Distribution Agreement

Signature:

____________________________________ ____________

Victor Manuel R. Aricheta Date

Monstrous moonshine, elliptic curves and vertex algebras

By

Victor Manuel R. Aricheta

Doctor of Philosophy

Mathematics

John Duncan

Advisor

David Zureick-Brown

Committee Member

David Borthwick

Committee Member

Accepted:

Lisa A. Tedesco, Ph.D.

Dean of the James T. Laney School of Graduate Studies

Date

Monstrous moonshine, elliptic curves and vertex algebras

By

Victor Manuel R. Aricheta

B.S., University of the Philippines Diliman, 2010

M.S., University of the Philippines Diliman, 2014

Advisor: John Duncan, Ph.D.

An abstract of

A dissertation submitted to the Faculty of the

James T. Laney School of Graduate Studies of Emory University

in partial fulfillment of the requirements for the degree of

Doctor of Philosophy

in Mathematics

2019

Abstract

Monstrous moonshine, elliptic curves and vertex algebras

By Victor Manuel R. Aricheta

The topic of this dissertation is monstrous moonshine, which refers to the unexpected relationship between the monster sporadic group and the modular j-invariant. Despite being the first and best understood example of moonshine, monstrous moonshine has aspects that lack complete understanding. We investigate here three such aspects.

First we revisit a theorem of Ogg on supersingular j-invariants, and generalize it to supersingular elliptic curves with level structure. Ogg observed that the level one case yields a characterization of the primes dividing the order of the monster. We now know that this is partly explained by monstrous moonshine. Here we show that the corresponding analyses for higher levels give analogous characterizations of the primes dividing the orders of other sporadic simple groups (e.g. baby monster, Fischer's largest group). More generally we characterize, in terms of supersingular elliptic curves with level, the primes arising as orders of Fricke elements in centralizer subgroups of the monster. We also present a connection between supersingular elliptic curves and umbral moonshine.

Second we propose a definition of moonshine with a higher genus property that naturally extends the genus zero property of monstrous moonshine. We outline a method, inspired by monstrous moonshine, for searching for examples of moonshine with the higher genus property. We demonstrate the success of this strategy by employing it to obtain several examples of moonshine with the genus one property.

Third we generalize to certain vertex operator algebras the results of Duncan, Griffin and Ono regarding the asymptotic structure of the homogeneous subspaces of the moonshine module. We prove that an analogous result holds for any vertex operator algebra satisfying certain hypotheses.

Monstrous moonshine, elliptic curves and vertex algebras

By

Victor Manuel R. Aricheta

B.S., University of the Philippines Diliman, 2010

M.S., University of the Philippines Diliman, 2014

Advisor: John Duncan, Ph.D.

A dissertation submitted to the Faculty of the
James T. Laney School of Graduate Studies of Emory University
in partial fulfillment of the requirements for the degree of
Doctor of Philosophy
in Mathematics
2019

Acknowledgments

Of the many people who directly shaped this dissertation and the ideas in it, I am most grateful to my PhD advisor John Duncan who invariably provided me with the mathematical and emotional support that I needed to perform my research. Any reader who finds clarity and rigor in this work may thank John for his editorial skills; the remaining obscurities are due to me.

I am also thankful to David Borthwick, John Duncan and David Zureick-Brown for agreeing to be members of my dissertation committee. I could not have asked for a better committee. I learned a lot about number theory, in particular about modular and mock modular forms, from Ken Ono and the weekly student seminar that he ran, and for this I am also grateful. Thanks too to Lea Beneish with whom I struggled on a problem about vertex algebras. This problem became the basis of Chapter 5 of this work. I am grateful too to Lea Beneish, Maryam Khaqan, Jackson Morrow, Jayanth Guhan and Alexander Clifton for studying vertex algebras with me for two semesters. Finally I had so many questions about my research, and I am indebted to Luca Candelori, Scott Carnahan, Robert Griess, Simon Norton, Preston Wake, Robert Wilson and David Zureick-Brown for graciously answering some of these questions. All of these people directly contributed to my dissertation and I am most thankful to them.

The Institute of Mathematics of the University of the Philippines Diliman allowed me to take a long leave to pursue my graduate studies. I thank the entire institute, led then when I left by Marian Roque and now by Carlene Arceo. Thank you to my colleagues and my friends for providing emotional support and for shouldering heavier teaching loads while I studied abroad. Thank you too to the administration staff members for being incredibly patient with me with many paperwork. American schools accepted me to their math programs based in part on the recommendations of Jose Maria Balmaceda, Fidel Nemenzo and Noli Reyes, professors at the institute. I am very grateful to them. Lastly I thank Fidel Nemenzo. I first learned number theory from him more than a decade ago. He has since then been a constant source of motivation and advice, and I consider him my greatest mentor.

I had a smooth transition from the Philippines to the United States thanks to the Belen family. I cannot overstate my appreciation to Tita Sylvia and Tito Zar, my cousins Ate Jen, Ate Melissa and Darlene, my cousins-in-law Kuya Jay and Kuya DJ, and my nephew Jacob and nieces Ella, Elena, Sienna and Lexi for welcoming me to their family.

For teaching me beautiful mathematics I am grateful to my math professors at Emory University: Raman Parimala, David Borthwick, Suresh Venapally, David Zureick-Brown, John Duncan and James Nagy. They were the most inspiring and knowledgeable math teachers I have had in my long student life. I am also thankful to Terry Ingram for all the help she gave me in navigating the graduate program. I would also like to express my gratitude to the many people I met during my stay at Emory for making graduate school more colorful; thanks to Gabi Artasanchez, Olivia Beckwith, Isabel Chen, Ruofei Chen, Keely Creedle, Maddie Dawsey, Brad Elliott, Michael Griffin, David Hofmann, Seokho Jin, Kelvin Kan, Noam Kantor, Ariel Keller, Chris Keyes, Maryam Khaqan, Massi Lupo Pasini, Jan Macdonald, Michael Mertens, Sumit Mishra, Pooya Mobadersany, Ace Park, Pascal Philipp, Daniel Rackl, Majo Ramirez, Tomer Reiter, Catalina Rivera, Robert Schneider, Jessi Stooksbury, Cecilia Tortoreto, Sarah Trebat-Leder, Alexander Viguerie, Ian Wagner and Zhengyao Wu.

Of course I thank Alessandro Barone, Lea Beneish, Pio Esguerra, Sofia Guzzetti, Yunyi Hu, Mica Mojica, Jackson Morrow, Samy Wu, Iw Zambrano and Shawn Wang. They provided me with so much emotional support throughout these last five years. And I have made a lot of fond memories with each of them, from the hilarious to the unspeakable. I consider them my best friends during my years in graduate school.

Finally I will never be tired of thanking my parents Leila and Eric. They instilled in me the value of education, and provided me with a conducive environment for learning while I was growing up. I owe to them everything that I have accomplished thus far.

Para kay Nanay at Papa

Contents

List of Tables

Chapter 1

Introduction and summary of results

This dissertation is about *moonshine*, which in mathematics refers to the unexpected connection between group theory (particularly, finite groups and their representation theory) and number theory (particularly, modular functions and their generalizations). More specifically this dissertation is mainly concerned with the first example of the subject: *monstrous moonshine*. It is doubtless the best understood and most studied instance of moonshine, chiefly due to its pioneering nature. However our comprehension of monstrous moonshine remains incomplete; certain aspects of it are even now enigmatic. In this dissertation we investigate three of these monstrous moonshine mysteries.

1.1 Monstrous moonshine

One of the crowning achievements of 20th century mathematics is the complete *classification of finite simple groups*. This theorem, whose proof consists of hundreds of journal articles written by hundreds of mathematicians over the course of several decades, states that: A finite simple group either belongs to a well-behaved infinite family (i.e. a cyclic group of prime order, an alternating group of degree at least 5, or a simple group of Lie type) or is one of the 26 *sporadic simple groups*—finite simple groups that resist the organization provided by the aforementioned families [Sol01].

The most salient of the sporadic groups, by virtue of being the largest, is the *monster group* $\mathbb{M}$. Evidence for its existence was independently given by Bernd Fischer and Robert Griess in 1973 [Gri76], but its construction by Griess would not be accomplished until 1980 [Gri82]. In the interim vital information about the monster, like its order and its character table, accrued. The monster's size is enormous and gives it its name:

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

It has 194 irreducible representations, and the three smallest dimensions of these representations are 1, 196883 and 21296876 [CCN+85].

The sum of 1 and 196883—the two smallest dimensions of the irreducible representations of the monster—is 196884, familiar to number theorists as the first interesting Fourier coefficient of the *(normalized) modular j-function*

$$\begin{aligned}J(\tau) :&= \frac{(1 + 240\sum_{n>0}\sum_{d|n} d^3 q^n)^3}{q\prod_{n>0}(1-q^n)^{24}} - 744 \\ &= q^{-1} + 196884q + 21493760q^2 + 864299970q^3 + \cdots .\end{aligned}$$

Here $q = e^{2\pi i \tau}$. This intriguing coincidence was observed by John McKay in 1978, who communicated it to John Thompson, who subsequently found further tantalizing coincidences including

$$1 + 196883 + 21296876 = 21493760$$

$$2 \cdot 1 + 2 \cdot 196883 + 21296876 + 842609326 = 864299970$$

that express coefficients of the j-function (right hand side) as simple linear combinations of dimensions of irreducible representations of the monster (left hand side) [Tho79].

The j-function, it seems, knows the monster. This became even more apparent after John Horton Conway and Simon Norton published in 1979 their seminal *Monstrous Moonshine* paper [CN79]. In it they considered a formal series

$$V_{-1}q^{-1} + V_0 + V_1 q + V_2 q^2 + V_3 q^3 + \cdots$$

where the coefficients V_n are certain representations of the monster. These representations are the ones suggested by the numerical equations of Thompson, so for example V_{-1} is the trivial representation, V_0 is the representation of dimension zero, and V_1 is the direct sum of the trivial representation and the irreducible representation of dimension 196883. Following the recommendation of Thompson they replaced V_n with $V_n(g)$, the character of V_n at an element g of the monster. The resulting computations led them to conjecture that the functions

$$T_g(\tau) = q^{-1} + 0 + V_1(g)q + V_2(g)q^2 + V_3(g)q^3 + \cdots ,$$

now called the *McKay-Thompson series*, behave like the j-function, in that they are the *normalized principal moduli* of certain groups of *genus zero* (see Sections 2.1 and 2.2 for definitions). Conway and Norton referred to this conjecture as monstrous moonshine, to convey “the impression that things here are dimly lit, and that [they] were ‘distilling information illegally’ from the monster character table” (cf. page 6 of [Gan06]).

A modern succinct way of stating the monstrous moonshine conjecture is as follows: There exists a naturally defined infinite-dimensional $\mathbb{Z}$-graded $\mathbb{M}$-module

$$V^\natural = \bigoplus_{n \geq -1} V_n^\natural$$

such that the graded dimension of $V^\natural$ is the normalized modular j-invariant, and such that the graded trace

$$T_g(\tau) = \sum_{n \geq -1} \mathrm{tr}(g|V_n^\natural)\, q^n$$

of $g \in \mathbb{M}$ acting on $V^\natural$ is the principal modulus for a certain group of genus zero.

The monstrous moonshine conjecture is now a theorem. The existence of such a monster module was first verified numerically by A. Oliver L. Atkin, Paul Fong and Stephen D. Smith [Fon80]. A candidate for this module, called the *moonshine module*, was later constructed by Igor Frenkel, James Lepowsky and Arne Meurman in 1984 [FLM84]. And finally Richard Borcherds showed in 1992 that the graded trace functions of the moonshine module are indeed the principal moduli predicted by Conway and Norton, thereby proving the monstrous moonshine conjecture [Bor92]. In a later interview Borcherds was quoted as saying, “I was over the moon when I proved the moonshine conjecture” [Sin]. Borcherds was awarded the Fields medal in 1998 in part for this proof.

As is with other great problems in mathematics, the solution to the monstrous moonshine conjecture required the introduction and development of novel ideas and concepts, including the theory of *vertex operator algebras* and *generalized Kac-Moody algebras.* (See Section 5.1 for more information on vertex operator algebras.) Vertex operator algebras, for which the moonshine module is an example, are essentially the mathematical formulations of two-dimensional conformal field theories. Thus the unexpected relationship between the modular j-invariant and the monster group obtains a physical (particularly string theoretical) origin. For a comprehensive introduction to the current state of moonshine, and its connection to physics, we refer the reader to [AC18].

1.2 Monstrous moonshine mysteries

Borcherds's resolution of the monstrous moonshine conjecture is a triumph and showed that moonshine is not only true but has deep underlying reasons. Nevertheless, there are questions about monstrous moonshine that remain. The following three questions, which we discuss in more detail in the succeeding sections of this chapter, are some of them.

1. **Ogg's observation.** In a 1975 lecture, Tits mentioned that the order of the monster group is $|\mathbb{M}| = 2^{46}\cdot 3^{20}\cdot 5^{9}\cdot 7^{6}\cdot 11^{2}\cdot 13^{3}\cdot 17\cdot 19\cdot 23\cdot 29\cdot 31\cdot 41\cdot 47\cdot 59\cdot 71$. Ogg recognized that the primes p in this factorization are precisely the ones for which the genus of the modular curve $X_0^+(p)$ is zero [Ogg74]. Monstrous moonshine partly explains this coincidence but a full comprehension of this phenomenon is still lacking. Can we achieve a better understanding of Ogg's observation?

2. **Genus zero property.** The theory of vertex operator algebras can associate to any finite group an infinite-dimensional module for which the trace functions are modular. Amongst these examples the genus zero property distinguishes monstrous moonshine. Understanding the genus zero property entails understanding "higher genus moonshine". Can we give a reasonable definition of higher genus moonshine, and can we find examples?

3. **Subspaces of the moonshine module.** What is the multiplicity of an irreducible representation in the homogeneous subspace $V_n^\natural$ of the moonshine

module? This is one of the questions that John Duncan, Michael Griffin and Ken Ono considered in a 2014 paper [DGO15a]. By obtaining exact formulas for these multiplicities, they discovered that as $n \to \infty$ the representations $V_n^\natural$ tend to a multiple of the regular representation of the monster. Is this "asymptotic regularity" a unique feature of the moonshine module, or does it apply to more general vertex operator algebras?

1.3 Ogg's observation

1.3.1 Introduction

It was the 1978 observation of McKay that initiated the development of monstrous moonshine, but an earlier remark of Andrew Ogg in 1975 foreshadowed it. Ogg was in the audience of the inaugural lecture of Jacques Tits at the Collège de France, when the latter mentioned the order of the monster. Recall that this is the number:

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

Ogg recognized that the primes in this factorization are precisely the ones he had recently obtained geometrically from his work on *supersingular elliptic curves*.

A supersingular elliptic curve is an elliptic curve E over a field K of positive characteristic p such that $E(\bar{K})$ has no p-torsion. It turns out that the supersingularity of an elliptic curve depends only on the j-invariant of the curve, and that the *characteristic p supersingular j-invariants* lie in $\mathbb{F}_{p^2}$ [Deu41, Has35]. (See [KZ98] for a self-contained introduction to supersingular elliptic curves.) Can all these supersingular j-invariants be in the prime field $\mathbb{F}_p$? What Ogg found, which we refer to here as *Ogg's theorem*, is that the following statements are equivalent (cf. Corollaire of [Ogg74]).

- The characteristic p supersingular j-invariants all lie in the prime field $\mathbb{F}_p$.
- The normalizer of $\Gamma_0(p)$ in $\mathrm{SL}_2(\mathbb{R})$, denoted $\Gamma_0^+(p)$, has genus zero.

He computed the primes that satisfy any of the equivalent statements in his theorem and found out that it must be the primes in the set

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

Ogg observed—and thus we refer to it here as *Ogg's observation*—that these are the primes in the factorization of the order of the monster. He famously offered a bottle of Jack Daniels for an explanation of this "coincidence" (cf. Remarque 1 of [Ogg74]).

Ogg's observation is partly explained by monstrous moonshine. For each prime divisor p of the order of the monster, there is an element of the monster whose McKay-Thompson series is the principal modulus for $\Gamma_0^+(p)$. The genus of $\Gamma_0^+(p)$ is then forced to be zero. In other words, the primes dividing the order of the monster are necessarily included in the set $\mathfrak{O}$. To explain why the set $\mathfrak{O}$ is also a subset of the set of primes dividing the order of the monster, one would need a construction that naturally produces an element of order p of the monster given a modular curve $\Gamma_0^+(p)$ of genus zero. This is still an open problem.

In Chapter 3 of this dissertation we show that both Ogg's theorem and Ogg's observation generalize naturally. In so doing we provide further evidence that Ogg's observation is more than just a coincidence. With our analysis we are also able to exhibit a relationship between supersingular elliptic curves and umbral moonshine. This chapter is adapted from [Ari19]. The following is a summary of our results from Chapter 3.

1.3.2 Summary of results

It is useful, for purposes of generalization, to state Ogg's theorem in terms of modular curves. The modular curve $X_0(1)$, whose non-cuspidal points parametrize isomorphism classes of elliptic curves, has good reduction modulo any prime p. We call a point of $X_0(1)$ modulo p that corresponds to a supersingular elliptic curve in characteristic p a *supersingular point* of $X_0(1)$ modulo p. A supersingular point is defined over the prime field $\mathbb{F}_p$ if and only if the j-invariant of the corresponding elliptic curve is in $\mathbb{F}_p$. Also, by definition, the genus of $\Gamma_0^+(p)$ is the genus of the compactified quotient space $X_0^+(p) := (\Gamma_0^+(p)\backslash\mathbb{H})^*$. We can thus restate Ogg's theorem as follows: the supersingular points of $X_0(1)$ modulo p are all defined over $\mathbb{F}_p$ if and only if the genus of $X_0^+(p)$ is zero.

