Moonshine in Number Theory and Geometry

John Duncan

Bogoliubov Laboratory of Theoretical Physics
Joint Institute for Nuclear Research
Dubna, Russia

2018 January 31

Abstract

Moonshine arose in the 1970s as a collection of coincidences connecting modular functions to the monster simple group, which was newly discovered at that time. The effort to elucidate these connections led to new algebraic structures (e.g. vertex algebras and generalized Kac–Moody algebras) which have since found applications in representation theory, number theory, geometry and string theory. In this century the theory has been further enriched, with the discovery of connections between K3 surfaces and certain distinguished groups in the early part of this decade, and connections between sporadic simple groups and the arithmetic of modular abelian varieties in recent months. In these lectures we will review monstrous moonshine, explain the number theoretic foundations of umbral moonshine, and describe recent results which reveal a role for sporadic groups in arithmetic geometry.

Contents

1 Classical Moonshine

1.1 Elliptic Curves

- An *elliptic curve* over a field $\mathbb{F}$ is a pair (E, O) where E is a non-singular projective algebraic curve over $\mathbb{F}$ with genus 1 and O is a point of E defined over $\mathbb{F}$.
- If the characteristic of $\mathbb{F}$ is not 2 or 3 then any elliptic curve over $\mathbb{F}$ is isomorphic to one of the form (E, O) where $E \subset \mathbb{P}^2(\mathbb{F})$ is given by

$$Y^2Z = X^3 + AXZ^2 + BZ^3 \tag{1.1}$$

  for some $A, B \in \mathbb{F}$ such that the *discriminant* $\Delta(E) := -16(4A^3 + 27B^2)$ is not zero, and $O = (0, 1, 0)$.
- The *j-invariant* of (1.1) is $j(E) := 1728\frac{4A^3}{4A^3+27B^2}$.
- Two elliptic curves over $\mathbb{F}$ are isomorphic over an algebraic closure of $\mathbb{F}$ if and only if they have the same j-invariant.
- It is a millennium prize problem (Birch–Swinnerton-Dyer conjecture) to determine the structure of the group of rational points of an elliptic curve over $\mathbb{Q}$.

1.2 Supersingular Elliptic Curves

- A *definite quaternion algebra* over $\mathbb{Q}$ is an algebra of the form $\mathcal{B} = \mathbb{Q} + \mathbb{Q}i + \mathbb{Q}j + \mathbb{Q}k$ where i^2 and j^2 are negative elements of $\mathbb{Q}$, and $ij = k = -ji$.
- An *order* of a definite quaternion algebra $\mathcal{B}$ is a subring $\mathcal{O}$ that is finitely generated as a $\mathbb{Z}$-module and satisfies $\mathcal{B} = \mathcal{O} \otimes \mathbb{Q}$.
- An elliptic curve E is called *supersingular* if its endomorphism ring is isomorphic to an order in a definite quaternion algebra over $\mathbb{Q}$.
- If $\mathbb{F}$ has characteristic zero then there are no supersingular elliptic curves defined over $\mathbb{F}$.
- If E is a supersingular elliptic curve over $\mathbb{F}$ and p is the characteristic of $\mathbb{F}$ then $j(E) \in \mathbb{F}_{p^2}$.
- Ogg (1974): let p be a prime. Then every supersingular elliptic curve E over $\overline{\mathbb{F}}_p$ has $j(E) \in \mathbb{F}_p$ if and only if p belongs to

$$\{2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 41, 47, 59, 71\}. \tag{1.2}$$

1.3 Ogg's Observation

- Fisher and Griess independently produced evidence for the existence of a new simple group—the Fischer–Griess *monster*—in 1973.
- On 14 January 1975 Tits described some of its conjectural properties, including the prime factorization of its order ($\approx 8 \times 10^{53}$), in a lecture at the Collège de France.
- Ogg was in attendance, and noticed that the primes dividing the order of the monster are precisely those that appear in his theorem on supersingular j-invariants.

$$\{2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 41, 47, 59, 71\} \tag{1.3}$$

1.4 Complex Elliptic Curves

- Any elliptic curve over $\mathbb{C}$ is isomorphic to $E_\tau := (\mathbb{C}/(\mathbb{Z}\tau + \mathbb{Z}), 0)$ for some τ in the complex upper-half plane $\mathbb{H}$.
- We have $E_{\tau'} \simeq E_\tau$ if and only if $\tau' = \gamma\tau$ for some $\gamma \in SL_2(\mathbb{Z})$ so $SL_2(\mathbb{Z})\backslash\mathbb{H}$ is a (coarse) moduli space for complex elliptic curves.
- The j-invariant induces a bijective holomorphic map $SL_2(\mathbb{Z})\backslash\mathbb{H} \to \mathbb{C}$, which extends naturally to an isomorphism

$$SL_2(\mathbb{Z})\backslash(\mathbb{H} \cup \mathbb{P}^1(\mathbb{Q})) \xrightarrow{\sim} \mathbb{P}^1(\mathbb{C}) \tag{1.4}$$

  of compact complex curves (i.e. Riemann surfaces).
- Regarding j as a holomorphic function on $\mathbb{H}$, and setting $q := e^{2\pi i\tau}$, we have

$$j(\tau) = q^{-1} + 744 + 196884q + \dots \tag{1.5}$$

1.5 Monstrous Moonshine

- Conway–Norton conjectured that there is an embedding of $\mathbb{M}$ in $GL_n(\mathbb{C})$ for $n = 196883$.
- McKay observed that $196884 = 196883 + 1$.
- Thompson–Conway–Norton conjecture (1978): there exists an $\mathbb{M}$-module $V = \bigoplus V_n$ such that $\sum_n \dim(V_n)q^n = j(\tau) - 744$, and more generally, for each $g \in \mathbb{M}$, the graded trace function

$$T_g(\tau) := \sum_n \mathrm{tr}(g|V_n)q^n \tag{1.6}$$

is a *principal modulus (Hauptmodul)* for a *genus zero group* $\Gamma_g < SL_2(\mathbb{R})$. That is, if

$$\Gamma_g := \{\gamma \in SL_2(\mathbb{R}) \mid T_g(\gamma\tau) = T_g(\tau)\} \tag{1.7}$$

then T_g induces an isomorphism

$$\Gamma_g\backslash(\mathbb{H} \cup \mathbb{P}^1(\mathbb{Q})) \xrightarrow{\sim} \mathbb{P}^1(\mathbb{C}) \tag{1.8}$$

of compact complex curves.

- The *genus zero property* of monstrous moonshine is the statement that the twisted partition functions T_g are principal moduli for all $g \in \mathbb{M}$.
- The genus zero property was verified—but not explained—by powerful work of Borcherds.

1.6 Monster Module

- Frenkel–Lepowsky–Meurman (and Borcherds): there exists a vertex operator algebra $V^\natural$ such that $\mathrm{Aut}(V^\natural) \simeq \mathbb{M}$ and $\mathrm{tr}\left(q^{L(0)-\frac{c}{24}}|V^\natural\right) = j - 744$.
- Frenkel–Lepowsky–Meurman conjecture: $V^\natural$ is the unique self-dual (i.e. holomorphic) VOA of rank 24 such that $L(0)v = v$ implies $v = 0$.
- Borcherds used $V^\natural$ to construct a generalized Kac–Moody algebra $\mathfrak{m}$, and used the denominator formula for $\mathfrak{m}$ to verify that

$$T_g(\tau) = \mathrm{tr}\left(gq^{L(0)-\frac{c}{24}}|V^\natural\right). \tag{1.9}$$

This confirms the Thompson–Conway–Norton conjecture.

