Moonshine beyond the Monster

Michael H. Mertens
(joint work with M. Griffin and J. Duncan and K. Ono)

Max-Planck-Institut für Mathematik, Bonn

01 March, 2017
Hong Kong University

Table of Contents

Basic Definitions

Definition

Let G be a (finite) group and V a vector space over $\mathbb{C}$.

- $\rho : G \to \mathrm{GL}(V)$ homomorphism is called a representation of G.

Basic Definitions

Definition

Let G be a (finite) group and V a vector space over $\mathbb{C}$.

- $\rho : G \to \mathrm{GL}(V)$ homomorphism is called a representation of G.
- (V, ρ) is called a G-module.

Basic Definitions

Definition

Let G be a (finite) group and V a vector space over $\mathbb{C}$.

- $\rho : G \to \mathrm{GL}(V)$ homomorphism is called a representation of G.
- (V, ρ) is called a G-module.
- A subspace $U \leq V$ is called a G-submodule of V if $\rho(g)(U) \leq U$ for all $g \in G$.

Basic Definitions

Definition

Let G be a (finite) group and V a vector space over $\mathbb{C}$.

- $\rho : G \to \mathrm{GL}(V)$ homomorphism is called a representation of G.
- (V, ρ) is called a G-module.
- A subspace $U \leq V$ is called a G-submodule of V if $\rho(g)(U) \leq U$ for all $g \in G$.
- V is called simple, if it has no non-trivial G-submodules. The associated representation is called irreducible.

Definition

Let G be a (finite) group and V a vector space over $\mathbb{C}$.

- $\rho : G \to \mathrm{GL}(V)$ homomorphism is called a representation of G.
- (V, ρ) is called a G-module.
- A subspace $U \leq V$ is called a G-submodule of V if $\rho(g)(U) \leq U$ for all $g \in G$.
- V is called simple, if it has no non-trivial G-submodules. The associated representation is called irreducible.
- $\chi : G \to \mathbb{C}$, $g \mapsto \chi(g) := \mathrm{tr}(g|V) := \mathrm{tr}(\rho(g))$ is called the character associated to ρ (or (V, ρ)).

Basic facts

Proposition

- Every G-module has a decomposition into simple G-modules.

Basic facts

Proposition

- Every G-module has a decomposition into simple G-modules.
- A character determines its representation uniquely.

Basic facts

Proposition

- Every G-module has a decomposition into simple G-modules.
- A character determines its representation uniquely.
- Characters are class functions, i.e. take the same value for all g in the same conjugacy class $[g]$.

Basic facts

Proposition

- Every G-module has a decomposition into simple G-modules.
- A character determines its representation uniquely.
- Characters are class functions, i.e. take the same value for all g in the same conjugacy class $[g]$.
- $\#\,\mathrm{Conj}(G) = \#\,\mathrm{Irr}(G)$ (irreducible characters of G).

Basic facts

Proposition

- Every G-module has a decomposition into simple G-modules.
- A character determines its representation uniquely.
- Characters are class functions, i.e. take the same value for all g in the same conjugacy class $[g]$.
- $\#\,\mathrm{Conj}(G) = \#\,\mathrm{Irr}(G)$ (irreducible characters of G).

Theorem (I. Schur)

Let chi_i, χ_j be irreducible characters of G and $g, h \in G$. We have the following Schur orthogonality relations

$$\frac{1}{\#G} \sum_{[g]\in\mathrm{Conj}(G)} \frac{\chi_i(g)\overline{\chi_j(g)}}{\#C_G(g)} = \delta_{i,j}, \qquad \sum_{\chi\in\mathrm{Irr}(G)} \chi(g)\overline{\chi(h)} = \delta_{[g],[h]}\#C_G(g).$$

Finite simple groups

Definition

A group G is called simple if it has no non-trivial normal subgroups.

Finite simple groups

Definition

A group G is called simple if it has no non-trivial normal subgroups.

Example

- cyclic groups C_p for p prime.
- alternating groups A_n for $n \geq 5$.
- $\mathrm{PSL}_n(\mathbb{F}_q)$ for $q \geq 4$ if $n = 2$ and all q for $n > 2$.
- finite groups of Lie type

Finite simple groups

Definition

A group G is called simple if it has no non-trivial normal subgroups.

Example

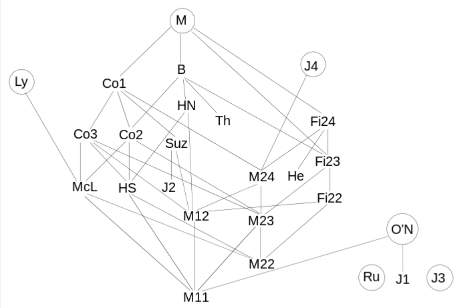
- cyclic groups C_p for p prime.
- alternating groups A_n for $n \geq 5$.
- $\mathrm{PSL}_n(\mathbb{F}_q)$ for $q \geq 4$ if $n = 2$ and all q for $n > 2$.
- finite groups of Lie type

By the Jordan–Hölder Theorem, finite simple groups form the building blocks of all finite groups.

Classification of finite simple groups

Theorem

A finite simple group G either belongs to one of 8 infinite families or is one of 26 sporadic simple groups,



Source: wikipedia

Table of Contents

Table of Contents

The Monster group $\mathbb{M}$

Some properties of the Monster

- The largest of the 26 sporadic finite simple groups

Some properties of the Monster

- The largest of the 26 sporadic finite simple groups
- $\#\mathbb{M} = 2^{46}\cdot 3^{20}\cdot 5^{9}\cdot 7^{6}\cdot 11^{2}\cdot 13^{3}\cdot 17\cdot 19\cdot 23\cdot 29\cdot 31\cdot 41\cdot 47\cdot 59\cdot 71 \approx 8.08\cdot 10^{53}$

Some properties of the Monster

- The largest of the 26 sporadic finite simple groups
- $\#\mathbb{M} = 2^{46} \cdot 3^{20} \cdot 5^{9} \cdot 7^{6} \cdot 11^{2} \cdot 13^{3} \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 41 \cdot 47 \cdot 59 \cdot 71 \approx 8.08 \cdot 10^{53}$
- 194 conjugacy classes, hence 194 irreducible representations (over $\mathbb{C}$) with characters $\chi_1, \ldots, \chi_{194}$

Reminder: $\mathrm{SL}_2(\mathbb{R})$ acts on the upper half-plane $\mathfrak{H}$ via

$$\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}, \tau\right) \mapsto \frac{a\tau + b}{c\tau + d}.$$

Modular forms and functions

Reminder: $\mathrm{SL}_2(\mathbb{R})$ acts on the upper half-plane $\mathfrak{H}$ via

$$\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}, \tau\right) \mapsto \frac{a\tau + b}{c\tau + d}.$$

Definition

Let $\Gamma \leq \mathrm{SL}_2(\mathbb{R})$ be a discrete subgroup such that $\mathrm{vol}(\Gamma \setminus \mathfrak{H}) < \infty$. A meromorphic function $f : \mathfrak{H} \to \widehat{\mathbb{C}}$ is called a modular function for Γ if

$$f(\gamma\tau) = f(\tau)$$

for all $\gamma \in \Gamma$, $\tau \in \mathfrak{H}$ (+growth condition at the boundary).

