Canad. Math. Bull. Vol. **45** (4), 2002 pp. 606–622

Postcards from the Edge, or Snapshots of the Theory of Generalised Moonshine

I dedicate this paper to a man who throughout his career has exemplified the power of conceptual thought in math: Bob Moody.

Terry Gannon

Abstract. We begin by reviewing Monstrous Moonshine. The impact of Moonshine on algebra has been profound, but so far it has had little to teach number theory. We introduce (using 'postcards') a much larger context in which Monstrous Moonshine naturally sits. This context suggests Moonshine should indeed have consequences for number theory. We provide some humble examples of this: new generalisations of Gauss sums and quadratic reciprocity.

In 1978, John McKay made an intriguing observation: $196\,884 \approx 196\,883$. *Monstrous Moonshine* is the collection of questions (and a few answers) inspired by this observation. In this paper we provide a few snapshots of what we call the underlying theory, showing some of the range. The primary originality of this paper is Figure 1 and all that it entails. We also give proofs and generalisations of Gauss sums and quadratic reciprocity at the end of the paper. But first let's begin with the familiar.

Definition 1 A *modular function* f (for $\mathrm{SL}_2(\mathbb{Z})$) is a meromorphic function $f\colon \overline{\mathbb{H}} \to \mathbb{C}$, obeying the symmetry $f(A.\tau) = f(\tau)$ for all $\tau \in \overline{\mathbb{H}}$ and $A \in \mathrm{SL}_2(\mathbb{Z})$.

Of course, $\mathbb{H}$ denotes the upper half-plane of $\mathbb{C}$, and the modular group $\mathrm{SL}_2(\mathbb{Z})$ acts on $\overline{\mathbb{H}} \stackrel{\text{def}}{=} \mathbb{H} \cup \mathbb{Q} \cup \{\infty\}$ by Möbius transformations. We can construct some modular functions as follows. Define the *(classical) Eisenstein series* by

$$G_k(\tau) = \sum_{\substack{m,n\in\mathbb{Z}\\(m,n)\neq(0,0)}} (m\tau + n)^{-k}. \tag{1}$$

For even $k > 2$ it converges absolutely, and so defines a (nonzero) function holomorphic throughout $\overline{\mathbb{H}}$. An easy calculation shows

$$G_k\left(\frac{a\tau + b}{c\tau + d}\right) = (c\tau + d)^k G_k(\tau) \quad \forall \begin{pmatrix} a & b\\ c & d\end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \tag{2}$$

and all τ. This is because the sum in (1) is really over all nonzero vectors x in the two-dimensional lattice $\mathbb{Z}\tau + \mathbb{Z} \subset \mathbb{C}$, and $\mathrm{SL}_2(\mathbb{Z})$ parametrises certain changes-of-basis $\{\tau, 1\} \mapsto \{w, z\}$ of $\mathbb{Z}\tau + \mathbb{Z}$. This transformation law (2) means that various

Received by the editors November 16, 2001.
AMS subject classification: Primary: 11F22; secondary: 17B67, 81T40.

homogeneous rational functions of these G_k will be modular functions—for example $G_8(\tau)/G_4(\tau)^2$ (which turns out to be constant) and $G_4(\tau)^3/G_6(\tau)^2$ (which doesn't). We'll see shortly that all modular functions arise in this way.

Why are modular functions interesting? At least in part, this has to do with the omnipresence of two-dimensional lattices. For instance, a modular function lives on the moduli space of conformally equivalent tori, and equivalently the moduli space of birationally equivalent elliptic curves. Elliptic curves are special because they're the only complex projective curves which have an algebraic group structure. In any case, modular functions and their various generalisations hold a central position in both classical and modern number theory. For an enjoyable account of the classical theory, see [24].

Can we characterise all modular functions? The key idea is to look directly at the moduli space $M = \mathrm{SL}_2(\mathbb{Z}) \setminus \overline{\mathbb{H}}$. We know that any modular function will be a meromorphic function on the surface M. Thanks to the presence of the cusps, M will be a compact Riemann surface. In fact, it can be easily seen to be a sphere. As we know, the only functions meromorphic on the Riemann sphere $\mathbb{C} \cup \{\infty\}$ are the rational functions $\frac{\text{polynomial in } z}{\text{polynomial in } z}$. So if j is a *uniformising* function from our moduli space M to the Riemann sphere, then J (interpreted as a function on the covering space $\overline{\mathbb{H}}$) will be a modular function, and any modular function $f(\tau)$ will be a rational function in $j(\tau)$: $f(\tau) = \frac{\text{polynomial in } j(\tau)}{\text{polynomial in } j(\tau)}$. And conversely, any rational function in j will be modular.

There is a standard historical choice for this function, namely

$$\begin{aligned} j(\tau) &\stackrel{\text{def}}{=} 1728 \frac{20G_4(\tau)^3}{20G_4(\tau)^3 - 49G_6(\tau)^2} \\ &= q^{-1} + 744 + 196\,884q + 21\,493\,760q^2 + 864\,299\,970q^3 + \cdots \end{aligned} \tag{3}$$

where as always $q = \exp[2\pi \mathrm{i}\tau]$. In fact, this choice is canonical, apart from the arbitrary constant 744. This function j is called the absolute invariant or *Hauptmodul* for $\mathrm{SL}_2(\mathbb{Z})$, or simply the *$j$-function*.

In any case, one of the best studied functions of classical number theory is the j-function. However, one of its most remarkable properties was discovered only recently: McKay's approximations $196\,884 \approx 196\,883$, $21\,493\,760 \approx 21\,296\,876$, and $864\,299\,970 \approx 842\,609\,326$. In fact,

$$196\,884 = 196\,883 + 1 \tag{4a}$$

$$21\,493\,760 = 21\,296\,876 + 196\,883 + 1 \tag{4b}$$

$$864\,299\,970 = 842\,609\,326 + 21\,296\,876 + 2 \cdot 196\,883 + 2 \cdot 1. \tag{4c}$$

The numbers on the left sides of (4) are the first few coefficients of the j-function (the number '744' in (3) is of no mathematical significance and can be ignored). The numbers on the right are the dimensions of the smallest irreducible representations of the *Monster finite simple group* $\mathbb{M}$. The finite simple groups consist of 18 infinite families (*e.g.* the cyclic groups $\mathbb{Z}/p\mathbb{Z}$ of prime order), together with 26 exceptional groups. The Monster $\mathbb{M}$ is the largest and richest of these exceptionals.

The equations (4) tell us that there is an infinite-dimensional graded representation

$$V = V_{-1} \oplus V_1 \oplus V_2 \oplus V_3 \oplus \cdots$$

of $\mathbb{M}$, where $V_{-1} = \rho_0$, $V_1 = \rho_1 \oplus \rho_0$, $V_2 = \rho_2 \oplus \rho_1 \oplus \rho_0$, $V_3 = \rho_3 \oplus \rho_2 \oplus \rho_1 \oplus \rho_1 \oplus \rho_0 \oplus \rho_0$, *etc.*, for the irreducible representations ρ_i of $\mathbb{M}$ (ordered by dimension), and that

$$j(\tau) - 744 = \dim(V_{-1})q^{-1} + \sum_{i=1}^{\infty} \dim(V_i)q^i$$

is the graded dimension of V. John Thompson then suggested that we 'twist' this, *i.e.*, that more generally we consider the *McKay-Thompson series*

$$T_g(\tau) \stackrel{\text{def}}{=} \mathrm{ch}_{V_{-1}}(g)q^{-1} + \sum_{i=1}^{\infty} \mathrm{ch}_{V_i}(g)q^i \tag{5}$$

for each element $g \in \mathbb{M}$. The point of (5) is that, for any group representation ρ, the character value $\mathrm{ch}_\rho(\mathrm{id.})$ equals the dimension of ρ, and so $T_{\mathrm{id.}}(\tau) = j(\tau) - 744$ and we recover (4) as special cases. But there are many other possible choices of $g \in \mathbb{M}$, although conjugate elements g, hgh^{-1} will trivially have identical McKay-Thompson series $T_g = T_{hgh^{-1}}$. In fact there are precisely 171 *distinct* functions T_g. Perhaps these functions $T_g(\tau)$ might also be interesting.

