RESEARCH STATEMENT

MARYAM KHAQAN

My research fits broadly into the framework of moonshine, a field of mathematics at the intersection of group theory, representation theory, and number theory. I'm particularly interested in using moonshine to answer questions in number theory, geometry and physics, as well as the other way around. In this document, I will give some background on moonshine (cf. Section 1), state a few of my results - explaining how my research fits into the story and uses the theory of moonshine to answer questions about elliptic curves (cf. Section 2), and summarize plans for future work (cf. Section 3.)

1. Moonshine

Group theory, broadly speaking, is the study of symmetries of an object, e.g., the symmetries of a square (rotations, reflections) form a finite group, and the symmetries of a circle form an infinite one. In the same way that integers can be broken down into their prime factors or molecules can be described based on the elements that make them up, finite groups can be decomposed into a composition of smaller groups. The ones that cannot be broken down any further (i.e., ones similar to elements) are called "simple groups." The classification of all finite simple groups is considered one of the most outstanding mathematical achievements of the 20th century. It took several decades of hundreds of mathematicians working worldwide to prove that (almost) all finite simple groups fit neatly into three infinite families - alternating groups, cyclic groups, and the finite groups of Lie type. There are 26 exceptions to this rule, the so-called "sporadic groups."

The largest of these sporadic groups is known as the "Monster group." The number of elements in the monster is $|\mathbb{M}| = 2^{46} \cdot 3^{20} \cdot 5^9 \cdot 7^6 \cdot 11^2 \cdot 13^3 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 41 \cdot 47 \cdot 59 \cdot 71$ which is $2^5 \cdot 3^7 \cdot 5^3 \cdot 7^4 \cdot 11 \cdot 13^2 \cdot 29 \cdot 41 \cdot 59 \cdot 71$ times that of the next largest sporadic simple group, the Baby Monster.

Since groups are fundamentally just symmetries of an object, one way of studying a finite group's structure is to categorize all the objects it describes the symmetries of. This is called representation theory, and the objects that the group acts on are called *representations*. The smallest non-trivial *irreducible representation* (i.e., one that cannot be broken down into smaller ones) of the Monster group is 196883-dimensional, and in some ways, this number is even more interesting than the number of elements of the Monster. For one, while 196883 is a lot smaller, it is still a decently large number, in that if it appears twice in two different contexts, you might wonder if the instances are related in some way.

This is what happened to John McKay, who noticed that 196884 appears as a Fourier coefficient of the normalized elliptic *modular invariant* $J(\tau) = q^{-1} + 196884q + 21493760q^2 + 864299970q^3 + O(q^4)$, which is a central object in the theory of modular forms. Here, $q = e^{2\pi i\tau}$ where τ is a complex number whose imaginary part is positive. Note that $f = q = e^{2\pi i\tau}$ is the simplest function that satisfies $f(\tau + 1) = f(\tau)$. In very basic terms, $J(\tau)$ is the simplest function (other than constants) that satisfies the equations $J(\tau + 1) = J(\frac{-1}{\tau}) = J(\tau)$. In fact, $J(\tau)$ is a generator of all such functions, i.e., you can write all other functions that satisfy $f(\tau + 1) = f(\frac{-1}{\tau}) = f(\tau)$ as a rational function in $J(\tau)$.

The coincidences don't stop there, either. John Thompson noted that the first few coefficients of $J(\tau)$ can actually be written as sums involving the smallest dimensions of irreducible representations of the Monster. For example:

$$\begin{aligned} 1 + 196883 &= 196884 \\ 1 + 196883 + 21296876 &= 21493760 \\ 2 \cdot 1 + 2 \cdot 196883 + 21296876 + 842609326 &= 864299970. \end{aligned} \tag{1}$$

In fact, if we look at the trace of an element of order two on the same representations, and add them together in a similar fashion,

$$\begin{aligned} 1 + 4371 &= 4372 \\ 1 + 4371 + 91884 &= 96256 \\ 2\cdot 1 + 2\cdot 4371 + 91884 + 1139374 &= 1240002 \end{aligned} \tag{2}$$

the numbers we get are Fourier coefficients of another well-known modular form, $T_{2A}(\tau) = q^{-1} + 4372q + 96256q^2 + 1240002q^3 + O(q^4)$. These observations inspired Thompson's conjecture [23] that there exists an infinite-dimensional $\mathbb{M}$-module V whose graded dimension is $J(\tau)$ and each of whose McKay–Thompson series $T_g(\tau) := \sum_{n\geq -1} \mathrm{tr}(g|V_n)q^n$ is a normalized principal modulus for a genus-zero subgroup Γ_g of $SL_2(\mathbb{R})$.