1.7 Super Moonshine

- In string theoretic terms, $V^\natural$ corresponds to the compactification of the 26-dimensional bosonic string on $\left(\mathbb{R}^{24}/\text{Leech}\right)/\{\pm 1\}$.
- The critical dimension of the superstring is 10, and $10 - 2 = 8$. So what about compactifications of the 10-dimensional superstring on $\mathbb{Z}/2$-orbifolds of 8-dimensional tori?
- Frenkel suggested to consider the VOSA $V^{s\natural}$ corresponding to the compactification of the 10-dimensional superstring on the orbifold $\left(\mathbb{R}^8/E_8\right)/\{\pm 1\}$.
- D (2006), D–Mack-Crane (2015): $V^{s\natural}$ is the unique self-dual VOSA of rank 12 such that $L(0)v = \frac{1}{2}v$ implies $v = 0$.
- D–Mack-Crane (2015): the *Conway group* $Co_0 := \text{Aut(Leech)}$ acts naturally on $V^{s\natural}$ and for every $g \in Co_0$ the trace function

  $$T^s_g(\tau) := \operatorname{tr}\left(g(-1)^F q^{L(0)-\frac{c}{24}} | V^{s\natural}\right) \tag{1.10}$$

  is a principal modulus for a genus zero group $\Gamma^s_g < SL_2(\mathbb{R})$.
- D–Mack-Crane (2015): the Conway group also acts naturally on the unique canonically twisted module (i.e. Ramond sector) $V^{s\natural}_{\text{tw}}$ for $V^{s\natural}$, and for every $g \in Co_0$ the trace function

  $$T^s_{g,\text{tw}}(\tau) := \operatorname{tr}\left(g(-1)^F q^{L(0)-\frac{c}{24}} | V^{s\natural}_{\text{tw}}\right) \tag{1.11}$$

  is either constant, or a principal modulus for a genus zero group $\Gamma^s_{g,\text{tw}} < SL_2(\mathbb{R})$.

1.8 Genus Zero Problem

- The genus zero problem is to *explain* the genus zero property of monstrous and Conway moonshine.
- Conformal invariance explains, at the physical level, why VOAs have modular invariant partition functions. (This was proven rigorously by Zhu in 1996). But most VOAs have partition functions that are not principal moduli.
- Is there a physical setup for which the (twisted) partition functions will manifestly be principal moduli?
- To explain the genus zero property it should incorporate the (S)CFTs corresponding to $V^\natural$ and $V^{s\natural}$.
- D–Frenkel (2011): 3d quantum gravity, connected to CFT via the AdS/CFT correspondence, should provide a setting in which twisted partition functions are manifestly principal moduli. (Cf. Rademacher sums.)

2 Umbral Moonshine

2.1 K3 Surfaces

- A *(complex) K3 surface* is a compact connected two-dimensional complex manifold with

$$\Omega_X^2 \simeq \mathcal{O}_X, \tag{2.1}$$

$$H^1(X, \mathcal{O}_X) = 0. \tag{2.2}$$

- Equivalently, a K3 surface is a choice of complex structure on the *Fermat quartic*

$$\left\{X^4 + Y^4 + Z^4 + W^4 = 0\right\} \subset \mathbb{P}^3(\mathbb{C}). \tag{2.3}$$

- For X a K3 surface

$$\chi(X) = \operatorname{rank} H^*(X, \mathbb{Z}) = 24. \tag{2.4}$$

- A K3 surface admits a nowhere vanishing holomorphic 2-form. An automorphism that acts trivially on such a form is called *symplectic.*
- Siu (1983): Every K3 surface is Kähler (actually hyperkähler). So K3 surfaces are Calabi–Yau manifolds.

2.2 Mathieu Groups

- The *Golay code* is the unique self-dual doubly even linear binary code of length 24 with no words of weight 4.
- The *largest Mathieu group* M_{24} is the automorphism group of the Golay code.
- M_{24} is a 5-transitive subgroup of S_{24}.
- M_{23} denotes the stabilizer in M_{24} of a point.
- Mukai (1988): a finite group acts faithfully by symplectic automorphisms on a K3 surface if and only if it is isomorphic to a subgroup of M_{23} that has 5 or more orbits in its action on 24 points.

2.3 Elliptic Genera

- Calabi–Yau manifolds are candidate consistent geometric backgrounds for superstrings.
- Non-linear sigma models with Calabi–Yau target govern string dynamics in such theories.
- The *(physical) elliptic genus* of a non-linear sigma model with Calabi–Yau target X is

$$EG_X(\tau,z) := \operatorname{tr}\left((-1)^{F_L+F_R} y^{J_L(0)} q^{L_L(0)-\frac{c_L}{24}} \bar{q}^{L_R(0)-\frac{c_R}{24}} | \mathcal{H}_{\mathrm{RR}}\right), \tag{2.5}$$

  where $\mathcal{H}_{\mathrm{RR}}$ is the Ramond-Ramond sector of an associated $N=(2,2)$ SCFT, and $q := e^{2\pi i\tau}$ and $y := e^{2\pi i z}$.

- For X Calabi–Yau, EG_X is a *weak Jacobi form* of weight 0 and index $m = \frac{1}{2}\dim(X)$ for $SL_2(\mathbb{Z})$. This means that

$$EG_X\left(\frac{a\tau+b}{c\tau+d}, \frac{z}{c\tau+d}\right) e^{-2\pi i m \frac{cz^2}{c\tau+d}} = EG_X(\tau,z) \tag{2.6}$$

  for $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in SL_2(\mathbb{Z})$, there exist holomorphic functions $h_r : \mathbb{H} \to \mathbb{C}$ for r mod $2m$ such that

$$EG_X(\tau,z) = \sum_{r \bmod 2m} h_r(\tau)\theta_{m,r}(\tau,z) \tag{2.7}$$

  where

$$\theta_{m,r}(\tau,z) := \sum_{\ell = r \bmod 2m} q^{\frac{\ell^2}{4m}} y^{\ell} \tag{2.8}$$

  is a theta function for $A_1(m) = \sqrt{2m}\mathbb{Z}$, and $\tau \mapsto EG_X(\tau,z)$ is bounded as $\Im(\tau) \to \infty$, for all $z \in \mathbb{C}$.

- We also have $EG_X(\tau,0) = \chi(X)$.