Modular forms and functions

Reminder: $\mathrm{SL}_2(\mathbb{R})$ acts on the upper half-plane $\mathfrak{H}$ via

$$\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}, \tau\right) \mapsto \frac{a\tau + b}{c\tau + d}.$$

Definition

Let $\Gamma \leq \mathrm{SL}_2(\mathbb{R})$ be a discrete subgroup such that $\mathrm{vol}(\Gamma \setminus \mathfrak{H}) < \infty$. A holomorphic function $f : \mathfrak{H} \to \widehat{\mathbb{C}}$ is called a (weakly holomorphic) modular form of weight k for Γ if

$$f(\gamma\tau) = (c\tau + d)^k f(\tau)$$

for all $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma$, $\tau \in \mathfrak{H}$ (+growth condition at the boundary). If $\mathrm{Im}(\tau)^{\frac{k}{2}} f(\tau)$ is bounded on $\mathfrak{H}$, we call f a cusp form.

Hauptmoduln

Facts

1. The quotient $\Gamma \setminus \mathfrak{H}$ can be compactified to a Riemann surface $X(\Gamma)$ of genus g. Modular functions for Γ define meromorphic functions on $X(\Gamma)$.

Hauptmoduln

Facts

1. The quotient $\Gamma \setminus \mathfrak{H}$ can be compactified to a Riemann surface $X(\Gamma)$ of genus g. Modular functions for Γ define meromorphic functions on $X(\Gamma)$.
2. The field of meromorphic functions on $X(\Gamma)$ is isomorphic to an algebraic extension of $\mathbb{C}(x)$ of degree g. In particular if $g = 0$, it is isomorphic to $\mathbb{C}(x)$.

Hauptmoduln

Facts

1. The quotient $\Gamma \setminus \mathfrak{H}$ can be compactified to a Riemann surface $X(\Gamma)$ of genus g. Modular functions for Γ define meromorphic functions on $X(\Gamma)$.
2. The field of meromorphic functions on $X(\Gamma)$ is isomorphic to an algebraic extension of $\mathbb{C}(x)$ of degree g. In particular if $g = 0$, it is isomorphic to $\mathbb{C}(x)$.

Definition

Let Γ be as above such that $X(\Gamma)$ has genus 0 (+ mild extra conditions). A suitably normalized generator for the field of modular functions for Γ is called the Hauptmodul for Γ.

Table of Contents

The Jack Daniels problem

For $N \in \mathbb{N}$ let

$$\Gamma_0(N) := \left\{ \gamma \in \mathrm{SL}_2(\mathbb{Z}) \; : \; \gamma \equiv \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \pmod{N} \right\}$$

and

$$\Gamma_0(p)^+ := N_{\mathrm{SL}_2(\mathbb{R})}(\Gamma_0(p)) \qquad (p \text{ prime}).$$

The Jack Daniels problem

For $N \in \mathbb{N}$ let

$$\Gamma_0(N) := \left\{ \gamma \in \mathrm{SL}_2(\mathbb{Z}) \ : \ \gamma \equiv \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \pmod{N} \right\}$$

and

$$\Gamma_0(p)^+ := N_{\mathrm{SL}_2(\mathbb{R})}(\Gamma_0(p)) \qquad (p \text{ prime}).$$

Theorem (A. Ogg)

For p prime, the Riemann surface $X(\Gamma_0(p)^+)$ has genus zero if and only if $p \in \{2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 41, 47, 59, 71\}$.

The Jack Daniels problem

For $N \in \mathbb{N}$ let

$$\Gamma_0(N) := \left\{ \gamma \in \mathrm{SL}_2(\mathbb{Z}) \;:\; \gamma \equiv \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \pmod{N} \right\}$$

and

$$\Gamma_0(p)^+ := N_{\mathrm{SL}_2(\mathbb{R})}(\Gamma_0(p)) \qquad (p \text{ prime}).$$

Theorem (A. Ogg)

For p prime, the Riemann surface $X(\Gamma_0(p)^+)$ has genus zero if and only if p divides $\#\mathbb{M}$.

The Jack Daniels problem

For $N \in \mathbb{N}$ let

$$\Gamma_0(N) := \left\{ \gamma \in \mathrm{SL}_2(\mathbb{Z}) \ : \ \gamma \equiv \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \pmod{N} \right\}$$

and

$$\Gamma_0(p)^+ := N_{\mathrm{SL}_2(\mathbb{R})}(\Gamma_0(p)) \qquad (p \text{ prime}).$$

Theorem (A. Ogg)

For p prime, the Riemann surface $X(\Gamma_0(p)^+)$ has genus zero if and only if p divides $\#\mathbb{M}$.

Question: Why is this so?

Monstrous Moonshine I

Dimensions of irreducible representations:

$$\chi_1(1) = 1, \quad \chi_2(1) = 196\,883, \quad \chi_3(1) = 21\,296\,876, \quad \chi_4(1) = 842\,609\,326.$$

Monstrous Moonshine I

Dimensions of irreducible representations:

$$\chi_1(1) = 1, \quad \chi_2(1) = 196\,883, \quad \chi_3(1) = 21\,296\,876, \quad \chi_4(1) = 842\,609\,326.$$

Hauptmodul for $\mathrm{SL}_2(\mathbb{Z})$ $\qquad (q := e^{2\pi i\tau})$:

$$J(\tau) = j(\tau) - 744 = \frac{E_4(\tau)^3}{\Delta(\tau)} - 744$$

$$= \sum_{n=-1}^{\infty} j_n q^n = q^{-1} + 196\,884q + 21\,493\,760q^2 + 864\,299\,970q^3 + O(q^4).$$