In particular, this means that the phenomenon we described above continues for each of the 194 columns in the Monster group's character table. Conway and Norton [4] investigated this further, explicitly described the relevant McKay-Thompson series, and christened this phenomenon "monstrous moonshine." In 1988, Frenkel, Lepowsky, and Meurmann [10] constructed a vertex operator algebra $V^\natural$ whose automorphism group is the Monster, and in 1992, Borcherds [1] proved that it satisfies the monstrous moonshine conjectures.

We note here that a normalized principal modulus is uniquely determined by its invariance group, so the assignment $g \to \Gamma_g$ determines each of the traces $\mathrm{tr}(g|V_n)$ for $g \in \mathbb{M}$ and $n \in \mathbb{Z}$. In particular, this allows one to compute the structure of V as an $\mathbb{M}$-module *without doing any computations with the Monster itself.*

2. My work

1. Moonshine for the Thomspon group. My recent work has focused on a subgroup of the Monster, *the Thompson group,* which is a sporadic simple group of order $2^{15}\cdot 3^{10}\cdot 5^3\cdot 7^2\cdot 13\cdot 19\cdot 31$. In [15], we prove the existence of an infinite-dimensional Thompson-module W whose graded dimension is the unique (weakly holomorphic) modular form of weight $\frac{3}{2}$ and level 4 in the Kohnen plus space with Fourier expansion $6q^{-5} + O(q)$, and whose McKay-Thompson series satisfy certain special properties. In fact, in the paper, we classify all such modules, but here we give a simpler version of the theorem for reference.

Theorem 1 ([15])**.** There exists an infinite-dimensional graded virtual Th-module

$$W := \bigoplus_{\substack{n>0 \\ n\equiv 0,3 \pmod 4}} W_n \tag{3}$$

such that for each rational conjugacy class $[g]$ of Th, the corresponding McKay–Thompson series,

$$\mathcal{F}_g(\tau) = 6q^{-5} + \sum_{\substack{n>0 \\ n\equiv 0,3 \pmod 4}} \mathrm{tr}\,(g|W_n)\,q^n \tag{4}$$

is a specific weakly holomorphic modular form with integer Fourier coefficients that satisfies the following properties:

- It has weight $\frac{3}{2}$, level $4|g|$ with a specific character (dictated by g) and satisfies the Kohnen plus space condition.
- It has a pole of order 5 at the cusp ∞, a pole of order $\frac{5}{4}$ at the cusp $\frac{1}{2|g|}$ if $|g|$ is odd, and vanishes at all other cusps.

This serves as an example of moonshine for the Thompson's group. We prove this theorem using techniques that were first suggested by Thompson and have been used extensively since (cf. [9, 21, 12]). For each rational conjugacy class, we define $f_g^{wh}(\tau)$ to be the projection onto the Kohnen plus-space of the Rademacher sum of weight $\frac{3}{2}$ and index -5 that transforms under the action of $\Gamma_0(4|g|)$ with a specific character ψ_g.

$$f_g^{wh}(\tau) = 6R^{[-5],+}_{\frac{3}{2},4|g|,\psi_g}(\tau) = 6q^{-5} + \sum_{\substack{n>0 \\ n\equiv 0,3 \pmod 4}} a_g(n)q^n. \tag{5}$$

Rademacher sums, when convergent, define mock modular forms of the specified weight and level. For f_g^{wh}, the space of shadows turns out to be zero, so f_g^{wh} satisfies the properties listed in the theorem for each g (cf. [3, 16, 2]). Specifying the behavior at the poles implies that the McKay–Thompson series $\mathcal{F}_g(\tau)$ is uniquely determined up to the addition of cusp forms. We thus have:

$$\mathcal{F}_g(\tau) = f_g^{wh}(\tau) + f_g^{cusp}(\tau) \tag{6}$$

for some f_g^{cusp} that lies in $S^+_{\frac{3}{2}}(\Gamma_0(4|g|), \psi_g)$.