Indeed, John Conway and Simon Norton [6] found that the first few terms of each McKay-Thompson series T_g coincided with the first few terms of certain special functions, namely the 'Hauptmoduls' of various 'genus-0 modular groups'. Monstrous Moonshine—which conjectured that the McKay-Thompson series *were* those Hauptmoduls—was officially born.

We should explain those terms. We can generalise Definition 1 by replacing $\mathrm{SL}_2(\mathbb{Z})$ with any discrete subgroup $\mathcal{G}$ of $\mathrm{GL}_2(\mathbb{Q})^+$, *i.e.*, 2×2 rational matrices with positive determinant. If $\mathcal{G}$ is not too big and not too small, then $\mathcal{G} \backslash \overline{\mathbb{H}}$ will again be a compact Riemann surface. When this surface is a sphere, we call the modular group $\mathcal{G}$ *genus-0*, and the (appropriately normalised) uniformising function from $\mathcal{G}\backslash\overline{\mathbb{H}}$ to the Riemann sphere $\mathbb{C} \cup \{\infty\}$ is again called the *Hauptmodul* for $\mathcal{G}$. All modular functions for a genus-0 group $\mathcal{G}$ will be rational functions of this Hauptmodul. (On the other hand, when $\mathcal{G}$ is not genus-0, two generators are needed, and unfortunately there is no canonical choice for them.)

The word 'moonshine' here is English slang for 'insubstantial or unreal', 'idle talk or speculation'. It was chosen by Conway to convey as well the impression that things here are dimly lit, and that Conway-Norton were 'distilling information illegally' from the Monster character table.

In hindsight, the first incarnation of Monstrous Moonshine goes back to Andrew Ogg in 1975. He was in France discussing his result that the primes p for which the group $\mathcal{G} = \Gamma_0(p)+$ has genus 0, are

$$p \in \{2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 41, 47, 59, 71\}.$$

$\Gamma_0(p)+$ is the group generated by all matrices $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$ with p dividing the entry c, along with the matrix $\left(\begin{smallmatrix} 0 & 1 \\ -p & 0 \end{smallmatrix}\right)$. He also attended at that time a lecture by Jacques Tits, who was describing a newly conjectured simple group. When Tits wrote down the order

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

of that group, Ogg noticed its prime factors precisely equalled his list of primes. Presumably as a joke, he offered a bottle of Jack Daniels' whisky to the first person to explain the coincidence. Incidentally, we now know (this is implicit in [6]) that each of Ogg's groups $\Gamma_0(p)+$ is the genus-0 modular group for the function T_g, for some element $g \in \mathbb{M}$ of order p.

The appeal of Monstrous Moonshine lies in its mysteriousness: it associates various special modular functions to the Monster, even though mathematically they seem fundamentally incommensurable. Now, 'understanding' something means to embed it naturally into a broader context. Why is the sky blue? Because of the way light scatters in gases. In order to understand Monstrous Moonshine, to resolve the mystery, we should search for similar phenomena, and fit them all into the same story.

In actual fact, Moonshine (albeit non-Monstrous) really began long ago. Euler (and probably people before) played with the power series $t(x) \stackrel{\text{def}}{=} 1 + 2x + 2x^4 + 2x^9 + 2x^{16} + \cdots$, primarily because it can be used to express the number of ways a given number can be written as a sum of squares of integers. In his study of elliptic integrals, Jacobi noticed that if we change variables by $x = e^{\pi \mathrm{i} \tau}$, then the resulting function $\theta_3(\tau) = 1 + 2e^{\pi \mathrm{i} \tau} + 2e^{4\pi \mathrm{i} \tau} + \cdots$ is a modular form for a certain subgroup of $\mathrm{SL}_2(\mathbb{Z})$. More generally, the same conclusion holds when we sum not over the squares of $\mathbb{Z}$, but the norms of any lattice $\Lambda \subset \mathbb{R}^n$: the lattice theta series

$$\Theta_\Lambda(\tau) = \sum_{x \in \Lambda} e^{\pi \mathrm{i} x \cdot x}$$

is also a modular form, provided all norms $x \cdot x$ in Λ are rational. See [7] for a readable account of lattice lore.

In the late 1960s Victor Kac [17] and Robert Moody [25] independently (and for completely different reasons) defined a new class of infinite-dimensional Lie algebras. Within a decade it was realised that the characters of the *affine* Kac-Moody algebras are (vector-valued) modular functions.

Indeed, McKay had also remarked in 1978 that similar coincidences to (4) hold if $\mathbb{M}$ and $j(\tau)$ respectively are replaced with the Lie group $E_8(\mathbb{C})$ and

$$j(q)^{\frac{1}{3}} = q^{-\frac{1}{3}}(1 + 248q + 4124q^2 + 34\,752q^3 + \cdots).$$

In particular, $248 = \dim L(\Lambda_7)$, $4124 = \dim\big(L(\Lambda_1) \oplus L(\Lambda_7) \oplus L(0)\big)$, $34\,752 = \dim\big(L(\Lambda_6) \oplus L(\Lambda_1) \oplus 2L(\Lambda_7) \oplus L(0)\big)$, where the Λ_i's are fundamental weights of $E_8(\mathbb{C})$, and the $L(\Lambda_i)$'s the corresponding highest weight representations. Incidentally, $j^{\frac{1}{3}}$ is the Hauptmodul of the genus-0 group $\Gamma(3)$, where

$$\Gamma(N) = \left\{ A \in \mathrm{SL}_2(\mathbb{Z}) \mid A \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod N \right\}.$$

https://doi.org/10.4153/CMB-2002-056-6 Published online by Cambridge University Press

In no time Kac [16] and James Lepowsky [23] independently remarked that the unique level 1 highest-weight representation $L(\Lambda_0)$ of the affine Kac-Moody algebra $E_8^{(1)}$ has character $\left(qj(q)\right)^{\frac{1}{3}}$. Since each graded piece of any representation $L(\lambda)$ of the affine Kac-Moody algebra $X_\ell^{(1)}$ must carry a representation of the associated finite-dimensional Lie group $X_\ell(\mathbb{C})$, and the characters χ_λ (multiplied by an appropriate power of q) of an affine algebra are modular functions for some $\mathcal{G} \subseteq \mathrm{SL}_2(\mathbb{Z})$, this explained McKay's E_8 observation. (Standard references for Kac-Moody algebras are [19] and [20].) His Monster observations took longer to clarify, because much of the mathematics needed was still to be developed.