2.4 Mathieu Moonshine

- The elliptic genus of a K3 surface is the unique weak Jacobi form $\phi(\tau, z)$ of weight 0 and index 1 for $SL_2(\mathbb{Z})$ such that $\phi(\tau, 0) = 24$.
- A hyperkähler structure equips the SCFT associated to a K3 surface with $N = (4, 4)$ supersymmetry, so we may decompose the K3 elliptic genus into characters of the (small) $N = 4$ superconformal algebra.

$$EG_X = 20 \operatorname{ch}_{\frac{1}{4},0} - 2 \operatorname{ch}_{\frac{1}{4},\frac{1}{2}} + \sum_{n \geq 1} A(n - \tfrac{1}{8}) \operatorname{ch}_{n+\frac{1}{4},\frac{1}{2}} \tag{2.9}$$

- Eguchi–Ooguri–Tachikawa (2010): $A(n - \frac{1}{8})$ is twice the dimension of an irreducible representation of M_{24}, for $1 \leq n \leq 5$.
- Gannon (2012): there exists a graded M_{24}-module $K = \bigoplus_{n \geq 1} K_{n-\frac{1}{8}}$ such that for $g \in M_{24}$ the function

$$\phi_g := (\chi(g) - 4) \operatorname{ch}_{\frac{1}{4},0} - 2 \operatorname{ch}_{\frac{1}{4},\frac{1}{2}} + \sum_{n \geq 1} \operatorname{tr}(g | K_{n-\frac{1}{8}}) \operatorname{ch}_{n+\frac{1}{4},\frac{1}{2}} \tag{2.10}$$

  is a weak Jacobi form of weight 0 and index 1 for $\Gamma_0(o(g))$, where $\chi(g)$ is the number of fixed points of g in the natural action on 24 points.
- There is no known M_{24}-invariant VOA or VOA-like structure on K (but $V^{s\natural}$ comes close to providing one).
- M_{24} has elements of order 11, 14, 15, and 23, but the corresponding $\Gamma_0(o(g))$ have genus greater than zero. Is there no genus zero property for Mathieu moonshine?

2.5 Mock Modularity

- The character $\mathrm{ch}_{n+\frac{1}{4},\frac{1}{2}}(\tau,z)$ is (essentially) modular, but $\mathrm{ch}_{\frac{1}{4},0}$ and $\mathrm{ch}_{\frac{1}{4},\frac{1}{2}}$ are not.
- As a consequence,

$$H^{(2)}(\tau) := -2q^{-\frac{1}{8}} + \sum_{n\geq 1} A(n-\tfrac{1}{8})q^{n-\frac{1}{8}} \tag{2.11}$$

  is a *mock modular form* of weight $\frac{1}{2}$ for $SL_2(\mathbb{Z})$ with *shadow* $\eta(\tau)^3 = q^{\frac{1}{8}}\prod_{n\geq 1}(1-q^n)^3$.
- This means that

$$\epsilon(\gamma)^3 H^{(2)}(\gamma\tau)(c\tau+d)^{-\frac{1}{2}} = H^{(2)}(\tau) + C\int_{-\gamma^{-1}\infty}^{\infty}(\tau+\tau')^{-\frac{1}{2}}\overline{\eta(-\overline{\tau'})^3}\mathrm{d}\tau' \tag{2.12}$$

  for some constant C (independent of γ), where (c,d) is the bottom row of γ and ϵ denotes the multiplier system for $\eta(\tau)$.
- Compare: a mock modular form of weight 0 for Γ with shadow g is a holomorphic function $f:\mathbb{H}\to\mathbb{C}$ such that

$$f(\gamma\tau) = f(\tau) + C\int_{-\gamma^{-1}\infty}^{\infty}\overline{g(-\overline{\tau'})}\mathrm{d}\tau' \tag{2.13}$$

  for all $\gamma\in\Gamma$. This is an *abelian integral* in the classical sense. In this case the shadow should be a cusp form of weight 2.
- Set $\theta^1_{m,r}(\tau) := \frac{1}{2\pi i}\frac{\mathrm{d}}{\mathrm{d}z}\theta_{m,r}(\tau,z)|_{z=0}$. Since $\eta(\tau)^3 = \pm\theta^1_{2,\pm1}(\tau)$ it follows that

$$\phi^{(2)}(\tau,z) := H^{(2)}(\tau)\theta_{2,-1}(\tau,z) - H^{(2)}(\tau)\theta_{2,1}(\tau,z) \tag{2.14}$$

  is a *(weak) mock Jacobi form* for $SL_2(\mathbb{Z})$ of weight 1 and index 2.
- The shadow of $\phi^{(2)}$ is the *skew-holomorphic* Jacobi form

$$\sum_{r \bmod 4}\overline{\theta^1_{2,r}(\tau)}\theta_{2,r}(\tau,z) = \overline{\eta(\tau)^3}(\theta_{2,1}(\tau,z)-\theta_{2,-1}(\tau,z)). \tag{2.15}$$

  of weight 2 and index 2.

2.6 Theta Series and Transcendence

- Let $J^{\mathrm{wh}}_{k,m}$ be the space of weakly holomorphic Jacobi forms of weight k and index m, let $\mathbb{J}^{\mathrm{wh}}_{k,m}$ denote weakly holomorphic mock Jacobi forms of weight k and index m, and write $S^{\mathrm{sk}}_{k,m}$ for cuspidal skew-holomorphic Jacobi forms of weight k and index m. Then we have a short exact sequence

$$0 \to J^{\mathrm{wh}}_{k,m} \to \mathbb{J}^{\mathrm{wh}}_{k,m} \to S^{\mathrm{sk}}_{3-k,m} \to 0 \tag{2.16}$$

  where the third arrow is the shadow map.

- We have

$$S^{\mathrm{sk}}_{2,m} = T^{\mathrm{sk}}_{2,m} \oplus P^{\mathrm{sk}}_{2,m} \tag{2.17}$$

  where $T^{\mathrm{sk}}_{2,m}$ consists of the forms whose theta coefficients are unary theta series of weight $\frac{3}{2}$ (i.e. linear combinations of the $\theta^{1}_{m,r}$), and $P^{\mathrm{sk}}_{2,m}$ is the orthogonal complement of $T^{\mathrm{sk}}_{2,m}$ with respect to the Petersson inner product.

- General expectation: a mock Jacobi form of weight 1 and index m has transcendental Fourier coefficients unless its shadow lies in $T^{\mathrm{sk}}_{2,m}$.

2.7 Skoruppa–Zagier and Shimura

- Skoruppa–Zagier proved the existence of (Hecke-module) embeddings

$$P^{\mathrm{sk}}_{2,m} \hookrightarrow S_2(\Gamma_0(m))^- \tag{2.18}$$

  where $S_2(\Gamma_0(m))^-$ denotes the space of cusp forms of weight 2 for $\Gamma_0(m)$ that are anti-invariant under the Fricke involution $\tau \mapsto -\frac{1}{m\tau}$.

- Let $\mathrm{Ex}(m)$ denote the group of exact divisors of m (i.e. $e|m$ but $\gcd(e, \frac{m}{e}) = 1$) with group structure $e * e' := \frac{ee'}{\gcd(e,e')^2}$.
- Then $\mathrm{Ex}(m)$ acts naturally on $S_2(\Gamma_0(m))$, $P^{\mathrm{sk}}_{2,m}$, $\mathbb{J}^{\mathrm{wh}}_{1,m}$, &c.
- Let $\alpha : \mathrm{Ex}(m) \to \{\pm 1\}$ be a character such that $\alpha(m) = -1$. Then (2.18) can be refined to

$$P^{\mathrm{sk},\alpha}_{2,m} \hookrightarrow S_2(\Gamma_0(m))^\alpha \tag{2.19}$$

  where

$$P^{\mathrm{sk},\alpha}_{2,m} := \left\{ \varphi \in P^{\mathrm{sk}}_{2,m} \mid \varphi|e = \alpha(e)\varphi \text{ for } e \in \mathrm{Ex}(m) \right\}, \tag{2.20}$$

  and $S_2(\Gamma_0(m))^\alpha$ is defined similarly.