In this work we consider elliptic curves with level structure by replacing $X_0(1)$ by more general modular curves X. We give a characterization for the primes p that have the *rationality property for* X, by which we mean that all the supersingular points of X modulo p are defined over $\mathbb{F}_p$ (or are $\mathbb{F}_p$-rational, hence the label *rationality* property). This analysis yields several consequences. First, as mentioned earlier, we find that Ogg's theorem generalizes naturally (Theorem 1.3.1). Second, we discover that Ogg's observation also generalizes naturally (Theorem 1.3.3). Third, we find that the primes that have the rationality property detect the existence of *mock modular forms* with nonzero *shadows* in *umbral moonshine* (Theorem 1.3.5). (See Sections 2.6 and 2.9 for definitions.)

We consider the quotient of $X_0(N)$ by Atkin-Lehner involutions w_e, w_f, ... which we denote by $X_0(N)+e, f, \ldots$. (See section 2.8 for definitions.) The non-cuspidal points of these modular curves represent isomorphism classes of elliptic curves with level structure. By a theorem of Igusa these modular curves have good reductions modulo primes p not dividing N. Let $X = X_0(N)+e, f, \ldots$. Denote by $Q_p(X)$ the number of supersingular points of X modulo p—or equivalently the number of isomorphism classes of supersingular elliptic curves with level structure in characteristic p—that are not defined over $\mathbb{F}_p$. Let *genus*(X) denote the genus of X, and X^p the modular curve $X_0(Np)+p, e, f, \ldots$ obtained by taking the quotient of $X_0(Np)$ by Atkin-Lehner involutions w_p, w_e, w_f, $\ldots$ where $\{p, e, f, \ldots\}$ is understood to be the set $\{e, f, \ldots, p, pe, pf, \ldots\}$. Our first theorem gives a characterization for the primes that have the rationality property for these modular curves.

Theorem 1.3.1. *Let N be a positive integer, let $e, f, \ldots$ be exact divisors of N, and let $X = X_0(N)+e, f, \ldots$. If p is a prime not dividing N, then*

$$\frac{1}{2}Q_p(X) = \mathit{genus}(X^p) - \mathit{genus}(X).$$

Consequently, p has the rationality property for X if and only if the modular curves X and X^p have the same genus.

Theorem 1.3.1 naturally generalizes Ogg's theorem. Indeed, by letting $X = X_0(1)$, so that *genus*$(X) = 0$ and $X^p = X_0^+(p)$, this theorem says that p has the rationality property for $X_0(1)$ if and only if the genus of $X_0^+(p)$ is zero, which is precisely Ogg's theorem.

We now discuss a generalization of Ogg's observation. For this we consider modular curves X of the form $X_0(N)+e, f, \ldots$ with genus equal to zero. All such modular curves except three (i.e. $X_0(25)$, $X_0(49)+49$, $X_0(50)+50$) arise in monstrous moonshine. By Theorem 1.3.1, identifying the primes that have the rationality property for X reduces to determining the complete list of primes p such that X^p has genus zero. We obtain the complete list of primes that have the rationality property for all such X, and we collect this information in Appendix A.1. Note from this table that there are no primes that have the rationality property for the three non-monstrous modular curves.

Table 1.1 shows the first few rows of the table found in Appendix A.1. It contains

Table 1.1: Primes that have the rationality property for low levels.

X	primes p that have the rationality property for X
$X_0^+(2)$	3, 5, 7, 11, 13, 17, 19, 23, 31, 47
$X_0(2)$	3, 5, 7, 11, 23
$X_0^+(3)$	2, 5, 7, 11, 13, 17, 23, 29
$X_0(3)$	2, 5, 11

modular curves X of levels 2 and 3 and the corresponding primes that have the rationality property for X. Notice that the primes on the first row—the primes that have the rationality property for $X_0^+(2)$—are exactly the odd primes dividing the order of the *baby monster* sporadic group. Similarly, the primes in the third row are the primes, not equal to 3, that divide the order of the largest *Fischer group*, another sporadic group. Thus the primes that have the rationality property for modular curves of higher level characterize the primes dividing the orders of other sporadic groups; these are natural generalizations of Ogg's observation.

Remark 1.3.2. *These generalizations of Ogg's observation to the baby monster group and the largest Fischer group have been found, recently and independently, by Nakaya using analytic methods (e.g. class number estimates) [Nak18]. He conjectured generalizations of Ogg's observation to the Harada-Norton and Held sporadic groups. Theorem 1.3.1 confirms this conjecture (cf. entries for $X_0(5)+$ and $X_0(7)+$ in Appendix A.1).*

In fact we generalize Ogg's observation to all *monstrous modular curves*—i.e. modular curves arising in monstrous moonshine—of the form $X_0(N)+e, f, \ldots$ as follows. If $X = \Gamma\backslash\mathbb{H}^* \neq X_0(27)+27$ we denote by $C(X)$ any of the conjugacy classes of the monster whose McKay-Thompson series is the principal modulus for Γ. If $X = X_0(27)+27$ then there are exactly two conjugacy classes of the monster whose McKay-Thompson series are both equal to the principal modulus for $\Gamma_0(27)+27$. We let $C(X_0(27)+27)$ be the smaller of these conjugacy classes; this class is labelled 27A in the ATLAS [CCN$^+$85]. Finally, by a *Fricke element* of the monster of prime order

p we mean an element of the monster whose McKay-Thompson series is the principal modulus for $X_0^+(p)$. A Fricke element of order p is the same as any representative of the conjugacy class labelled pA in the ATLAS.

Theorem 1.3.3. *Let X be a monstrous modular curve X of the form $X_0(N)+e, f, \ldots$. If p is a prime that does not divide N, then p has the rationality property for X if and only if the centralizer of $g \in C(X)$ in the monster contains a Fricke element of order p.*

Ogg's observation is again recovered from Theorem 1.3.3 by setting $X = X_0(1)$, and thus we find that Ogg's observation, just like Ogg's theorem, is the first case of a more general phenomenon. Theorem 1.3.3 suggests that Ogg's observation is not a statement about the primes dividing the order of the monster per se, but a statement about the Fricke elements of the monster. This hints that a better understanding of the Fricke elements is necessary for a full understanding of Ogg's observation.

Remark 1.3.4. *For the monstrous modular curves of the form $X = X_0(n|h)+e, f, \ldots$, i.e. compactified quotients of the upper half-plane by groups of $n|h$-type, one can analogously define X^p to be the modular curve $X_0(np|h)+p, e, f, \ldots$ where as before $\{p, e, f, \ldots\}$ is the set $\{e, f, \ldots, p, pe, pf, \ldots\}$. In view of the characterization given by Theorem 1.3.1, we may say that a prime p has the rationality property for a monstrous modular curve X if X and X^p have the same genus. With this generalized definition Theorem 1.3.3 holds for any monstrous modular curve X.*

Theorem 1.3.3 gives a connection between supersingular elliptic curves with level structure and monstrous moonshine. We point out another connection, an unexpected one, between supersingular elliptic curves and umbral moonshine. (See Section 2.9 for definitions.) Each of the 23 cases of moonshine in umbral moonshine has an associated genus zero modular curve called its *lambency*. We refer to these 23 modular curves as *umbral modular curves*. For each umbral modular curve X there is an *umbral* *group* G^X that serves as an analogue of the monster group, i.e. there exists a graded representation K^X of G^X such that the graded trace H_g^X of the action of $g \in G^X$ on K^X is a distinguished vector-valued mock modular form of weight one-half. There is also a naturally defined quotient of G^X denoted $\bar{G}^X$, and we denote by n_g the order of the image of $g \in G^X$ in $\bar{G}^X$. This integer n_g is the level of H_g^X.

Theorem 1.3.5. *Let X be an umbral modular curve and let p be a prime not dividing the level of X. Then the prime p has the rationality property for X if and only if there exists an element $g \in G^X$ such that $n_g = p$ and the shadow of H_g^X is nonzero.*

A mock modular form is a classical modular form if and only if its shadow is zero. Therefore Theorem 1.3.5 says that the primes that have the rationality property for the umbral modular curves are exactly the primes that occur as levels of genuinely mock modular graded trace functions.

Theorem 1.3.5 gives a connection between supersingular elliptic curves and umbral moonshine, while Theorem 1.3.3 provides another connection between supersingular elliptic curves and monstrous moonshine. We may thus regard supersingular elliptic curves as a link between monstrous and umbral moonshine. We record this in the following corollary, where the notations are as in Theorems 1.3.3 and 1.3.5.

Corollary 1.3.6. *Let X be a modular curve that is both a monstrous modular curve (i.e. a modular curve that appears in monstrous moonshine) and an umbral modular curve (i.e. a modular curve that appears as a lambency in umbral moonshine). Let p be a prime that does not divide the level of X. The centralizer of an element in the conjugacy class $C(X)$ of the monster contains an order p Fricke element if and only if there is an element g of the umbral group G^X such that corresponding mock modular form H_g^X has level p and nonzero shadow.*

Lastly, we consider the modular curves of the form $X_0(N)$ of genus zero and present another way of checking whether a prime has the rationality property for

$X_0(N)$. This alternative method explicitly computes *supersingular polynomials for* $X_0(N)$, which we will define shortly. The point is that a prime p has the rationality property for $X_0(N)$ if and only if the pth supersingular polynomial for $X_0(N)$ splits completely into linear factors over $\mathbb{F}_p$. Note that these supersingular polynomials have already appeared in the literature, for example, in relation to the Kaneko-Zagier differential equations for low level Fricke groups [Sak15] and in connection to Atkin orthogonal polynomials [Tsu07, Sak11]. However, the methods for computing these supersingular polynomials have been written down only for low levels. We give here a way of calculating these polynomials for all $X_0(N)$ of genus zero.

Let p be a prime not dividing N, and let T_N be the principal modulus for $X_0(N)$ given in Appendix A.2. Let $\mathrm{SS}_p(N)$ be the set of supersingular points of $X_0(N)$ modulo p. The pth supersingular polynomial for $X_0(N)$ is the polynomial

$$\mathrm{ss}_p^{(N)}(x) := \prod_{E \in \mathrm{SS}_p(N)} (x - T_N(E)).$$

That the rationality property can be determined by looking at the splitting property of this polynomial follows from the definition, because a point x in $X_0(N)$ modulo p is defined over $\mathbb{F}_p$ if and only if $T_N(x) \in \mathbb{F}_p$.

In Section 3.5 we describe how a certain polynomial $f_p^{(N)} \in \mathbb{Q}[x]$ arises from a modular form f of weight $p-1$ and level one. If f is chosen to be the weight $p-1$ Eisenstein series (among others) then this polynomial turns out to encode almost all the T_N-values of supersingular points on $X_0(N)$ modulo p. The few supersingular points not covered by this polynomial is encoded in another polynomial $g_p^{(N)}$ which we give in Appendix A.4. (See also Section 3.5.)

Theorem 1.3.7. *Let $p \geq 5$ be a prime, and let f be any of E_{p-1}, G_{p-1}, or H_{p-1} as*

Table 1.2: Supersingular polynomials for $X_0(2)$.

p	$ss_p^{(2)}(x)$
5	$(x+1)$
7	$(x+1)\cdot(x+6)$
11	$(x+3)\cdot(x+5)\cdot(x+9)$
13	$(x+1)\cdot(x^2+8x+1)$
17	$(x+1)\cdot(x+16)\cdot(x^2+13x+16)$
19	$(x+1)\cdot(x+7)\cdot(x+11)\cdot(x^2+9x+11)$
23	$(x+3)\cdot(x+5)\cdot(x+15)\cdot(x+16)\cdot(x+17)\cdot(x+18)$
29	$(x+16)\cdot(x+23)\cdot(x+24)\cdot(x^2+24x+16)\cdot(x^2+25x+23)$

defined in Section 3.5. Then

$$ss_p^{(N)} \equiv \pm f_p^{(N)} g_p^{(N)} \pmod{p}.$$

It is straightforward to write an algorithm in a computer algebra system (e.g. Sage [Dev16], PARI/GP [G$^+$]) that takes a modular form f of weight $p-1$ and level one as an input and produces the polynomial $f_p^{(N)}$ as an output. Therefore Theorem 1.3.7 provides a simple way of explicitly computing supersingular polynomials for $X_0(N)$. The first few supersingular polynomials for $X_0(2)$ are given in Table 1.2. Note that these polynomials split completely into linear factors over $\mathbb{F}_p$ for $p = 5, 7, 11, 23$. Therefore these primes have the rationality property for $X_0(2)$, a fact that agrees with the information in Table 1.1. Moreover the number of quadratic factors in $\mathrm{ss}_p^{(2)}$ coincides with the genus of $X_0(2)^p = X_0(2p)+p$ (cf. Table 3.1 in Section 3.2) which is consistent with Theorem 1.3.1.

1.4 Genus zero property

1.4.1 Introduction

Another intriguing aspect of monstrous moonshine is the genus zero property. Recall that this means that the McKay-Thompson series T_g for $g \in \mathbb{M}$ is not only a modular function for a certain discrete subgroup Γ_g of $\mathrm{SL}_2(\mathbb{R})$ but also the generator of the field of functions that are Γ_g-invariant. Since two functions are needed to generate the field of functions that are invariant under subgroups of positive genera, the subgroups Γ_g appearing in monstrous moonshine must necessarily have genus zero. This genus zero property is also shared by Conway moonshine [Dun07, DMC15], another example of moonshine where the graded trace functions are modular forms of weight zero—a weight zero moonshine. Are there examples of weight zero moonshine that possess a “higher genus property”, assuming we can reasonably define such a property?

We note that, naively, this genus zero property is not shared by Mathieu moonshine (and other recent examples of moonshine) which features mock modular forms of weight $\frac{1}{2}$ for subgroups that are not genus zero. (See Section 2.9 for more information about Mathieu moonshine.) However John Duncan and Igor Frenkel showed that the genus zero property of monstrous moonshine is equivalent to another property known as *Rademacher summability* [DF11]. (See Section 2.7 for definitions.) As it turns out, Mathieu moonshine and umbral moonshine also satisfy this property [CD12, CDH18]. The Rademacher summability property may therefore be considered as a generalization of the genus zero property.

In Chapter 4 of this dissertation we propose a definition of weight zero moonshine with the higher genus property, and provide examples. The following is a summary of our results from Chapter 4.

1.4.2 Statement of results

The first thing that we propose is a definition of higher genus moonshine. We believe that, similar to the genus zero case, a reasonable definition should require the graded trace functions to be generators of certain fields of modular functions. As mentioned earlier, two functions are needed to generate the field of Γ-invariant functions whenever the genus of Γ is positive. This explains the existence of two modules, instead of just one, in our proposed definition.

Definition 1.4.1 (genus g moonshine for X)**.** *Let X be a modular curve of genus g. We say that there is a* genus g moonshine for X *if there exists a non-trivial finite group G and a pair of graded G-modules $K^{(x)}$ and $K^{(y)}$ such that: the graded dimension functions of $K^{(x)}$ and $K^{(y)}$ generate the function field of X; and for each non-identity $h \in G$ the graded traces of h acting on $K^{(x)}$ and $K^{(y)}$ generate the function field of a modular curve $X_h \neq X$ of genus g.*

We consider genus one moonshine[1], for which the main theorem is the following. (See Section 2.8 for notations.)

Theorem 1.4.2. *There is genus one moonshine for X, where X is any of the following: $X_0(11)$; $X_0(14)$+2; $X_0(15)$; $X_0(15)$+3; $X_0(17)$; $X_0(19)$; $X_0(21)$; $X_0(21)$+7; $X_0(26)$+2; $X_0(26)$+13; $X_0(35)$+5; $X_0(37)$+; $X_0(39)$+3; $X_0(43)$+; $X_0(53)$+; $X_0(55)$ +11; $X_0(57)$+; $X_0(58)$+; $X_0(65)$+; $X_0(77)$+; $X_0(91)$+.*

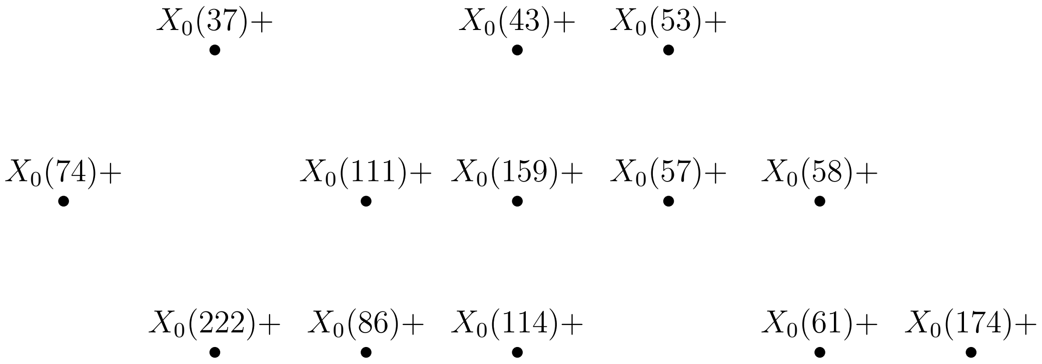
Theorem 1.4.2 says that genus one moonshine exists and is in fact in abundance. For the remainder of this subsection we briefly provide the idea of how we were able to obtain these examples of genus one moonshine.