For the collection $\{\mathcal{F}_g(\tau), g \in Th\}$ to be the McKay–Thompson series of a virtual module (as in Theorem 1), they must satisfy congruences modulo certain powers of primes that divide the order of the Thompson group. In simplified terms, the coefficients of $\mathcal{F}_g(\tau)$ need to satisfy all the congruences that the irreducible rational characters of Th do. We can check this by using the Sturm bound [22] and Brauer's characterization of generalized characters (cf. [21]) to reduce this to a feasible computation and then performing that computation using computer algebra systems PARI/GP [19] and GAP [11].

2. Applications to elliptic curves. An elliptic curve E over the rationals can be described as a smooth projective curve given by an equation of the form

$$y^2 = x^3 + ax + b \tag{7}$$

where $4a^3 + 27b^2 \neq 0$. It is well-known that the set of rational points $E(\mathbb{Q})$ of E has the structure of a finitely generated abelian group. That is, $E(\mathbb{Q}) = \mathbb{Z}^r \oplus E(\mathbb{Q})_{\text{tor}}$. Here $r \geq 0$ is called the (algebraic) rank of E, and $E(\mathbb{Q})_{\text{tor}}$ is a finite abelian group (cf. [20]). This is particularly interesting because elliptic curves and conic sections are the only examples of (smooth) curves where the set of rational points is not *apriori* finite (cf. Faltings' Theorem, [8]). At the same time, computing the rank r of a general elliptic curve is considered a hard problem in number theory. In fact, (proving or disproving) the *Birch and Swinnerton-Dyer Conjecture,* which, in its weak form states that the rank of a general elliptic curve equals the order of vanishing of its L-function $L_E(s)$ at $s = 1$, is one of the seven Millennium Prize Problems [24].

Consider the elliptic curve $E/\mathbb{Q}$ given by the Weierstrass equation,

$$E\colon y^2 = x^3 + 864x - 432. \tag{8}$$

For $d < 0$ a fundamental discriminant, let E^d denote the d^{th} quadratic twist of E,

$$E^d\colon y^2 = x^3 + 864d^2x - 432d^3. \tag{9}$$

Let $F(\tau)$ denote the unique (weakly holomorphic) modular form in $M^{+,!}_{\frac{3}{2}}(\Gamma_0(4))$ such that $F(q) = q^{-5} + O(q)$, and let $c(d)$ denote the coefficient of q^{-d} in the q-expansion for $F(\tau)$. Then in [15], we prove,

Theorem 2 ([15])**.** Let $d < 0$ be a fundamental discriminant which is not a quadratic residue modulo 19. If $c(d) \not\equiv 0 \pmod{19}$, then the Mordell–Weil group $E^d(\mathbb{Q})$ is finite i.e., rank$(E^d) = 0$.

Note that this theorem gives information about the rank of certain elliptic curves *without any computations on the curves themselves,* a fact that is reminiscent of moonshine.

To prove this theorem, we let g be an element of order 19 in the Thompson group. Then $S_g := S^+_{\frac{3}{2}}(\Gamma_0(4|g|), \psi_g)$ has dimension 1, so we let $b_g(n)$ denote the coefficients of the unique normalized cusp form in S_g. From the proof of Theorem 1, we get,

$$\mathcal{F}_g(\tau) = 6q^{-5} + \sum_{\substack{n>0 \\ n\equiv 0,3 \pmod{4}}} (a_g(n) + 18b_g(n))\, q^n, \tag{10}$$

where the 18 is a consequence of the congruences dictated by the irreducible rational characters of Thompson. Furthermore, since W is a virtual module for the Thompson group, we know the following congruence holds for each $p|\#Th$ (and in particular for $p = 19$) and for all $n > 0$,

$$\dim(W_n) \equiv \mathrm{tr}(g_p|W_n) \pmod{p} \tag{11}$$

where g_p is an element of order p. Thus, for all $n > 0$, we have:

$$\dim(W_n) \equiv a_g(n) + 18b_g(n) \pmod{19}, \tag{12}$$

for g an element of order 19 in the Thompson group.