2.8 Umbral Moonshine

- Say that $\phi \in \mathbb{J}^{\mathrm{wh}}_{k,m}$ is *optimal* if $h_r(\tau) = O(q^{-\frac{1}{4m}})$ for all r when $\phi = \sum_{r \bmod 2m} h_r \theta_{m,r}$.
- Given a character α for $\mathrm{Ex}(m)$ write $\mathbb{J}^{\mathrm{opt},\alpha}_{k,m}$ for the space of optimal weakly holomorphic mock Jacobi forms of weight k and index m that transform under $\mathrm{Ex}(m)$ according to α.
- Cheng-D (2016): if α is a character of $\mathrm{Ex}(m)$ such that $\alpha(m) = -1$ and $\phi \in \mathbb{J}^{\mathrm{opt}}_{1,\alpha}$ then there exists C such that $C\phi$ has algebraic Fourier coefficients if and only if the genus of $\Gamma_0(m) + e, f, \cdots$ is zero, where $\{1, e, f, \cdots\}$ is the kernel of α.
- Cheng-D (2016): If $\alpha(m) = -1$ and the genus of $\Gamma_0(m) + \ker(\alpha)$ is zero then there exists a unique, up to scale, $\phi \in \mathbb{J}^{\mathrm{opt}}_{1,\alpha}$ and it can be chosen to have rational integer Fourier coefficients.
- The mock Jacobi forms arising from genus zero groups in this way are precisely the mock Jacobi forms of umbral moonshine.
- In particular, Mathieu moonshine satisfies a genus zero property: the trace function for elements of order 11 exists *because* $\Gamma_0(22) + 11$ has genus zero. The genus zero group $\Gamma_0(46) + 23$ is responsible for the trace function for elements of order 23.
- All of Ramanujan's mock theta functions, discovered by him almost a 100 years earlier, appear as theta-coefficients of these optimal mock Jacobi forms.

Figure 1: Super blue blood moon over the Acropolis of Athens on 31 January 2018 (AP)

3 New Directions

3.1 Atkin–Lehner Operators

- Recall that the *exact divisors* of m

  $$\mathrm{Ex}(m) := \left\{e > 0 \mid e|m \text{ and } \gcd(e, \tfrac{m}{e}) = 1\right\} \tag{3.1}$$

  form a group when equipped with the multiplication rule

  $$e * f := \frac{ef}{\gcd(e,f)^2}. \tag{3.2}$$

- This is a 2-*group* because $e * e = \frac{e^2}{\gcd(e,e)^2} = 1$ for all $e \in \mathrm{Ex}(m)$.
- For each $e \in \mathrm{Ex}(m)$ choose $a, b, c, d \in \mathbb{Z}$ such that $ade - bc\frac{m}{e} = 1$, and set

  $$W_e := \frac{1}{\sqrt{e}} \begin{pmatrix} ae & b \\ cm & de \end{pmatrix}. \tag{3.3}$$

- Let $N(\Gamma_0(m))$ be the normalizer of $\Gamma_0(m)$ in $SL_2(\mathbb{R})$. Then the association $e \mapsto W_e$ defines an embedding

  $$\mathrm{Ex}(m) \hookrightarrow N(\Gamma_0(m))/\Gamma_0(m). \tag{3.4}$$

- So $\mathrm{Ex}(m)$ acts naturally, via the matrices W_e, on modular forms for $\Gamma_0(m)$.
- The embedding (3.4) is surjective when m is squarefree.
- The *Fricke involution* for $\Gamma_0(m)$ is

  $$W_m := \frac{1}{\sqrt{m}} \begin{pmatrix} 0 & -1 \\ m & 0 \end{pmatrix} : \tau \mapsto -\frac{1}{m\tau} \tag{3.5}$$

- Given a subgroup $K = \{1, e, f, \ldots\} < \mathrm{Ex}(m)$ write

  $$\Gamma_0(m) + K \;\text{ or }\; \Gamma_0(m) + e, f, \ldots \;\text{ or }\; m + e, f, \ldots \tag{3.6}$$

  for the subgroup of $SL_2(\mathbb{R})$ generated by $\Gamma_0(m)$ and the W_e for $e \in K$.

3.2 Cusp Forms

- Call a holomorphic function $F : \mathbb{H} \to \mathbb{C}$ a *cusp form* of weight 2 for $\Gamma_0(m)$ if

$$F(\tau)\mathrm{d}\tau = F(\tau')\mathrm{d}\tau' \tag{3.7}$$

when $\tau' = \frac{a\tau+b}{c\tau+d}$ and $ad - bc = 1$ and $c \equiv 0 \bmod m$, and if

$$F(\tau') \to 0 \text{ as } \Im(\tau) \to \infty \tag{3.8}$$

when $\tau' = \frac{a\tau+b}{c\tau+d}$ and $ad - bc = 1$.

- The cusp forms of weight 2 for $\Gamma_0(m)$ are in natural correspondence with the holomorphic 1-forms on the level m *modular curve*

$$X_0(m) := \Gamma_0(m)\backslash(\mathbb{H} \cup \mathbb{P}^1(\mathbb{Q})). \tag{3.9}$$

- Let $S_2(\Gamma_0(m))$ denote the space of cusp forms of weight 2 for $\Gamma_0(m)$. Then

$$\dim S_2(\Gamma_0(m)) = \mathrm{genus}(X_0(m)). \tag{3.10}$$

- Let $\widehat{\mathrm{Ex}}(m) := \hom(\mathrm{Ex}(m), \mathbb{C}^*)$ be the group of characters of $\mathrm{Ex}(m)$.
- Given $\alpha \in \widehat{\mathrm{Ex}}(m)$ define

$$S_2(\Gamma_0(m))^\alpha := \{F \in S_2(\Gamma_0(m)) \mid F|W_e = \alpha(e)F \text{ for all } e \in \mathrm{Ex}(m)\}, \tag{3.11}$$

$$X_0(m) + \ker(\alpha) := (\Gamma_0(m) + \ker(\alpha))\backslash(\mathbb{H} \cup \mathbb{P}^1(\mathbb{Q})). \tag{3.12}$$

- Then we have

$$S_2(\Gamma_0(m)) = \bigoplus_{\alpha \in \widehat{\mathrm{Ex}}(m)} S_2(\Gamma_0(m))^\alpha, \tag{3.13}$$

$$\dim S_2(\Gamma_0(m))^\alpha = \mathrm{genus}(X_0(m) + \ker(\alpha)). \tag{3.14}$$

3.3 Penumbral Moonshine

- We have explained that the mock modular forms of umbral moonshine are the optimal mock Jacobi forms of weight 1 with integer Fourier coefficients, and these are classified by the 34 genus zero groups $\Gamma_0(m)+\ker(\alpha)$ where $\alpha \in \widehat{\mathrm{Ex}}(m)$ is such that $\alpha(m)=-1$.