Let X be a modular curve of genus one. The first step in finding an example of genus one moonshine for X is to formulate an educated guess, a guess informed by monstrous moonshine, about the other genus one modular curves X_h that could appear as domains of our graded trace functions. In their monstrous moonshine paper Conway and Norton defined the power of a modular curve of the form $X_0(n|h)+e, f, \ldots$. (See Section 4.2 for the definition of this power map.) If X_1 and X_2 are the modular curves assigned by monstrous moonshine to the conjugacy classes C_1 and C_2 of the monster respectively, then under their definition $X_1 = X_2^d$ if and only if $C_1 = C_2^d$. In particular, since every conjugacy class of the monster powers

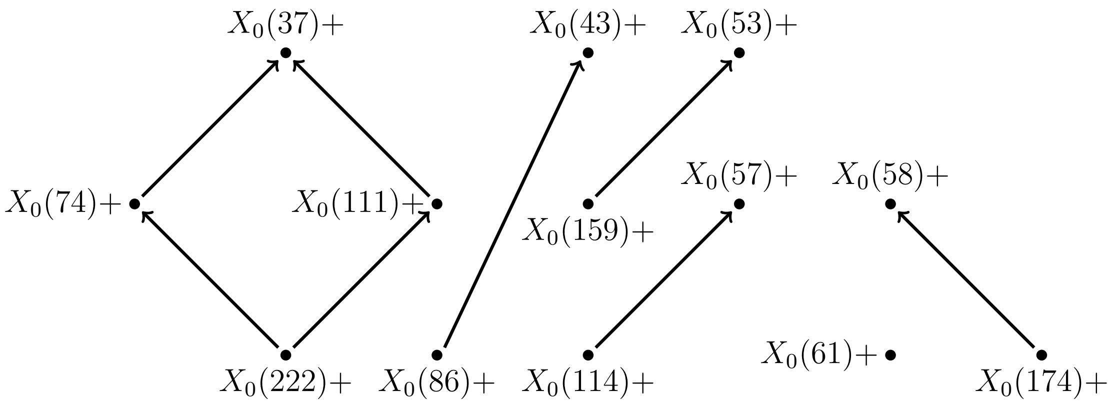
[1] We are also aware of examples of genus two and genus three moonshine.

up to the conjugacy class $1A$ of the identity element, this means that every modular curve appearing in monstrous moonshine powers up to the one associated to the class $1A$, i.e. the modular curve $X_0(1)$. We hypothesize, following this simple observation, that if a genus one moonshine for X exists then the modular curves X_h appearing in this moonshine power up to the modular curve associated to the class $1A$ of the identity element, i.e. the modular curve X. Moreover, and again following monstrous moonshine, we guess that if this genus one moonshine assigns modular curves X_1 and X_2 to the conjugacy classes C_1 and C_2 of a group G respectively, then $X_1 = X_2^d$ if and only if $C_1 = C_2^d$.

For example, the following (non-exhaustive) list of genus one modular curves, each represented by a node:



may be grouped into several constellations using the power maps of Conway and Norton. In the following diagram a directed arrow from node X_1 to node X_2 means that $X_1^d = X_2$ for some positive integer d.



We call a set $\mathcal{X}$ of modular curves a *compatible collection of modular curves with base* X if the modular curves in $\mathcal{X}$ all have the same genus, and if there exists $X \in \mathcal{X}$ such that every $Y \in \mathcal{X}$ powers up to X. For example, the modular curves appearing in monstrous moonshine form a compatible collection of genus zero modular curves with base $X_0(1)$. The set $\{X_0(37)+, X_0(74)+, X_0(111)+, X_0(222)+\}$ is a compatible collection of genus one modular curves with base $X_0(37)+$.

Given a compatible collection $\mathcal{X}$ of modular curves with base X, the next step is to find a group G with the following property: to each conjugacy class C of G we may assign a modular curve $Y \in \mathcal{X}$ such that this assignment preserves the power maps—i.e. if X_1 and X_2 are the modular curves assigned to C_1 and C_2 respectively, then $X_1 = X_2^d$ if and only if $C_1 = C_2^d$.

Once the initial guesses have been produced the final step is to compute, via Rademacher sums, generators for the modular curves in $\mathcal{X}$ (cf. Section 4.3) and then show computationally that these generators may in fact be interpreted as the graded traces of the action of G on certain graded G-modules. This gives a genus one moonshine for X. The details of these steps are provided in the fourth chapter of this dissertation.

Theorem 1.4.2 gives rise to several questions. For instance, in each example of genus one moonshine that we offer the modular curves that appear in it turn out to be elliptic curves that are isogenous to each other. Can moonshine detect the arithmetic of these elliptic curves? Also, all of our examples come from considering compatible collection of modular curves. Is it possible to find an example of genus one moonshine where the modular curves do not form a compatible collection? And finally, in coming up with examples we only used modular curves of the form $X_0(n)+e, f, \ldots$. What other groups could appear if we consider modular curves of a more general type? We still do not have the answers to these questions; Theorem 1.4.2 and the questions that emerge from it are only the beginning of the study of higher genus moonshine.

1.5 Subspaces of the moonshine module

1.5.1 Introduction

McKay and Thompson's observation—that the coefficients of the modular j-function may be expressed as sums of dimensions of irreducible representations of the monster—does not seem to be interesting on the surface, mainly because one may trivially declare the homogeneous subspaces $V_n^\natural$ to be an appropriate multiple of the trivial representation of dimension one. This is of course not what Thompson had in mind when he proposed the existence of an infinite-dimensional representation of the monster with graded dimension equal to the normalized modular j-invariant. What he meant was later crystallized by Conway and Norton into the monstrous moonshine conjecture.

Still, could it be that copies of the trivial representation crowd out the other arguably more interesting irreducible representations of the monster in the homogeneous subspaces $V_n^\natural$? How many copies of each irreducible representation are there in $V_n^\natural$? In a 2014 paper John Duncan, Michael Griffin and Ken Ono provided an answer to this question [DGO15a].

Let $M_1^{(\mathbb{M})}, \ldots, M_{194}^{(\mathbb{M})}$ be the irreducible representations of $\mathbb{M}$ and let $\mathrm{m}_i(n)$ be the multiplicity of the irreducible representation $M_i^{(\mathbb{M})}$ in $V_n^\natural$:

$$V_n^\natural = \mathrm{m}_1(n)M_1^{(\mathbb{M})} \oplus \cdots \oplus \mathrm{m}_{194}(n)M_{194}^{(\mathbb{M})}.$$

They obtained exact formulas for the multiplicities $\mathrm{m}_i(n)$ by expressing them as linear combinations of the coefficients of the principal moduli in monstrous moonshine, whose exact formulas may then be obtained using the theory of *Maass-Poincaré series*. These exact formulas imply in particular that

$$\mathrm{m}_i(n) \sim \frac{e^{4\pi\sqrt{n}}}{\sqrt{2}|\mathbb{M}|n^{3/4}} \dim M_i^{(\mathbb{M})} \tag{1.1}$$

as $n \to \infty$. Thus copies of the trivial representation in fact occur the least among the irreducible representations of the monster. Moreover, these formulas show that

$$\lim_{n\to\infty} \frac{\mathrm{m}_i(n)}{\sum_{j=1}^{194} \mathrm{m}_j(n)} = \frac{\dim M_i}{\sum_{j=1}^{194} \dim M_j} \tag{1.2}$$

which means that the representations $V_n^\natural$ tend to a multiple of the regular representation as $n \to \infty$. Thus the moonshine module exhibits another curious property: the moonshine module is *asymptotically* $\mathbb{M}$*-regular*, the phrase we employ to say that it satisfies (1.2).

In Chapter 5 of this dissertation we show, in a joint work with Lea Beneish, that asymptotic regularity is a property that is possessed by vertex operator algebras for which the moonshine module is the first natural example. This chapter is an expanded version of Section 3.2 of [AB16]. The following is a summary of our results from Chapter 5.

1.5.2 Summary of results

Let $K = \bigoplus K_n$ be a $\mathbb{Z}$-graded representation of a finite group G. We define two notions that concern K. First, we say that K is *asymptotically G-regular* or that it possesses *asymptotic G-regularity* if

$$\lim_{n\to\infty} \frac{\mathrm{m}_i(n)}{\sum_{i=1}^{s} \mathrm{m}_i(n)} = \frac{\dim M_i}{\sum_{i=1}^{s} \dim M_i},$$

where $M_1, \ldots, M_s$ are the irreducible representations of G and $\mathrm{m}_i(n)$ is the multiplicity of M_i in the homogeneous subspace K_n. This is the abstraction of the asymptotic $\mathbb{M}$-regularity of the moonshine module. Second, suppose $c_g(n) := \mathrm{tr}(g|K_n) \in \mathbb{R}$ for all $g \in G$ and all n. We say that K has *dominant identity trace* if for every $g \in G$ that is not equal to the identity element e we have $c_g(n) = o(c_e(n))$ as $n \to \infty$. The following lemma shows that the dominant identity trace property is sufficient for the asymptotic G-regularity of a graded representation.

Lemma 1.5.1. *Let G be a finite group with identity element e and let $K = \bigoplus K_n$ be a $\mathbb{Z}$-graded representation of G. Let $M_1, \ldots, M_s$ be the irreducible representations of G and let $\mathrm{m}_i(n)$ be the multiplicity of M_i in K_n. If K has dominant identity trace then*

$$\mathrm{m}_i(n) \sim \frac{1}{|G|} \dim M_i \dim K_n$$

as $n \to \infty$. Consequently K is asymptotically G-regular.

In some cases the dimension of K_n has known asymptotics in terms of simple functions. This is the case with the Mathieu moonshine module $K^\natural = \bigoplus K_n^\natural$, an example of a graded representation of the largest Mathieu group M_{24} that has dominant identity trace, and whose homogeneous subspaces have dimensions that satisfy

$$\dim K_n \sim \frac{4}{\sqrt{8n-1}} e^{\pi\sqrt{8n-1}/2}$$

as $n \to \infty$ [CD12]. These asymptotics and Lemma 1.5.1 imply the following corollary, which is the Mathieu moonshine analogue of (1.1).

Corollary 1.5.2. *Let $K^\natural = \bigoplus K_n^\natural$ be the Mathieu moonshine module. Let $M_i^{(M_{24})}$ denote an irreducible representation of the largest Mathieu group M_{24}, and let $\mathrm{m}_i(n)$ be the multiplicity of $M_i^{(M_{24})}$ in $K_n^\natural$. Then*

$$\mathrm{m}_i(n) \sim \frac{4e^{\pi\sqrt{8n-1}/2}}{|M_{24}|\sqrt{8n-1}} \dim M_i^{(M_{24})}$$

as $n \to \infty$, and $K^\natural$ is asymptotically M_{24}-regular.

Our goal is to apply Lemma 1.5.1 to graded representations that possess a rich algebraic structure—more precisely, vertex operator algebra structure—like that of the moonshine module. (See Section 5.1 for more information on vertex operator algebras.) Vertex operator algebras are in particular graded vector spaces

$$V = \bigoplus_{n=0}^{\infty} V_{n+\rho(V)} \qquad (\rho(V) \in \mathbb{Z})$$

satisfying several axioms, and the moonshine module is a beautiful example of a vertex operator algebra that is:

- *holomorphic*, meaning a vertex operator algebra whose only irreducible module is itself;
- *C_2-cofinite*, a technical condition on a vertex operator algebra introduced by Yongchang Zhu in [Zhu96] to ensure the modularity of its characters;
- and *CFT type*, meaning a vertex operator algebra where $\rho(V) = 0$ and $V_0 \cong \mathbb{C}$.

Remark 1.5.3. *The moonshine module as we have written it starts with $V_{-1}^\natural$, and so it seems that it is not of CFT type. However this is just an issue of notation. The correct indexing of the moonshine module, for it to satisfy the axioms a vertex operator algebra, is $V^\natural = \bigoplus_{n=0}^{\infty} \hat{V}_n^\natural$ where $\hat{V}_n^\natural = V_{n-1}^\natural$.*

Another important notion concerning vertex operator algebras, which we will need to finally state our theorem, is the following: To each *automorphism* g of a holomorphic vertex operator algebra V—i.e. a linear operator satisfying properties that respect the axioms of a vertex operator algebra—of finite order T there is an associated vector space, essentially unique, called the *g-twisted sector* of V. (See Section 5.2 for more details.) The g-twisted sector of V, which we denote by $V(g)$, has a grading

$$V(g) = \bigoplus_{n=0}^{\infty} \hat{V}(g)_{\frac{n}{T}+\rho(V(g))}.$$

The following theorem states that holomorphic C_2-cofinite vertex operator algebras of CFT types, that is to say vertex operator algebras that are very much like the moonshine module, have the dominant identity trace property provided that they satisfy a condition concerning their twisted sectors.

Theorem 1.5.4. *Let V be a holomorphic C_2-cofinite vertex operator algebra of CFT type. Let G be a finite group of automorphisms of V. Let $g \in G$ and denote by $V(g)$ the unique (up to equivalence) g-twisted sector of V. If the conformal weight $\rho(V(g))$ of $V(g)$ is positive for all $g \neq e$ then the G-module V has dominant identity trace. Consequently V is asymptotically G-regular.*

Theorem 1.5.4 generalizes the asymptotic $\mathbb{M}$-regularity of the moonshine module to other vertex operator algebras. This theorem however requires the knowledge of the *positivity condition on twisted sectors*, meaning that $\rho(V(g))$ is positive for all $g \in G\backslash\{e\}$. Is this assumption needed? We used this assumption in the proof, but it turns out that the positivity condition on twisted sectors may be an unnecessary hypothesis since it is conjectured to always hold for any such pair (V, G). See Conjecture 1.1 in [Möl18]. Sven Möller however has shown that the positivity condition holds for certain pairs (V, G), and from this we have the following corollary. (See Section 5.5 for notations.)

Corollary 1.5.5. *Let (V, G) be either of the following:*

- *$V = W^{\otimes k}$ ($k \in \mathbb{Z}_{\geq 0}$) where W is a holomorphic C_2-cofinite vertex operator algebra of CFT type, and $G \leq S_k$;*

- *V is a vertex algebra associated to an even, unimodular and positive-definite lattice, and $G \leq K_0 \cdot O(\hat{L})$.*

Then the G-module V has dominant identity trace. Consequently V is asymptotically G-regular.

Chapter 2

Preliminaries

2.1 The upper half-plane and its quotients

The domain of definition of modular forms and functions is the complex *upper half-plane* $\mathbb{H}$, defined to be the set of complex numbers $x + iy$ where x and y are real numbers with $y > 0$. It is equipped with the metric $(\mathrm{d}s)^2 = y^{-2}((\mathrm{d}x)^2 + (\mathrm{d}y)^2)$, and is a model of two-dimensional hyperbolic geometry.

The isometries of $\mathbb{H}$ are the linear fractional transformations

$$F : \tau \mapsto \frac{a\tau + b}{c\tau + d}$$

where a, b, c, d are real numbers satisfying $ad - bc > 0$. As such, the isometries of $\mathbb{H}$ may be naturally identified with (pairs of) elements of the *special linear group* $\mathrm{SL}_2(\mathbb{R})$, whose elements are 2×2 real matrices with determinant one[1]. More explicitly, for $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{R})$ and $\tau \in \mathbb{H}$, we have the action

$$\gamma\tau := \frac{a\tau + b}{c\tau + d}. \tag{2.1}$$

[1] The group of isometries of $\mathbb{H}$ is identified with $\mathrm{PSL}_2(\mathbb{R}) = \mathrm{SL}_2(\mathbb{R})/\{\pm I\}$.

There is an obvious discrete subgroup of $\mathrm{SL}_2(\mathbb{R})$ which is the *modular group* $\mathrm{SL}_2(\mathbb{Z})$, consisting of 2×2 integer matrices with determinant one. We will be interested with discrete subgroups of $\mathrm{SL}_2(\mathbb{R})$ that are commensurable with $\mathrm{SL}_2(\mathbb{Z})$. For a positive integer N, the *Hecke group*

$$\Gamma_0(N) := \{ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z}) : c \equiv 0 \pmod{N} \}$$

is an example of such a group.

In this dissertation we will assume that Γ is a discrete subgroup of $\mathrm{SL}_2(\mathbb{R})$ commensurable with $\mathrm{SL}_2(\mathbb{Z})$. Since Γ is commensurable with $\mathrm{SL}_2(\mathbb{Z})$, the action (2.1) of Γ on $\mathbb{H}$ extends to an action of Γ on $\mathbb{H}^* := \mathbb{H} \cup \mathbb{P}^1(\mathbb{Q})$. There are only finitely many orbits of Γ on $\mathbb{P}^1(\mathbb{Q})$, and we call these the *cusps* of Γ. (We refer to Chapter 1 of [Shi71] for a justification of these assertions.) We will abuse the terminology and refer to the points of $\mathbb{P}^1(\mathbb{Q})$ also as cusps. The quotient space $\Gamma\backslash\mathbb{H}$ is naturally a Riemann surface whose compactification is $\Gamma\backslash\mathbb{H}^*$, and we define the *genus* of Γ to be the topological genus of $\Gamma\backslash\mathbb{H}^*$.