Suppose for now that $a_g(n)$ is zero for $n = |d|$. Then, since the graded dimension of W is just $6F(\tau)$, we would get that if $19 \nmid c(d)$ as in the statement of the theorem, then $19 \nmid b_g(n)$. For $n = |d|$ where $d < 0$ is a fundamental discriminant such that $\left(\frac{d}{19}\right) = -1$, a lemma of Duncan, Mertens and Ono [7, Lemma 6.5] gives us that $L_{E^d}(1) \not\equiv 0 \pmod{19}$ and thus, in particular, $L_{E^d}(1) \neq 0$. By work of Kolyvagin (cf. [13, 17]) it is known that if $L_E(1)$ is non-zero, then $E(\mathbb{Q})$ is finite, which is a special case of the Birch and Swinnerton– Dyer Conjecture.

To prove that $a_g(d)$ is zero for d as above, we let $\mathcal{Q}_D^{(N)}$ be the set of positive definite quadratic forms $Q = [a, b, c] := ax^2 + bxy + cy^2$ of discriminant $-D = b^2 - 4ac < 0$ such that $N|a$. Then, $\Gamma_0(N)$ acts on $\mathcal{Q}_D^N$ with finitely many orbits. For $Q = [a, b, c] \in \mathcal{Q}_D^{(N)}$, we let τ_Q denote the unique root of $Q(x, 1)$ in the upper half-plane $\mathbb{H}$. Then we can use Corollary 1.3 of [18] to write

$$a_g(n) = \text{const.}^* \sum_{Q \in \mathcal{Q}_{5n}^{(19)}/\Gamma_0(19)} \chi_5(Q) \frac{J_{19}^+(\tau_Q)}{\omega^{(19)}(Q)}, \tag{13}$$

where J_{19}^+ is the normalized principle modulus for the group $\Gamma_0^+(19)$ (see [18] for a definition of $\omega^{(N)}(Q)$ and $\chi_D(Q)$). The important thing to note in Equation (13) is the following: for $n = |d|$ as above, we have that $-5|d| = 5d$ is not a square mod 19. Thus, there are no quadratic forms $[a, b, c]$ of discriminant $b^2 - 4ac = 5d$ such that $19|a$, and so $a_g(n) = 0$.

3. Other results. In [15], we also prove a more subtle result for quadratic twists of elliptic curves of conductor 14, which involves using the modules from Theorem 1 to detect the non-triviality of the Selmer and Tate–Shafarevich groups of these twists. The common theme is the same: these theorems are examples where one can use moonshine to answer number theoretic questions, and they allow one to extract information about elliptic curves *without any computations on the curves themselves*.

3. Future plans

My work in [15] opened the door to some further lines of inquiry that I am currently pursuing. Here I will describe two of these ideas in some detail.

1. Zagier's Grid. The function $F(\tau)$ introduced in Theorem 1 is part of a bigger story of its own. In [25], Zagier defined a sequence of modular forms of weight $\frac{3}{2}$ in the following way: for each positive integer $D \equiv 0, 1 \pmod 4$, let $g_D(\tau)$ denote the unique form in $M^{+,!}_{\frac{3}{2}}(\Gamma_0(4))$ of the form

$$g_D(\tau) = q^{-D} + \sum_{\substack{d \geq 0 \\ d \equiv 0,3 \pmod 4}} B(D, d) q^d. \tag{14}$$

Note that for $D = 5$, this is just $F(\tau)$ from Theorem 1, and in particular, $B(5, d) = c(d)$. Furthermore, for each $d > 0$ with $d \equiv 0, 3 \pmod 4$, we define $f_d(\tau)$ to be the unique modular form such that

$$f_d(\tau) = q^{-d} + \sum_{\substack{D > 0 \\ D \equiv 0,1 \pmod 4}} A(D, d) q^D. \tag{15}$$

Then, Zagier proved that $A(D, d) = -B(D, d)$ for all D and d (cf. [25, Theorem 4]).

