The 26 sporadic cases are the only finite simple groups that do not belong to any of the infinite families mentioned above. Some of them are relatively small (in terms of their order, that is, the number of their elements), with the smallest one being the Mathieu group M_{11} that has 7920 elements, but there are also a few mastodons. The next-to-biggest one is called the *baby monster* $\mathbb{B}$ and has around 4×10^{33} elements. It is nevertheless far beyond the biggest one called the *monster* $\mathbb{M}$, with order:

$$|\mathbb{M}| = 2^{46} \cdot 3^{20} \cdot 5^9 \cdot 7^6 \cdot 11^2 \cdot 13^3 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 41 \cdot 47 \cdot 59 \cdot 71 \sim 8 \times 10^{53}.$$

Rise of the monster While studying 3-transposition groups (leading for example to the discovery of the sporadic groups Fi_{22}, Fi_{23} and Fi'_{24}) [Fis71], Fischer provided evidence suggesting the existence of the simple finite group now known as the *baby monster* $\mathbb{B}$. Even if the existence of the latter was only proved in 1977 by Leon and Sims [LS77], Fischer (in 1973) and Griess (in 1976) predicted the *monster group* $\mathbb{M}$ as a simple finite group containing a double cover of $\mathbb{B}$. Just as its baby, the monster was only proven to exist about a decade after it was predicted. However, its conjectural properties were enough to compute its order, as well as others of its features.

Recall that for G a finite group and for $\gamma \in G$, the *conjugacy class* of γ in G is the set

$$\mathcal{C}(\gamma) = \{h \in G | h = g\gamma g^{-1},\ g \in G\}\ .$$

The conjugacy classes partition the group G. The monster, if any, was expected to have 194 conjugacy classes.

A (complex linear finite-dimensional) *representation* of G is a couple (ρ, V) where V is a finite-dimensional complex vector space, and $\rho : G \to \mathrm{GL}(V)$ is a group morphism. The group G is seen as a finite subgroup of the group of invertible $n \times n$ matrices acting on V. The dimension of V is the *dimension of the representation.* Every group has a *trivial representation* where V is a one-dimensional complex vector space and ρ is constant and equal to 1, and also a *regular representation*, whose vector space is of dimension the order of the group, with basis $(e_g)_{g\in G}$, and where ρ is the morphism assigning to each $h \in G$ the matrix $\rho(h)$ defined on the basis according to

$$\rho(h)e_g = e_{hg},\ \forall g \in G\ .$$

Every (finite-dimensional linear complex) representation of a finite group G is isomorphic to a direct sum of special representations called *irreducible representations.* Hence, up to a change of basis in V, ρ is valued in block-diagonal matrices whose sizes are dimensions of irreducible representations. There are as many irreducible representations of a group G as conjugacy classes in G, and any piece of information about those irreducible representations, such as their dimension, is a big step forward in the understanding of G. See [Ser77] or [FH04] for a general introduction to representations.

Going back to the monster, under the assumption that the smallest non-trivial irreducible representation is 196883-dimensional (a numbered conjectured thanks to finite groups theoretical considerations by Conway and Norton), the 194 irreducible dimensions were determined in 1978 by Fischer, Livingstone and Thorne through clever computer calculations. This 194-uplet is encoded in the Online Encyclopaedia of Integer Sequences (OEIS) under the number $A001379$. The first few terms are:

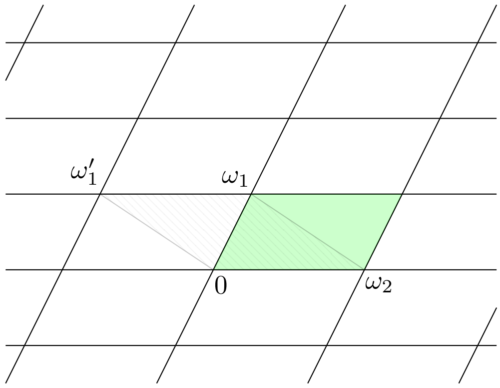
$$(r_n)_{n=1..194} = (1, 196883, 21296876, 842609326, 18538750076, ...)$$

2 Complex tori, rank-2 lattices and modularity

Isomorphism classes of complex tori A (full) *lattice* Λ in $\mathbb{C}$ is a subgroup of $\mathbb{C}$ isomorphic to $\mathbb{Z}^2$, and such that the real vector space that it generates is 2-dimensional (hence is the whole complex plane). Equivalently, there exists $\omega_1, \omega_2 \in \mathbb{C}^\times$ such that $\omega_1/\omega_2 \notin \mathbb{R}$ and such that

$$\Lambda = \mathbb{Z} \cdot \omega_1 + \mathbb{Z} \cdot \omega_2 = \{a\omega_1 + b\omega_2 | a, b \in \mathbb{Z}\} \subset \mathbb{C}.$$

Let $\Lambda(\omega_1, \omega_2)$ be the lattice generated by ω_1 and ω_2.