We've known for years that lattices and affine Kac-Moody algebras are associated to modular forms and functions. But these observations, albeit now familiar, are also a little mysterious, we should confess. For instance, compare the unobvious fact that $\theta_3(-1/\tau) = \sqrt{\frac{\tau}{i}}\theta_3(\tau)$, with the trivial observation (2) that $G_k(-1/\tau) = \tau^k G_k(\tau)$ for the Eisenstein series G_k in (1). The modularity of θ_3, unlike that of G_k, begs a *conceptual* explanation, even though its *logical* explanation (*i.e.*, proof) follows in a few moves from *e.g.* the Poisson summation formula:

$$\sum_{x\in\Lambda} f(x) = \frac{1}{\sqrt{|\Lambda|}} \sum_{y\in\Lambda^*} \widehat{f}(y), \tag{6}$$

where $\Lambda \subset \mathbb{R}^n$ is any lattice, $\Lambda^* \subset \mathbb{R}^n$ is its dual lattice, f is any 'rapidly decreasing smooth function' on $\mathbb{R}^n$, and $\widehat{f}(y)$ is the Fourier transform of f (see *e.g.* Section 6.1 of [29] for details). The key to the simple $\tau \mapsto -1/\tau$ transformation of θ_3 is that the Fourier transform of the Gaussian distribution $e^{-\pi x^2}$ is itself.

> *At minimum, Moonshine should be regarded as a certain collection of related examples where algebraic structures have been associated automorphic functions or forms.*

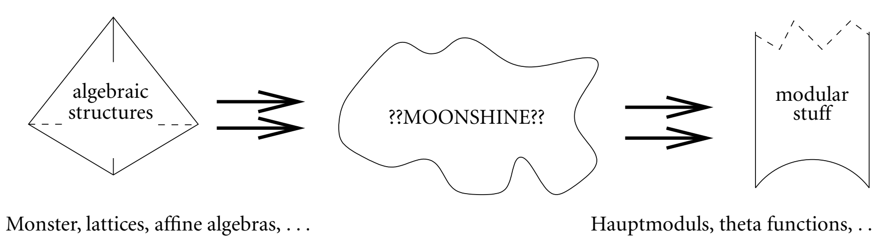

Figure 1: Moonshine in a broader sense.

From this larger perspective, illustrated in Figure 1, what is so special about the isolated example called *Monstrous* Moonshine is that the associated modular functions are of a special class (namely are Hauptmoduls). For lack of a better name, we call the theory of the blob of Figure 1, the *Theory of Generalised Moonshine*.

https://doi.org/10.4153/CMB-2002-056-6 Published online by Cambridge University Press

The first major step in the proof of Monstrous Moonshine was accomplished in the mid 1980s with the construction by Frenkel-Lepowsky-Meurman (see *e.g.* [11]) of the Moonshine module $V^\natural$ and its interpretation by Richard Borcherds [3] as a *vertex (operator) algebra*. A vertex operator algebra is an infinite-dimensional vector space with infinitely many heavily constrained vector-valued bilinear products. Now, the Monster $\mathbb{M}$ is presumably a natural mathematical object, so we can expect that an elegant construction for it would exist. Since $\mathbb{M}$ is the automorphism group of $V^\natural$, and $V^\natural$ seems to be a natural though extremely intricate mathematical structure, the hope it seems has been fullfilled.

In 1992 Borcherds [4] completed the proof of the Monstrous Moonshine conjectures by showing that the graded characters T_g of $V^\natural$ are indeed the Hauptmoduls conjectured by Conway and Norton, and hence that $V^\natural$ is indeed the desired representation V of $\mathbb{M}$ conjectured by McKay and Thompson. The explanation of Moonshine suggested by this picture is given in Figure 2. The algebraic structure can arise as the automorphism group of the associated vertex operator algebra, or it can be hardwired into the structure of the vertex operator algebra. The modular forms/functions arise as the characters of the (possibly twisted) modules of the vertex operator algebra.

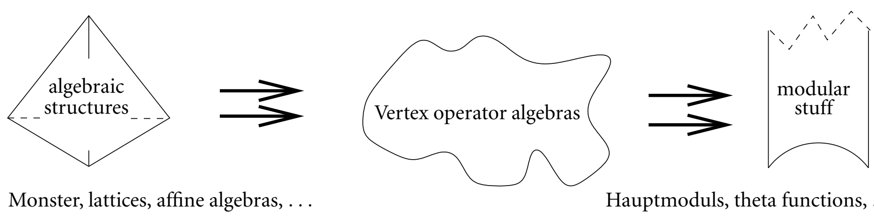

Figure 2: The 'modern' picture of Moonshine.

It must be emphasised that Figure 2 is meant to address Moonshine in the broader sense of Figure 1, so certain special features of *e.g.* Monstrous Moonshine (in particular that Hauptmoduls arise) will have to be treated by special arguments.

To see this genus-0 property of the T_g, Borcherds constructed a Kac-Moody-like Lie algebra from $V^\natural$. The '(twisted) denominator identities' of this algebra supply us with infinitely many equations which the coefficients $a_n(g)$ of the series T_g must obey. For different reasons, the same equations must be obeyed by the coefficients of the Hauptmoduls. These equations mean that both the series T_g, and the Hauptmoduls, are uniquely determined by their first few coefficients, so an easy computer check verifies that each T_g equals the appropriate Hauptmodul. A more conceptual proof of this Hauptmodul property was supplied in [8]: the denominator identities can be reinterpreted as saying that the T_g possess infinitely many 'modular equations'; it can be shown that any function obeying enough modular equations must necessarily be a Hauptmodul.

Moonshine for other finite groups is explored in [27]. But what is so special about the Monster $\mathbb{M}$ that makes the McKay-Thompson series T_g be Hauptmoduls? It has

https://doi.org/10.4153/CMB-2002-056-6 Published online by Cambridge University Press

been conjectured [26] that it has to do with the '6-transposition property' of $\mathbb{M}$. This thought has been further developed by Conway, Hsu, Norton, and Parker in their theory of quilts (see *e.g.* [15]). The genus-0 property for $\mathbb{M}$ has also been related [30] to the conjectured uniqueness of the Moonshine module $V^\natural$.

Connections of Moonshine with physics—namely conformal field theory (CFT) [9] and string theory—abound. A vertex operator algebra is an algebraic abstraction of (one 'chiral half' of) conformal field theory. The Moonshine module $V^\natural$ can be interpreted as the string theory for a $\mathbb{Z}_2$-orbifold of free bosons compactified on the torus $\mathbb{R}^{24}/\Lambda_{24}$ associated to the Leech lattice Λ_{24}. Many aspects of Moonshine make complete sense within CFT, but some (in particular the genus-0 property) remain more obscure. In any case, although our story is primarily a mathematical one, most of the chairs on which we sit were warmed by physicists. In particular, what CFT (or what is essentially the same thing, string theory) is, at least in part, is a machine for producing modular functions. Figure 2 becomes Figure 3. More precisely, the algebraic structure is an underlying symmetry of the CFT, and its characters are the various modular functions. The lattice theta functions come from bosonic strings living on the torus $\mathbb{R}^n/\Lambda$. The affine Kac-Moody characters arise in a string theory where the string lives on a Lie group. And the Monster is the automorphism group of a special 'holomorphic' CFT intimately connected with $V^\natural$.