$$2,\ \ 3,\ \ 4,\ \ 5,\ \ 6+2,\ \ 6+3,\ \ 7,\ \ 8,\ \ 9,\ \ \ldots,\ \ 78+6,26,39. \tag{3.15}$$

- What about the 84 genus zero groups $\Gamma_0(m)+\ker(\alpha)$ with $\alpha(m)=1$?

$$1,\ \ 2+2,\ \ 3+3,\ \ 4+4,\ \ 5+5,\ \ 6+2,3,6,\ \ 6+6,\ \ 7+7,\ \ \ldots,\ \ 119+7,17,119. \tag{3.16}$$

- According to Ogg's result on supersingular elliptic curves $\Gamma_0(p)+p$, for p prime, has genus zero exactly when p divides the order of the Monster.
- For umbral moonshine we considered the sequence

$$0 \to J^{\mathrm{wh},\alpha}_{1,m} \to \mathbb{J}^{\mathrm{wh},\alpha}_{1,m} \to S^{\mathrm{sk},\alpha}_{2,m} \to 0. \tag{3.17}$$

- That sequence vanishes identically when $\alpha(m)=1$ because for $\phi \in \mathbb{J}^{\mathrm{wh}}_{k,m}$ and $\varphi \in \mathbb{J}^{\mathrm{ws}}_{k,m}$ (weakly skew-holomorphic) we have

$$\begin{aligned}(\phi|W_m)(\tau,z) &= \phi(\tau,-z) = (-1)^k\phi(\tau,z),\\ (\varphi|W_m)(\tau,z) &= \varphi(\tau,-z) = (-1)^{k+1}\varphi(\tau,z).\end{aligned} \tag{3.18}$$

- So for Fricke extensions of $\Gamma_0(m)$ we should consider

$$0 \to J^{\mathrm{ws},\alpha}_{1,m} \to \mathbb{J}^{\mathrm{ws},\alpha}_{1,m} \to S^{\alpha}_{2,m} \to 0. \tag{3.19}$$

3.4 Rational Skew-Holomorphic Mock Jacobi Forms

- Recall: a mock Jacobi form of weight 1 is expected to have transcendental Fourier coefficients unless its shadow is of theta type.
- Similar to before we have an orthogonal decomposition

  $$S^{\alpha}_{2,m} = T^{\alpha}_{2,m} \oplus P^{\alpha}_{2,m}, \tag{3.20}$$

  where $T^{\alpha}_{2,m}$ denotes the cusp forms of theta type, and Skoruppa–Zagier provide a (Hecke-equivariant) embedding

  $$P^{\alpha}_{2,m} \hookrightarrow S_2(m)^{\alpha} \tag{3.21}$$

  when $\alpha(m) = 1$.
- So the Fricke genus zero groups $\Gamma_0(m) + \ker(\alpha)$ should give rise to distinguished rational skew-holomorphic mock Jacobi forms, similar to the non-Fricke ($\alpha(m) = -1$) case.
- Surprise: we have $T^{\alpha}_{2,m} = 0$ when $\alpha(m) = 1$.
- So optimal (i.e. minimal growth) skew-holomorphic mock Jacobi forms with rational coefficients should actually be modular.
- D–Harvey–Rayhaun (to appear): if α is a character of $\mathrm{Ex}(m)$ such that $\alpha(m) = 1$ and the genus of $\Gamma_0(m)+\ker(\alpha)$ is zero then $\mathbb{J}^{\mathrm{ws},\alpha}_{1,m} = J^{\mathrm{ws},\alpha}_{1,m}$. That is, every weakly skew-holomorphic mock Jacobi form of weight 1 for α is modular.

3.5 Thompson Moonshine

- Thompson, Smith (1976): there exists a finite simple group *Th* of order

$$2^{15}.3^{10}.5^3.7^2.13.19.31 \approx 9 \times 10^{16} \tag{3.22}$$

which acts by automorphisms on a certain self-dual (unimodular) lattice of rank 248.

- Harvey–Rayhaun conjecture (2015): a certain weight $\frac{1}{2}$ modular form for $\Gamma_0(4)$

$$\mathcal{F}_3(\tau) = 2q^{-3} + 248 + 54000q^4 - 171990q^5 + \dots \tag{3.23}$$

should be interpreted as the graded dimension of a (non-trivial) graded module for *Th*.

- Griffin–Mertens (2016): the Harvey–Rayhaun conjecture is true.
- The coefficients of $\mathcal{F}_3(\tau) = \sum c(n)q^n$ are supported on exponents n such that $n \equiv 0, 1 \bmod 4$.
- For $j \in \{0,1\}$ let $f^j(\tau) := \sum_{n\equiv j \bmod 4} c(n)q^{\frac{n}{4}}$. Then

$$\varphi^{(1,-3)}(\tau,z) := \overline{f^0(\tau)}\theta_{1,0}(\tau,z) + \overline{f^1(\tau)}\theta_{1,1}(\tau,z) \tag{3.24}$$

is an optimal element of $\mathbb{J}^{\mathrm{ws},\alpha}_{1,m} = J^{\mathrm{ws},\alpha}_{1,m}$ for $m = 1$ and $\alpha \equiv 1$.

- Thompson moonshine of Harvey–Rayhaun is the first example of *penumbral moonshine.*
- D–Harvey–Rayhaun (to appear): a detailed description of penumbral moonshine.

3.6 Another Example

- For $m = 6$ and $\ker(\alpha) = \{1, 6\}$ we obtain

$$q^{-\frac{23}{24}} - q^{\frac{1}{24}} + 196883q^{\frac{25}{24}} + 21296876q^{\frac{49}{24}} + 842609326q^{\frac{73}{24}} + 19360062527q^{\frac{97}{24}} + \dots \quad (3.25)$$

- Do you recognize these numbers? Can you relate them to objects from the first lecture?

3.7 Singular Moduli

- A particular value $j(\tau_0)$ is called *singular* if the endomorphism ring of the corresponding elliptic curve $\mathbb{C}/(\mathbb{Z}\tau_0 + \mathbb{Z})$ has rank 2 over $\mathbb{Z}$.
- The value $j(\tau_0)$ is singular exactly when τ_0 is a quadratic irrational.
- The coefficients of $\mathcal{F}_3$ can be realized as linear combinations of singular values with fixed discriminants.
- For example, $Q_1 = x^2 - xy + 4y^2$ and $Q_2 = 2x^2 - xy + 2y^2$ represent the two $SL_2(\mathbb{Z})$-equivalence classes of quadratic forms of discriminant -15.
- Corresponding quadratic irrationalities in $\mathbb{H}$ are $\alpha_1 = \frac{1}{2} + \frac{\sqrt{15}}{2}i$ and $\alpha_2 = \frac{1}{4} + \frac{\sqrt{15}}{4}i$.
- We have

$$j(\alpha_1) = -\frac{191025}{2} - \frac{85995}{2}\sqrt{5}, \tag{3.26}$$

$$j(\alpha_2) = -\frac{191025}{2} + \frac{85995}{2}\sqrt{5}, \tag{3.27}$$

so

$$\frac{2}{\sqrt{5}}(j(\alpha_1) - j(\alpha_2)) = -2 \times 85995 = c(5). \tag{3.28}$$

- The Thompson group has a dual pair of irreducible representations of dimension 85995.
- Replacing j with a principal modulus of a genus zero of the form $\Gamma_0(m) + \ker(\alpha)$ (for any $\alpha \in \widehat{\mathrm{Ex}}(m)$) we can obtain analogous *trace formulas* for all the functions of umbral and penumbral moonshine.