A (compact) *complex torus* is a *quotient* $\mathbb{C}/\Lambda$. Topologically indeed, $\mathbb{C}/\Lambda(\omega_1, \omega_2)$ is a torus, obtained as one glues together the opposite sides of the parallelogram with vertices $0, \omega_1$ and ω_2, paying attention to preserve the orientation of each side. The gluing of the first couple of edges yields a cylinder, and then the gluing of the second, an objet that typically has the shape of the surface of a donut, that is, a *torus*.

There is a *single topological torus*, meaning that any torus can be mapped to a reference one by continuous deformations that do not tear the surface up. These deformations are called *homeomorphisms* (the ancien greek translation of *transformations that preserve the shape*). There is also a notion of *complex isomorphism* (also called *conformal isomorphism*), that is more constraining than homeomorphism, since that on top of having not to tear the surface up, they also have to *preserve the angles* at each point, as the surface is deformed. Subsequently, there might be more than one complex torus (that are necessarily homeomorphic, but still not conformally equivalent).

One can show that two complex tori $\mathbb{C}/\Lambda_1$ and $\mathbb{C}/\Lambda_2$ are conformally equivalent if and only if there exists an $\alpha \in \mathbb{C}^\times$ such that $\Lambda_2 = \alpha\Lambda_1$. One can assume (possibly after multiplying by ω_2^{-1}) that the lattice we consider is of the form $\Lambda_\tau = \Lambda(\tau, 1)$ where $\tau = \omega_1/\omega_2$. Moreover (possibly after exchanging τ and 1 and then multiplying by τ^{-1}), one can suppose that τ lives in the complex upper-half plane. The latter is called the *Poincaré plane* and denoted $\mathbb{H}$.

To sum up, we have defined a complex torus as an equivalence class of lattices in the complex plane, the equivalence relation being the one induced by complex dilatation with non-zero factors. In each equivalence class there is a lattice of the form Λ_τ for some $\tau \in \mathbb{H}$.

However, it could be that $\Lambda_\tau = \Lambda_{\tau'}$ for two distinct $\tau, \tau' \in \mathbb{H}$. As in the figure above, the couples (ω_1, ω_2) and (ω_1', ω_2) generate the same lattice, it is reasonable not to think that the $\tau \in \mathbb{H}$ characterise the equivalence classes.

Consider a lattice Λ generated by the two couples (ω_1, ω_2) and (Ω_1, Ω_2). Then there are $A_i, B_i, a_i, b_i \in \mathbb{Z}$, for $i \in \{1, 2\}$, such that:

$$\Omega_1 = A_1\omega_1 + B_1\omega_2 \text{ and } \Omega_2 = A_2\omega_1 + B_2\omega_2, \text{ as well as}$$

$$\omega_1 = a_1\Omega_1 + b_1\Omega_2 \text{ and } \omega_2 = a_2\Omega_1 + b_2\Omega_2.$$

This leads to:

$$A_1a_1 + B_1a_2 = A_2b_1 + B_2b_2 = 1, \text{ and}$$
$$A_1b_1 + B_1b_2 = A_2a_1 + B_2b_1 = 0.$$

Hence the quadruples (A_1, B_1, A_2, B_2) and (a_1, b_1, a_2, b_2) form matrices with integer coefficients that are mutual inverses (and that implies that their determinant is ± 1). Equivalently, the transition matrices between the *bases* of a lattice form the group $\mathrm{SL}_2(\mathbb{Z})$.