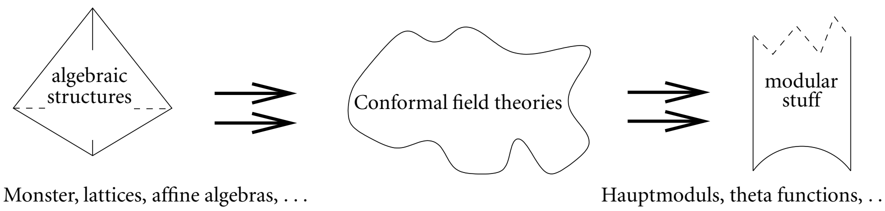

Figure 3: The stringy picture of Moonshine.

Historically speaking, Figure 3 preceded Figure 2. The stringy picture is exciting because the CFT machine in Figure 3 outputs much more than merely modular functions—it generates automorphic functions and forms for the various mapping class groups of surfaces. And all this is still poorly explored. We can thus expect more from Moonshine than Figure 2 alone suggests. On the other hand, once again, Figure 3 by itself can only explain the broader aspects of Moonshine. More importantly, no one really knows what a CFT is (an influential but incomplete attempt is by Graeme Segal [28]). Though that too may be exciting to some physicists (and dismissed as inconsequential by others), most mathematicians find it a disturbing flaw with Figure 3. Indeed, the definition by Borcherds and Frenkel-Lepowsky-Meurman of a vertex operator algebra can be regarded as the first precise definition of the *chiral algebra* of a CFT, and for this reason alone is a major achievement.

In spite of the work of Borcherds and others, the special features of Monstrous Moonshine still beg questions. The full conceptual relationship between the Monster and the Hauptmoduls (like j) arguably remains 'dimly lit', although much progress

https://doi.org/10.4153/CMB-2002-056-6 Published online by Cambridge University Press

has been realised. This is a subject where it is much easier to conjecture than to prove, and we are still awash in unresolved conjectures.

Nevertheless, Borcherds' paper [4] brings to a close the opening chapter of the saga of Monstrous Moonshine. We are now in a period of consolidation and synthesis, and it is in this spirit that this paper is offered.

So far, all of our 'postcards' have been directly in the spirit of Monstrous Moonshine. But the blob of Figure 1 is much more versatile than that. We describe next three other postcards from the realm of generalised Moonshine, which are *orthogonal* to Monstrous Moonshine.

Consider the following scenario. Let A, B and C be $n \times n$ Hermitian matrices with eigenvalues $\alpha_1 \geq \alpha_2 \geq \cdots \geq \alpha_n$, $\beta_1 \geq \cdots \geq \beta_n$, $\gamma_1 \geq \cdots \geq \gamma_n$. What are the conditions on these eigenvalues so that $C = A + B$? The answer consists of a number of inequalities involving the numbers α_i, β_j, γ_k. Discretise this problem, by requiring all α_i, β_j, γ_k to be nonnegative integers. Then the following are equivalent (see *e.g.* [13]):

(a) Hermitian matrices A, B, and $C = A + B$ exist with eigenvalues α, β, γ, respectively;

(b) the $\mathrm{GL}_n(\mathbb{C})$ tensor product coefficient $T_{\alpha\beta}^{\gamma}$ is nonzero. (The finite-dimensional irreducible modules L of $\mathrm{GL}_n(\mathbb{C})$ are naturally labelled by such n-tuples α, β, γ. The number $T_{\alpha\beta}^{\gamma}$ is the number of times the module $L(\gamma)$ appears in the tensor product $L(\alpha) \otimes L(\beta)$.)

Now consider instead $n \times n$ unitary matrices with determinant 1. Any such matrix $D \in \mathrm{SU}_n(\mathbb{C})$ can be assigned a unique n-tuple $\delta = (\delta_1, \ldots, \delta_n)$ as follows. Write its eigenvalues as $e^{2\pi \mathrm{i}\, \delta_i}$, where $\delta_1 \geq \cdots \geq \delta_n$, $\sum_{i=1}^{n} \delta_i = 0$, and $\delta_1 - \delta_n \leq 1$. Let Δ_n be the set of all such n-tuples δ, as D runs through $\mathrm{SU}_n(\mathbb{C})$. Note that D will have finite order iff all $\delta_i \in \mathbb{Q}$, and that D will be a scalar matrix dI iff all differences $\delta_i - \delta_j \in \mathbb{Z}$. Of course, a sum of Hermitian matrices corresponds here to a product of unitary matrices.

Choose any *rational* n-tuples $\alpha, \beta, \gamma \in \Delta_n \cap \mathbb{Q}^n$. Then the following are equivalent [1]:

(i) there exist matrices $A, B, C \in \mathrm{SU}_n(\mathbb{C})$, where $C = AB$, with n-tuples α, β, γ;

(ii) there is a positive integer k such that all differences $k\alpha_i - k\alpha_j, k\beta_i - k\beta_j, k\gamma_i - k\gamma_j$ are integers, and the $\mathrm{sl}_n^{(1)}$ level k fusion coefficient $N_{k\alpha,k\beta}^{(k)\,k\gamma}$ is nonzero.

$\mathrm{sl}_n^{(1)}$ is an affine Kac-Moody algebra. Here we interpret $k\alpha$ *etc.* as lying in the weight lattice A_{n-1}^*, and so they correspond to the Dynkin labels $\lambda_i = k\alpha_i - k\alpha_{i+1}$, *etc.* of level k integrable highest-weights λ, μ, ν.

The $\mathrm{GL}_n(\mathbb{C})$ tensor product coefficients $T_{\alpha\beta}^{\gamma}$—or *Littlewood-Richardson coefficients* —are classical quantities, appearing in numerous and varied contexts. The $\mathrm{sl}_n^{(1)}$ fusion coefficients $N_{\lambda\mu}^{(k)\,\nu}$ are equally fundamental, equally ubiquitous, but are more modern. For example, they arise as tensor product coefficients for quantum groups at roots of 1, as dimensions of spaces of generalised theta functions, as dimensions of conformal blocks in CFT, and as coefficients in the quantum cohomology ring. They are perhaps the most interesting example of a *fusion ring* (defined shortly). Fusion

https://doi.org/10.4153/CMB-2002-056-6 Published online by Cambridge University Press

rings are an aspect of generalised Moonshine complementary to Monstrous Moonshine, in the sense that the fusion ring associated to Monstrous Moonshine is trivial (*i.e.*, one-dimensional).

Definition 2 A *fusion ring* [12], [9], [14] (over $\mathbb{Q}$ say) is an associative commutative unital $\mathbb{Q}$-algebra R, together with a finite basis Φ containing 1, such that:

F1. The structure constants N_{ab}^{c} are all nonnegative integers;
F2. There is a ring endomorphism $x \mapsto x^*$ stabilising the basis Φ;
F3. $N_{ab}^{1} = \delta_{b,a^*}$.

In addition, a self-duality condition identifying R with its dual should probably be imposed—see [14] for details. As an abstract ring it is not so interesting, as it is isomorphic (as an algebra) to a direct sum of number fields. What is essential here is the preferred basis Φ.