Dimensions of irreducible representations:

$$\chi_1(1) = 1, \quad \chi_2(1) = 196883, \quad \chi_3(1) = 21\,296\,876, \quad \chi_4(1) = 842\,609\,326.$$

Hauptmodul for $\mathrm{SL}_2(\mathbb{Z})$ $\qquad (q := e^{2\pi i\tau})$:

$$J(\tau) = j(\tau) - 744 = \frac{E_4(\tau)^3}{\Delta(\tau)} - 744$$

$$= \sum_{n=-1}^{\infty} j_n q^n = q^{-1} + 196\,884q + 21\,493\,760q^2 + 864\,299\,970q^3 + O(q^4).$$

Observation (J. McKay & J. G. Thompson, 1979)

$$j_1 = \chi_1(1) + \chi_2(1).$$

Monstrous Moonshine I

Dimensions of irreducible representations:

$$\chi_1(1) = 1, \quad \chi_2(1) = 196883, \quad \chi_3(1) = 21\,296\,876, \quad \chi_4(1) = 842\,609\,326.$$

Hauptmodul for $\mathrm{SL}_2(\mathbb{Z})$ $\qquad (q := e^{2\pi i\tau})$:

$$J(\tau) = j(\tau) - 744 = \frac{E_4(\tau)^3}{\Delta(\tau)} - 744$$

$$= \sum_{n=-1}^{\infty} j_n q^n = q^{-1} + 196\,884q + 21\,493\,760q^2 + 864\,299\,970q^3 + O(q^4).$$

Observation (J. McKay & J. G. Thompson, 1979)

$$j_2 = \chi_1(1) + \chi_2(1) + \chi_3(1)$$

Monstrous Moonshine I

Dimensions of irreducible representations:

$$\chi_1(1) = 1, \quad \chi_2(1) = 196883, \quad \chi_3(1) = 21\,296\,876, \quad \chi_4(1) = 842\,609\,326.$$

Hauptmodul for $\mathrm{SL}_2(\mathbb{Z})$ $\qquad (q := e^{2\pi i \tau})$:

$$J(\tau) = j(\tau) - 744 = \frac{E_4(\tau)^3}{\Delta(\tau)} - 744$$

$$= \sum_{n=-1}^{\infty} j_n q^n = q^{-1} + 196\,884q + 21\,493\,760q^2 + 864\,299\,970q^3 + O(q^4).$$

Observation (J. McKay & J. G. Thompson, 1979)

$$j_3 = 2\chi_1(1) + 2\chi_2(1) + \chi_3(1) + \chi_4(1)$$

Monstrous Moonshine II

Values of irreducible characters at other conjugacy classes.

$$\chi_1(2A) = 1, \quad \chi_2(2A) = 4\,371, \quad \chi_3(2A) = 91\,884, \quad \chi_4(2A) = 1\,139\,374.$$

Monstrous Moonshine II

Values of irreducible characters at other conjugacy classes.

$$\chi_1(2A) = 1, \quad \chi_2(2A) = 4\,371, \quad \chi_3(2A) = 91\,884, \quad \chi_4(2A) = 1\,139\,374.$$

Hauptmodul for $\Gamma_0(2)^+$:

$$J_2^+(\tau) = \frac{\eta(\tau)^{24}}{\eta(2\tau)^{24}} + 2^{12}\frac{\eta(2\tau)^{24}}{\eta(\tau)^{24}} + 24$$
$$= \sum_{n=-1}^{\infty} \alpha_n q^n = q^{-1} + 4\,372q + 96\,256q^2 + 1\,240\,002q^3 + O(q^4).$$

Monstrous Moonshine II

Values of irreducible characters at other conjugacy classes.

$$\chi_1(2A) = 1, \quad \chi_2(2A) = 4\,371, \quad \chi_3(2A) = 91\,884, \quad \chi_4(2A) = 1\,139\,374.$$

Hauptmodul for $\Gamma_0(2)^+$:

$$J_2^+(\tau) = \frac{\eta(\tau)^{24}}{\eta(2\tau)^{24}} + 2^{12}\frac{\eta(2\tau)^{24}}{\eta(\tau)^{24}} + 24$$
$$= \sum_{n=-1}^{\infty} \alpha_n q^n = q^{-1} + 4\,372q + 96\,256q^2 + 1\,240\,002q^3 + O(q^4).$$

Observation (J. H. Conway & S. P. Norton, 1979)

$$\alpha_1 = \chi_1(2A) + \chi_2(2A).$$

Values of irreducible characters at other conjugacy classes.

$$\chi_1(2A) = 1, \quad \chi_2(2A) = 4\,371, \quad \chi_3(2A) = 91\,884, \quad \chi_4(2A) = 1\,139\,374.$$

Hauptmodul for $\Gamma_0(2)^+$:

$$J_2^+(\tau) = \frac{\eta(\tau)^{24}}{\eta(2\tau)^{24}} + 2^{12}\frac{\eta(2\tau)^{24}}{\eta(\tau)^{24}} + 24$$
$$= \sum_{n=-1}^{\infty} \alpha_n q^n = q^{-1} + 4\,372q + 96\,256q^2 + 1\,240\,002q^3 + O(q^4).$$

Observation (J. H. Conway & S. P. Norton, 1979)

$$\alpha_2 = \chi_1(2A) + \chi_2(2A) + \chi_3(2A)$$

Monstrous Moonshine II

Values of irreducible characters at other conjugacy classes.

$$\chi_1(2A) = 1, \quad \chi_2(2A) = 4\,371, \quad \chi_3(2A) = 91\,884, \quad \chi_4(2A) = 1\,139\,374.$$

Hauptmodul for $\Gamma_0(2)^+$:

$$J_2^+(\tau) = \frac{\eta(\tau)^{24}}{\eta(2\tau)^{24}} + 2^{12}\frac{\eta(2\tau)^{24}}{\eta(\tau)^{24}} + 24$$
$$= \sum_{n=-1}^{\infty} \alpha_n q^n = q^{-1} + 4\,372q + 96\,256q^2 + 1\,240\,002q^3 + O(q^4).$$

Observation (J. H. Conway & S. P. Norton, 1979)

$$\alpha_3 = 2\chi_1(2A) + 2\chi_2(2A) + \chi_3(2A) + \chi_4(2A)$$

Monstrous Moonshine II

Observation (J. H. Conway & S. P. Norton, 1979)

There are 194 Hauptmoduln whose coefficients agree, as those of J above, with character values of $\mathbb{M}$.