2.2 Modular functions and principal moduli

A *modular function* for Γ is a complex-valued meromorphic function on $\Gamma\backslash\mathbb{H}^*$. Equivalently, a modular function for Γ is a meromorphic function $f : \mathbb{H} \to \mathbb{C}$ that is Γ-*invariant* (i.e. $f(\tau) = f(\gamma\tau)$ for all $\gamma \in \Gamma, \tau \in \mathbb{H}$) and *meromorphic at the cusps.* For the infinite cusp the following is what meromorphicity means. Let h be the smallest positive number such that $\left(\begin{smallmatrix} 1 & h \\ 0 & 1 \end{smallmatrix}\right) \in \Gamma$. Any Γ-invariant function f has a Fourier expansion

$$f(\tau) = \sum_{n\in\mathbb{Z}} a(n) q_h^n, \tag{2.2}$$

where $a(n) \in \mathbb{C}$ and

$$q_h = e^{2\pi i\tau/h}.$$

(When $h = 1$ we will drop the subscript and simply write q instead of q_1.) We may take q_h as the local coordinate at the infinite cusp of Γ, and we say that a Γ-invariant function f is meromorphic at the infinite cusp if its Fourier expansion is of the form

$$f(\tau) = \sum_{n \geq n_0} a(n) q_h^n$$

where $n_0 \in \mathbb{Z}$. If $n_0 = 0$ we say that f is *holomorphic* at the infinite cusp, and when $n_0 > 0$ we say that f *vanishes* at the infinite cusp. Meromorphicity, holomorphicity and vanishing at the other cusps are defined similarly using local coordinates at the other cusps. Alternatively these conditions may be defined via the following growth conditions: f is meromorphic at the cusp s if $f(\tau)$ grows at most exponentially as $\tau \to s$; f is holomorphic at s if $f(\tau)$ remains bounded as $\tau \to s$; and f vanishes at s if $f(\tau) \to 0$ as $\tau \to s$.

When Γ has genus zero the field of meromorphic functions on $\Gamma\backslash\mathbb{H}^*$ is generated by a single element called a *principal modulus* for Γ. There are several choices for this generator, the canonical choice being the modular function T_Γ that has a unique simple pole at the infinite cusp, and that has a Fourier expansion of the form

$$T_\Gamma(\tau) = q_h^{-1} + O(q_h).$$

This generator is referred to as the *normalized principal modulus* for Γ.

2.3 Modular forms

One way of constructing modular functions is by way of modular forms. Modular functions may be obtained by taking quotients of modular forms of the same weight, analogous to constructing rational functions on a projective space by taking ratios of homogeneous polynomials of the same degree. In this section we define what modular forms are.

Let k be an integer. A *weakly holomorphic modular form* of weight k for Γ is a holomorphic function $f : \mathbb{H} \to \mathbb{C}$ satisfying

$$f\left(\frac{a\tau + b}{c\tau + d}\right) = (c\tau + d)^k f(\tau) \tag{2.3}$$

for all $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma$ and $\tau \in \mathbb{H}$, that is meromorphic at the cusps of Γ. We explain now what the meromorphic condition means. Even though f is not Γ-invariant, the functional equation (2.3) satisfied by f implies that f is invariant under $\left(\begin{smallmatrix} 1 & h \\ 0 & 1 \end{smallmatrix}\right)$. Therefore it has a Fourier expansion as in (2.2). As in the case of modular functions, meromorphicity and holomorphicity and vanishing at the infinite cusp (and similarly for the other cusps) are defined using this Fourier expansion. A *modular form* is a weakly holomorphic modular form that is holomorphic at the cusps, and a *cusp form* is a modular form that vanishes at the cusps.[2] If Γ contains the *principal congruence subgroup of level N*

$$\Gamma(N) := \left\{ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z}) : a-1, b, c, d-1 \equiv 0 \pmod{N} \right\},$$

then we say that f has *level N*.

Modular forms for Γ of a given weight k form a vector space over $\mathbb{C}$. We will denote this vector space by $M_k(\Gamma)$. Its dimension is finite. Thus the coincidence of two modular forms $f, g \in M_k(\Gamma)$ may be proven by showing that their first few Fourier coefficients agree; the number of coinciding coefficients that needs to be checked to guarantee equality of modular forms for Γ is called *Sturm's bound* for Γ [Stu87].

[2] If one prefers, these may also be defined, as in the case of modular functions, using appropriate growth conditions.

Multiplying modular forms produces another modular form: if $f \in M_k(\Gamma)$ and $g \in M_l(\Gamma)$ then $fg \in M_{k+l}(\Gamma)$. Taking the quotient of modular forms of the same weight yields a modular function: if $f, g \in M_k(\Gamma)$, then f/g is a modular function for Γ.

Modular forms may be generalized in various directions. For example, the automorphic factor $(c\tau + d)^k$ in the transformation formula (2.3) may be replaced with $\psi(\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right))(c\tau + d)^k$, where ψ is a *multiplier system* for Γ with weight $k \in \mathbb{R}$ (i.e. a function $\psi : \Gamma \to \mathbb{C}^*$ such that $\psi(\gamma_1\gamma_2)\mathrm{j}(\gamma_1\gamma_2, \tau)^{k/2} = \psi(\gamma_1)\psi(\gamma_2)\mathrm{j}(\gamma_1, \gamma_2\tau)^{k/2}\mathrm{j}(\gamma_2, \tau)^{k/2}$, where $\mathrm{j}(\gamma, \tau) := (c\tau + d)^{-2}$ if $(c \quad d)$ is the bottom row of γ). This gives us *modular forms with multiplier systems*. Owing largely to Shimura, we also possess a solid theory of *modular forms of half-integral weight*, i.e. modular forms whose weights are in $\frac{1}{2}\mathbb{Z}$. The codomain $\mathbb{C}$ of a modular form may also be changed to $\mathbb{C}^n$, for some positive integer n, giving rise to the notion of a *vector-valued modular form*. These generalizations may further be combined to create other types of modular forms. Diverse as these generalizations of a modular form may be, they all satisfy functional equations that are similar to (2.3). One may thus think of (2.3) as the defining and essential feature of a modular form and its generalizations, including, as we will see in Section 2.6, mock modular forms.

2.4 Modular forms and functions of level one

We will describe in this section some examples of modular forms and functions of level one. Central to moonshine is the j-function, a level one modular function. As mentioned in the previous section, modular functions may be constructed from modular forms. We illustrate this idea in this section by first defining Eisenstein series—which are modular forms—and then using these functions to create the j-function—which is a modular function.

Let $k > 2$ be an even integer and let ζ be the Riemann zeta function. The (normalized) *Eisenstein series* of weight k is defined to be the function

$$E_k(\tau) = \frac{1}{2\zeta(k)} \sum_{(c,d)\in\mathbb{Z}^2\setminus\{(0,0)\}} \frac{1}{(c\tau+d)^k}.$$

It can be shown (cf. Section 2.2 of [Shi71]) that this is a modular form of weight k for $\mathrm{SL}_2(\mathbb{Z})$, with Fourier expansion

$$E_k(\tau) = 1 - \frac{2k}{B_k} \sum_{n\geq 0} \sigma_{k-1}(n) q^n.$$

Here B_k is the kth Bernoulli number and $\sigma_{k-1}(n) := \sum_{1\leq d|n} d^{k-1}$. An important cusp form, the *Delta function*, may be formed from these Eisenstein series; this is the cusp form

$$\Delta(\tau) := \frac{1}{1728}(E_4(\tau)^3 - E_6(\tau)^2)$$

of weight 12 and level one. That it is a cusp form follows from that fact that it vanishes at the unique cusp of $\mathrm{SL}_2(\mathbb{Z})$. The Delta function admits the following infinite product (cf. Section 3.3 of [Apo12]):

$$\Delta(\tau) = q\prod_{n=1}^{\infty}(1-q^n)^{24}.$$

From this product formulation we find that Δ does not vanish on the upper half-plane.

Using these modular forms we can now construct our most important modular function. Because the numerator and the denominator have equal weights, the *j-function* given by

$$\begin{aligned} j(\tau) &:= \frac{E_4(\tau)^3}{\Delta(\tau)} \\ &= q^{-1} + 744 + 196884q + 21493760q^2 + \cdots \end{aligned}$$

is a modular function for $\mathrm{SL}_2(\mathbb{Z})$. It has a unique simple pole at the infinite cusp, thus

$$J(\tau) := j(\tau) - 744$$

is the normalized principal modulus for the genus zero group $\mathrm{SL}_2(\mathbb{Z})$.

2.5 Eta quotients

The Eisenstein series of the previous section provided us with important examples of modular forms and functions of level one. In this section we will define eta quotients, which as we shall see provide a supply of modular forms of higher levels. Eta quotients, as may be inferred from the name, are functions built from the *eta function*, the holomorphic and nonvanishing function on $\mathbb{H}$ given by

$$\eta(\tau) := q^{1/24} \prod_{n=1}^{\infty} (1 - q^n).$$

The eta function is a modular form of weight $\frac{1}{2}$ and level one with a certain multiplier system (cf. Appendix A of [CD12] for an explicit description of this multiplier system). By an *eta quotient* we simply mean a function of the form

$$\prod_{0 \leq n | N} \eta(n\tau)^{r_n}$$

where N is a positive integer and r_n are integers. Note that Δ is an example of an eta quotient.

If f, an eta quotient as above, satisfies the conditions

$$\sum_{0 \leq n | N} n r_n \equiv 0 \pmod{24},$$

$$\sum_{0\leq n|N} \frac{N}{n} r_n \equiv 0 \pmod{24},$$

$$\text{and} \prod_{0\leq n|N} n^{r_n} \text{ is a perfect square,}$$

then

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

for all $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_0(N)$ and $\tau \in \mathbb{H}$, where $k = \frac{1}{2}\sum_{0\leq n|N} r_n$ (cf. Theorem 1.64 of [Ono04]). In other words, f is a weakly holomorphic modular form of weight k and level N.

Note that if $k = 0$ then f is a modular function of level N. Indeed (up to an additive constant) many principal moduli may be expressed as an eta quotient. For example, the normalized principal modulus for $\Gamma_0(2)$ is $T_{\Gamma_0(2)} = \eta(\tau)^{24}/\eta(2\tau)^{24} + 24$. (See Appendix A.2 for more examples.)

Representatives for the cusps of $\Gamma_0(N)$ may be taken from the set of rational numbers of the form $\frac{c}{d}$ where $(c,d) = 1$ and $d|N$. The order of vanishing of the eta quotient f at $\frac{c}{d}$ is given by the quantity

$$\frac{N}{24(d,\frac{N}{d})d} \sum_{0\leq n|N} \frac{(d,n)^2 r_n}{n}.$$

2.6 Mock modular forms

In his last letter to Hardy, dated 12 January 1920, Ramanujan gave seventeen mysterious q-series and purported that they were examples of a new class of objects he had just discovered called “mock theta functions”. No formal definition of these functions was given. Instead Ramanujan described the properties that they should possess. In the succeeding decades several mathematicians worked on demystifying these functions by, for instance, extending the list of known examples and by proving theorems and further identities between them. A breakthrough in the understanding of these functions occurred in 2001 when Zwegers in his PhD thesis showed that the mock theta functions were among the first examples of mock modular forms [Zwe08]. Mock modular forms, which generalize modular forms, are now found in several areas of contemporary mathematics including combinatorics, mathematical physics, number theory and—of primary importance to us—moonshine. In this section we provide a definition of a mock modular form. We refer to the expository articles [Duk14, Fol17, Zag07] for overviews of mock modular forms and their applications, and the book [BFOR17] for a more thorough treatment.

Let Γ be a discrete subgroup of $\mathrm{SL}_2(\mathbb{R})$ and let $k \in \frac{1}{2}\mathbb{Z}$. We say that a holomorphic function f on $\mathbb{H}$ is a *weakly holomorphic mock modular form of weight k for Γ* if it has at most exponential growth as τ approaches any cusp of Γ, and if there exists a modular form $S(f)$ of weight $2-k$ on Γ such that the sum $f + S(f)^*$ transforms (as in (2.3)) like a weakly holomorphic modular form of weight k on Γ. Here, the function $S(f)^*$ is given by

$$S(f)^*(\tau) := \left(\frac{i}{2}\right)^{k-1} \int_{-\bar{\tau}}^{\infty} (z+\tau)^{-k}\overline{S(f)(-\bar{z})}\, dz.$$

A *mock modular form* is a weakly holomorphic mock modular form that is bounded at the cusps. The modular form $S(f)$ is called the *shadow of f* and is uniquely determined by f. Note that the shadow of f is equal to zero if and only if f is a modular form in the classical sense. Thus every (weakly holomorphic) modular form is a (weakly holomorphic) mock modular form[3].

[3] Others refer to mock modular forms with nonzero shadow as *pure mock modular forms.*

2.7 Rademacher sums

Besides the mock theta functions discovered by Ramanujan, what are other examples of mock modular forms? We describe in this section Rademacher sums, a rich source of weakly holomorphic mock modular forms.

Naively, one can construct Γ-invariant functions in the following way. Starting with any function $f : \mathbb{H} \to \mathbb{C}$ one can form the function $F(\tau) = \sum_{\gamma \in \Gamma} f(\gamma\tau)$. This function F has the required Γ-invariance, but only formally, since such sums rarely converge. The idea of Poincaré, to restore convergence, is to start instead with a function f that is already invariant under the action of a large subgroup of Γ, and to consider a sum that runs over a collection of coset representatives. This sum has a better chance at convergence.

This idea extends to the construction of functions that satisfy the more general transformation formula (2.3). For example, in the case of $\mathrm{SL}_2(\mathbb{Z})$ one may take, for any integer m, the exponential function $e_m(\tau) = e^{2\pi i m\tau}$. This function is invariant under the action of the subgroup $\mathrm{SL}_2(\mathbb{Z})_\infty := \{\left(\begin{smallmatrix} 1 & n \\ 0 & 1 \end{smallmatrix}\right) : n \in \mathbb{Z}\}$. If k is an integer then the sum

$$\sum_{\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})_\infty \backslash \mathrm{SL}_2(\mathbb{Z})} e_m\left(\frac{a\tau + b}{c\tau + d}\right)(c\tau + d)^{-k}$$

is formally $\mathrm{SL}_2(\mathbb{Z})$-invariant. When $k > 2$ the sum is absolutely convergent for any $\tau \in \mathbb{H}$, and hence we obtain a weakly holomorphic modular form. However when $k \leq 2$, absolute convergence fails. Rademacher's idea, which has now been generalized to various groups Γ and weights k, is to modify the summation so that convergence is achieved. We will describe this modification here.

Let Γ be a discrete subgroup of $\mathrm{SL}_2(\mathbb{R})$ that is commensurable with $\mathrm{SL}_2(\mathbb{Z})$. Let h be the smallest positive number such that the subgroup Γ_∞ of upper triangular matrices in Γ is given by $\{\left(\begin{smallmatrix} 1 & nh \\ 0 & 1 \end{smallmatrix}\right) : n \in \mathbb{Z}\}$. For each $K > 0$, define the set $\Gamma_{K,K^2} := \{\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma : |c| < K, |d| < K\}$. Given integers k and m, the *Rademacher* *sum of weight k and index m* for Γ is defined to be

$$R^{[m]}_{\Gamma,k}(\tau) = c^{[m]}_{\Gamma,k}(0) + \lim_{K\to\infty} \sum_{\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)\in\Gamma_\infty\backslash\Gamma_{K,K^2}} e_m\left(\frac{a\tau+b}{c\tau+d}\right) r^{[m]}_k(\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right),\tau)(c\tau+d)^{-k},$$

where $e_m(\tau) = e^{2\pi i m\tau}$, $r^{[m]}_k$ is some regularization factor (cf. equation (2.26) of [CD14]) and $c^{[m]}_{\Gamma,k}(0)$ is some constant (cf. equation (2.29) of [CD14]). In this dissertation we will be interested mainly with $k=0$ and $k=2$, in which case

$$r^{[m]}_2(\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right),\tau) = 1, \qquad c^{[m]}_{\Gamma,2}(0) = 0,$$

$$r^{[m]}_0(\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right),\tau) = 1 - e_m\left(\frac{a}{c} - \frac{a\tau+b}{c\tau+d}\right),$$

$$\text{and } c^{[m]}_{\Gamma,0}(0) = -\frac{m(2\pi)^2}{h} \lim_{K\to\infty} \sum_{\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)\in\Gamma_\infty\backslash\Gamma^\times_K/\Gamma_\infty} \frac{e_m(\frac{a}{c})}{c^2}.$$

Here $\Gamma^\times_K := \{\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma : 0 < |c| < K\}$.

The Rademacher sum $R^{[m]}_{\Gamma,k}(\tau)$ is uniformly convergent on compact subsets of the upper half-plane. Specializing to the case $k=0$, we have for negative m that $R^{[m]}_{\Gamma,0}(\tau)$ is a weakly holomorphic mock modular form of weight 0 for Γ with shadow $-mR^{[-m]}_{\Gamma,2}$. By construction, it has a pole of order m at the infinite cusp, with q-expansion of the form

$$R^{[m]}_{\Gamma,0}(\tau) = q^m + \sum_{n\geq 0} c^{[m]}_{\Gamma,0}(n) q^n_h.$$

The coefficients $c^{[m]}_{\Gamma,0}(n)$ are explicitly given, in terms of $\mathrm{Kl}(\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right), m, n) := e_m\left(\frac{a}{c}\right) e_n\left(\frac{d}{c}\right)$ and the *Bessel function*[4]

$$\mathrm{Bl}(\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right), m, n) := \sum_{t=0}^{\infty} \left(\frac{2\pi}{c}\right)^{2t+2} \frac{(-m)^{t+1}}{\Gamma(t+2)} \frac{n^t}{t!},$$

[4] In this formula, Γ is the usual Gamma function.

by the *Rademacher series*

$$c_{\Gamma,0}^{[m]}(n) := \frac{1}{h} \lim_{K\to\infty} \sum_{\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)\in\Gamma_\infty\backslash\Gamma_K^\times/\Gamma_\infty} \mathrm{Kl}(\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right), m, n)\mathrm{Bl}(\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right), m, n).$$

The Rademacher sums we have defined have poles at the infinite cusp. It is possible to define Rademacher sums that have poles at the other cusps. Also Rademacher sums may be extended to the cases of weights that are half-integers, and to include multiplier systems. We say that a function f is *Rademacher summable* if it is equal to a (constant multiple of a) single Rademacher sum—i.e. $f = cR_{\Gamma,k}^{[m]}$—and that an example of moonshine has the *Rademacher summability property* if each graded trace function is Rademacher summable up to addition of a constant or a *unary theta function*[5]. Monstrous moonshine and umbral moonshine have the Rademacher summability property.