Any basis of a lattice Λ_τ with $\tau \in \mathbb{H}$ has the form $(a\tau + b, c\tau + d)$, for some quadruple $(a, b, c, d) \in \mathbb{Z}^4$ that satisfies $ad - bc = 1$. Now:

$$\mathbb{C}/\Lambda_\tau \simeq \mathbb{C}/\Lambda(\tau, 1) \simeq \mathbb{C}/\Lambda(a\tau + b, c\tau + d) \simeq \mathbb{C}/\Lambda_{\frac{a\tau+b}{c\tau+d}}.$$

Two points $\tau, \tau' \in \mathbb{H}$ correspond to the same complex torus if and only if there is $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ such that

$$M \cdot \tau = \frac{a\tau + b}{c\tau + d} = \tau',$$

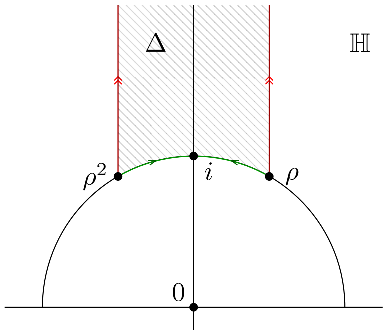
and hence the isomorphism classes of complex tori are in bijection with the orbits of the action of $\mathrm{SL}_2(\mathbb{Z})$ on $\mathbb{H}$.

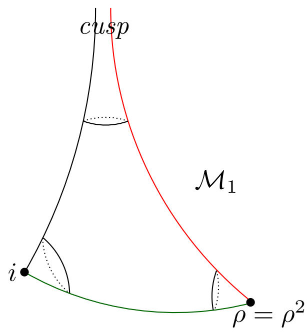
Actually, one can observe that $-\mathrm{Id} \in \mathrm{SL}_2(\mathbb{Z})$ acts trivially on $\mathbb{H}$; subsequently one rather considers the *modular group* $\mathrm{PSL}_2(\mathbb{Z})$ obtained by identifying each matrix with its opposite in $\mathrm{SL}_2(\mathbb{Z})$.

The moduli space $\mathcal{M}_1$ We have seen the natural action of the modular group on $\mathbb{H}$ defined by:

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

This action is - by chance - quite nicely-behaved. It is indeed possible to choose a *fundamental domain* in $\mathbb{H}$, that is, a closed subset of $\mathbb{H}$ that is connected and simply-connected (i.e it has only one component, and no hole), and that contains exactly one point of each orbit for this action of $\mathrm{PSL}_2(\mathbb{Z})$ (except maybe on its boundary). The iterates of this domain under $\mathrm{PSL}_2(\mathbb{Z})$ *tesselate* the upper-half plane $\mathbb{H}$. The fundamental domain Δ given in the next figure is a widespread conventional choice.





$$(\tau \in \Delta) \;\Leftrightarrow\; |\tau| \geq 1 \text{ and } -\frac{1}{2} \leq \mathrm{Re}(\tau) \leq \frac{1}{2}$$

The set of orbits $\mathcal{M}_1 = \mathbb{H}/\mathrm{PSL}_2(\mathbb{Z})$ has a natural topology (shape), that one gets by gluing the two vertical sides of Δ together (both going up), as well as the two arcs (ρ^2, i) and (ρ, i) (in that order, meaning that $\rho = e^{2\pi i/3}$ is identified with ρ^2). The resulting space has a *cusp* going to infinity, as well as two corners, but if one adds a point at the cusp so the surface closes there, and smoothens the latter at the folding points, it is homeomorphic to a sphere. This space $\mathcal{M}_1$ is called the *moduli space of complex tori*, as its points are in bijection with isomorphism classes of complex tori. It is a quite interesting fact that the set of isomorphism classes of complex tori *has a shape* (and moreover, $\mathcal{M}_1$ even has a *complex structure* induced by the upper-half plane $\mathbb{H}$).

Modular functions and modular forms One may wonder if there are any complex functions on $\mathbb{H}$ that are invariant under the action of $\mathrm{PSL}_2(\mathbb{Z})$, that is, functions f that satisfy:

$$f(\tau) = f(M \cdot \tau) = f(\frac{a\tau + b}{c\tau + d})$$

for any $M = \mathrm{Mat}(a, b, c, d) \in \mathrm{PSL}_2(\mathbb{Z})$. Since $\mathrm{PSL}_2(\mathbb{Z})$ is *generated* by the two matrices:

$$T = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \text{ and } S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix},$$

(meaning that any element in $\mathrm{PSL}_2(\mathbb{Z})$ can be decomposed as a product of S's and positive powers of T), the conditions on f for it to be invariant under $\mathrm{PSL}_2(\mathbb{Z})$ become:

$$f(\tau + 1) = f(\tau) \text{ and } f(\frac{-1}{\tau}) = f(\tau).$$

Such a (meromorphic) function (in $\mathbb{H}$ and at the cusp) is called a *modular function.*

In practise, it is quite difficult to brute-force the study of modular functions. The salvation here comes from the release of some of the hypotheses that one demands for the modular functions.