Observation (J. H. Conway & S. P. Norton, 1979)

There are 194 Hauptmoduln whose coefficients agree, as those of J above, with character values of $\mathbb{M}$.

Definition

For a finite group G let $V = \bigoplus_n V_n$ be a graded G-module, where all graded components V_n are finite-dimensional. Then for each $g \in G$ we call the power series

$$\mathcal{T}_g(q) = \sum_n \mathrm{tr}(g|V_n)q^n$$

the McKay-Thompson series of g with respect to V.

Monstrous Moonshine III

Monstrous Moonshine Conjecture

There is an infinite dimensional graded representation $V^\natural$ of $\mathbb{M}$ whose McKay-Thompson series are the 194 Hauptmoduln found by Conway–Norton.

Monstrous Moonshine III

Monstrous Moonshine Conjecture

There is an infinite dimensional graded representation $V^\natural$ of $\mathbb{M}$ whose McKay-Thompson series are the 194 Hauptmoduln found by Conway–Norton.

"Theorem" (Atkin–Fong–Smith, $\sim$ 1985)

The Moonshine module $V^\natural$ exists (abstract existence proof).

Monstrous Moonshine III

Monstrous Moonshine Conjecture

There is an infinite dimensional graded representation $V^\natural$ of $\mathbb{M}$ whose McKay-Thompson series are the 194 Hauptmoduln found by Conway–Norton.

"Theorem" (Atkin–Fong–Smith, $\sim$ 1985)

The Moonshine module $V^\natural$ exists (abstract existence proof).

Theorem (R. E. Borcherds, 1992)

The Moonshine module $V^\natural$ is a vertex operator algebra constructed by Frenkel–Lepowsky–Meurman, whose automorphism group is isomorphic to $\mathbb{M}$.

Table of Contents

There are 23 even unimodular lattices in dimension 24 with rootsystem of full rank, the Niemeier lattices.
Examples: ${A_1}^{24}, \quad {A_2}^{12}$.

The Umbral groups

There are 23 even unimodular lattices in dimension 24 with rootsystem of full rank, the Niemeier lattices.
Examples: ${A_1}^{24}$, ${A_2}^{12}$.

For a Niemeier lattice L, its Umbral Group G^L is defined as

$$G^L := \mathrm{Aut}(L)/\mathsf{Weyl}(L).$$

Examples: $G^{{A_1}^{24}} = M_{24}$, $G^{{A_2}^{12}} = M_{12}$.

Umbral Moonshine I

Observation (Eguchi–Ooguri–Tachikawa, 2010)

Some dimensions of irreducible representations of M_{24} are multiplicities of superconformal algebra characters of the K3 elliptic genus, which are known to be coefficients of a (vector-valued) mock theta function.

Umbral Moonshine I

Observation (Eguchi–Ooguri–Tachikawa, 2010)

Some dimensions of irreducible representations of M_{24} are multiplicities of superconformal algebra characters of the K3 elliptic genus, which are known to be coefficients of a (vector-valued) mock theta function.

Theorem (T. Gannon, 2012)

There is an infinite-dimensional graded M_{24}-module whose McKay-Thompson series are specific (vector-valued) mock theta functions.

Umbral Moonshine II

Umbral Moonshine Conjecture (Cheng–Duncan–Harvey, 2012)

For every Umbral Group G^L, there is an an infinite-dimensional graded G^L-module whose McKay-Thompson series are specific (vector-valued) mock theta functions.

Umbral Moonshine II

Umbral Moonshine Conjecture (Cheng–Duncan–Harvey, 2012)

For every Umbral Group G^L, there is an an infinite-dimensional graded G^L-module whose McKay-Thompson series are specific (vector-valued) mock theta functions.

Theorem (Duncan–Griffin–Ono, 2015)

The Umbral Moonshine conjecture is true.

Table of Contents

Table of Contents

The Thompson group Th

Some properties of Th

- Essentially the automorphism group of the Thompson lattice, an even unimodular 248-dimensional lattice.

The Thompson group Th

Some properties of Th

- Essentially the automorphism group of the Thompson lattice, an even unimodular 248-dimensional lattice.
- $\#Th = 90\,745\,943\,887\,872\,000 = 2^{15} \cdot 3^{10} \cdot 5^3 \cdot 13 \cdot 19 \cdot 31.$

The Thompson group Th

Some properties of Th

- Essentially the automorphism group of the Thompson lattice, an even unimodular 248-dimensional lattice.
- $\#Th = 90\,745\,943\,887\,872\,000 = 2^{15} \cdot 3^{10} \cdot 5^3 \cdot 13 \cdot 19 \cdot 31.$
- 48 conjugacy classes, hence 48 irreducible representations (over $\mathbb{C}$) with characters $\chi_1, ..., \chi_{48}$.

The Thompson group Th

Some properties of Th

- Essentially the automorphism group of the Thompson lattice, an even unimodular 248-dimensional lattice.
- $\#Th = 90\,745\,943\,887\,872\,000 = 2^{15} \cdot 3^{10} \cdot 5^3 \cdot 13 \cdot 19 \cdot 31.$
- 48 conjugacy classes, hence 48 irreducible representations (over $\mathbb{C}$) with characters $\chi_1, ..., \chi_{48}$.

Dimensions of irreducible characters:

$$\chi_1(1) = 1, \quad \chi_2(1) = 248, \quad \chi_4(1) = \chi_5(1) = 27\,000,$$
$$\chi_9(1) = \chi_{10}(1) = 85\,995.$$

The Thompson group Th

Some properties of Th

- Essentially the automorphism group of the Thompson lattice, an even unimodular 248-dimensional lattice.
- $\#Th = 90\,745\,943\,887\,872\,000 = 2^{15} \cdot 3^{10} \cdot 5^3 \cdot 13 \cdot 19 \cdot 31.$
- 48 conjugacy classes, hence 48 irreducible representations (over $\mathbb{C}$) with characters $\chi_1, ..., \chi_{48}$.

Dimensions of irreducible characters:

$$\chi_1(1) = 1, \quad \chi_2(1) = 248, \quad \chi_4(1) = \chi_5(1) = 27\,000,$$
$$\chi_9(1) = \chi_{10}(1) = 85\,995.$$

In terms of Zagier's basis of $M^{!,+}_{\frac{1}{2}}(\Gamma_0(4))$:

$$2f_3(\tau) + 248\vartheta(\tau) = 2q^{-3} + 248 + 54\,000q^4 - 171\,990q^5 + O(q^8).$$

Thompson Moonshine Conjecture

Conjecture (J. A. Harvey & B. C. Rayhaun, 2015)

There is an infinite-dimensional graded Th-supermodule $W = \bigoplus_{m\equiv 0,1\ (4)} W_m$, where $W_m = W_m^+ \oplus W_m^-$ has vanishing odd part if m is even and vice versa, whose McKay-Thompson series

$$\mathcal{T}_{[g]}(\tau) = 2q^{-3} + \sum_{\substack{m=0 \\ m\equiv 0,1\ (4)}} \mathrm{str}(g|W_m)q^m$$

are specific weakly holomorphic weight $\frac{1}{2}$ modular forms.