2.8 Groups of $n|h$-type

The purpose of this section is to describe certain discrete subgroups of $\mathrm{SL}_2(\mathbb{R})$ known as $n|h$-type groups. There are at least two reasons why these groups are important. First, the normalizer of $\Gamma_0(N)$ in $\mathrm{SL}_2(\mathbb{R})$ is an $n|h$-type group. And second, in monstrous moonshine the graded trace function T_g is Γ_g-invariant where Γ_g is a certain subgroup of an $n|h$-type group.

Let n be a positive integer and let $h|(n, 24)$. The group $\Gamma_0(n|h)$ is defined to be

$$\Gamma_0(n|h) := \left\{ \begin{pmatrix} a & b/h \\ cn & d \end{pmatrix} : a, b, c, d \in \mathbb{Z}, ad - \frac{bcn}{h} = 1 \right\}.$$

This is a subgroup of $\mathrm{SL}_2(\mathbb{R})$, and is generated by the group $\Gamma_0(nh)$ together with

[5] Unary theta functions may be thought of as the half-integral weight analogue of a constant (since the theta function's contribution to the growth of the coefficients is also negligible).

the matrices $\left(\begin{smallmatrix} 1 & 1/h \\ 0 & 1 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} 1 & 0 \\ n & 1 \end{smallmatrix}\right)$.

An *exact divisor* of a positive integer N is a positive divisor d of N such that $(d, \frac{N}{d}) = 1$. For an exact divisor e of $\frac{n}{h}$, the coset w_e of $\Gamma_0(n|h)$ is defined as the set

$$w_e := \left\{ \frac{1}{\sqrt{e}} \begin{pmatrix} ae & b/h \\ cn & de \end{pmatrix} : a, b, c, d \in \mathbb{Z}, ade^2 - \frac{bcn}{h} = e \right\}.$$

We will abuse notation and also denote by w_e any matrix in this coset. We call w_e, both the coset and the element, an *Atkin-Lehner involution* of $\Gamma_0(n|h)$.

Let d and d' be exact divisors of N, and define $d * d' = \frac{dd'}{(d,d')^2}$. Note that $d * d'$ is also an exact divisor of N, and the set $\mathrm{Ex}(N)$ of exact divisors of N, equipped with the binary operation $*$, is an abelian group. This is relevant to us because if w_e and $w_{e'}$ are Atkin-Lehner involutions of $\Gamma_0(n|h)$, then $w_e w_{e'} = w_{e*e'}$. Therefore given a subgroup $\{1, e, f, \ldots\}$ of $\mathrm{Ex}(\frac{n}{h})$, the set

$$\Gamma_0(n|h)+e, f, \ldots := \left\langle \Gamma_0\left(\frac{n}{h}\right), w_e, w_f, \ldots \right\rangle$$

is also a subgroup of $\mathrm{SL}_2(\mathbb{R})$. Groups of the form $\Gamma_0(n|h)+e, f, \ldots$ are called *$n|h$-type groups.*

We will adopt the following conventions in abbreviating the notation $\Gamma_0(n|h)+e, f, \ldots$: when $h = 1$ we omit "$|h$" and simply write $\Gamma_0(n)+e, f, \ldots$; when $\{1, e, f, \ldots\}$ is the full group $\mathrm{Ex}(\frac{n}{h})$, we simply write $\Gamma_0(n|h)+$; and when $\{1, e, f, \ldots\}$ is the trivial subgroup, we either write $\Gamma_0(n|h)-$ or $\Gamma_0(n|h)$.

As discussed in [CN79] the normalizer of $\Gamma_0(N)$ in $\mathrm{SL}_2(\mathbb{R})$ is given by $\Gamma_0(n|h)+$ where h is the largest integer such that $h^2|N$ and $h|24$, and $n = \frac{N}{h}$. Moreover, they defined a homomorphism $\lambda : \Gamma_0(n|h)+e, f, \ldots \to \mathbb{C}$. The kernel of λ is a subgroup of $\Gamma_0(n|h)+e, f, \ldots$ of index h, and the groups Γ_g appearing in monstrous moonshine are of this form. We refer the reader to Section 1.3 of [Fer93] for a definition of λ.

(Note that this homomorphism λ is not well-defined for all choices of n, h, e, f, ... See Section 2 of [Fer93].)

2.9 Umbral Moonshine

In 2010 Eguchi, Ooguri and Tachikawa observed a numerical coincidence [EOT11] reminiscent of the McKay-Thompson observation . The decomposition of the elliptic genus of a K3 surface into irreducible characters of the $\mathcal{N} = 4$ superconformal algebra gives rise to a q-series

$$H(\tau) = 2q^{-1/8}(-1 + 45q + 231q^2 + 770q^3 + 2277q^4 + \cdots).$$

It was noted that $H(\tau)$ is a mock modular form and its first few coefficients are dimensions of irreducible representations of the largest Mathieu group M_{24}. Mathieu moonshine, formulated in a series of papers [Che10, EH11, GHV10a, GHV10b] and proven by Gannon [Gan16], is the statement that there exists an infinite-dimensional graded representation of M_{24} with the following property: the graded trace functions are certain distinguished mock modular forms of weight $\frac{1}{2}$. These graded trace functions are Rademacher summable, and therefore are natural analogues of the principal moduli in monstrous moonshine [CD12]. Mathieu moonshine thus expanded the class of automorphic objects considered in moonshine to include mock modular forms and other weights. In a series of papers Cheng, Duncan and Harvey identified Mathieu moonshine as one of a family of correspondences between finite groups and mock modular forms [CDH14a, CDH14b, CDH18]. They referred to this conjectured family of correspondences as umbral[6] moonshine.

Briefly, umbral moonshine is a collection of 23 cases of moonshine relating groups arising from lattices to (vector-valued) mock modular forms. The lattices in umbral

[6] The word umbral was chosen to highlight the existence of *shadows* in this moonshine.

moonshine are the *Niemeier lattices*, which are the even unimodular self-dual lattices with roots (i.e. lattice vectors of length 2), and they are determined by their *Niemeier root systems*. (For more information about root systems and their Dynkin diagrams, see [Hum12].) These root systems have rank 24 and their simple components are root systems of ADE type of the same Coxeter number. A Niemeier root system is said to be of *A-type* if it has a simple component of type A, it is said to be of *D-type* if it has a simple component of type D but no type A component, and it is said to be of *E-type* if it only has type E components.

Given a Niemeier root system there is a group of genus zero naturally attached to it called its *lambency*. The lambencies are defined as follows: The Coxeter number of a Niemeier lattice is the common Coxeter number of its simple components. The Coxeter numbers of the A-type Niemeier lattices are the same integers N for which the genus of $\Gamma_0(N)$ is zero, and the lambency of such a Niemeier lattice of Coxeter number N is defined to be $\Gamma_0(N)$. Similarly, the Coxeter numbers of the D-type Niemeier lattices are the same integers $2N$ for which the genus of $\Gamma_0(2N)+N$ is zero, and the lambency of such a Niemeier lattice of Coxeter number $2N$ is defined to be $\Gamma_0(2N)+N$. As discussed in [CDH14b] the genus zero groups naturally attached to the Niemeier root systems E_6^4 and E_8^3 of E-type are $\Gamma_0(12)+4$ and $\Gamma_0(30)+6, 10, 15$ respectively, and these corresponding groups are defined to be their lambencies.

Remark 2.9.1. *There is a more conceptual way to define lambency. Namely, for X a Niemeier root system let $W(X)$ be the subgroup of the group of automorphisms of the associated Niemeier lattice that is generated by roots. Then a Coxeter element of $W(X)$ is any element that can be expressed as a product over simple roots of the reflections in those roots. For g a Coxeter element of $W(X)$ let η_g be the corresponding eta product (determined in the usual way by its Frame shape). Any two Coxeter elements are conjugate in $W(X)$ so η_g is independent of any choices made so far. It turns out that $T^X := 1/\eta_g$ is a principal modulus for the lambency of X. Thus the* *lambency is naturally determined by X. We thank John Duncan for this remark.*

Let X be a Niemeier root system and let L^X be the associated Niemeier lattice. The reflections through the roots of L^X generate a normal subgroup of the full automorphism group of L^X known as the *Weyl group* of X. The *umbral group* G^X, which plays the same role as the monster in monstrous moonshine, is defined to be the quotient of the group of automorphisms of L^X by the Weyl group of X. Umbral moonshine associates to each element $g \in G^X$ a distinguished (vector-valued) mock modular form H_g^X. Duncan, Griffin and Ono showed the existence of an infinite-dimensional graded representation of G^X with graded trace functions equal to H_g^X [DGO15b]. There is also a naturally defined quotient of G^X denoted $\bar{G}^X$, and we denote by n_g the order of the image of $g \in G^X$ in $\bar{G}^X$. This integer n_g is the level of H_g^X.

Chapter 3

Supersingular elliptic curves and moonshine

3.1 Modular curves modulo p

In this section we describe the Deligne-Rapoport model for $X_0(pN)$ modulo a prime p not dividing N, closely following Ogg's description in [Ogg75]. We assume here familiarity with the group law on an elliptic curve.

Let E_1 and E_2 be elliptic curves defined over a field K. By an *isogeny* from an elliptic curve E_1 to an elliptic curve E_2 we mean a map $\phi : E_1 \to E_2$ given by rational functions (with coefficients in K) that maps the identity element of E_1 to the identity element of E_2. An isogeny $\phi : E_1 \to E_2$ gives rise to an injection of function fields $\phi^* : \bar{K}(E_2) \to \bar{K}(E_1)$, and the *degree* of ϕ is by definition the degree of the finite extension $\bar{K}(E_1)/\phi^*\bar{K}(E_2)$. Given a nonconstant isogeny $\phi : E_1 \to E_2$ of degree m, there is a unique isogeny $\hat{\phi} : E_2 \to E_1$ such that $\hat{\phi} \circ \phi = [m]$, where $[m]$ is the multiplication-by-m map. The isogeny $\hat{\phi}$ is called the *transpose* or the *dual* of ϕ. If K is a field of positive characteristic p and E is an elliptic curve defined over K, then an example of an isogeny is the *Frobenius*, which is the isogeny $\phi : E \to E^{(p)}$ that sends (x, y) to (x^p, y^p). Here $E^{(p)}$ is the curve obtained by raising the coefficients of the equation for E to the pth power. (For a reference of these facts, see Section III.4 and III.6 of [Sil09].)

For every positive integer N the orbit space $Y_0(N) := \Gamma_0(N)\backslash\mathbb{H}$ is naturally a Riemann surface, and admits a moduli interpretation: the points of $Y_0(N)$ parametrize isomorphism classes of cyclic N-isogenies of complex elliptic curves, i.e. isogenies of degree N with cyclic kernels. The Riemann surface $X_0(N) := \Gamma_0(N)\backslash\mathbb{H}^*$ (cf. Section 2.1 for the notation) is a compactification of $Y_0(N)$.

By a theorem of Igusa [DR73, Igu59], for any prime p not dividing N there exists an integral model of the modular curve $X_0(N)$ that has good reduction modulo p, i.e. $X_0(N)$ modulo p is nonsingular. On the other hand, the reduction of $X_0(pN)$ modulo p is a singular curve obtained from glueing two copies of $X_0(N)$ modulo p at the supersingular points [DR73]. (We refer to this as the *Deligne-Rapoport model* of $X_0(pN)$ modulo p.) More precisely, the non-cuspidal points of $X_0(pN)$ modulo p parametrize pN-isogenies of elliptic cuves over $\mathbb{F}_p$. We separate a pN-isogeny into its N-part and its p-part. There are as many N-isogenies in characteristic 0 as in characteristic p, but there are only two p-isogenies in characteristic p, namely the Frobenius and its transpose. The first copy of $X_0(N)$ modulo p parametrizes those isogenies whose p-part is the Frobenius; the second copy, those whose p-part is the transpose of the Frobenius. Their intersection consists of the supersingular points of $X_0(N)$ modulo p (these are the points that correspond to cylic N-isogenies $\phi : E \to E'$ such that E is supersingular) where the p-part may be thought of as either the Frobenius or its transpose [Ogg75].

Let e be an exact divisor of N. If w_e is an Atkin-Lehner involution of $\Gamma_0(N)$ then $\frac{1}{\sqrt{e}}w_e$ lies in the normalizer of $\Gamma_0(N)$ in $\mathrm{SL}_2(\mathbb{R})$ (cf. Section 2.8). This element of the normalizer induces an involution on $X_0(N)$, also called an Atkin-Lehner involution of $X_0(N)$, and which we also denote by w_e. The action of the Atkin-Lehner involution

w_p on the Deligne-Rapoport model of $X_0(pN)$ modulo p is as follows: it gives an isomorphism between the two copies of $X_0(N)$ modulo p, and it fixes the $\mathbb{F}_p$-rational supersingular points and switches the non-rational supersingular points with their conjugates (cf. Section 5 of [Has97]).

3.2 Higher level Ogg's theorem

In this section we prove Theorem 1.3.1, a generalization of Ogg's theorem, and use this to obtain the primes that have the rationality property for the curves $X_0(N)+e, f, \ldots$ of genus zero.

Let $X = X_0(N)+e, f, \ldots$ and let p be a prime not dividing N. Recall the following notations: $Q_p(X)$ is the number of supersingular points of X modulo p that are not defined over $\mathbb{F}_p$; *genus*(X) is the genus of X; and X^p is the modular curve $X_0(Np)+p, e, f, \ldots$ obtained by taking the quotient of $X_0(Np)$ by Atkin-Lehner involutions w_p, w_e, w_f, $\ldots$ where $\{p, e, f, \ldots\}$ is understood to be the set $\{e, f, \ldots, p, pe, pf, \ldots\}$.

Theorem 3.2.1 (Theorem 1.3.1)**.** *Let N be a positive integer, let $e, f, \ldots$ be exact divisors of N, and let $X = X_0(N)+e, f, \ldots$. If p is a prime not dividing N then*

$$\frac{1}{2}Q_p(X) = \mathit{genus}(X^p) - \mathit{genus}(X).$$

Consequently p has the rationality property for X if and only if the modular curves X and X^p have the same genus.

Proof. The proof follows that of Ogg [Ogg75]. The ingredient that we need for his proof to go through is a model for the (singular) curve $X_0(Np)+e, f, \ldots$ modulo p. We recall the model for this curve here which is explained in Section 5 of [FH99]. If

$e, f, \ldots$ are exact divisors of N, so that each of them is coprime with p, and if

$$X := X_0(N){+}e, f, \ldots \mod p$$
$$X(p) := X_0(Np){+}e, f, \ldots \mod p$$

then $X(p)$ consists of two copies of X that intersect at the supersingular points of X modulo p. Note that this is a generalization of the model described in Section 3.1.

From here the proof of Ogg goes through: If X_1 and X_2 are the components of $X(p)$ then w_p defines an isomorphism of X_1 onto X_2 that acts as the Frobenius on $X_1 \cap X_2$—the supersingular points of X. Therefore the model of $X(p)/(w_p) = X^p$ modulo p is given by one copy of X which intersects itself at each point corresponding to a pair of conjugate supersingular points of X, i.e, the supersingular points of X not defined over $\mathbb{F}_p$. From this model of X^p we obtain $\mathit{genus}(X^p) = \mathit{genus}(X) + \frac{1}{2}Q_p(X)$, which is the first part of Theorem 1.3.1. The second part of the theorem readily follows since by definition p has the rationality property for X if and only if $Q_p(X) = 0$. □

We apply Theorem 1.3.1 to the case when the genus of $X = X_0(N){+}e, f, \ldots$ is zero. Considering such cases leads to a generalization of Ogg's observation which is the subject of the next section. According to Theorem 1.3.1, given such an X the prime p has the rationality property for X if and only if the genus of X^p is zero. For example, Table 3 gives the genus of X^p for X of level 2 and for the first few primes. From this we see that the primes 3, 5, 7, 11, 13, 17, 19, 23, 31, 47 have the rationality property for $X_0^+(2)$ and the primes 3, 5, 7, 11, 23 have the rationality property for $X_0(2)$. Moreover we know from [Fer93] that this list is complete since 94 is the largest level of the form $2p$ for which there exists a genus zero quotient of $X_0(2p)$ by Atkin-Lehner involutions. Similarly, we enumerate all the primes p for which X^p has genus zero for all $X = X_0(N){+}e, f, \ldots$ of genus zero, and we compile the results in Appendix A.1.