A *modular form* f of weight $2k$ (for $k \in \mathbb{N}$) is a (holomorphic) function (in $\mathbb{H}$ and at the cusp) that satisfies:

$$f(\tau) = (c\tau + d)^{2k} f(\frac{a\tau + b}{c\tau + d})$$

for any $M = \mathrm{Mat}(a, b, c, d) \in \mathrm{PSL}_2(\mathbb{Z})$. The set M_k of modular forms of weight $2k$ obviously has the structure of a complex vector space. Moreover, the product of two modular forms of respective weights $2k$ and $2l$ is a modular form of weight $2(k + l)$, thus

$$M = \bigoplus_{k \geq 0} M_k$$

is a ring with unit.

It is quite easy to construct nice and non-trivial examples of modular forms. For example, the lattices Λ_τ induce series that can be shown to be modular forms. For example, let $k \in \mathbb{N}_{\geq 2}$. The k-th Eisenstein G_{2k} series defined as follows is a well-defined modular form of weight $2k$:

$$G_{2k}(\tau) = \sum_{\omega \in \Lambda_\tau \setminus \{0\}} \frac{1}{\omega^{2k}}.$$

The general theory of modular forms yields the nice result that:

$$M = \mathbb{C}[G_4, G_6].$$

Now, one can build modular functions from modular forms. The easiest non-trivial choice (since the lcd of 4 and 6 is 12) is to look at the vector space M_{12} which is the M_k with the smallest k whose dimension is strictly bigger than 1. Klein's J-invariant is defined as:

$$J(\tau) = 1728 \frac{g_2(\tau)^3}{g_2(\tau)^3 - 27 g_3(\tau)^2},$$

where $g_2 = 60G_4$ and $g_3 = 140G_6$. This J is a modular function, and interestingly *any modular function is a rational fraction of J*. Equivalently, the ring (field) of modular functions is $\mathbb{C}(J)$.

q-expansions Both modular forms and functions have to satisfy $f(\tau+1) = f(\tau)$. This periodicity condition allows a decomposition in Fourier series, in terms of $q = e^{2\pi i \tau}$. The transformation $\tau \mapsto q(\tau)$ maps $\mathbb{H}$ to the punctured unit disk, and of course any function f defined as a series of q is invariant under $\tau \mapsto \tau + 1$.

Quite miraculously, the coefficients of the Fourier series of some important modular objects (functions or forms) are integers. For example (and for $k \in \mathbb{N}_{\geq 2}$):

$$G_{2k}(\tau) = 2\zeta(2k) + 2\frac{(2\pi i)^{2k}}{(2k-1)!} \sum_{n=1}^{\infty} \sigma_{2k-1}(n) q^n$$

where $\sigma_k(n) = \sum_{d|n} d^k$. The coefficients of the q-expansion of J are also integers, but it is harder to understand the meaning of those. Do they count something ? Those coefficients are anyways pretty interesting because of their very definition, and their (infinite) sequence in referred to as A000521 in the OEIS. The first few terms of the latter are:

$$J(\tau) = \sum_{n=-1}^{\infty} c(n) q^n = \frac{1}{q} + 744 + 196884q + 21493760q^2 + 864299970q^3 + 20245856256q^4 + ...$$

In the sequel, we will write $\tilde{J}$ for the *normalised J-function* $J - 744$.

For a general introduction to the theory of modular functions and modular forms, see [Mil97] for example.

3 Monstrous Moonshine

First observations and Thompson's conjecture Even if the J-invariant (known since the 19th century) and the monster group (intuited at the beginning of the 70's) do not seem to be related at all, these two objects are intimately tied together. The correspondence between them has been called *Monstrous Moonshine.* In 1978, John McKay noted that:

$$196884 = 196883 + 1$$

Keeping the notations of the first two sections, this equality has to be understood as $c(2) = r_1 + r_2$. The size of the numbers involved makes this equality quite thrilling, but of course it could be a mere coincidence, just as most of the people originally thought. A few months later though, Thompson came out with the following new observations [Tho79a]:

$$\begin{aligned} c(3) &= r_1 + r_2 + r_3, \\ c(4) &= 2r_1 + 2r_2 + r_3 + r_4, \\ c(5) &= 3r_1 + 3r_2 + r_3 + 2r_4 + r_5, \\ c(6) &= 4r_1 + 5r_2 + 3r_3 + 2r_4 + r_5 + r_6 + r_7, \end{aligned}$$

and he subsequently proposed the following conjecture:

Conjecture 1 (Thompson's conjecture)**.** *There is a (somehow) natural infinite-dimensional graded representation of the monster group ($\rho_\natural, V^\natural = \bigoplus_{i \geq -1} V_i^\natural$), such that each graded part $V_i^\natural$ is finite dimensional, and such that:*

$$\tilde{J}(\tau) = \sum_{i \geq -1} \dim(V_i^\natural) q^i.$$

Equivalently, the elements of $\mathbb{M}$ act naturally as (infinite) matrices on an infinite-dimensional graded vector space (these matrices are block-diagonal with every block of finite size), and the graded-dimension of $V^\natural$ is the q-expansion of the normalised J-function.

Conway-Norton's Monstrous Moonshine Let us briefly return to representations of finite groups. We have defined a representation of a finite group G as a pair (ρ, V) where V is a finite-dimensional vector space and ρ and group morphism from G to $\mathrm{GL}(V)$. For any such representation, the *character of* (ρ, V) is:

$$\begin{array}{rcl} \chi_{(\rho,V)} : G & \to & \mathbb{C} \\ g & \mapsto & \mathrm{Tr}(\rho(g)) \end{array} .$$

By cyclicality of the trace (and since ρ is a morphism of groups), $\chi_{(\rho,V)}$ is constant on each conjugacy class. Functions $G \to \mathbb{C}$ with that property are called *class functions*.

If $\mathrm{CC}(G)$ denotes the set of conjugacy classes in G, the set of class functions is $\mathbb{C}^{\mathrm{CC}(G)}$. The following result is a cornerstone of the theory of characters of finite groups (again, see [Ser77] or [FH04] for a more more precise introduction to that topic).

Theorem 2. *1. The characteristic functions of the conjugacy classes of G form an orthogonal basis of* $\mathbb{C}^{\mathrm{CC}(G)}$.

2. The set of class functions $\mathbb{C}^{\mathrm{CC}(G)}$ *of a finite group G is endowed with a natural hermitian product, and the characters of the irreducible representations form an orthonormal basis of* $\mathbb{C}^{\mathrm{CC}(G)}$.

The transition matrix from the basis of characteristic functions to the basis of irreducible characters is called the *character table* of G. Computing the character table of a given finite group G is the holy grail of the character theory of G.

Since the dimension of a representation is nothing else but the trace of the identity element $\rho(e)$, Thompson suggested to study the series:

$$T_{[g]} = \sum_{i \geq -1} \mathrm{Tr}(\rho_{\mathbb{M}}(g)_{|V_i^\natural}) q^i = \frac{1}{q} + \sum_{n=0}^{\infty} H_n([g]) q^n,$$

that now carry the name of *McKay-Thompson series.* There is one such series for each conjugacy class $[g]$ of $\mathbb{M}$. In the formula above, $g \in \mathbb{M}$ is any representative of $[g]$. The class-functions H_n were called the *Head characters* of $\mathbb{M}$, even if at that point nobody knew for sure that they really were characters of representations of $\mathbb{M}$.

We already mentioned the 1978 calculation of Fischer, Livingstone and Thorne. In fact, they did not only compute the dimensions of the irreducible representations of $\mathbb{M}$, but obtained these as a corollary of the knowledge of the whole character table of the monster, the main aim of their work. Using this very deep piece of information, Conway and Norton extended in 1979 Thompson's conjecture [CN79] to the following.

Conjecture 2 (Conway-Norton's Monstrous Moonshine)**.** *There is a (somehow) natural infinite-dimensional graded representation* $(\rho_{\mathbb{M}}, V^\natural = \bigoplus V_i^\natural)$ *of the monster group, with finite dimensional graded parts* $V_i^\natural$*, and such that for each conjugacy class* $[g]$ *of the monster, the series* $T_{[g]}$ *is the q-expansion of the normalised Hauptmodul of some subgroup* $\Gamma_{[g]}$ *of* $\mathrm{PSL}_2(\mathbb{R})$ *commensurable with* $\mathrm{PSL}_2(\mathbb{Z})$.