Main result

Theorem 1 (M. J. Griffin & M., 2016)

The Thompson Moonshine Conjecture is true. Moreover, for each $g \in Th$ there is a multiplier $\psi_{[g]}$ on $\Gamma_0(4|g|)$, s.t. $\mathcal{T}_{[g]}(\tau)$ is the unique form $\mathcal{F}_{[g]} \in M^{!,+}_{\frac{1}{2}}(\Gamma_0(4|g|), \psi_{[g]})$ with

- $\mathcal{F}_{[g]}(\tau) = 2q^{-3} + \chi_2(g) + (\chi_4(g) + \chi_5(g))q^4 + O(q^5)$,
- $\mathcal{F}_{[g]}$ has a pole of order 3 (essentially) only at the cusp ∞ and vanishes at the other cusps.

Strategy of the proof

- Take

$$\mathcal{F}_{[g]}(\tau) =: 2q^{-3} + \sum_{n=0}^{\infty} \alpha_{[g]}(n) q^n$$

Strategy of the proof

- Take

$$\mathcal{F}_{[g]}(\tau) =: 2q^{-3} + \sum_{n=0}^{\infty} \alpha_{[g]}(n) q^n$$

- Define $\mathbb{C}$-valued class function

$$\omega_n : \ Th \to \mathbb{C}, \ g \mapsto \alpha_{[g]}(n).$$

Strategy of the proof

- Take

$$\mathcal{F}_{[g]}(\tau) =: 2q^{-3} + \sum_{n=0}^{\infty} \alpha_{[g]}(n) q^n$$

- Define $\mathbb{C}$-valued class function

$$\omega_n : \ Th \to \mathbb{C}, \ g \mapsto \alpha_{[g]}(n).$$

- Theorem follows if we can show that

$$(-1)^n \omega_n = \sum_{j=1}^{48} m_j(n) \chi_j,$$

with $m_j(n) \in \mathbb{N}_0$ for all j and n.

Strategy of the proof

- Take
$$\mathcal{F}_{[g]}(\tau) =: 2q^{-3} + \sum_{n=0}^{\infty} \alpha_{[g]}(n) q^n$$
- Define $\mathbb{C}$-valued class function
$$\omega_n : \ Th \to \mathbb{C}, \ g \mapsto \alpha_{[g]}(n).$$
- Theorem follows if we can show that
$$(-1)^n \omega_n = \sum_{j=1}^{48} m_j(n) \chi_j,$$
with $m_j(n) \in \mathbb{N}_0$ for all j and n.
- Idea of Thompson can reduce this to a finite computation.

Strategy of the proof

- Take

$$\mathcal{F}_{[g]}(\tau) =: 2q^{-3} + \sum_{n=0}^{\infty} \alpha_{[g]}(n) q^n$$

- Define $\mathbb{C}$-valued class function

$$\omega_n : \; Th \to \mathbb{C}, \; g \mapsto \alpha_{[g]}(n).$$

- Theorem follows if we can show that

$$(-1)^n \omega_n = \sum_{j=1}^{48} m_j(n) \chi_j,$$

with $m_j(n) \in \mathbb{N}_0$ for all j and n.
- Idea of Thompson can reduce this to a finite computation.

BUT: There is a difference between 'finite' and 'feasible'.

Table of Contents

Construction

Let

$$\Gamma_{K,K^2}(N) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N) \ : \ |c| < K, \ |d| < K^2 \right\}.$$

Construction

Let

$$\Gamma_{K,K^2}(N) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N) \ : \ |c| < K, \ |d| < K^2 \right\}.$$

Definition

For $\mu \in \mathbb{Z}$, $k \in \frac{1}{2}\mathbb{Z}$, and ψ a multiplier system for $\Gamma_0(N)$ of weight k, we define the Rademacher sum

$$R^{[\mu]}_{\psi,k}(\tau) := \lim_{K\to\infty} \sum_{\gamma \in \Gamma_\infty \backslash \Gamma_{K,K^2}(N)} \overline{\psi}(\gamma)(q^\mu|_k\gamma).$$

Let

$$\Gamma_{K,K^2}(N) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N) \ : \ |c| < K, \ |d| < K^2 \right\}.$$

Definition

For $\mu \in \mathbb{Z}$, $k \in \frac{1}{2}\mathbb{Z}$, and ψ a multiplier system for $\Gamma_0(N)$ of weight k, we define the Rademacher sum

$$R_{\psi,k}^{[\mu]}(\tau) := \lim_{K\to\infty} \sum_{\gamma \in \Gamma_\infty \backslash \Gamma_{K,K^2}(N)} \overline{\psi}(\gamma)(q^\mu|_k\gamma).$$

- Low-weight analogue of Poincaré series.

Construction

Let

$$\Gamma_{K,K^2}(N) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N) \ : \ |c| < K, \ |d| < K^2 \right\}.$$

Definition

For $\mu \in \mathbb{Z}$, $k \in \frac{1}{2}\mathbb{Z}$, and ψ a multiplier system for $\Gamma_0(N)$ of weight k, we define the Rademacher sum

$$R_{\psi,k}^{[\mu]}(\tau) := \lim_{K\to\infty} \sum_{\gamma \in \Gamma_\infty \backslash \Gamma_{K,K^2}(N)} \overline{\psi}(\gamma)(q^\mu|_k\gamma).$$

- Low-weight analogue of Poincaré series.
- Converges for $k \geq 1$, with regularization sometimes for $k < 1$.

Properties of Rademacher sums

Facts

Let $\mu < 0$.

- $R^{[\mu]}_{\psi,k}$ is a weight k mock modular form for $\Gamma_0(N)$ with multiplier ψ with shadow $R^{[-\mu]}_{\overline{\psi},2-k} \in S_{2-k}(\Gamma_0(N), \overline{\psi})$.

Properties of Rademacher sums

Facts

Let $\mu < 0$.