Table 3.1: Genus of X^p.

p	3	5	7	11	13	17	19	23	29	31	37	41	43	47
$\mathrm{gen}((X_0^+(2))^p)$	0	0	0	0	0	0	0	0	1	0	1	1	1	0
$\mathrm{gen}((X_0(2))^p)$	0	0	0	0	1	1	1	0	2	1	4	3	4	1

Remark 3.2.2. *We identified the primes that have the rationality property for modular curves $X_0(N)+e, f, \ldots$ of genus zero. We mention here that Ogg already obtained the primes that have the rationality property for modular curves $X_0(N)$ regardless of the genus [Ogg75]. He did not however consider their quotients by Atkin-Lehner involutions. His result is as follows:* 2 *is the only prime that has the rationality property for $X_0(11)$ and $X_0(17)$; also, if $N \neq 11, 17$ and if the genus of $X_0(N)$ is positive, then there are no primes that have the rationality propery for $X_0(N)$. We point out here that there is a typo in his list for $X_0(4)$; the prime* 5 *should not be in the list.*

3.3 Higher level Ogg's observation

Suppose that $X = X_0(N)+e, f, \ldots$ is a monstrous modular curve, by which we mean a modular curve that appears in monstrous moonshine. In this section we provide a characterization, which generalizes Ogg's observation, of the primes that have the rationality property for X.

Recall that we defined $C(X)$ to be any of the conjugacy classes of the monster associated via monstrous moonshine to X if $X \neq X_0(27)+27$, and we defined $C(X_0(27)+27)$ to be the conjugacy class of the monster labelled 27A in the ATLAS [CCN+85]. We also defined a Fricke element of prime order p to be an element of the monster whose graded trace function is the principal modulus for $\Gamma_0^+(p)$.

Theorem 3.3.1 (Theorem 1.3.3)**.** *Let X be a monstrous modular curve X of the form $X_0(N)+e, f, \ldots$. If p is a prime that does not divide N, then p has the rationality property for X if and only if the centralizer of $g \in C(X)$ in the monster contains a Fricke element of order p.*

Table 3.2: Checking containment of Fricke elements.

	3	5	7	11	13	17	19	23	29	31	41	47	59	71
$2A$	$\boldsymbol{6A}$ $6D$	$\boldsymbol{10A}$ $10C$	$\boldsymbol{14A}$	$\boldsymbol{22A}$	$\boldsymbol{26A}$	$\boldsymbol{34A}$	$\boldsymbol{38A}$	$\boldsymbol{46CD}$		$\boldsymbol{62AB}$		$\boldsymbol{94AB}$		
$2B$	$6B$ $\boldsymbol{6C}$ $6E$ $6F$	$\boldsymbol{10B}$ $10D$ $10E$	$\boldsymbol{14B}$ $14C$	$\boldsymbol{22B}$	$26B$			$\boldsymbol{46AB}$						

Proof. Suppose C_1 and C_2 are conjugacy classes of orders n_1 and n_2 such that $(n_1, n_2) = 1$. Then the classes C_1 and C_2 have representatives that commute if and only if there exists a conjugacy class C of order n_1n_2 such that $C^{n_2} = C_1$ and $C^{n_1} = C_2$.

Now, the centralizer of $g \in C(X)$ in the monster contains a Fricke element of order p if and only if the conjugacy classes $C(X)$ and pA have representatives that commute. From the previous paragraph, this occurs if and only if there exists a conjugacy class of order pN whose Nth power is pA and whose pth power is $C(X)$. One can manually check from the power maps of the conjugacy classes of the monster, using GAP [GAP18] for instance, that this latter condition occurs if and only if p has the rationality property for X. □

We illustrate by way of an example how this proof works. We consider the case when $N = 2$. This implies that $X = X_0^+(2)$ or $X_0(2)$, and the conjugacy class $C(X)$ is $2A$ or $2B$ respectively. In Table 3.2 we label the columns by the primes p dividing the order of the monster—these are the primes that can occur as prime orders of Fricke elements—and we label the rows by $C(X)$. The entries in row $C(X)$ and column p are the conjugacy classes of the monster of order $2p$ whose pth power is $C(X)$. For each cell, we can check which of those conjugacy classes have 2nd power equal to pA, and write these in boldface. Then from the proof, there is a conjugacy class in row $C(X)$ and column p in boldface if and only if the centralizer of $g \in C(X)$ contains a Fricke element of order p.

From this table, we find that the odd primes arising as order of Fricke elements in the centralizer of $g \in C(X_0^+(2))$ in the monster are 3, 5, 7, 11, 13, 17, 19, 23, 31, 47. These are the same primes that have the rationality property for $X_0^+(2)$. Similarly, the Fricke elements of odd prime orders in the centralizer of $g \in C(X_0(2))$ in the monster have orders 3, 5, 7, 11, 23, and these coincide with the primes that have the rationality property for $X_0(2)$.

3.4 Connections to umbral moonshine

In this section we consider the modular curves that occur as lambencies in umbral moonshine. Given such an umbral modular curve X we present another characterization of the primes that have the rationality property for X. This will be in terms of the modularity properties of certain graded trace functions.

Recall from Section 2.9 that associated to each of the 23 cases of umbral moonshine are: a modular curve X of genus zero called its lambency; an umbral group G^X; and a set of graded trace functions H_g^X for each $g \in G^X$. The functions H_g^X are vector-valued mock modular forms of weight $\frac{1}{2}$ and level n_g, and a formula for the shadow of H_g^X may be given in terms of naturally defined characters of G^X called *twisted Euler characters* (cf. Section 5.1 of [CDH14b]). The formulas show that the shadow of H_g^X is zero if and only if the value of all the twisted Euler characters at g is 0.

Consider the case of umbral moonshine of lambency $X_0(2)$ (i.e. Mathieu moonshine). This has umbral group equal to the largest Mathieu group M_{24}. The following table gives the conjugacy classes $[g]$ of M_{24} with n_g an odd prime, and the values of the twisted Euler character $\overline{\chi}_g^A$ at these conjugacy classes.

$[g]$	$3A$	$3B$	$5A$	$7AB$	$11A$	$23AB$
n_g	3	3	5	7	11	23
$\overline{\chi}_g^A$	6	0	4	3	2	1

From this table, we see that there exists an element g of G^X, where n_g is an odd prime, for which the shadow H_g^X is *nonzero* if and only if $p = 3, 5, 7, 11, 23$. These primes are precisely the ones that have the rationality property for $X_0(2)$. In this example, one could argue that these primes are also simply the primes appearing as n_g, but as the next example shows, in some cases there are primes that appear as n_g but not as the level of a mock modular form with non-vanishing shadow.

Consider the umbral moonshine case of lambency $X = X_0(5)$. The following table gives the conjugacy classes $[g]$ of G^X whose order n_g is a prime $p \neq 5$, and the values of the twisted Euler characters $\overline{\chi}_g^A$ and χ_g^A at these conjugacy classes.

$[g]$	$2B$	$2C$	$3A$	$6A$
n_g	2	2	3	3
$\overline{\chi}_g^A$	2	2	0	0
χ_g^A	-2	2	0	0

In this case of umbral moonshine, the graded trace function H_g^X for any order 3 element g of G^X has shadow equal to zero, i.e., H_g^X is a classical modular form. There is an element g, of prime order $p \neq 5$, of G^X for which the shadow of H_g^X is nonzero if and only if $p = 2$. The prime 2 happens to be the only prime that has the rationality property for $X_0(5)$.

In fact this pattern persists and we have the following theorem.

Theorem 3.4.1 (Theorem 1.3.5)**.** *Let X be an umbral modular curve, and let p be a prime not dividing the level of X. Then the prime p has the rationality property for X if and only if there exists an element $g \in G^X$ such that $n_g = p$ and the shadow of H_g^X is nonzero.*

Proof. From the tables of values of the twisted Euler characters in [CDH14b], one can enumerate the primes p not dividing N with the following properties: (1) there is a $g \in G^X$ with $n_g = p$; and (2) there is a twisted Euler character that does not vanish at g, or equivalently, the shadow of H_g^X is nonzero. By inspection the primes that satisfy these properties are the same primes that have the rationality property for X. □

Remark 3.4.2. *We considered only the primes that do not divide the level in the formulation of our notion of rationality. It would be interesting to extend this notion so as to include all primes. Can this be done in such a way that Theorems 1.3.3 and 1.3.5 also generalize?*

Remark 3.4.3. *As explained in a recent work of Cheng and Duncan, naturally attached to any lambency X—i.e. a genus zero quotient of $X_0(N)$ by a set of Atkin-Lehner involutions that does not include the Fricke involution—is an "optimal mock Jacobi form" ϕ^X of level 1 with integer coefficients [CD16]. These optimal mock Jacobi forms allow the recovery of the graded trace functions in umbral moonshine; if X is an umbral lambency, then the components of H_e^X are the coefficients in the theta decomposition of ϕ^X, and the components of the other graded trace functions H_g^X may be obtained, via certain multiplicative relations (cf. Table 8 and 9 of [CDH14b]), from $\phi^{X'}$ where X' is of lower lambency. There are extra lambencies in [CD16] that do not occur in umbral moonshine. A natural guess is that there is a generalization of umbral moonshine that incorporates these more general lambencies, and Theorem 1.3.5 could serve as a consistency check for this generalization.*

Remark 3.4.4. *We have proven Theorems 1.3.3 and 1.3.5 by checking their validity case by case. For Theorem 1.3.3, generalized moonshine could possibly explain conceptually why the prime orders of Fricke elements appear in our list of primes with the rationality property, similar to how monstrous moonshine explains why the primes dividing the order of the monster are included in Ogg's list of primes. Beyond this, it remains a big challenge to find conceptual proofs for these theorems.*

3.5 Supersingular polynomials with level

In this section we prove Theorem 1.3.7. For an even positive integer k we denote by E_k the normalized Eisenstein series of weight k, by G_k the coefficient of X^k in $(1-3E_4(\tau)X^4+2E_6(\tau)X^6)^{-1/2}$, and by H_k the coefficient of X^k in $(1-3E_4(\tau)X^4+2E_6(\tau)X^6)^{k/2}$.

Suppose that the genus of $X_0(N)$ is zero, and let T_N be the principal modulus for $\Gamma_0(N)$. There is a normalized modular form $\Delta_N \in M_{12}(\Gamma_0(N))$, whose formula is given in Appendix A.3, that vanishes only at the infinite cusp of $\Gamma_0(N)$ and nowhere else. Since Δ is a modular form of weight 12 and level one that vanishes only at the infinite cusp and nowhere else, the modular form Δ_N may be considered as a higher level analogue of Δ and hence the choice for its notation.

Let p be prime. Note that we can uniquely write $p-1$ in the form

$$p-1 = 12m + 4\delta + 6\epsilon \quad \text{where} \quad m \geq \mathbb{Z}_{\geq 0}, \quad \delta, \epsilon \in \{0,1\}.$$

Using the classical valence formula (cf. Section 6.3 of [Apo12]), if $f \in M_{p-1}(\Gamma_0(1))$, then $f/(E_4^\delta E_6^\epsilon) \in M_{12m}(\Gamma_0(1))$. We get a modular function on $\Gamma_0(N)$ by dividing $f/(E_4^\delta E_6^\epsilon)$ by Δ_N^m. Moreover, since Δ_N vanishes only at the infinite cusp, the poles of $f/(E_4^\delta E_6^\epsilon \Delta_N^m)$ are supported at ∞. Thus there exists a polynomial $f_p^{(N)} \in \mathbb{C}[x]$ such that

$$\frac{f}{E_4^\delta E_6^\epsilon \Delta_N^m} = f_p^{(N)}(T_N).$$

Note that if f has integral Fourier coefficients, which is true for the modular forms E_{p-1}, G_{p-1}, H_{p-1} then $f_p^{(N)}$ has rational coefficients.

Later, in proving Theorem 1.3.7, we will be using the following result—which is the $N=1$ case of Theorem 1.3.7—due to Deuring, Hasse, Deligne, Kaneko and Zagier [KZ98].

Proposition 3.5.1. *Let $p \geq 5$ be a prime and let f be any of E_{p-1}, G_{p-1} or H_{p-1}. Then*

$$ss_p^{(1)}(x) \equiv \pm f_p^{(1)}(x) x^{\delta} (x - 1728)^{\epsilon} \pmod{p}.$$

We denote by $g_p^{(N)}$ the higher level analogues of the factor x^{δ} and $(x - 1728)^{\epsilon}$ found in this proposition which we obtain as follows. The factor x corresponds to the (isomorphism class of the) elliptic curve $y^2 = x^3 + 1$ with j-invariant equal to 0. The exponent δ is equal to 1 when $p \equiv 2 \pmod{3}$. The proposition says that these are precisely the primes p for which the elliptic curve $y^2 = x^3 + 1$ is supersingular in characteristic p. Similarly, the factor $x - 1728$ corresponds to the (class of) curve $y^2 = x^3 + x$ with j-invariant 1728, and the proposition says that this elliptic curve is supersingular when $\epsilon = 1$ or when $p \equiv 3 \pmod{4}$.

These distinguished isomorphism classes of elliptic curves with j-invariants 0 and 1728—or equivalently points on the moduli space $X_0(1)$ with j-values 0 or 1728—break up into several isomorphism classes when we consider them as elliptic curves with level structure N, or as points on the moduli space $X_0(N)$. The T_N-values of these points constitute the roots of the polynomial analogue of $x^{\delta}(x - 1728)^{\epsilon}$ that we seek.

To obtain the T_N-values given a j-value, we need a *modular relation* between j and T_N, by which we mean a relation $j(\tau) = r_N(T_N(\tau))$ for some rational function $r_N \in \mathbb{Q}(x)$. In Appendix A.5 we present the complete list of modular relations for j and T_N for the N's such that $X_0(N)$ has genus zero. One can verify these identities by checking that the Fourier coefficients for the left and the right hand side coincide up to the Sturm bound. In practice, one can check that the first

$$[\mathrm{SL}_2(\mathbb{Z}) : \Gamma_0(N)] = N \prod_{\substack{p \mid N \\ p,\ \text{prime}}} \left(1 + \frac{1}{p}\right)$$

coefficients coincide.

To find the T_N-values of the points with j-invariants 0 and 1728, we need only to solve the equations $0 = r_N(T_N)$ and $1728 = r_N(T_N)$. For example, for $N = 2$, we have $r_2(T) = (T + 256)^3/T^2$ and so:

$$r_2(T) = 0 \quad \Rightarrow \quad T + 256 = 0,$$

$$r_2(T) = 1728 \quad \Rightarrow \quad (T - 512)(T + 64) = 0.$$

Therefore the level 2 analogue of $x^\delta(x - 1728)^\epsilon$ is $(x + 256)^\delta(x - 512)^\epsilon(x + 64)^\epsilon$. One can do the same for the other levels to obtain all the polynomials $g_p^{(N)}$.

Proof of Theorem 1.3.7. Note that the supersingular points of $X_0(N)$ modulo p are the points lying above the supersingular points of $X_0(1)$ modulo p. Therefore Proposition 3.5.1 tells us that the roots of the equation $f_p^{(1)}(j)j^\delta(j - 1728)^\epsilon = 0$ are the j-values of the supersingular points of $X_0(N)$ modulo p. From the definition of $f_p^{(N)}$ we have the relation

$$f_p^{(N)}(T_N)\Delta_N^m = f_p^{(1)}(j)\Delta^m. \tag{3.1}$$

Therefore $f_p^{(1)}(j) = 0$ if and only if $f_p^{(N)}(T_N) = 0$. Also by definition of $g_p^{(N)}$, the equation $j^\delta(j - 1728)^\epsilon = 0$ holds if and only if $g_p^{(N)}(T_N) = 0$. Therefore the roots of $g_p^{(N)}(T_N)f_p^{(N)}(T_N) = 0$ are the T_N-values of the supersingular points of $X_0(N)$ modulo p. Finally, the coefficient of $g_p^{(N)}(T_N)f_p^{(N)}(T_N)$ is ±1 because: $g_p^{(N)}$ is monic, and by (1) the leading term of $f_p^{(N)}$ is the same as the leading term of $f_p^{(1)}$, which is ±1 by Proposition 3.5.1. □

Chapter 4

Towards higher genus moonshine

4.1 Searching for genus one moonshine

In this chapter we give several examples of moonshine with the genus one property. Recall that by this we mean the following: There exists a non-trivial finite group G and a pair of graded G-modules $K^{(x)}$ and $K^{(y)}$ such that for each $g \in G$, the graded traces x_g and y_g of g on $K^{(x)}$ and $K^{(y)}$ are generators for the function field of a certain genus one modular curve X_g. We also require, to ensure that the module is not trivial, that $X_g \neq X_{1A}$ when g is not the identity element $1A$ of G.

We will systematically search for examples of moonshine with the genus one property using the following procedure.

1. The genus zero modular curves that appear in monstrous moonshine are all compactified quotients of the upper half-plane by $n|h$-type groups. Similarly we restrict our search of modular curves to a set $\mathcal{G}$ of genus one curves of a particular type.

2. We then use the power maps of Conway and Norton to determine which modular curves in $\mathcal{G}$ form a compatible collection.

3. Let $\mathcal{X}$ be a compatible collection of modular curves obtained from the previous step. We search for a group G with the following property: to each conjugacy class C of G we may assign a modular curve $Y \in \mathcal{X}$ such that this assignment preserves the power maps—i.e. if X_1 and X_2 are the modular curves assigned to C_1 and C_2 respectively, then $X_1 = X_2^d$ if and only if $C_1 = C_2^d$.

4. If a group G exists we then compute for each $X \in \mathcal{X}$ a pair of functions that generate the function field of X. There are multiple choices for these generators. We choose these generators so that they may be interpreted as the graded trace functions of the action of G on some module.