In [14], Harvey and Reyhaun conjectured the existence of a moonshine module for the Thompson group, where the graded dimension is $2f_3(\tau) + 248f_0(\tau)$. Their conjecture was proven in [12]. The involvement of both $f_d(\tau)$ and $g_D(\tau)$ in moonshine for the Thompson group begs the question: is there a broader framework that incorporates the entire grid? For instance, for each choice of D, is there a moonshine module for the Thompson group whose graded dimension is $g_D(\tau)$ and whose McKay–Thompson series $\mathcal{F}_g^D(\tau)$ satisfy properties analogous to the ones listed in Theorem 1?

This project fits into the broader question: what other modular forms out there can be in a similar relationship with the Thompson group? Can we classify them all?

2. Conway Groups. Another well-known example of moonshine is one for the Conway groups, Co_0, and Co_1. The largest of the Conway groups, Co_0 is the group of automorphisms of the Leech lattice. It is not a simple group, but the quotient of Co_0 by its center, Co_1 is a sporadic simple group of order $2^{21}\cdot 3^9\cdot 5^4\cdot 7^2\cdot 11\cdot 13\cdot 23$. In [5, 6], Duncan and Mack-Crane construct super vertex operator algebras $V^{f\natural}$ and $V^{s\natural}$ whose automorphism groups are Co_0 and Co_1 respectively. In this case, the McKay–Thompson series also turns out to be normalized principle moduli for genus-zero subgroups of $SL_2(\mathbb{R})$.

I am currently working on computing traces of elements of the Conway group on g-twists of $V^{f\natural}$ and $V^{s\natural}$, for each g in Co_0. This project is aimed towards better understanding the algebraic structures in the moonshine modules that we already have an explicit construction for.

3. Long-term plans. Apart from the two projects mentioned above, one of my long-term research goals is to construct a moonshine module for the Thompson group with an underlying algebraic structure, such as a vertex operator algebra or a Lie algebra. Such a construction would provide more insight into the riddles of moonshine, as well as open avenues of future research.

At my future institution, I plan to collaborate with other researchers in various fields, especially number theory and physics, to explore further some of the connections that moonshine exhibits. I also look forward to including undergraduate and graduate students in my research, both by working with them individually and by teaching courses relevant to my research. For example, I would like to design a topics course consisting of short modules on all the math one needs to learn to read a classical paper in moonshine.

I look forward to continue exploring these areas both at Emory and at my next institution.

References

[1] Richard E. Borcherds. Monstrous moonshine and monstrous Lie superalgebras. *Inventiones mathematicae*, 109(1):405–444, 1992.

[2] Jan Hendrik Bruinier, Jens Funke, et al. On two geometric theta lifts. *Duke Mathematical Journal*, 125(1):45–90, 2004.

[3] Miranda C. N. Cheng and John F. R. Duncan. Rademacher sums and Rademacher series. In *Conformal field theory, automorphic forms and related topics*, pages 143–182. Springer, 2014.

[4] John H Conway and Simon P Norton. Monstrous moonshine. *Bulletin of the London Mathematical Society*, 11(3):308–339, 1979.

[5] John F. Duncan. Super-moonshine for Conway's largest sporadic group. *Duke Math. J.*, 139(2): 255–315, 2007. ISSN 0012-7094. doi: 10.1215/S0012-7094-07-13922-X. URL https://doi.org/10.1215/S0012-7094-07-13922-X.

[6] John F. R. Duncan and Sander Mack-Crane. The moonshine module for Conway's group. *Forum Math. Sigma*, 3:Paper No. e10, 52, 2015. doi: 10.1017/fms.2015.7. URL https://doi.org/10.1017/fms.2015.7.