- $R^{[\mu]}_{\psi,k}$ is a weight k mock modular form for $\Gamma_0(N)$ with multiplier ψ with shadow $R^{[-\mu]}_{\overline{\psi},2-k} \in S_{2-k}(\Gamma_0(N), \overline{\psi})$.
- $R^{[\mu]}_{\psi,k}$ has a pole of order $|\mu|$ at ∞ and vanishes at all other cusps.

Properties of Rademacher sums

Facts

Let $\mu < 0$.

- $R^{[\mu]}_{\psi,k}$ is a weight k mock modular form for $\Gamma_0(N)$ with multiplier ψ with shadow $R^{[-\mu]}_{\overline{\psi},2-k} \in S_{2-k}(\Gamma_0(N), \overline{\psi})$.
- $R^{[\mu]}_{\psi,k}$ has a pole of order $|\mu|$ at ∞ and vanishes at all other cusps.

"Definition"

A hol. function $f : \mathfrak{H} \to \mathbb{C}$ is called a mock modular form for $\Gamma_0(N)$ of weight k and multiplier ψ if there is a cusp form $g \in S_{2-k}(\Gamma_0(N), \overline{\psi})$ s.t.

$$\widehat{f}(\tau) := f(\tau) + \int_{-\overline{\tau}}^{\infty} \frac{\overline{g(\overline{z})}}{(z+\tau)^k} dz$$

transforms like a modular form. g is called the shadow of f, $\widehat{f}$ is the corresponding harmonic Maaß form.

Table of Contents

Modularity

Let

$$Z^{[\mu]}_{\frac{1}{2},\psi} = R^{[\mu]}_{\frac{1}{2},\psi} |\,\mathrm{pr},$$

the projection to the Kohnen plus space.

Modularity

Let

$$Z^{[\mu]}_{\frac{1}{2},\psi} = R^{[\mu]}_{\frac{1}{2},\psi} |\, \mathrm{pr},$$

the projection to the Kohnen plus space.

Proposition 1

For $g \in Th$ we have

$$Z^{[-3]}_{\frac{1}{2},\psi_{[g]}} \in M^{!,+}_{\frac{1}{2}}(\Gamma_0(4|g|, \psi_{[g]}).$$

Let

$$Z^{[\mu]}_{\frac{1}{2},\psi} = R^{[\mu]}_{\frac{1}{2},\psi} | \operatorname{pr},$$

the projection to the Kohnen plus space.

Proposition 1

For $g \in Th$ we have

$$Z^{[-3]}_{\frac{1}{2},\psi_{[g]}} \in M^{!,+}_{\frac{1}{2}}(\Gamma_0(4|g|, \psi_{[g]}).$$

Proof.

- $\dim(S^{+}_{\frac{3}{2}}(\Gamma_0(4|g|, \overline{\psi}_{[g]})) = 0$ in most cases.

□

Modularity

Let

$$Z^{[\mu]}_{\frac{1}{2},\psi} = R^{[\mu]}_{\frac{1}{2},\psi}|\,\mathrm{pr},$$

the projection to the Kohnen plus space.

Proposition 1

For $g \in Th$ we have

$$Z^{[-3]}_{\frac{1}{2},\psi_{[g]}} \in M^{!,+}_{\frac{1}{2}}(\Gamma_0(4|g|,\psi_{[g]}).$$

Proof.

- $\dim(S^{+}_{\frac{3}{2}}(\Gamma_0(4|g|,\overline{\psi}_{[g]})) = 0$ in most cases.
- In other cases: $f \in S^{+}_{\frac{3}{2}}(\Gamma_0(4|g|,\overline{\psi}_{[g]})) \Rightarrow f = O(q^4)$, so the shadow of Z is 0 by the Bruinier-Funke pairing.

□

Properties of $\mathcal{F}_{[g]}$

Proposition 2

1. $\mathcal{F}_{[g]} = 2Z^{[-3]}_{\frac{1}{2},\psi_{[g]}} +$ unary theta function.

Properties of $\mathcal{F}_{[g]}$

Proposition 2

1. $\mathcal{F}_{[g]} = 2Z^{[-3]}_{\frac{1}{2},\psi_{[g]}} +$ unary theta function.
2. $\mathcal{F}_{[g]}$ has integer Fourier coefficients $\alpha_{[g]}(n)$.

Properties of $\mathcal{F}_{[g]}$

Proposition 2

1. $\mathcal{F}_{[g]} = 2Z^{[-3]}_{\frac{1}{2},\psi_{[g]}} +$ unary theta function.
2. $\mathcal{F}_{[g]}$ has integer Fourier coefficients $\alpha_{[g]}(n)$.

Proof.

1. Serre-Stark basis theorem.

□

Properties of $\mathcal{F}_{[g]}$

Proposition 2

1. $\mathcal{F}_{[g]} = 2Z^{[-3]}_{\frac{1}{2},\psi_{[g]}} +$ unary theta function.
2. $\mathcal{F}_{[g]}$ has integer Fourier coefficients $\alpha_{[g]}(n)$.

Proof.

1. Serre-Stark basis theorem.
2. Multiply by a suitable cusp form and apply Sturm bound.

□

Integrality of multiplicities I

Let

$$\mathcal{F}_{\chi_j}(\tau) := \frac{1}{\#Th} \sum_{g \in Th} \overline{\chi_j(g)} \mathcal{F}_{[g]}(\tau)$$

Integrality of multiplicities I

Let

$$\mathcal{F}_{\chi_j}(\tau) := \frac{1}{\#Th} \sum_{g \in Th} \overline{\chi_j(g)} \mathcal{F}_{[g]}(\tau) \stackrel{\text{Schur}}{=} 2q^{-3} + \sum_{n=0} m_j(n) q^n.$$

Integrality of multiplicities I

Let

$$\mathcal{F}_{\chi_j}(\tau) := \frac{1}{\#Th} \sum_{g \in Th} \overline{\chi_j(g)} \mathcal{F}_{[g]}(\tau) \overset{\text{Schur}}{=} 2q^{-3} + \sum_{n=0} m_j(n) q^n.$$

- Propositions 1 & 2 yield: $\mathcal{F}_{\chi_j}$ is a weakly hol. modular form of weight $\frac{1}{2}$ of level N_{χ_j} with rational coefficients

Integrality of multiplicities I

Let

$$\mathcal{F}_{\chi_j}(\tau) := \frac{1}{\#Th} \sum_{g \in Th} \overline{\chi_j(g)} \mathcal{F}_{[g]}(\tau) \overset{\text{Schur}}{=} 2q^{-3} + \sum_{n=0} m_j(n) q^n.$$

- Propositions 1 & 2 yield: $\mathcal{F}_{\chi_j}$ is a weakly hol. modular form of weight $\frac{1}{2}$ of level N_{χ_j} with rational coefficients
- Checking integrality naively by Sturm bound not feasible ($N_{\chi_1} = 2\,778\,572\,160$)

Integrality of the multiplicities II

Proposition 3

$\mathcal{F}_{\chi_j}$ have all integer Fourier coefficients.