4.2 Genus one modular curves

In this section we discuss the first two steps outlined in Section 4.1.

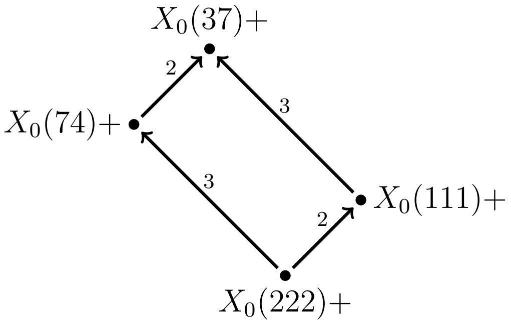
For the first step we consider $\mathcal{G}$ to be the set of all genus one modular curves of the form $X_0(N)+e, f, \ldots$ where N is squarefree. There are 96 curves in $\mathcal{G}$ and we reproduce in Appendix B.1 the complete list of such genus one curves. We give two reasons for this relatively restricted choice. The first is that we already have the complete list of these curves thanks to the work of Cummins (cf. Table 2 in [Cum04]), and the second is that even with such a restricted list we have already found many examples of genus one moonshine. We believe that more examples of genus one moonshine may be obtained if we consider, as in the case of monstrous moonshine, all genus one modular curves of $n|h$-type instead. However our current choice of $\mathcal{G}$ provides a quick way of achieving our modest goal of presenting evidence for the proliferation of moonshine with the genus one property.

In [CN79] Conway and Norton defined the power of an $n|h$-type group or modular curve. We will not be needing the full description of this power map, since the groups under present consideration have $h = 1$. In this special setting the dth power of

$X_0(n)$+$e, f, \ldots$ is given by $X_0(n')$+$e', f', \ldots$ where $n' = \frac{n}{(n,d)}$ and e', f', $\ldots$ are the divisors of n' among the numbers $e, f, \ldots$.

We may now proceed to the second step as outlined in Section 4.1. We may now determine which curves in $\mathcal{G}$ form a compatible collection. We give an example of how we do this.

Consider the curve $X_0(37)$+, which is the first genus one modular curve of the form $X_0(p)$+ where p is a prime. The complete list of genus one modular curves in $\mathcal{G}$ that power up to $X_0(37)$+ are $X_0(37)$+, $X_0(74)$+, $X_0(111)$+ and $X_0(222)$+. This list may be obtained by noting that any curve that powers up to $X_0(37)$+ must have level equal to a multiple of 37. There are only four curves with levels equal to multiples of 37—the ones just listed—and one can simply check that all of them power up to $X_0(37)$+. The following is a graph where the vertices represent these modular curves, and where an arrow from X to Y with label d means that $X^d = Y$.



It is clear that the set $\mathcal{X} = \{X_0(37)+, X_0(74)+, X_0(111)+, X_0(222)+\}$ is a compatible collection of modular curves with base $X_0(37)$+. The following lemma is obtained by inspection of the list in Appendix B.1.

Lemma 4.2.1. *Let $\mathcal{G}$ be the set of modular curves of the form $X_0(N)$+$e, f, \ldots$ of genus one such that N is squarefree. Let $\mathcal{X}$ be a subset of $\mathcal{G}$, $|\mathcal{X}| \geq 2$, that is a compatible collection of modular curves with base X. Then the following are the possible choices for X: $X_0(11)$; $X_0(14)$+2; $X_0(15)$; $X_0(15)$+3; $X_0(17)$; $X_0(19)$; $X_0(21)$; $X_0(21)$+7; $X_0(26)$+2; $X_0(26)$+13; $X_0(35)$+5; $X_0(37)$+; $X_0(39)$+3; $X_0(43)$+;*

$X_0(53)+$; $X_0(55)+11$; $X_0(57)+$; $X_0(58)+$; $X_0(65)+$; $X_0(77)+$; $X_0(91)+$.

For each base X, a compatible collection of modular curves with base X is given in Appendix B.2.

4.3 Function field generators

Let $X = \Gamma\backslash\mathbb{H}^*$ be a genus one modular curve. Unlike the case of genus zero curves, two functions are now needed to generate the function field of X. These generators x and y may be chosen so that they respectively have poles of orders 2 and 3 at the infinite cusp and are holomorphic everywhere else. As such we can express these generators in terms of Rademacher sums, say:

$$x = R^{[-2]}_{\Gamma,0} + AR^{[-1]}_{\Gamma,0}, \qquad y = R^{[-3]}_{\Gamma,0} + BR^{[-2]}_{\Gamma,0} + CR^{[-1]}_{\Gamma,0}$$

for some constants A, B and C. These generators are modular functions and therefore we can identify the value of A, and the relationship between B and C, by noting that the shadows of x and y must be zero. We have the equations:

$$\begin{aligned} S(x) = 2R^{[2]}_{\Gamma,2} + AR^{[1]}_{\Gamma,2} &= 0 \\ S(y) = 3R^{[3]}_{\Gamma,2} + 2BR^{[2]}_{\Gamma,2} + CR^{[1]}_{\Gamma,2} &= 0 \end{aligned}$$

where $S(x)$ and $S(y)$ denote the shadows of x and y respectively.

For example if $X = X_0(37)+$ so that $\Gamma = \Gamma_0(37)+$ then

$$\begin{aligned} 2R^{[2]}_{\Gamma,2} + AR^{[1]}_{\Gamma,2} &= 2(-0.4q + 0.8q^2 + 1.2q^3 - 0.8q^4 + 0.8q^5 - 2.5q^6 + \cdots) \\ &\quad +A(0.4q - 0.8q^2 - 1.2q^3 + 0.8q^4 - 0.8q^5 + 2.5q^6 + \cdots), \end{aligned}$$

so for this to be zero, A must be 2, and

$$\begin{aligned} 3R^{[3]}_{\Gamma,2} + 2BR^{[2]}_{\Gamma,2} + CR^{[1]}_{\Gamma,2} &= 3(-0.4q + 0.8q^2 + 1.2q^3 - 0.8q^4 + 0.8q^5 + \cdots) \\ &+2B(-0.4q + 0.8q^2 + 1.2q^3 - 0.8q^4 + 0.8q^5 + \cdots) \\ &+C(0.4q - 0.8q^2 - 1.2q^3 + 0.8q^4 - 0.8q^5 + \cdots), \end{aligned}$$

therefore this is zero if $C - 2B = 3$. We may choose $B = 0$, in which case $C = 3$, so that we have the following generators x and y for $X_0(37)+$.

$$\begin{aligned} x &= q^{-2} + 2q^{-1} + 9q + 18q^2 + 29q^3 + 51q^4 + 82q^5 + 131q^6 + \cdots \\ y &= q^{-3} + 3q^{-1} + 19q + 38q^2 + 93q^3 + 176q^4 + 347q^5 + 630q^6 + \cdots \end{aligned}$$

Note that the results of [JST16], who obtained these generators for $X_0(37)+$ using a different method, justify the numerical approximations that we use above. Using Table 5 of their paper, or the method we just outlined, we obtain the following values of A, and the relationship between B and C, for the generators $x = q^{-2} + Aq^{-1} + \cdots$ and $y = q^{-3} + Bq^{-2} + Cq^{-1} + \cdots$ of the function field of the modular curves in the compatible collection $\mathcal{X}$ with base $X_0(37)+$. (We give in Appendix B.2 the generators for the function field of the modular curves appearing in a compatible collection $\mathcal{X}$ in Lemma 4.2.1.) This is summarized in the following table.

X	A	relationship between B and C
$X_0(37)+$	2	$C - 2B = 3$
$X_0(74)+$	0	$C = 3$, B is any constant
$X_0(111)+$	2	$C - 2B = 0$
$X_0(222)+$	0	$C = 0$, B is any constant

Choosing $B = 0$ for each case we get generators, compiled in the following table, for the function field of each $X \in \mathcal{X}$.

X	generators x and y for the function field of X
$X_0(37)+$	$x = q^{-2} + 2q^{-1} + 9q + 18q^2 + 29q^3 + 51q^4 + 82q^5 + 131q^6 + \cdots$ $y = q^{-3} + 3q^{-1} + 19q + 38q^2 + 93q^3 + 176q^4 + 347q^5 + 630q^6 + \cdots$
$X_0(74)+$	$x = q^{-2} + q + 4q^2 + 3q^3 + 7q^4 + 6q^5 + 13q^6 + 13q^7 + 22q^8 + 22q^9 + \cdots$ $y = q^{-3} + 3q^{-1} + 7q + 6q^2 + 17q^3 + 16q^4 + 35q^5 + 38q^6 + 71q^7 + \cdots$
$X_0(111)+$	$x = q^{-2} + 2q^{-1} + 3q + 3q^2 + 2q^3 + 3q^4 + 4q^5 + 5q^6 + 7q^7 + 9q^8 + \cdots$ $y = q^{-3} + q + 2q^2 + 6q^3 + 5q^4 + 8q^5 + 12q^6 + 14q^7 + 18q^8 + \cdots$
$X_0(222)+$	$x = q^{-2} + q + q^2 + q^4 + q^6 + q^7 + q^8 + q^9 + 2q^{10} + \cdots$ $y = q^{-3} + q + 2q^3 + q^4 + 2q^5 + 2q^6 + 2q^7 + 2q^8 + 5q^9 + \cdots$

4.4 Moonshine with the genus one property

Now that generators for function fields of modular curves have been identified we are now ready to give an example of moonshine with the genus one property that illustrates the general situation. Consider the set

$$\mathcal{X} = \{X_0(37)+, X_0(74)+, X_0(111)+, X_0(222)+\}$$

of compatible modular curves with base $X_0(37)+$. For each $Y \in \mathcal{X}$ there is a smallest positive power d such that $Y^d = X_0(37)+$. These powers are:

$$(X_0(222)+)^6 = (X_0(111)+)^3 = (X_0(74)+)^2 = X_0(37)+.$$

We try to look for a group G whose conjugacy classes have orders 1, 2, 3 and 6 (which are precisely these powers) because our aim is to assign to each conjugacy class of G a modular curve in $\mathcal{X}$, with the condition that the corresponding power maps are preserved. The group $\mathbb{Z}/6\mathbb{Z}$ has the desired orders of conjugacy classes. It has six conjugacy classes: conjugacy class $1A$ of order 1; class $2A$ of order 2; classes $3A$ and $3B$ of order 3; and classes $6A$ and $6B$ of order 6. Moreover, if we make the following assignment then the respective power maps are preserved.

$$\begin{aligned} 1A &\rightsquigarrow X_0(37)+ \qquad & 3A, 3B &\rightsquigarrow X_0(111)+ \\ 2A &\rightsquigarrow X_0(74)+ \qquad & 6A, 6B &\rightsquigarrow X_0(222)+ \end{aligned}$$

Conjecture 4.4.1. *There exist graded $\mathbb{Z}/6\mathbb{Z}$-modules $K^{(x)}$ and $K^{(y)}$ such that for each $g \in \mathbb{Z}/6\mathbb{Z}$ the graded traces of g on $K^{(x)}$ and $K^{(y)}$ generate $X_0(37 \cdot \mathrm{ord}(g))+$. In other words, there is a genus one moonshine for $X_0(37)+$.*

Let x_g be the generator of $X_0(37{\cdot}\mathrm{ord}(g))+$ that has a pole of order 2 at the infinite cusp, and write

$$x_g(\tau) = \sum_{n=-2}^{\infty} c_{\mathrm{ord}(g)}(n).$$

The congruences

$$\begin{aligned} c_1(n) &\equiv c_2(n) \pmod 2 \qquad & c_2(n) &\equiv c_6(n) \pmod 3 \\ c_1(n) &\equiv c_3(n) \pmod 3 \qquad & c_3(n) &\equiv c_6(n) \pmod 2, \end{aligned}$$

which may be verified from the first 222 Fourier coefficients, imply that

$$\begin{aligned} m_1(n) &= c_1(n) + c_2(n) + 2c_3(n) + 2c_6(n) \\ m_2(n) &= c_1(n) - c_2(n) + 2c_3(n) - 2c_6(n) \\ m_3(n) = m_4(n) &= c_1(n) - c_2(n) - c_3(n) + c_6(n) \\ m_5(n) = m_6(n) &= c_1(n) + c_2(n) - c_3(n) - c_6(n) \end{aligned}$$

are all integers. Let M_i be the irreducible representation of $\mathbb{Z}/6\mathbb{Z}$ with character χ_i, and construct the $\mathbb{Z}/6\mathbb{Z}$-module

$$K^{(x)} = \bigoplus_{n=-2}^{\infty} K_n^{(x)}$$

where

$$K_n^{(x)} = m_1(n)M_1 \oplus m_2(n) \oplus \cdots \oplus m_6(n)M_6.$$

Using the character table of $\mathbb{Z}/6\mathbb{Z}$, one can check that the graded trace of g on $K^{(x)}$ is precisely x_g.

Similarly—because of the congruences satisfied by the coefficients of the generators of the function fields—there exists a graded $\mathbb{Z}/6\mathbb{Z}$-module $K^{(y)}$ such that if $g \in \mathbb{Z}/6\mathbb{Z}$ then the graded trace of g on $K^{(y)}$ is the generator y_g of $X_0(37 \cdot \mathrm{ord}(g))+$. Therefore we have the following theorem.

Theorem 4.4.2. *Conjecture 4.4.1 is true.*

How do we obtain the other examples of genus one moonshine? We start with a compatible collection $\mathcal{X}$ of modular curves with base X as provided by Lemma 4.2.1. For $Y \in \mathcal{X}$ let $d = d(Y)$ be the smallest positive integer for which $Y^d = X$, and define $d(\mathcal{X}) := \{d(Y) : Y \in \mathcal{X}\}$. Just like our illustrative example, we hope to find a group G whose conjugacy classes have orders that are precisely equal to the numbers in $d(\mathcal{X})$, and then make the assignment:

$$\text{conjugacy class of order } d \rightsquigarrow Y \in \mathcal{X} \text{ such that } Y^d = X.$$

Sometimes this step of finding such a group is unsuccessful. (Perhaps we need more modular curves that are not of the type that we have considered.) Nevertheless given any compatible collection $\mathcal{X}$ of Lemma 4.2.1, there exists a compatible subcollection $\mathcal{X}'$ of modular curves with base X where we can apply the methods outlined in this section. For these subcollections, the following table gives groups G that one may use, and the congruences that must be checked for the method we just outlined to go through. Here $c_d(n)$ denotes the coefficient of q^n of (any of) the generators of $Y \in \mathcal{X}'$ corresponding to the conjugacy class of order d.

$d(\mathcal{X}')$	G	congruences to check
$\{1,2\}$	cyclic group $\mathbb{Z}/2\mathbb{Z}$	$c_1(n) \equiv c_2(n) \pmod 2$
$\{1,3\}$	cyclic group $\mathbb{Z}/3\mathbb{Z}$	$c_1(n) \equiv c_3(n) \pmod 3$
$\{1,2,3\}$	symmetric group S_3	$c_1(n) \equiv c_2(n) \pmod 2$, $c_1(n) \equiv c_3(n) \pmod 3$
$\{1,2,5\}$	dihedral group D_{10}	$c_1(n) \equiv c_2(n) \pmod 2$, $c_1(n) \equiv c_5(n) \pmod 5$

Note that these congruences may be confirmed by showing that they hold for all n up to the Sturm bound. We have the following theorem.

Theorem 4.4.3 (Theorem 1.4.2)**.** *There is a genus one moonshine for X, where X is any of the following:* $X_0(11)$*;* $X_0(14)$+2*;* $X_0(15)$*;* $X_0(15)$+3*;* $X_0(17)$*;* $X_0(19)$*;* $X_0(21)$*;* $X_0(21)$+7*;* $X_0(26)$+2*;* $X_0(26)$+13*;* $X_0(35)$+5*;* $X_0(37)$+*;* $X_0(39)$+3*;* $X_0(43)$+*;* $X_0(53)$+*;* $X_0(55)$+11*;* $X_0(57)$+*;* $X_0(58)$+*;* $X_0(65)$+*;* $X_0(77)$+*;* $X_0(91)$+*.*

Chapter 5

Homogeneous subspaces of vertex operator algebras

5.1 Vertex operator algebras: basic notions

Vertex operator algebras are algebraic objects that play important roles in mathematics and physics. They were introduced to mathematics in the 1980s by Frenkel, Lepowsky and Meurman—building on the earlier work of Borcherds on the notion of a vertex algebra [Bor86]—to understand the monster and the structure of the moonshine module [FLM89]. Vertex operator algebras are now ubiquitous in the study of infinite-dimensional Lie algebras, and are essentially the mathematical formulations of two-dimensional conformal field theories [Gab00]. In this section we recall basic definitions and facts about vertex operator algebras and their representations. We refer the reader to [FBZ04], [FLM89] and [LL12] for comprehensive treatments of the subject.

A *vertex operator algebra* is a complex vector space V equipped with two distinguished vectors $\mathbf{1}$ and ω, called the *vacuum element* and the *conformal vector* respectively, and a map $Y(\cdot, z) : V \to \mathrm{End}(V)[[z, z^{-1}]]$ that assigns to each element

$v \in V$ a formal power series

$$Y(v,z) := \sum_{n \in \mathbb{Z}} v(n) z^{-n-1}$$

called the *vertex operator* attached to v. The quadruple $(V, \mathbf{1}, \omega, Y)$ must satisfy several axioms, a complete list of which is given for instance in Chapter 3 of [LL12]. One of these axioms is that the coefficients of the vertex operator attached to the conformal vector generate a copy of the Virasoro algebra of central charge c. By this we mean that if

$$Y(\omega, z) = \sum_{n \in \mathbb{Z}} L(n) z^{-n-2}$$

then

$$[L(m), L(n)] = (m-n)L(m+n) + \frac{1}{12}(m^3 - m)\delta_{m+n,0} c \mathrm{Id}_V.$$

We refer to c as the *central charge* of V.