The endomorphism $x \mapsto x^*$ can be shown to be an involution. We can derive that there will be a unitary matrix S, with rows and columns parametrised by Φ, such that both $S_{1a}, S_{a1} > 0\ \forall a$, and

$$N_{ab}^{c} = \sum_i \frac{S_{ai} S_{bi} \overline{S_{ci}}}{S_{1i}} \tag{7}$$

where $\overline{S}$ denotes complex conjugate. The aforementioned self-duality condition amounts to a relation between S and S^t [14].

The fusion ring of a nontwisted affine algebra $X_\ell^{(1)}$ at 'level' $k \in \{1, 2, 3, \dots\}$ is

$$R = \mathrm{Ch}(X_\ell)/\mathcal{I}_k$$

where $\mathrm{Ch}(X_\ell)$ is the character ring of the Lie algebra X_ℓ (which has preferred basis given by the characters ch_λ, and whose structure constants are the tensor product coefficients), and where $\mathcal{I}_k$ is the ideal generated by all characters of X_ℓ with level $k+1$. (For $X_\ell = A_\ell$, the level of representation λ is given by $\sum_{i=1}^{\ell} \lambda_i$.) The preferred basis for the fusion ring R consists of all characters ch_λ with λ of level $\leq k$. It is known that the $N_{\lambda\mu}^{\nu(k)}$ are nonnegative integers, which increase with k to the corresponding tensor product coefficient $T_{\lambda\mu}^{\nu}$. Incidentally, the *twisted* affine algebras also appear very naturally here, in the context of 'NIM-reps' or 'fusion graphs', but this is another story.

What has a fusion ring to do with 'modular stuff'? That is explained in our next postcard: *modular data*.

Choose any even integer $n > 0$. The matrix $S = (\frac{1}{\sqrt{n}} e^{-2\pi \mathrm{i}\, mm'/n})_{0 \leq m,m' < n}$ is the finite Fourier transform. Define the diagonal matrix T by $T_{mm} = \exp(\pi \mathrm{i}\, m^2/n - \pi \mathrm{i}/12)$. The assignment $\left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right) \mapsto S$, $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right) \mapsto T$ defines an n-dimensional representation ρ of $\mathrm{SL}_2(\mathbb{Z})$, since the matrices $\left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ generate $\mathrm{SL}_2(\mathbb{Z})$. In fact this is essentially a Weil representation of $\mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z})$. This is the simplest (and least interesting) example of what we'll call *modular data*—a refinement of fusion rings to be defined shortly. Verlinde's formula (7) here is the product rule for discrete exponentials, namely

$$e^{2\pi\,\mathrm{i}\,mm'/n} \cdot e^{2\pi\,\mathrm{i}\,mm''/n} = e^{2\pi\,\mathrm{i}\,m(m'+m'')/n}.$$

This representation is realised by modular functions. For each $m \in \{0, 1, \ldots, n-1\}$, define the functions

$$\psi_m(\tau) = \frac{1}{\eta(\tau)} \sum_{k=-\infty}^{\infty} q^{n(k+m/n)^2/2}$$

where as always $q = e^{2\pi\,\mathrm{i}\,\tau}$ and where $\eta(\tau)$ is the Dedekind eta function:

$$\eta(\tau) = \sum_{k=-\infty}^{\infty} (q^{6(k+\frac{1}{12})^2} - q^{6(k+\frac{5}{12})^2}) = \left\{ \frac{675}{256\pi^{12}} \big(20G_4(\tau)^3 - 49G_6(\tau)^2\big) \right\}^{\frac{1}{24}}.$$

If we write Λ for the lattice $\sqrt{n}\mathbb{Z}$, then $\Lambda^* = \frac{1}{\sqrt{n}}\mathbb{Z}$ is the dual lattice, the number $0 \leq m < n$ parametrises the cosets Λ^*/Λ, and ψ_m is the theta series of the m-th coset. It's easy to see that $\psi_m(\tau+1) = T_{mm}\psi_m(\tau)$; the Poisson summation formula (6) gives us $\psi_m(-1/\tau) = \sum_{m'=0}^{n-1} S_{mm'}\psi_{m'}(\tau)$. Thus $\vec{\psi} = (\psi_0, \psi_1, \ldots, \psi_{n-1})^t$ is a 'vector-valued modular function with multiplier ρ' for $\mathrm{SL}_2(\mathbb{Z})$, in the sense that $\vec{\psi}(A.\tau) = \rho(A)\vec{\psi}(\tau)$ for any $A \in \mathrm{SL}_2(\mathbb{Z})$.

More generally, to various algebraic structures (in the above special case this is the lattice $\Lambda = \sqrt{n}\mathbb{Z}$) can be associated an $\mathrm{SL}_2(\mathbb{Z})$ representation. Interesting examples of this come from affine Kac-Moody algebras and finite groups. The role of ψ_m is played by the characters of vertex operator algebras [32] (or Kac-Moody algebras or CFT). Verlinde's formula (7) associates a fusion ring to modular data. In Monstrous Moonshine, the modular data is trivial: each matrix U is the 1×1 matrix (1).

Definition 3 Let Φ be a finite set of labels, one of which—denoted '1' and called the 'identity'—is distinguished. By *modular data* we mean matrices $S = (S_{ab})_{a,b\in\Phi}$, $T = (T_{ab})_{a,b\in\Phi}$ of complex numbers such that [14]:

- M1. S is unitary and symmetric, and T is diagonal and of finite order: *i.e.*, $T^N = I$ for some N;
- M2. $S_{1a} > 0$ for all $a \in \Phi$;
- M3. $S^2 = (ST)^3$;
- M4. The numbers N_{ab}^c defined by Verlinde's formula (7) are nonnegative integers.

Axiom M2 as stated is too strong, although Perron-Frobenius theory (which describes the spectral theory of nonnegative matrices) tells us that some scalar multiple of some column of S must be strictly positive. Modular data defines a representation of the modular group $\mathrm{SL}_2(\mathbb{Z})$ as above. Each entry S_{ab} lies in some cyclotomic field extension $\mathbb{K}_n \stackrel{\text{def}}{=} \mathbb{Q}[\exp(2\pi\,\mathrm{i}\,/n)]$. There is a simple and important action of $\mathrm{Gal}(\mathbb{K}_n/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^*$ on S, which generalises the $g \mapsto g^\ell$ symmetry of the character table of a finite group—we'll return to it at the end of the paper. In all known examples, the $SL_2(\mathbb{Z})$ representation is trivial on the principal congruence subgroup $\Gamma(N)$ defined earlier, where N is the order of T, which means that the characters are modular functions for $\Gamma(N)$, and that we really have a representation for the finite group $SL_2(\mathbb{Z})/\Gamma(N) \cong SL(\mathbb{Z}/N\mathbb{Z})$.

A *knot* K in $\mathbb{R}^n$ is a smooth one-to-one embedding of S^1 into $\mathbb{R}^n$. The Jordan curve theorem states that all knots in $\mathbb{R}^2$ are trivial. Are there any nontrivial knots in $\mathbb{R}^3$?

In Figures 4 and 5 we draw some knots in $\mathbb{R}^3$, by flattening them into the plane of the paper. A moment's consideration will confirm that the second knot of Figure 4 is indeed trivial. What about the trefoil?

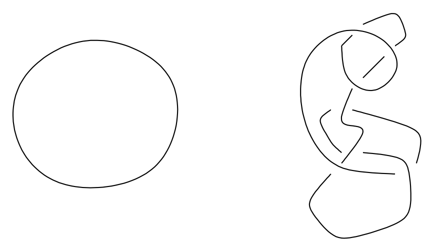

Figure 4: Some trivial knots.