Integrality of the multiplicities II

Proposition 3

$\mathcal{F}_{\chi_j}$ have all integer Fourier coefficients.

Proof.

- The $\mathcal{F}_{[g]}$ satisfy numerous congruences modulo powers of $p \mid \#Th$ (proved by Sturm bound argument, $\sim 2\,000$ coefficients to be checked at worst).

□

Integrality of the multiplicities II

Proposition 3

$\mathcal{F}_{\chi_j}$ have all integer Fourier coefficients.

Proof.

- The $\mathcal{F}_{[g]}$ satisfy numerous congruences modulo powers of $p \mid \#Th$ (proved by Sturm bound argument, $\sim 2\,000$ coefficients to be checked at worst).
- One can then verify directly that $m_j(n)$ are p-integral for all $p \mid \#Th$, hence by Proposition 2, the claim follows.

□

Table of Contents

Basic strategy

Fact

Given convergence, Rademacher sums have a Fourier expansion whose coefficients are given in terms of infinite sums of Kloosterman sums

$$K_\psi(m,n,c) = \sum_{d\ (c)^*} \psi\left(\begin{pmatrix} * & * \\ c & d \end{pmatrix}\right) e^{2\pi i \frac{m\bar{d}+nd}{c}}$$

times I-Bessel functions.

Basic strategy

Fact

Given convergence, Rademacher sums have a Fourier expansion whose coefficients are given in terms of infinite sums of Kloosterman sums

$$K_\psi(m,n,c) = \sum_{d\ (c)^*} \psi\left(\begin{pmatrix} * & * \\ c & d \end{pmatrix}\right) e^{2\pi i \frac{m\bar{d}+nd}{c}}$$

times I-Bessel functions.

By the triangle inequality we have

$$m_j(n) \geq \frac{|\operatorname{str}(1|W_n)|}{\#Th} - \sum_{[g]\neq 1A} \frac{|\operatorname{str}(g|W_n)|}{\#C_{Th}(g)} |\chi_j(g)|.$$

Basic strategy

Fact

Given convergence, Rademacher sums have a Fourier expansion whose coefficients are given in terms of infinite sums of Kloosterman sums

$$K_\psi(m,n,c) = \sum_{d\ (c)^*} \psi\left(\begin{pmatrix} * & * \\ c & d \end{pmatrix}\right) e^{2\pi i \frac{m\overline{d}+nd}{c}}$$

times I-Bessel functions.

By the triangle inequality we have

$$m_j(n) \geq \frac{|\operatorname{str}(1|W_n)|}{\#Th} - \sum_{[g]\neq 1A} \frac{|\operatorname{str}(g|W_n)|}{\#C_{Th}(g)} |\chi_j(g)|.$$

Show that from a certain point on, the first term dominates.

Positivity of the multiplicities

Proposition 4

The multiplicities $m_j(n)$ are all non-negative.

Positivity of the multiplicities

Proposition 4

The multiplicities $m_j(n)$ are all non-negative.

Ingredients of the proof.

- Careful, explicit estimates for Selberg-Kloosterman zeta functions.

□

Positivity of the multiplicities

Proposition 4

The multiplicities $m_j(n)$ are all non-negative.

Ingredients of the proof.

- Careful, explicit estimates for Selberg-Kloosterman zeta functions.
- Write Kloosterman sums as sums over a sparse set, i.e. equivalence classes of binary quadratic forms.

□

Positivity of the multiplicities

Proposition 4

The multiplicities $m_j(n)$ are all non-negative.

Ingredients of the proof.

- Careful, explicit estimates for Selberg-Kloosterman zeta functions.
- Write Kloosterman sums as sums over a sparse set, i.e. equivalence classes of binary quadratic forms.

$$\Rightarrow \qquad m_j(n) \geq 0 \text{ for } n \geq 375.$$

□

Positivity of the multiplicities

Proposition 4

The multiplicities $m_j(n)$ are all non-negative.

Ingredients of the proof.

- Careful, explicit estimates for Selberg-Kloosterman zeta functions.
- Write Kloosterman sums as sums over a sparse set, i.e. equivalence classes of binary quadratic forms.

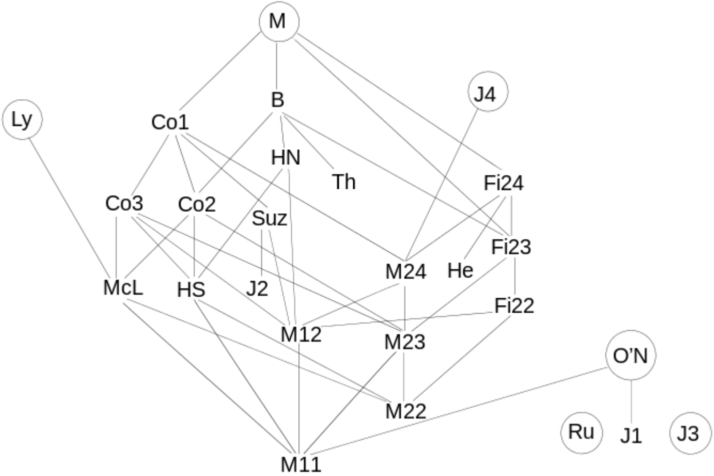
$$\Rightarrow \qquad m_j(n) \geq 0 \text{ for } n \geq 375.$$

- Check rest by inspection.

□

Table of Contents

Finite simple groups



Source: wikipedia

Pariah Moonshine?

Observation

All known “Moonshine groups” so far are subquotients of $\mathbb{M}$.

Question: What about the pariahs?

Pariah Moonshine?

Observation

All known "Moonshine groups" so far are subquotients of $\mathbb{M}$.

Question: What about the pariahs?