3.8 Pushing Down

- We just saw how modular forms of integer weight can be lifted, via traces, to (mock) Jacobi forms of integer weight.
- We may push down from Jacobi forms to modular forms using Borcherds products.
- For $\mathcal{F}_3(\tau) = \sum_n c(n)q^n$ we have

$$q^{-\frac{1}{3}} \prod_{n>0} (1-q^n)^{c(n^2)} = T_{3C}(\tfrac{1}{3}\tau)^2 \eta(\tau)^{248} \tag{3.29}$$

  where T_{3C} is the function attached by monstrous moonshine to the largest conjugacy class of elements of order 3 in $\mathbb{M}$.
- Note that $T_{3C}\left(\frac{1}{3}\tau\right)^3 = j(\tau)$, and the centralizer of a $3C$ element in $\mathbb{M}$ is $\mathbb{Z}/3\mathbb{Z} \times Th$.
- So penumbral moonshine for Th enriches the moonshine that Th inherits from the monster.
- Similar product formulas can be obtained for all the functions of umbral and penumbral moonshine using work of Bruinier–Ono, but generally the modular forms arising are meromorphic with poles in $\mathbb{H}$.

3.9 Quadratic Forms

- Let us consider *binary quadratic forms* $Q(x,y) = Ax^2 + Bxy + Cy^2$ for $A, B, C \in \mathbb{Z}$.
- The modular group $SL_2(\mathbb{Z})$ acts naturally on these, via

$$\left(Q| \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)\right)(x,y) := Q(ax+by, cx+dy). \tag{3.30}$$

- The *discriminant* $D := B^2 - 4AC$ is $SL_2(\mathbb{Z})$-invariant so consider

$$\mathscr{Q}_D := \left\{Q(x,y) = Ax^2 + Bxy + Cy^2 \mid A > 0,\, D = B^2 - 4AC\right\}. \tag{3.31}$$

- Restrict to $D < 0$ since then $Q \in \mathscr{Q}_D$ is positive definite (and much less is known for $D > 0$).
- For $D < 0$ the *Hurwitz class number* of D is

$$H(D) := 2 \sum_{Q \in \mathscr{Q}_D/\Gamma} \frac{1}{\#\Gamma_Q} \tag{3.32}$$

where $\Gamma = SL_2(\mathbb{Z})$ and $\Gamma_Q := \{\gamma \in \Gamma \mid Q|\gamma = Q\}$.

- The first few values of $H(D)$ are as follows.

D	-3	-4	-7	-8	-11	-12	-15
$H(D)$	$\frac{1}{3}$	$\frac{1}{2}$	1	1	1	$\frac{4}{3}$	2

- Zagier (1975): the generating function $\mathscr{H}(\tau) := -\frac{1}{12} + \sum_{D<0} H(D)q^{|D|}$ is a mock modular form of weight $\frac{3}{2}$ for $\Gamma_0(4)$ with shadow $\theta(\tau) := \sum_n q^{n^2}$.
- If we set $f^j(\tau) := \sum_{D \equiv j \bmod 4} H(D)q^{\frac{|D|}{4}}$ then

$$\phi^{(1,0)}(\tau,z) := \overline{f^0(\tau)}\theta_{1,0}(\tau,z) + \overline{f^1(\tau)}\theta_{1,1}(\tau,z) \tag{3.33}$$

is a skew-holomorphic Jacobi form of weight 2 and index 1 for $SL_2(\mathbb{Z})$.

3.10 O'Nan Moonshine

- Let $J^{ON}(\tau)$ denote the unique $SL_2(\mathbb{Z})$-invariant holomorphic function on $\mathbb{H}$ such that $J^{ON}(\tau) = q^{-2} - q^{-1} + O(q)$ as $\Im(\tau) \to \infty$.
- For $D < 0$ set

$$a(D) := -\sum_{Q \in \mathcal{Q}_D/\Gamma} \frac{J^{ON}(\alpha_Q)}{\#\Gamma_Q} \tag{3.34}$$

  where $\Gamma = SL_2(\mathbb{Z})$ and α_Q is the unique root of $Q(x,1)$ in $\mathbb{H}$.
- Then

$$F^{ON}(\tau) := -q^{-4} + 2 + \sum_{D<0} a(D) q^{|D|} \tag{3.35}$$

  is a weakly holomorphic modular form of weight $\frac{3}{2}$ for $\Gamma_0(4)$. (We can also regard it as a weakly holomorphic Jacobi form of weight 2 and index 1 for $SL_2(\mathbb{Z})$.)
- We have $a(-3) = 26752$.
- O'Nan (1976): There exists a finite simple group ON of order

$$2^9.3^4.5.7^3.11.19.31 \approx 5 \times 10^{11} \tag{3.36}$$

  and it admits an irreducible representation of dimension 26752.
- D–Mertens–Ono (2017): there is a virtual graded ON-module $W = \bigoplus W_D$ whose graded dimension is given by F^{ON}.
- In the next lecture we will explain how the ON-module W realizes the O'Nan group as a source of hidden symmetry for quadratic forms and elliptic curves.
- Griess (1982): the O'Nan group is not involved in the monster (i.e. not a quotient of any subgroup of the monster).

4 Arithmetic

4.1 Modularity of Elliptic Curves

- Recall that an elliptic curve over $\mathbb{Q}$ is an equation $y^2 = x^3 + Ax + B$ with $A, B \in \mathbb{Z}$ such that $4A^3 + 27B^2 \neq 0$.
- Write $E(\mathbb{Q})$ for the set of rational solutions to an elliptic curve E.
- Mordell (1922): $E(\mathbb{Q}) \simeq \mathbb{Z}^r \oplus E(\mathbb{Q})_{\mathrm{tor}}$ for some non-negative integer $r = r_E$, and $\#E(\mathbb{Q})_{\mathrm{tor}}$ is finite. Call r the *rank* of E.
- To study r_E and $E(\mathbb{Q})_{\mathrm{tor}}$ we consider the *L-function*

  $$L_E(s) := \prod_p (1 - a_p p^{-s} + \varepsilon_p p^{1-2s})^{-1} \tag{4.1}$$

  where $a_p := p + 1 - \#E(\mathbb{F}_p)$ and ε_p is 0 or 1 according as p divides Δ or not.
- The modularity theorem (Taniyama, Shimura, Weil, Wiles, Taylor, &c.) states that $L_E(s)$ is the Mellin transform of a cuspidal modular form F of weight 2 for $\Gamma_0(N)$ for some N.

  $$L_E(s) = \frac{(2\pi)^s}{\Gamma(s)} \int_0^\infty F(it) t^{s-1} \mathrm{d}t \tag{4.2}$$

- The modularity theorem reveals (modular) hidden symmetry in E.