[7] John F. R. Duncan, Michael H. Mertens, and Ken Ono. Pariah moonshine. *Nature Communications*, 9(1), 2017. doi: 10.1038/s41467-017-00660-y. URL https://www.nature.com/articles/s41467-017-00660-y.

[8] G. Faltings. Endlichkeitssätze für abelsche Varietäten über Zahlkörpern. *Invent. Math.*, 73(3): 349–366, 1983. ISSN 0020-9910. doi: 10.1007/BF01388432. URL https://doi.org/10.1007/BF01388432.

[9] Paul Fong. Characters arising in the Monster-modular connection. In *The Santa Cruz Conference on Finite Groups (Univ. California, Santa Cruz, Calif., 1979)*, volume 37 of *Proc. Sympos. Pure Math.*, pages 557–559. Amer. Math. Soc., Providence, R.I., 1980.

[10] Igor Frenkel, James Lepowsky, and Arne Meurman. *Vertex operator algebras and the Monster*, volume 134 of *Pure and Applied Mathematics*. Academic Press, Inc., Boston, MA, 1988. ISBN 0-12-267065-5.

[11] GAP. *GAP – Groups, Algorithms, and Programming, Version 4.10.1*. The GAP Group, 2019. URL https://www.gap-system.org.

[12] Michael J Griffin and Michael H Mertens. A proof of the Thompson moonshine conjecture. *Research in the Mathematical Sciences*, 3(1):36, 2016.

[13] Benedict H. Gross and Don B. Zagier. Heegner points and derivatives of L-series. *Invent. Math.*, 84(2):225–320, 1986. ISSN 0020-9910. doi: 10.1007/BF01388809. URL https://doi.org/10.1007/BF01388809.

[14] Jeffrey Harvey and Brandon Rayhaun. Traces of singular moduli and moonshine for the Thompson group. *Communications in Number Theory and Physics*, 10, 04 2015. doi: 10.4310/CNTP.2016.v10.n1.a2.

[15] Maryam Khaqan. Elliptic curves and Thompson's sporadic simple group. *arXiv preprint arXiv:2008.01607*, 2020.

[16] Winfried Kohnen. Fourier coefficients of modular forms of half-integral weight. *Mathematische Annalen*, 271(2):237–268, 1985.

[17] Victor A. Kolyvagin. Finiteness of and for a subclass of Weil curves. *Mathematics of the USSR-Izvestiya*, 32(3):523, 1989.

[18] Alison Miller and Aaron Pixton. Arithmetic traces of non-holomorphic modular invariants. *International Journal of Number Theory*, 6(01):69–87, 2010.

[19] *PARI/GP version* 2.11.2. The PARI Group, Univ. Bordeaux, 2019. available from http://pari.math.u-bordeaux.fr/.

[20] Joseph H Silverman. *The arithmetic of elliptic curves*, volume 106. Springer Science & Business Media, 2009.

[21] Stephen D. Smith. On the head characters of the Monster simple group. In *Finite groups—coming of age (Montreal, Que., 1982)*, volume 45 of *Contemp. Math.*, pages 303–313. Amer. Math. Soc., Providence, RI, 1985. doi: 10.1090/conm/045/822245. URL https://doi.org/10.1090/conm/045/822245.

[22] Jacob Sturm. On the congruence of modular forms. In *Number theory*, pages 275–280. Springer, 1987.

[23] John G. Thompson. Finite Groups and Modular Functions. *Bulletin of the London Mathematical Society*, 11(3):347–351, 10 1979. ISSN 0024-6093. doi: 10.1112/blms/11.3.347. URL https://doi.org/10.1112/blms/11.3.347.

[24] Andrew Wiles. The Birch and Swinnerton-Dyer conjecture. In *The millennium prize problems*, pages 31–41. Clay Math. Inst., Cambridge, MA, 2006.

[25] Don Zagier. Traces of singular moduli. In *Motives, Polylogarithms and Hodge Theory (Eds. F. Bogomolov, L. Katzarkov), Lecture Series 3*, pages 209–244. International Press, Somerville, 2002.