This requires some explanations. First, two subgroups G and H of $\mathrm{PSL}_2(\mathbb{R})$ are said to be *commensurable* if their intersection has finite index in both G and H. When $[g] = \{e\}$, the group $\Gamma_{\{e\}}$ is of course $\mathrm{PSL}_2(\mathbb{Z})$, and the functions on the upper-half plane that are $\mathrm{PSL}_2(\mathbb{Z})$-invariant (the modular functions) can all be expressed as rational functions of J (or, equivalently, $\tilde{J}$). This property of $\tilde{J}$, together with the fact that it is normalised, makes it the *normalised Hauptmodul* for $\mathrm{PSL}_2(\mathbb{Z})$. Some subgroups of $\mathrm{PSL}_2(\mathbb{R})$ commensurable with $\mathrm{PSL}_2(\mathbb{Z})$ also have normalised Hauptmoduln defined in the same way: every modular function for that group is a rational function of the Hauptmodul. The groups for which this is the case are said to be of *genus zero*.

Conway and Norton not only proposed this conjecture, but also computed a huge amount of evidence for it. First, using Thompson's work, as well as the character table of $\mathbb{M}$, they could determine empirically all the groups that would be the ones appearing in the correspondence (if their conjecture was valid). For example, to the class $2A$ of the group $\mathbb{M}$ (2 means that it is a conjugacy class of elements of order 2 and A distinguishes such classes; there is for instance another class of involutions judiciously named $2B$), the data produced by Thompson was enough so they could guess that it corresponds to a group $\Gamma_0(2)$ called the *Hecke congruence subgroup of level* 2 of $\mathrm{PSL}_2(\mathbb{Z})$.

They also showed that instead of the 194 expected McKay-Thompson series, there are only 172 different ones (since for any $g \in \mathbb{M}$, the classes $[g]$ and $[g^{-1}]$ share the same series). Moreover, linear relations between the series even lowers (down to 163) the dimension of the space that they generate.

Besides, they computed $\mathrm{Tr}(\rho_{\mathbb{M}}(g)_{|V_i^\natural})$ for all $g \in \mathbb{M}$ and $i \leq 10$, and verified that the functions

$$\begin{array}{rcl} G & \to & \mathbb{C} \\ g & \mapsto & \mathrm{Tr}(\rho_{\mathbb{M}}(g)_{|V_i^\natural}) \end{array}$$

are indeed characters of some representations of $\mathbb{M}$. Their paper [CN79] quickly became the main reference in that topic. The term moonshine also first appeared in it, meaning "crazy idea", as the first feeling one more or less normally has when thinking to such a possible link between the monster group and the J-invariant.

String theory, vertex operators algebras and the moonshine Even if the monster has been first conjectured in the first half of the 70's, its uniqueness was only proved in 1979 by Thompson [Tho79b] (assuming that $\mathbb{M}$ (if any) would have a representation of dimension 196883, as conjectured a while earlier by Conway and Norton). Moreover, one has to wait until 1982 for Griess to prove its existence [Gri82], by explicitly constructing it as the automorphism group of a 196884-dimensional commutative, non-associative algebra now called the *Griess algebra*.

In 1979, Atkin, Fong and Smith performed a huge computer calculation [Smi85] to show that the class functions H_n of $\mathbb{M}$ are really characters of the monster group. Using powerful results of finite-group theory such as *Brauer's characterisation of characters*, they could reduce the infinite number of verifications the conjecture demands, to a finite one. It was still lengthy and tedious though, especially on the IBM 370/158 computer they were using.

Around that time, Frenkel, Lepowsky and Meurman were developing another approach of $\mathbb{M}$ using what had been called vertex operators representations of affine Lie algebras [FLM85]. This method strongly relies on the existence of very symmetrical *even unimodular lattices* $L_{E_8} \simeq \mathbb{Z}^8$ and $\Lambda \simeq \mathbb{Z}^{24}$, that are respectively the *root lattice of* E_8 and the *Leech lattice* (the latter was also quite central in Griess' construction of the monster). Both lattices are related to the q-expansion of J, and through them one can construct a particular *vertex operator algebra* (an algebra whose multiplication depends on a parameter instead of being defined in a single way, together with additional axioms) whose automorphism group is exactly $\mathbb{M}$. This *monster vertex algebra* is graded and the graded-dimension is exactly the q-expansions of $\tilde{J}$. In particular, it contains a version of the Griess algebra as its second graded part. Hence the module whose existence had been confirmed by Atkin, Fong and Smith was now constructed explicitly. See [FLM88] for more details on vertex operator algebras, and in particular the introduction that gives a very nice summary of the historical framework, as well as of the ideas.