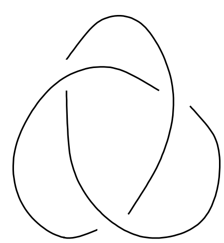

Figure 5: The trefoil.

A knot diagram cuts the knotted S^1 into several connected components (*arcs*), whose endpoints lie at the various *crossings* (double-points of the projection). By a *3-colouring*, we mean to colour each arc in the knot diagram either red, blue or green, so that at each crossing either 1 or 3 distinct colours are used. For example, the first two colourings in Figure 6 are allowed, but the third one isn't. By considering the Reidemeister moves, which tell how to move between equivalent knot diagrams, different diagrams for equivalent knots (such as the two in Figure 4) can be seen to have the same number of distinct 3-colourings. Hence the number of different 3-colourings is a knot invariant.

For example, consider the diagrams in Figure 4 for the trivial knot: the reader can quickly verify that all arcs must be given the same colour, and thus there are

https://doi.org/10.4153/CMB-2002-056-6 Published online by Cambridge University Press

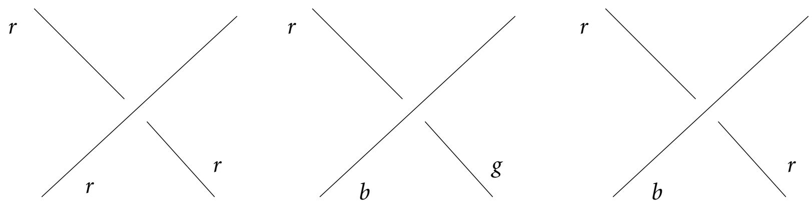

Figure 6: Colourings at a crossing.

precisely three distinct 3-colourings. On the other hand, the trefoil has nine distinct 3-colourings—the bottom two arcs of Figure 5 can be assigned arbitrary colour, and that choice fixes the colour of the top arc. Thus the trefoil is nontrivial.

Essentially what we are doing here is counting the number of homomorphisms φ from the *knot group* $\pi_1(\mathbb{R}^3/K)$ to the symmetric group S_3. The reason is that any knot diagram gives a presentation for $\pi_1(\mathbb{R}^3/K)$, where there is a generator g_i for each arc and a relation of the form $g_i^{\pm 1} g_j g_i^{\mp 1} = g_k$ for each crossing. The map φ is defined using *e.g.* the identification $r \leftrightarrow (12)$, $b \leftrightarrow (23)$, $g \leftrightarrow (13)$, and the above 3-colouring condition at each crossing is equivalent to requiring that φ obeys each group relation. Our homomorphism φ will be onto iff at least two different colours are used. Incidentally, the knot group of the trivial knot is $\mathbb{Z}$ while that of the trefoil is the braid group B_3 on three strands.

By considering more general (nonabelian) colourings, the target (S_3 here) can be made to be any other group G, resulting in a different knot invariant. This class of knot invariants is an example of one coming from *topological field theory* (a refinement of modular data related to but simpler than CFT), in this case associated to an arbitrary finite group G. Another deep and fascinating source of topological field theories (and modular data *etc.*) is subfactor theory for von Neumann algebras—a gentle introduction to some aspects of this is [21]. The definition of topological field theory is too long and complicated to give here, but an excellent account is [31]. A standard introduction to knot theory is [5].

What has topological field theory to do with modular stuff? The matrix S comes from the knot invariants attached to the so-called Hopf link (two linked circles in $\mathbb{R}^3$). The knots and links here are really 'framed', *i.e.*, are ribbons, and the diagonal matrix T describes what happens when the ribbon is twisted. If S and T constitute modular data (defined earlier), then the topological field theory will yield knot invariants in any closed 3-manifold (via the process called surgery). The fusion coefficients come from three parallel circles $p_i \times S^1$ in the 3-manifold $S^2 \times S^1$. There is no canonical choice of characters (modular functions) though which realise this $\mathrm{SL}_2(\mathbb{Z})$ representation.

From this perspective, a key to understanding Figure 1 is that the braid group B_3 (which plays a fundamental and explicit role in topological field theory and related structures such as ribbon categories) maps homomorphically onto $\mathrm{SL}_2(\mathbb{Z})$, via a specialisation of the Burau representation.

For instance, returning to the topological field theory and modular data associated

https://doi.org/10.4153/CMB-2002-056-6 Published online by Cambridge University Press

to the finite group S_3, we have $T = \mathrm{diag}(1, 1, 1, 1, e^{2\pi \mathrm{i}/3}, e^{-2\pi \mathrm{i}/3}, 1, -1)$, and

$$S = \frac{1}{6}\begin{pmatrix} 1 & 1 & 2 & 2 & 2 & 2 & 3 & 3 \\ 1 & 1 & 2 & 2 & 2 & 2 & -3 & -3 \\ 2 & 2 & 4 & -2 & -2 & -2 & 0 & 0 \\ 2 & 2 & -2 & 4 & -2 & -2 & 0 & 0 \\ 2 & 2 & -2 & -2 & -2 & 4 & 0 & 0 \\ 2 & 2 & -2 & -2 & 4 & -2 & 0 & 0 \\ 3 & -3 & 0 & 0 & 0 & 0 & 3 & -3 \\ 3 & -3 & 0 & 0 & 0 & 0 & -3 & 3 \end{pmatrix}.$$

In this paper we have sketched some of the possibilities inherent in a study of generalised Moonshine. We believe this is a natural challenge, given that it serves as a general context for Monstrous Moonshine. The theory itself seems quite rich, although it is still rather undeveloped mathematically. The implications of Moonshine to algebra have already been striking: *e.g.* the formulation of generalised Kac-Moody algebras and vertex operator algebras. Its consequences to number theory have been minor, and in fact the number theory here has remained completely classical. Presumably this is simply a reflection of the kind of mathematicians attracted so far to this area. Anticipating a more sophisticated contact with modern number theory is a primary motivation for writing this paper. For instance, inherent in this theory are automorphic functions for the other mapping class groups, but surely with a little effort other automorphic forms and functions will be found here. Is there any relation of generalised Moonshine to Langlands' Programme (obviously it's closely related to the *geometrical* Langlands correspondence)? Perhaps this relation is anticipated by a representation of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})^{ab}$ which plays a fundamental role in *e.g.* modular data (see equation (9a) below). Indeed Drinfeld [10], building on earlier work by Grothendieck and Ihara, finds an action of the absolute Galois group $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on a set of quasitriangular quasi-Hopf algebras or, what is closely related, a set of ribbon categories; a natural conjecture is that his action is the ultimate source of (9a).