4.2 The Birch–Swinnerton-Dyer Conjecture

- The Birch–Swinnerton-Dyer conjecture connects r_E and $E(\mathbb{Q})_{\text{tor}}$ to the behavior of $L_E(s)$ near $s = 1$.
- The modularity theorem gives the only known general proof that $L_E(s)$ can be continued past $\Re(s) > \frac{3}{2}$.
- Weak Birch–Swinnerton-Dyer conjecture: $r = r_E$ is the minimum non-negative integer such that $L_E^{(r)}(1) \neq 0$.
- Kolyvagin (1990): (assuming modularity) if $L_E(1) \neq 0$ then $r = 0$, and if $L_E(1) = 0$ and $L'_E(1) \neq 0$ then $r = 1$.

4.3 Tate–Shafarevich Groups

- The *Tate–Shafarevich group* $\text{Ш}(E)$ encodes the failure of the local-to-global principle for computing $E(\mathbb{Q})$.

$$\text{Ш}(E) := \ker\left(H^1(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}), E(\overline{\mathbb{Q}})) \to \prod_p H^1(\mathrm{Gal}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p), E(\overline{\mathbb{Q}_p}))\right) \tag{4.3}$$

- Strong Birch–Swinnerton-Dyer conjecture:

$$\frac{L_E^{(r)}(1)}{r!\Omega_E} = \frac{c_E \# \text{Ш}(E)}{(\# E(\mathbb{Q})_{\mathrm{tor}})^2} \tag{4.4}$$

where $r = r_E$, and Ω_E and c_E are computable.

4.4 Selmer Groups

- Tate–Shafarevich groups are hard to compute.
- It is known that $Ш(E)$ is finite if $L_E(1) \neq 0$ or $L'_E(1) \neq 0$, but it is not known if $Ш(E)$ is finite in general.
- For each prime ℓ there is the more accessible ℓ-th *Selmer group* $\mathrm{Sel}_\ell(E)$, which satisfies

$$0 \to E(\mathbb{Q})/\ell E(\mathbb{Q}) \to \mathrm{Sel}_\ell(E) \to Ш(E)[\ell] \to 0, \tag{4.5}$$

where $Ш(E)[\ell]$ denotes the kernel of multiplication by ℓ on $Ш(E)$.

$$\mathrm{Sel}_\ell(E) := \ker\left(H^1(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}), E(\overline{\mathbb{Q}})[\ell]) \to \prod_p H^1(\mathrm{Gal}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p), E(\overline{\mathbb{Q}_p}))[\ell]\right) \tag{4.6}$$

4.5 Pariah Symmetry in Quadratic Forms

- An integer D is called a *discriminant* if it is the discriminant of a binary quadratic form, and a *fundamental discriminant* if it is 1 or the discriminant of a quadratic extension of $\mathbb{Q}$.
- The fundamental discriminants are the square-free numbers congruent to 1 modulo 4 together with the $D = 4d$ such that d is square-free and congruent to 2 or 3 modulo 4.
- Recall that

$$f^{ON}(\tau) = -q^{-4} + 2 + \sum_{D<0} a(D) q^{|D|} \tag{4.7}$$

denotes the graded dimension function of O'Nan moonshine. For $g \in ON$ define

$$f_g^{ON}(\tau) := -q^{-4} + 2 + \sum_{D<0} \mathrm{tr}(g|W_D) q^{|D|}. \tag{4.8}$$

- Duncan–Mertens–Ono (2017): Let $D < 0$ be a fundamental discriminant. If $D < -8$ is even then $-24H(D)$ is congruent to $a(D)$ modulo 16. If D is not a square modulo 3 then $-24H(D)$ is congruent to $a(D)$ modulo 9. If p is 5 or 7, and if D is not a square modulo p then $-24H(D)$ is congruent to $a(D)$ modulo p.

4.6 Generalized Class Numbers

- For N a positive integer define the *generalized Hurwitz class number*

$$H^{(N)}(D) := 2 \sum_{Q \in \mathscr{Q}_D^{(N)}/\Gamma_0(N)} \frac{1}{\#\Gamma_0(N)_Q} \tag{4.9}$$

where

$$\mathscr{Q}_D^{(N)} := \left\{ Q \mid A > 0,\, A \equiv 0 \bmod N,\, D = B^2 - 4AC \right\}. \tag{4.10}$$

- Then the generating function

$$\mathscr{H}^{(N)}(\tau) := -\frac{[\Gamma_0(1) : \Gamma_0(N)]}{12} + \sum_{D<0} H^{(N)}(D) q^{|D|} \tag{4.11}$$

is a mock modular form of weight $\frac{3}{2}$ for $\Gamma_0(4N)$.

4.7 Pariah Symmetry in Elliptic Curves

- For $D \in \mathbb{Z}$ define elliptic curves $E_{14} \otimes D$ and $E_{15} \otimes D$ as follows.

$$E_{14} \otimes D : \qquad y^2 = x^3 + 5805D^2x - 285714D^3 \tag{4.12}$$

$$E_{15} \otimes D : \qquad y^2 = x^3 - 12987D^2x - 263466D^3 \tag{4.13}$$

- Duncan–Mertens–Ono (2017): Let $D < 0$ be a fundamental discriminant. Suppose that D is congruent to 1 modulo 2 and is not a square modulo 7, and let g be a two-fold symmetry in the O'Nan group. Then $\mathrm{Sel}_7(E_{14} \otimes D)$ is non-trivial if and only if $a_g(D)$ is congruent to $3H(D) - 9H^{(2)}(D)$ modulo 7. Also, if $L_{E_{14}(D)}(1) \neq 0$ then $|Ш(E_{14} \otimes D)|$ is congruent to 0 modulo 7 if and only if $a_g(D)$ is congruent to $3H(D) - 9H^{(2)}(D)$ modulo 7.
- Duncan–Mertens–Ono (2017): Let $D < 0$ be a fundamental discriminant. Let $D < 0$ be a fundamental discriminant. Suppose that D is congruent to 1 modulo 3 and is not a square modulo 5, and let g be a three-fold symmetry in the O'Nan group. Then $\mathrm{Sel}_5(E_{15} \otimes D)$ is non-trivial if and only if $a_g(D)$ is congruent to $2H(D) - 4H^{(3)}(D)$ modulo 5. Also, if $L_{E_{15} \otimes D}(1) \neq 0$ then $|Ш(E_{15} \otimes D)|$ is congruent to 0 modulo 5 if and only if $a_g(D)$ is congruent to $2H(D) - 4H^{(3)}(D)$ modulo 5.