Later on, it was realised that these vertex algebras play a very central role in a specific field of theoretical physics, called *string theory*. This theory first appeared (under the name *dual resonance theory*) as an attempt to explain strong interactions (that bind the nucleons of an atom's nucleus together, and explain the behaviour of some particles called *hadrons*), before being demoted to the benefit of another theory called *quantum chromodynamics*.

Despite this discomfiture, Yoneda, Scherk and Schwarz realised around 1973-1974 that string theory could be an interesting approach to quantum gravity, and the theoretical physics community regained interest in it. In string theory, the *vibration modes* of a tiny string (either closed or open) embedded in a *target space* (interpreted as the space-time) are the particles of the theory. There are different types of strings theories, depending on which kind of strings one uses (either closed strings only, or open and closed strings together) or which kind of geometries are allowed, as strings move through the target-space (with or without an orientability constraint). However, the theory is not necessarily mathematically consistent, and for it to be so, some constraints (that typically depend on the type of the theory) have to be fulfilled. An easy way to satisfy some of these is to fix the dimension of the target space. That having been done, the shape of the target space still impacts the way strings vibrate in it, and *vertex operators* as well as *chiral algebras* (the physics counterpart of vertex operator algebras) encode the dependence of the vibration modes on the geometry of the target-space. The construction of Frenkel, Lepowsky and Meurman can *a posteriori* be understood as the vertex operator algebra of a *bosonic string theory* with target space a specific $\mathbb{Z}_2$*-orbifold associated with the Leech lattice*. Once again, the introduction of [FLM88] gives a nice historical account of the early years of string theory, and explains some of the links between string theory and the Monstrous Moonshine. The first chapter of the classical textbook [GSW87] is also a very nice and accessible introduction to the ideas of string theory.

Borcherd's proof of Conway and Norton's conjecture Starting form the vertex operator algebra that Frenkel, Lepowsky and Meurman had constructed, Borcherds used the 1972 Goddard-Thorn *no-ghost theorem* of string theory to construct an infinite dimensional Lie algebra. He called it the *monster Lie algebra* (see [Bor86]). Borcherds built a general theory of the mathematical objects of that type (called *generalised Kac-Moody algebras*) and derived *denominator identities* and *twisted denominator identities* for those, mimicking the more classical case of Kac-Moody algebras. In particular, these identities applied to the monster Lie algebra are related to the coefficients of the McKay-Thompson series. At that point, the proof of the Monstrous Moonshine could be completed in a finite number of verifications, that Conway and Norton had already partly done. Hence Borcherds achieved the proof of the monstrous moonshine correspondence in 1992 [Bor92].

Moonshine nowadays

Borcherds' proof of Conway and Norton's original conjecture has shed intense light on the structure of $\mathbb{M}$ and also on the modular side of the Monstrous Moonshine. For instance, the *Koike-Norton-Zagier formula*:

$$p^{-1} \prod_{m,n\in\mathbb{Z},\ m>0} (1-p^m q^n)^{c(mn)} = J(\sigma) - J(\tau)$$

arose as the denominator identity for the monster Lie algebra and taught relationships between the coefficients of J that were at that time still unknown. As before $q = e^{2\pi i\tau}$ (and similarly $p = e^{2\pi i\sigma}$) and the $c(n)$ are the coefficients of the q-expansion of J. There are of course other consequences of the moonshine, see [DGO15a] for some of those.

The Monster also led to the discovery of two new sporadic groups, as quotients of some of its subgroups. In fact, 20 sporadic groups (out of the 26) are *subquotients* of $\mathbb{M}$. Robert Griess dubbed the set they form *the happy family*, and the six remaining ones the *pariah groups* [Gri82]. The Monstrous Moonshine induces moonshines for all the groups that are subquotients of the monster, and this observation led to a set of conjectures gathered in 1987 under the name of *generalised moonshine* by Norton. The proof of those conjectures has been completed by Carnahan in 2016. The question whether the pariah groups also admit some kind of moonshine was already asked in [CN79]. It turned out recently that the pariah O'Nan $O'N$ admits moonshine-like properties linking it to arithmetic [DMO18]. The pariah J_1 (Janko 1), as a subgroup of $O'N$, admits subsequently the same type of correspondences.

Moreover, new types of "moonshines" have been discovered. The most famous is probably the *umbral moonshine* correspondence, conjectured in 2010 [CDH12] as a mysterious representation of the Mathieu sporadic group M_{24} in terms of elliptic geni of $K3$ surfaces, and proved in 2015 [DGO15b].