We will close this paper with two humble examples hinting we hope at the number-theoretic potential of generalised Moonshine. First, consider the modular data given earlier, corresponding to even numbers $n > 0$. That this yields modular data, is a corollary to Poisson summation. The $\mathrm{SL}_2(\mathbb{Z})$ relation $STS = T^{-1}ST^{-1}$ reads

(8a)
$$\frac{e^{-\pi \mathrm{i}/12}}{\sqrt{n}} \sum_{d=0}^{n-1} \exp[\pi \mathrm{i}(-2ad + d^2 - 2db)/n] = e^{\pi \mathrm{i}/6} \exp[\pi \mathrm{i}(-a^2 - 2ab - b^2)/n]$$

which is clearly equivalent to the classical Gauss sum

(8b)
$$\sum_{d=0}^{n-1} \exp[\pi \mathrm{i}\, d^2/n] = (1 + \mathrm{i})\sqrt{n/2}.$$

(A somewhat similar derivation of the classical Gauss sum, due to Schur, involves taking the trace of the matrix we call S.) More generally, the modular data associated

https://doi.org/10.4153/CMB-2002-056-6 Published online by Cambridge University Press

to any d-dimensional even lattice Λ, yields

$$\sum_{[x]\in\Lambda^*/\Lambda} \exp[\pi\,\mathrm{i}\,x\cdot x] = \exp[\pi\,\mathrm{i}\,d/4]\sqrt{\|\Lambda\|}. \tag{8c}$$

Among other things, (8c) implies that 8 divides the dimension of an even self-dual lattice.

Likewise, the relation $STS = T^{-1}ST^{-1}$ applied to the modular data associated to the characters of an untwisted affine algebra $\mathfrak{g}^{(1)}$, can be interpreted as a *nonabelian* generalisation of the classical Gauss sum (8b), one for every finite-dimensional complex semisimple Lie algebra $\mathfrak{g}$ and choice of positive integer k (the *level* of the associated $\mathfrak{g}^{(1)}$ representations). In fact an easy extension of this construction associates Gauss sums to any finite-dimensional complex reductive Lie algebra. The Gauss sums (8b) and (8c) correspond to the abelian Lie algebras $\mathbb{C}$ and $\mathbb{C}^d$, respectively. The simplest *nonabelian* Gauss sum, corresponding to sl_2, reads

$$\begin{aligned}\sum_{d=1}^{n-1} &\sin(\pi ad/n)\sin(\pi bd/n)e^{\pi\,\mathrm{i}\,d^2/2n} \\ &= \sqrt{n/2}e^{3\pi\,\mathrm{i}/4}\exp[-\pi\,\mathrm{i}(a^2+b^2)/2n]\sin(\pi ab/n)\end{aligned} \tag{8d}$$

and is valid for any integer $n > 0$, and any integers $0 < a, b < n$. As is the case with denominator identities, higher rank yields considerably less obvious formulas. In the higher-rank formulas, a, b, d will be highest weights, d^2 *etc.* will be values of the quadradic Casimir, and 'sine' will be replaced by alternating sums over the appropriate Weyl group. To our knowledge, these 'nonabelian' Gauss sums are new. See [2] for a discussion of a number of generalisations of Gauss sums, which however do not seem to include ours.

For our second and final example, we turn to the Galois action on modular data, found by Coste-Gannon, to which we briefly alluded earlier. Given modular data S, T, define $\mathbb{Q}[S]$ to be the field obtained from $\mathbb{Q}$ by adjoining all entries S_{ab}. For any automorphism $\sigma \in \mathrm{Gal}(\mathbb{Q}[S]/\mathbb{Q})$, we have

$$\sigma(S_{ab}) = \epsilon_\sigma(a)S_{a^\sigma,b} \tag{9a}$$

where $\epsilon_\sigma(a) \in \{\pm 1\}$ and $a \mapsto a^\sigma$ is a permutation of Φ. This action, and particularly the 'parities' $\epsilon_\sigma(a)$, plays a fundamental role in *e.g.* the classification of rational conformal field theories—see [14]. For convenience, restrict here to the data associated to the affine algebra $\mathrm{sl}_n^{(1)}$ at level k. Then Φ consists of n-tuples λ of nonnegative integers, obeying $\sum_i \lambda_i = k$, our Galois group $\mathrm{Gal}(\mathbb{Q}[S]/\mathbb{Q})$ can be taken to be the multiplicative group $\big(\mathbb{Z}/4n(n+k)\mathbb{Z}\big)^\times$, and the parity $\epsilon_\sigma(\lambda)$ can be factored into $\epsilon'_\ell(\lambda)\epsilon''_\ell$, where

$$\epsilon'_\ell(\lambda) = \mathrm{sign}\Big\{\prod_{1\le i<j\le n} \sin\big(\pi\ell\lambda_{ij}/(n+k)\big)\Big\} \tag{9b}$$

https://doi.org/10.4153/CMB-2002-056-6 Published online by Cambridge University Press

where $\lambda_{ij} = j - i + \sum_{h=i}^{j-1} \lambda_h$. The other factor ϵ''_ℓ is independent of λ and for this reason is generally irrelevant; it turns out to equal $(-1)^{\lfloor n/2 \rfloor}$ times the Jacobi symbol $(\frac{m}{\ell})$, where $m = n$ for n odd and $m = n(n+k)$ otherwise. The numbers $\epsilon'_\ell(\lambda)$ are quite interesting, and are related for instance to the affine Weyl group of $\mathrm{sl}_n^{(1)}$, and to congruences involving generalised Bernoulli numbers; understanding better their properties certainly would be valuable [14].

For simplicity let's further restrict here to the unit 1, *i.e.*, to the highest-weight $\lambda = (k, 0, \dots, 0)$. Then (9b) becomes

$$\begin{aligned}\epsilon'_\ell(0) &= \prod_i \sin\big(2\pi\ell i/(n+k)\big) \\ &= (-1)^{(\ell-1)\lfloor n/2 \rfloor/2} \prod_i \prod_{j=1}^{(\ell-1)/2} \Big(\sin^2\big(2\pi i/(n+k)\big) - \sin^2(2\pi j/\ell)\Big)\end{aligned} \tag{9c}$$

where the product over i ranges (in increments of 1) from $i = 1$ to $(n-1)/2$ when n is odd, and from $i = 1/2$ to $(n-1)/2$ when n is even. We've used here the trigonometric identity (valid for odd ℓ)

$$\sin(\ell x) = (-4)^{(\ell-1)/2} \sin(x) \prod_{j=1}^{(\ell-1)/2} \big(\sin^2(x) - \sin^2(2\pi j/\ell)\big).$$

Define the quantities

$$\epsilon^{a,b}_{c,d} = \prod_i^{(a-1)/2} \prod_j^{(c-1)/2} \Big(\sin^2\big(2\pi i/(a+b)\big) - \sin^2\big(2\pi j/(c+d)\big)\Big)$$

where the product over i starts at 1 (resp. 1/2) for a odd (resp. even), and similarly for the product over j. Then

$$\epsilon'_\ell(0) = (-1)^{(\ell-1)\lfloor n/2 \rfloor/2} \epsilon^{n,k}_{\ell,0}.$$