4.8 Modular Abelian Varieties

- In forthcoming work with M. Cheng and M. Mertens we formulate moonshine conjectures for certain modular abelian varieties.
- The modular form F corresponding to an elliptic curve E has symmetry beyond $\Gamma_0(N)$: it's an eigenvector for the action of the *Hecke operators* T_p, for $(p,N)=1$.

$$(F|T_p)(\tau) := F(p\tau) + \sum_{0\leq b<p} F\left(\frac{\tau+b}{p}\right) \tag{4.14}$$

- Such a *Hecke eigenform* F naturally defines a quotient A_F of the Jacobian $J_0(N) := \mathrm{Pic}^0(X_0(N))$ of the *modular curve* $X_0(N) := \Gamma_0(N)\backslash\widetilde{\mathbb{H}}$ of $\Gamma_0(N)$.

$$A_F := J_0(N)/I_F J_0(N) \tag{4.15}$$

$$0 \to I_F \to \mathbb{T} \to \mathrm{End}(\mathbb{C}F) \to 0 \tag{4.16}$$

$$\mathbb{T} = \langle T_p\rangle < \mathrm{End}(J_0(N)) \tag{4.17}$$

- (For X a ringed space, $\mathrm{Pic}^0(X)$ is the connected component of the identity in the group $H^1(X,\mathcal{O}_X^*)$ of invertible sheaves on X.)
- If F corresponds to E under modularity then E admits a surjective morphism from A_F with finite kernel.

$$0 \to \text{ finite} \to A_F \to E \to 0 \tag{4.18}$$

  (That is, E is *isogenous* to A_F.)
- The variety A_F is an elliptic curve exactly when the Fourier coefficients of F are integers.

$$F(\tau) = \sum_{n>0} c_F(n)e^{2\pi i\tau n},\ c_F(1)=1 \tag{4.19}$$

  In general the coefficients of a Hecke eigenform F are algebraic integers, and $\dim A_F$ is the size of the orbit of F under the action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on the $c_F(n)$.
- The A_F, and varieties isogenous to these, are what we have in mind when we speak of modular abelian varieties.

4.9 Cyclic Moonshine Conjectures

- Set $h_1(\tau) := 12\mathscr{H}(\tau) = -1 + O(q^3)$, and for N prime define

$$h_N(\tau) := \frac{12}{N^2-1}\left(N\mathscr{H}^{(N)}(\tau) - (N+1)\mathscr{H}(\tau)\right). \tag{4.20}$$

  Then $h_N(\tau) = -1 + O(q^3)$ has rational coefficients with bounded denominators.

- For $N > 3$ prime set

$$m_N := \begin{cases} \frac{N^2-1}{24} & \text{if } N \equiv 1 \bmod 4, \\ \frac{N^2-1}{12} & \text{if } N \equiv 3 \bmod 4. \end{cases} \tag{4.21}$$

- Lemma: m_N is the smallest positive integer such that $m_N h_N(\tau) \in \mathbb{Z}[[q]]$.
- For N prime let $F \in S_2(\Gamma_0(N))$ be a Hecke eigenform and set $n_F := \#A_F(\mathbb{Q})_{\mathrm{tor}}$. Mazur proved that n_F divides $\frac{N-1}{12}$, so n_F divides m_N.
- Cheng–D–Mertens conjecture (to appear): For N prime let $F \in S_2(\Gamma_0(N))$ be a Hecke eigenform and set $n_F := \#A_F(\mathbb{Q})_{\mathrm{tor}}$. Then there exists $f \in S_{\frac{3}{2}}(\Gamma_0(4N))_F$ such that

$$m_N h_N \equiv Nf \bmod n_F. \tag{4.22}$$

- Consequence: For N, F, n_F and f as above the assignment

$$\mathsf{g} \mapsto \mathscr{H}^{[F]}_{\mathsf{g}} := \begin{cases} \frac{m_N}{n_F} h_1 & \text{if } \mathsf{g} = \mathsf{e}, \\ \frac{m_N}{n_F} h_N - \frac{N}{n_F} f & \text{if } \mathsf{g} \neq \mathsf{e}, \end{cases} \tag{4.23}$$

  defines a graded (virtual) $\mathbb{Z}/N\mathbb{Z}$-module whose graded dimension function is $\frac{m_N}{n_F} h_1(\tau) = -\frac{m_N}{n_F} + O(q^3)$.

4.10 Arithmetic Application

- Take $N = 11$. Then $m_{11} = \frac{11^2-1}{12} = 10$. The only choice for F is $F(\tau) = \eta(\tau)^2\eta(11\tau)^2$.
- We have $A_F = E$ where E is defined by $y^2 = x^3 - 13392x - 1080492$. In this case $E(\mathbb{Q})_{\mathrm{tor}} \simeq \mathbb{Z}/5\mathbb{Z}$ so $n_F = 5$ and $\frac{m_N}{n_F} = 2$.
- For $\mathsf{g} \in \mathbb{Z}/11\mathbb{Z}$ we have

$$\mathscr{H}_{\mathsf{g}}^{[F]}(\tau) = \begin{cases} -2 + 8q^3 + 12q^4 + 24q^7 + 24q^8 + 24q^{11} + 32q^{12} + 48q^{15} + \dots & \text{if } \mathsf{g} = \mathsf{e}, \\ -2 - 3q^3 + q^4 + 2q^7 + 2q^8 + 2q^{11} - q^{12} - 7q^{15} + \dots & \text{if } \mathsf{g} \neq \mathsf{e}. \end{cases} \tag{4.24}$$

- Define $E \otimes D$ by $y^2 = x^3 - 13392D^2x - 1080492D^3$.
- Theorem: if $D < 0$ is the discriminant of a quadratic imaginary number field and if D is not a quadratic residue modulo 11 then $\mathrm{Sel}_5(E \otimes D) \neq \{0\}$ if and only if $H(D) \equiv 0 \bmod 5$.
- Example: $D = -15$ is not a quadratic residue modulo 11 and $H(-15) = 2$. The groups $(E \otimes D)(\mathbb{Q})$ and $Ш(E \otimes D)$ are both trivial so $\mathrm{Sel}_5(E \otimes D)$ is trivial. The coefficient of q^{15} in $2h_{11}$ is $-\frac{24}{5}$.
- Example: $D = -47$ is not a quadratic residue modulo 11 and $H(-47) = 5$. The group $(E \otimes D)(\mathbb{Q})$ has rank 2 so $\mathrm{Sel}_5(E \otimes D)$ is non-trivial. The coefficient of q^{47} in $2h_{11}$ is -12.
- The theorem was first obtained by Antoniadis–Kohnen (1986). Our conjecture furnishes counterparts for every optimal quotient of $J_0(N)$ with non-trivial torsion.

4.11 Class Number Mathieu Moonshine

- Moonshine for class numbers and modular abelian varieties is not restricted to prime levels.
- Cheng–D–Mertens (to appear): There exists a virtual graded M_{11}-module

  $$W^{\mathsf{M}_{11}} = \bigoplus_{D\leq 0} W_D^{\mathsf{M}_{11}} \tag{4.25}$$

  whose graded dimension function is $24\mathscr{H}(\tau) = -2 + O(q^3)$.
- Cheng–D–Mertens (to appear): There exists a virtual graded M_{23}-module

  $$W^{\mathsf{M}_{23}} = \bigoplus_{D\leq 0} W_D^{\mathsf{M}_{23}} \tag{4.26}$$

  whose graded dimension function is $48\mathscr{H}(\tau) = -4 + O(q^3)$.
- The M_{23}-module $W^{\mathsf{M}_{23}}$ interweaves the arithmetic of the quadratic twists $J_0(N) \otimes D$ for $N \in \{11, 14, 15, 23\}$.