Observation (J. F. R. Duncan & M., 2016)

Zagier's weight $\frac{3}{2}$ weakly holomorphic modular form g_4:

$$-g_4 = -q^{-4} + 2 + 26\,752 q^3 + 143\,376 q^4 + 8\,288\,256 q^7 + 26\,124\,256 q^8 + O(q^{11}).$$

Some dimensions of irreducible representations of ON:

$$\chi_7(1) = 26\,752$$
$$\chi_1(1) = 1,\ \chi_{12}(1) = 58\,311,\ \chi_{18}(1) = 85\,064$$

New Moonshine

Theorem (Duncan-M.-Ono, 2017)

There is a (virtual) infinite-dimensional graded ON-module

$$W := \bigoplus_{0<m\equiv 0,3 \pmod 4} W_m$$

whose associated McKay-Thompson series are specific weight $\frac{3}{2}$ (mock) modular forms.

Theorem (Duncan-M.-Ono, 2017)

There is a (virtual) infinite-dimensional graded $\mathrm{O'N}$-module

$$W := \bigoplus_{0<m\equiv 0,3 \pmod 4} W_m$$

whose associated McKay-Thompson series are specific weight $\frac{3}{2}$ (mock) modular forms.

Remark

We have that

$$\dim W_{163} = \frac{1}{2}(\alpha^2 + \alpha - 393768),$$

where

$$\alpha = \left\lceil e^{\pi\sqrt{163}} \right\rceil = \lceil 262537412640768743.99999999999942...\rceil.$$

ON "knows" p-parts in ideal class groups

Theorem 2 (Duncan–M.–Ono, 2017)

Suppose that $-D < 0$ is a fundamental discriminant. Then the following are true:

ON "knows" p-parts in ideal class groups

Theorem 2 (Duncan–M.–Ono, 2017)

Suppose that $-D < 0$ is a fundamental discriminant. Then the following are true:

1. If $-D < -8$ is even and $g_2 \in \mathrm{ON}$ has order 2, then

$$\dim W_D \equiv \mathrm{tr}(g_2|W_D) \equiv -24H(D) \pmod{2^4}.$$

ON "knows" p-parts in ideal class groups

Theorem 2 (Duncan–M.–Ono, 2017)

Suppose that $-D < 0$ is a fundamental discriminant. Then the following are true:

1. If $-D < -8$ is even and $g_2 \in \mathrm{ON}$ has order 2, then

$$\dim W_D \equiv \mathrm{tr}(g_2|W_D) \equiv -24H(D) \pmod{2^4}.$$

2. If $p \in \{3, 5, 7\}$, $\left(\frac{-D}{p}\right) = -1$ and $g_p \in \mathrm{ON}$ has order p, then

$$\dim W_D \equiv \mathrm{tr}(g_p|W_D) \equiv \begin{cases} -24H(D) \pmod{3^2} & \text{if } p = 3, \\ -24H(D) \pmod{p} & \text{if } p = 5, 7. \end{cases}$$

ON "knows" about Selmer and Tate-Shafarevich groups I

Theorem 3 (Duncan–M.–Ono, 2017)

Assume BSD. If $p = 11$ or 19 and $-D < 0$ is a fundamental discriminant for which $\left(\frac{-D}{p}\right) = -1$, and $g_p \in \mathrm{ON}$ has order p, then the following are true.

ON "knows" about Selmer and Tate-Shafarevich groups I

Theorem 3 (Duncan–M.–Ono, 2017)

Assume BSD. If $p = 11$ or 19 and $-D < 0$ is a fundamental discriminant for which $\left(\frac{-D}{p}\right) = -1$, and $g_p \in \mathrm{ON}$ has order p, then the following are true.

1. $\mathrm{Sel}(E_p(-D))[p] \neq \{0\}$ if and only if

$$\dim W_D \equiv \mathrm{tr}(g_p|W_D) \equiv -24H(D) \pmod{p}.$$

ON "knows" about Selmer and Tate-Shafarevich groups I

Theorem 3 (Duncan–M.–Ono, 2017)

Assume BSD. If $p = 11$ or 19 and $-D < 0$ is a fundamental discriminant for which $\left(\frac{-D}{p}\right) = -1$, and $g_p \in \mathrm{ON}$ has order p, then the following are true.

1. $\mathrm{Sel}(E_p(-D))[p] \neq \{0\}$ if and only if

$$\dim W_D \equiv \mathrm{tr}(g_p|W_D) \equiv -24H(D) \pmod{p}.$$

2. Suppose further that $L(E_p(-D), 1) \neq 0$. Then $p \mid \#Ш(E_p(-D))$ if and only if

$$\dim W_D \equiv \mathrm{tr}(g_p|W_D) \equiv -24H(D) \pmod{p}.$$

Theorem 4 (Duncan–M.–Ono, 2017)

Let $N \in \{14, 15\}$ and write $N = p'p$, $p' < p$, and let $\delta_p := \frac{p-1}{2}$. If $-D < 0$ is a fundamental discriminant for which $\left(\frac{-D}{p}\right) = -1$, then the following are true.

Theorem 4 (Duncan–M.–Ono, 2017)

Let $N \in \{14, 15\}$ and write $N = p'p$, $p' < p$, and let $\delta_p := \frac{p-1}{2}$. If $-D < 0$ is a fundamental discriminant for which $\left(\frac{-D}{p}\right) = -1$, then the following are true.

1. $\mathrm{Sel}(E_N(-D))[p] \neq \{0\}$ if and only if

$$\mathrm{tr}(g_{p'}|W_D) \equiv \mathrm{tr}(g_N|W_D) \equiv \delta_p \cdot (H(D) - \delta_p H^{(p')}(D)) \pmod{p}.$$

ON "knows" about Selmer and Tate-Shafarevich groups II

Theorem 4 (Duncan–M.–Ono, 2017)

Let $N \in \{14, 15\}$ and write $N = p'p$, $p' < p$, and let $\delta_p := \frac{p-1}{2}$. If $-D < 0$ is a fundamental discriminant for which $\left(\frac{-D}{p}\right) = -1$, then the following are true.

1. $\mathrm{Sel}(E_N(-D))[p] \neq \{0\}$ if and only if
$$\mathrm{tr}(g_{p'}|W_D) \equiv \mathrm{tr}(g_N|W_D) \equiv \delta_p \cdot (H(D) - \delta_p H^{(p')}(D)) \pmod{p}.$$
2. Suppose further that $L(E_N(-D), 1) \neq 0$.
Then $p \mid \#Ш(E_N(-D))$ if and only if
$$\mathrm{tr}(g_{p'}|W_D) \equiv \mathrm{tr}(g_N|W_D) \equiv \delta_p \cdot (H(D) - \delta_p H^{(p')}(D)) \pmod{p}.$$

Thank you for your attention.