Using this we get some special values: *e.g.*

$$\epsilon^{a,b}_{\ell,0} = \begin{cases} (\frac{a+b}{\ell}) & \text{if } a+b \text{ is odd} \\ 1 & \text{otherwise} \end{cases}$$

$$\epsilon^{c,d}_{\ell,0} = (-1)^{(\ell-1)/2 + \lfloor (c-1)\ell/(c+d) \rfloor}$$

$$\epsilon^{e,d}_{\ell,0} = \begin{cases} 1 & \text{if } m - \frac{1}{e-1} < \frac{\ell}{d+e} < m + \frac{1}{e-1} \text{ for some } m \in \mathbb{Z} \\ -1 & \text{otherwise} \end{cases}$$

where $b = 0, 1$, $c = 2, 3$, $e = 4, 5$, and a and d are arbitrary. Note that, for any a, b, c, d,

$$\epsilon^{a,b}_{c,d} = (-1)^{\lfloor a/2 \rfloor \lfloor c/2 \rfloor} \epsilon^{c,d}_{a,b} \tag{9d}$$

$$\epsilon^{a+b,0}_{c,d} = \epsilon^{a,b}_{c,d} \epsilon^{b,a}_{c,d}. \tag{9e}$$

Equation (9d), for the choice $b = d = 0$, is quadratic reciprocity. This proof of quadratic reciprocity is essentially Eisenstein's in disguise, but much more interesting should be the generalised reciprocity (9d), which seems to be new, and which suggests a tantalising and unexpected duality between ϵ'_ℓ for $\mathrm{sl}_n^{(1)}$ level k, and ϵ'_{n+k} for $\mathrm{sl}_m^{(1)}$ level $\ell - m$. This reciprocity will probably yield the solution to Problem 2 in [18]. Equation (9e) for $d = 0$ gives us a 'rank-level' duality between $\mathrm{sl}_n^{(1)}$ level k and $\mathrm{sl}_k^{(1)}$ level n; it says that their $\epsilon'_\ell(0)$'s differ by a factor of $(-1)^{(\ell-1)(\lfloor n/2\rfloor+\lfloor k/2\rfloor)/2}$, times 1 or $(\frac{n+k}{\ell})$ depending on whether or not $n + k$ is even (a similar duality holds for any highest-weight λ). Certainly other relations are satisfied—*e.g.* if both a and b are odd, then $\epsilon^{a,b}_{\ell,0}$ is determined by $\epsilon^{(a-1)/2,(b+1)/2}_{\ell,0}\epsilon^{(a+1)/2,(b-1)/2}_{\ell,0}$—but this should be enough to illustrate some of the possibilities here. A modern discussion of a variety of reciprocity laws is [22].

Like moonlight itself, Moonshine is an indirect phenomenon. Just as in the theory of moonlight one must introduce the sun, so in the theory of Moonshine one should go beyond the Monster. Much as a talk discussing moonlight may include a few words on sunsets or comet tails, so have we sent postcards of fusion rings, $\mathrm{SL}_2(\mathbb{Z})$ representations, and knot invariants.

References

[1] S. Agnihotri and C. Woodward, *Eigenvalues of products of unitary matrices and quantum Schubert calculus.* Math. Res. Lett. **5**(1998), 817–836.

[2] B. C. Berndt, R. J. Evans and K. S. Williams, *Gauss and Jacobi Sums.* Wiley, New York, 1998.

[3] R. E. Borcherds, *Vertex algebras, Kac-Moody algebras, and the Monster.* Proc. Nat. Acad. Sci. USA **83**(1986), 3068–3071.

[4] ———, *Monstrous moonshine and monstrous Lie superalgebras.* Invent. Math. **109**(1992), 405–444.

[5] G. Burke and H. Zieschang, *Knots.* de Gruyter, Berlin, 1995.

[6] J. H. Conway and S. P. Norton, *Monstrous moonshine.* Bull. London Math. Soc. **11**(1979), 308–339.

[7] J. H. Conway and N. J. A. Sloane, *Sphere Packings, Lattices and Groups.* 3rd edition, Springer, Berlin, 1999.

[8] C. J. Cummins and T. Gannon, *Modular equations and the genus zero property.* Invent. Math. **129**(1997), 413–443.

[9] P. Di Francesco, P. Mathieu and D. Sénéchal, *Conformal Field Theory.* Springer, New York, 1996.

[10] V. G. Drinfeld, *On quasitriangular quasi-Hopf algebras and a group closely connected with* $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Leningrad Math. J. **2**(1991), 829–860.

[11] I. Frenkel, J. Lepowsky and A. Meurman, *Vertex Operator Algebras and the Monster.* Academic Press, San Diego, 1988.

[12] J. Fuchs, *Fusion rules in conformal field theory.* Fortsch. Phys. **42**(1994), 1–48.

[13] W. Fulton, *Eigenvalues, invariant factors, highest weights, and Schubert calculus.* math.AG/9908012.

[14] T. Gannon, *Modular data: the algebraic combinatorics of conformal field theory.* math.QA/0103044.

[15] T. Hsu, *Quilts: Central Extensions, Braid Actions, and Finite Groups.* Lecture Notes in Math. **1731**, Springer, Berlin, 2000.

[16] V. G. Kac, *Simple irreducible graded Lie algebras of finite growth.* Math. USSR-Izv. **2**(1968), 1271–1311.

[17] ———, *An elucidation of: Infinite-dimensional algebras, Dedekind's* η*-function, classical Möbius function and the very strange formula.* $E_8^{(1)}$ *and the cube root of the modular invariant* j. Adv. in Math. **35**(1980), 264–273.

[18] ———, *Simple Lie groups and the Legendre symbol.* In: Algebra (Carbondale, 1980), Lecture Notes in Math. **848**, Springer, New York, 1981, 110–123.

[19] ———, *Infinite Dimensional Lie Algebras*. 3rd edition, Cambridge University Press, Cambridge, 1990.

[20] S. Kass, R. V. Moody, J. Patera and R. Slansky, *Affine Lie Algebras, Weight Multiplicities, and Branching Rules*. Vol. 1, University of California Press, Berkeley, 1990.

https://doi.org/10.4153/CMB-2002-056-6 Published online by Cambridge University Press

[21] V. Kodiyalam and V. S. Sunder, *Topological Quantum Field Theories from Subfactors.* Chapman & Hall, New York, 2001.
[22] F. Lemmermeyer, *Reciprocity Laws.* Springer, Berlin, 2000.
[23] J. Lepowsky, *Euclidean Lie algebras and the modular function j.* Proc. Sympos. Pure Math. **37**, Amer. Math. Soc., Providence, 1980, 567–570.
[24] H. McKean and V. Moll, *Elliptic Curves: Function Theory, Geometry, Arithmetic.* Cambridge University Press, Cambridge, 1999.
[25] R. V. Moody, *A new class of Lie algebras.* J. Algebra **10**(1968), 211–230.
[26] S. P. Norton, *Generalized moonshine.* Proc. Symp. Pure Math. **47**, Amer. Math. Soc., Providence, 1987, 208–209.
[27] L. Queen, *Modular functions arising from some finite groups.* Math. Comp. **37**(1981), 547–580.
[28] G. Segal, *Geometric aspects of quantum field theory.* In: Proc. Intern. Congr. Math. (Kyoto, 1990), Math. Soc. Japan, Tokyo, 1991, 1387–1396.
[29] J.-P. Serre, *A Course in Arithmetic.* Springer, Berlin, 1973.
[30] M. Tuite, *On the relationship between Monstrous moonshine and the uniqueness of the Moonshine module.* Commun. Math. Phys. **166**(1995), 495–532.
[31] V. G. Turaev, *Quantum Invariants of Knots and 3-Manifolds.* de Gruyter, Berlin, 1994.
[32] Y. Zhu, *Modular invariance of characters of vertex operator algebras.* J. Amer. Math. Soc. **9**(1996), 237–302.

Department of Mathematical Sciences
University of Alberta
Edmonton, Alberta
T6G 2G1
email: tgannon@math.ualberta.ca

https://doi.org/10.4153/CMB-2002-056-6 Published online by Cambridge University Press