Sporadic groups, and in particular the monster, are without doubt very interesting mathematical objects. There are still a lot of unexplained exciting coincidences that relate them to other fields in mathematics. For example, another observation of McKay's (that became famous as *McKay's E_8 observation*) relates the order of the elements one may obtain by multiplying together two elements of the class $2A$ in the monster, and the Dynkin diagram of the affine algebra $\hat{E}_8$. There are other hints letting one hope for a link between the three biggest sporadic groups ($\mathbb{M}$, $\mathbb{B}$ and Fi'_{24}) and the three biggest exceptional finite-dimensional semi-simple Lie algebras (E_8,E_7 and E_6) [HM15]. However, these hints still look like coincidences... just as McKay's original observation firstly!

Exceptional objects in mathematics have always been fascinating, because of their mere existence, that is already incredible enough to be amazed. Their study surely is an amazing fountain of knowledge, and it is very likely that we are not done being surprised.

References

[Bor86] R.E. Borcherds. Vertex algebras, Kac-Moody algebras and the Monster. *Proc. Natl. Acad. Sci. USA*, 83:3068–3017, 1986.

[Bor92] R.E. Borcherds. Monstrous Moonshine and Monstrous Lie Superalgebras. *Invent. Math.*, 109:405–444, 1992.

[CDH12] M.C.N. Cheng, J.F.R. Duncan, and J.A. Harvey. Umbral Moonshine. 2012.

[CN79] J.H. Conway and S.P. Norton. Monstrous Moonshine. *Bull. Lond. Math. Soc.*, 11:308–339, 1979.

[DGO15a] J.F.R. Duncan, M.J. Griffin, and K. Ono. Moonshine. *Resea. Math. Sci.*, 2, 2015.

[DGO15b] J.F.R. Duncan, M.J. Griffin, and K. Ono. Proof of the Umbral Moonshine Conjecture. *Resea. Math. Sci.*, 2, 2015.

[DMO18] J.F.R. Duncan, M.H. Mertens, and K. Ono. O'Nan Moonshine and Arithmetic. recommended for publication in Am. Jour. of Math., 2018.

[FH04] W. Fulton and J. Harris. *Representation Theory*. Graduate Texts in Mathematics. Springer-Verlag, 2004.

[Fis71] B. Fischer. Finite groups generated by 3-transpositions. *Inventiones mathematicae*, 13(3):232–246, 1971.

[FLM85] I. Frenkel, J. Lepowsky, and A. Meurman. An E_8 approach to F_1. In *Finite Groups - coming of Age*, volume 45, pages 99–120. J. McKay, 1985.

[FLM88] I. Frenkel, J. Lepowsky, and A. Meurman. *Vertex Operator Algebras and the Monster*. Pure and applied mathematics. Academic Press, Inc., 1988.

[Gri82] R.L. Griess. The Friendly Giant. *Inventiones Mathematicae*, 69(1):1–102, 1982.

[GSW87] M.B. Green, J. H. Schwarz, and E. Witten. *Superstring theory: Volume 1, Introduction*. Cambridge Monographs on Mathematical Physics. Cambridge University Press, 1987.

[HM15] Y.H He and J. McKay. Sporadic and Exceptional. 2015.

[LS77] J.S. Leon and C.C. Sims. The existence and uniqueness of a simple group generated by {3,4}-transpositions. *Bull. Amer. Math. Soc.*, 83(5):1039–1040, 1977.

[Mil97] J.S. Milne. Modular Functions and Modular Forms. Lecture notes, 1997.

[Ser77] J.P. Serre. *Linear Representations of Finite Groups*. Graduate Texts in Mathematics. Springer-Verlag, 1977.

[Smi85] S.D. Smith. On the Head Characters of the Monster Simple Group. In *Finite Groups - coming of Age*, volume 45, pages 303–313. J. McKay, 1985.

[Sol01] R. Solomon. A Brief History of the Classification of the Finite Simple Groups. *Bull. Amer. Math. Soc.*, 38(3):315–352, 2001.

[Tho79a] J.G. Thompson. Some Numerology between the Fischer-Griess Monster and the Elliptic Modular Function. *Bull. Lond. Math. Soc.*, 11:352–353, 1979.

[Tho79b] J.G. Thompson. Uniqueness of the Fischer-Griess Monster. *Bull. Lond. Math. Soc.*, 11:340–346, 1979.