A vertex operator algebra V admits a $\mathbb{Z}$-grading with gradation bounded from below

$$V = \bigoplus_{n \in \mathbb{Z}} V_n$$

and part of the axioms is that the subspaces V_n are precisely the eigenspaces of the $L(0)$ operator. That is,

$$V_n = \{v \in V : L(0)v = nv\}$$

are finite-dimensional complex vector spaces, and are equal to the zero space for all sufficiently small n. We refer to the eigenspaces V_n as the *homogeneous subspaces* of V. The smallest n for which $V_n \neq \{0\}$ is called the *conformal weight* of V; thus, if $\rho(V)$ denotes the conformal weight of V then

$$V = \bigoplus_{n=0}^{\infty} V_{\rho(V)+n}.$$

We say that V is of *CFT type* if $\rho(V) = 0$ and $V_0 = \mathbb{C}\mathbf{1}$.

As is the case with other algebraic structures there is a concept of *(irreducible) V-modules* for a vertex operator algebra V. We again refer the reader to Chapter 4 of [LL12] for the full definition of a module for a vertex operator algebra. We simply mention here that an irreducible V-module M is a vector space equipped with an operation $Y_M : V \to \mathrm{End}(M)[[z^{\pm 1}]]$ which assigns to each $v \in V$ a formal power series, and these power series must satisfy certain axioms. (Whenever we want to emphasize the map Y_M, as in Section 5.3 for example, we shall write (M, Y_M) for the V-module M.) It admits the following grading

$$M = \bigoplus_{n=0}^{\infty} M_{\rho(M)+n}$$

where M_α are finite-dimensional vector spaces, and $\rho(M)$ is a constant called the *conformal weight* of M.

We will restrict our attention to vertex operator algebras V for which every V-module is completely reducible. Such vertex operator algebras are called *rational.* As shown in [DLM98] this condition implies that there are only finitely many irreducible V-modules. In other words, the category of V-modules for a rational vertex operator algebra V is semisimple. Examples of rational vertex operator algebras are vertex operator algebras associated to even positive-definite lattices [Don93], vacuum representations of affine Kac-Moody algebras [FZ92] and the moonshine module [Don94]. We say that a vertex operator algebra V is *holomorphic* if it is rational and if the only irreducible V-module is V itself. The moonshine module is an example of a holomorphic vertex operator algebra of central charge 24 [Don94].

We will also be imposing, aside from rationality, a certain finiteness condition on our vertex operator algebras. In his work on the modularity of characters of vertex operator algebras (cf. Section 5.3) Zhu introduced the following notion [Zhu96]. We say that a vertex operator algebra V is *C_2-cofinite* if

$$C_2(V) := \mathrm{span}\{v(-2)w|v, w \in V\}$$

has finite codimension in V. Rationality is conjecturally equivalent to C_2-cofiniteness [ABD04]. Indeed the aforementioned examples of rational vertex operator algebras—vertex operator algebras associated to even positive-definite lattices, vacuum representations of affine Kac-Moody algebras, the moonshine module—are all known to be C_2-cofinite (cf. Section 12 of [DLM00]).

Given a module W of a vertex operator algebra V, there is another V-module W' associated to W called the *dual* of W. We refer the reader to Section 5.2 of [FHL93] for the definition of the dual module. We say that the vertex operator algebra V is *self-dual* if the adjoint module V is isomorphic as a V-module to its dual V'. Holomorphic vertex operator algebras are always self-dual. Vertex operator algebras associated to even positive-definite lattices are also self-dual [Don93].

5.2 Twisted modules and orbifold theory

One of the main tools in the construction of Frenkel, Lepowsky and Meurman of the moonshine module is orbifold theory. In orbifold theory one tries to understand the representation theory of fixed point vertex subalgebras [DRX17]. In this section we briefly address recent results in orbifold theory. We also discuss twisted sectors here; twisted sectors are a main feature of orbifold theory, and appear in some of the earliest papers in the conformal field theory literature [DHVW85].

An *automorphism* g of a vertex operator algebra V is a linear operator of V that preserves $\mathbf{1}$ and ω such that

$$gY(v, z)g^{-1} = Y(gv, z)$$

for $v \in V$. Suppose that g is an automorphism of V of finite order T. One may modify the axioms of a V-module to define *g-twisted V-modules.* We refer the reader to Section 3 of [DLM00] for the definition, and only mention here that an irreducible g-twisted V-module M, also known as a *g-twisted sector* of V, has a grading

$$M = \bigoplus_{n=0}^{\infty} M_{\rho(M)+\frac{n}{T}}$$

for some constant $\rho(M)$ called the *conformal weight* of M. As in the case of (untwisted) V-modules, we will be considering vertex operator algebras V where every g-twisted V-module is a direct sum of g-twisted sectors of V. We call such vertex operator algebras *g-rational.* As shown in [DLM98] this condition implies that there are only finitely many g-twisted sectors of V.

If V is holomorphic and C_2-cofinite, and g is an automorphism of V of finite order then V is g-rational. Moreover there is a unique (up to equivalence) g-twisted sector of V, which we denote by $V(g)$ [DLM00].

Given a finite group G of automorphisms of V, one can consider the space V^G of vectors in V that are G-invariant. The space V^G is also a vertex operator algebra, which we call a *fixed point vertex subalgebra.* Naturally one tries to understand the module category of V^G; this is known as *orbifold theory.* If V is a rational C_2-cofinite vertex operator algebra and G is a finite group of automorphism of V then the orbifold theory conjecture states that V^G is also rational and C_2-cofinite, and moreover, that every irreducible V^G-module occurs in a g-twisted sector of V for some $g \in G$. Recent progress towards the resolution of this conjecture is discussed in [CM16], [DRX17] and [Miy15]. Their results when combined state that if V is a rational C_2-cofinite vertex operator algebra of CFT type, and if G is a finite solvable group of automorphisms of V then V^G is rational and C_2-cofinite. More recently, it was shown in [Miy18] that if V is a C_2-cofinite simple vertex operator algebra of CFT type with a nonsingular invariant bilinear form and if G is any finite automorphism group of V, then V^G is also C_2-cofinite.

5.3 Modular invariance of characters

We discuss in this section the modular invariance of twisted sectors of rational C_2-cofinite vertex operator algebras. The results in this section are due to Zhu [Zhu96] and Dong, Li and Mason [DLM00].

Let V be a vertex operator algebra and let

$$M = \bigoplus_{n=0}^{\infty} M_{\rho(M)+n}$$

be an irreducible V-module. The *character* of M is defined as the formal power series

$$\mathrm{Ch}(M) := \sum_{n=0}^{\infty} \dim(M_{\rho(M)+n}) q^{\rho(M)+n-\frac{c}{24}}.$$

Here c is the central charge of V.

Suppose that V is rational, so that there are only finitely many irreducible V-modules, say $M_1, \ldots, M_s$. As usual we set $q = e^{2\pi i\tau}$ where $\tau \in \mathbb{H}$, and treat the characters as functions on the upper half-plane. Assuming that V is also C_2-cofinite, Zhu proved that the characters $\mathrm{Ch}(M_1), \ldots, \mathrm{Ch}(M_s)$ converge absolutely in $\mathbb{H}$, and moreover, that the vector space spanned by the characters $\mathrm{Ch}(M_1), \ldots, \mathrm{Ch}(M_s)$ is invariant under the action of $\mathrm{SL}_2(\mathbb{Z})$. More precisely if $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ then there exists a linear representation ρ of $\mathrm{SL}_2(\mathbb{Z})$ of degree s such that

$$\begin{bmatrix} \mathrm{Ch}(M_1)(\gamma\tau) \\ \vdots \\ \mathrm{Ch}(M_s)(\gamma\tau) \end{bmatrix} = \rho(\gamma) \begin{bmatrix} \mathrm{Ch}(M_1)(\tau) \\ \vdots \\ \mathrm{Ch}(M_s)(\tau) \end{bmatrix}.$$

In other words, Zhu showed that the characters of the irreducible modules of rational C_2-cofinite vertex operator algebras form a vector-valued modular function for $\mathrm{SL}_2(\mathbb{Z})$ with a multiplier system. Dong, Lin and Ng showed that the kernel of the representation ρ is in fact a congruence subgroup of $\mathrm{SL}_2(\mathbb{Z})$ if V is also self-dual [DLN15]. Hence if V is a rational, C_2-cofinite and self-dual vertex operator algebra then the characters of the irreducible modules of V are modular functions for congruence subgroups of $\mathrm{SL}_2(\mathbb{Z})$.

The characters of the irreducible modules are specializations of more general graded trace functions. Dong, Li and Mason showed that these functions are also modular, and what follows is a description of this result. We refer the reader to [DLM00] for more details.

Let V be a vertex operator algebra and let g be an automorphism of V of order T. Any automorphism h of V induces a bijection from the set of g-twisted sectors of V to the set of hgh^{-1}-twisted sectors of V. More precisely: if (M, Y_M) is a g-twisted sector of V and h is an automorphism of V, then the map

$$M = (M, Y_M) \longmapsto h \circ M := (M, Y_M \circ h)$$

where $(Y_M \circ h)(v, z) := Y_M(h^{-1}v, z)$, sends the g-twisted sector (M, Y_M) to the hgh^{-1}-twisted sector $(M, Y_M \circ h)$. Whenever g and h commute, we may therefore consider the collection of *h-stable* g-twisted sectors of V, by which we mean g-twisted sectors M such that $M \cong h \circ M$. Suppose that

$$M = \bigoplus_{n=0}^{\infty} M_{\rho(M)+\frac{n}{T}}$$

is an h-stable g-twisted sector of V. This means that there is a linear map $\phi(h) : M \to M$ satisfying

$$\phi(h) Y_M(v, z) \phi(h)^{-1} = Y_M(h^{-1}v, z)$$

for $v \in V$. By abuse of notation, we write h for $\phi(h)$. We define the graded trace function

$$Z_{M,g,h}(\tau) := \sum_{n=0}^{\infty} \operatorname{tr}(h|M_{\rho(M)+\frac{n}{T}})q^{\rho(M)+\frac{n}{T}-\frac{c}{24}}.$$

Here c is the central charge of V. This graded trace function is holomorphic on $\mathbb{H}$. Note that the graded trace functions reduce to the characters when h is taken to be the identity automorphism.

We require for the modularity of the graded trace functions, as in Zhu's modularity theorem, that V is a rational C_2-cofinite vertex operator algebra. Suppose V is such a vertex operator algebra and let G be a finite group of automorphisms of V. If V is also g-rational for all $g \in G$ then the vector space spanned by the graded trace functions $Z_{M,g,h}(\tau)$ for all possible choices of g, h and M—that is, for all commuting pairs of elements (g, h) of G, and all h-stable g-twisted sector M of V—is invariant under the action of $\mathrm{SL}_2(\mathbb{Z})$. More precisely, if $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$[1] then

$$Z_{M,g,h}(\gamma\tau) = \sum_{W} \sigma_W Z_{W,g^a h^c,g^b h^d}(\tau)$$

where the sum runs over all $g^b h^d$-stable $g^a h^c$-twisted sectors W of V, and where σ_W are constants that depend only on g, h, γ and W. Note that by Theorem 2.8 of [DR18], the assumption that V is g-rational for all $g \in G$ is satisfied whenever V is a rational C_2-cofinite vertex operator algebra of CFT type and G is a finite group of automorphisms of V.

Finally we describe the modularity of the graded trace functions in the following special cases where it is the simplest. First let us suppose that V is a holomorphic and C_2-cofinite vertex operator algebra of CFT type, and that g is an automorphism of V of order T. As mentioned in Section 5.2 there is a unique g-twisted sector $V(g)$

[1] We use the symbol c both for the central charge of V and the lower left entry of γ. This should not cause any confusion since the only place where the central charge appears in this work is in the exponent of q, where it always appears as the numerator of the fraction $c/24$.

of V. Given an automorphism h of V that commutes with g, we simplify our notation and write

$$Z_{g,h}(\tau) := Z_{V(g),g,h} = \sum_{n=0}^{\infty} \mathrm{tr}(h|V(g)_{\rho(V(g))+\frac{n}{T}})q^{\rho(V(g))+\frac{n}{T}-\frac{c}{24}}$$

for our graded trace function. If G is a finite group of automorphisms of V then for any commuting pair of elements $g, h \in G$ we have the transformation formula

$$Z_{g,h}(\gamma\tau) = \xi_{g,h}(\gamma)Z_{g^a h^c, g^b h^d}(\tau)$$

where $\xi_{g,h}(\gamma)$ is a nonzero complex number.

Next let us suppose that V is a rational, C_2-cofinite and self-dual vertex operator algebra of CFT type, and let G be a finite group of automorphisms of V. Given commuting elements g and h of G and an h-stable g-twisted sector M of V, Dong showed—see Lemma 4.3 of [DR18]—that the graded trace function $Z_{M,g,h}(\tau)$ may be written as a linear combination of characters $\mathrm{Ch}(M_i)$. Here the modules M_i are irreducible modules of certain fixed point vertex subalgebras of V. Since the characters are modular functions on congruence subgroups, we immediately get the following.

Lemma 5.3.1. *Let V be a rational, C_2-cofinite and self-dual vertex operator algebra of CFT type, and G be a finite group of automorphisms of V. Let g and h be commuting elements of G, and M be an h-stable g-twisted sector of V. Then the function $Z_{M,g,h}$ is a modular function on a congruence subgroup of $SL_2(\mathbb{Z})$.*

5.4 Asymptotic G-regularity of certain vertex operator algebras

In this section we prove Theorem 1.5.4 which generalizes the asymptotic $\mathbb{M}$-regularity of the moonshine module $V^\natural$ to certain vertex operator algebras V and groups G of automorphisms of V. This is joint work with Lea Beneish. First we prove the following lemma.

Lemma 5.4.1 (Lemma 1.5.1)**.** *Let G be finite group and let $K = \bigoplus_{n\in\mathbb{Z}} K_n$ be a graded representation of G. Let $M_1, \ldots, M_s$ be the irreducible representations of G and let $\mathrm{m}_i(n)$ be the multiplicity of M_i in K_n. If K has dominant identity trace then*

$$\mathrm{m}_i(n) \sim \frac{1}{|G|} \dim M_i \dim K_n$$

as $n \to \infty$. Consequently K is asymptotically G-regular.

Proof. Let χ_i be the character of M_i. Note that the character of K_n is given by $\psi_n(g) = \mathrm{tr}(g|K_n) = c_g(n)$. By the usual orthogonality of characters, the multiplicity $\mathrm{m}_i(n)$ of M_i in K_n is given by

$$\mathrm{m}_i(n) = \langle \chi_i, \psi_n \rangle = \frac{1}{|G|} \sum_{g\in G} \overline{\chi_i(g)} c_g(n).$$

Isolating the $g = e$ term and using the assumption that K has dominant identity trace (note: $c_e(n) = \dim K_n$) we get

$$\mathrm{m}_i(n) = \frac{1}{|G|} \dim M_i \dim K_n + o(\dim K_n)$$

as $n \to \infty$. Therefore

$$\mathrm{m}_i(n) \sim \frac{1}{|G|} \dim K_n \dim M_i$$

as $n \to \infty$. It immediately follows that

$$\lim_{n\to\infty} \frac{\mathrm{m}_i(n)}{\sum_{i=1}^{s} \mathrm{m}_i(n)} = \frac{\dim M_i}{\sum_{i=1}^{s} \dim M_i},$$

meaning K is asymptotically G-regular. □

If K is the Mathieu moonshine module then the graded trace functions of K may be written as Rademacher sums [CD12]. The coefficients of these Rademacher sums have known asymptotics, and from these we find that K has dominant identity trace and that

$$\dim K_n \sim \frac{4}{\sqrt{8n-1}} e^{\pi\sqrt{8n-1}/2}$$

as $n \to \infty$. We therefore have the following corollary.

Corollary 5.4.2. *Let $K = \bigoplus_{n=0}^{\infty} K_n$ be the Mathieu moonshine module. Let $M_i^{(M_{24})}$ denote an irreducible representation of the largest Mathieu group M_{24}, and let $\mathrm{m}_i(n)$ be the multiplicity of $M_i^{(M_{24})}$ in K_n. Then*

$$\mathrm{m}_i(n) \sim \frac{4e^{\pi\sqrt{8n-1}/2}}{|M_{24}|\sqrt{8n-1}} \dim M_i^{(M_{24})}$$

as $n \to \infty$, and K is asymptotically M_{24}-regular.

We now prove the main theorem of this chapter.

Theorem 5.4.3 (Theorem 1.5.4)**.** *Let V be a holomorphic C_2-cofinite vertex operator algebra of CFT type. Let G be a finite group of automorphisms of V. Let $g \in G$ and denote by $V(g)$ the unique (up to equivalence) g-twisted sector of V. If the conformal weight $\rho(V(g))$ of $V(g)$ is positive for all $g \neq e$ then the G-module V has dominant identity trace. Consequently V is asymptotically G-regular.*

Proof. We want to show that the G-module $V = \bigoplus_{n=0}^{\infty} V_n$ has dominant identity trace, i.e., that $c_h(n) = o(c_e(n))$ for all $h \neq e$ as $n \to \infty$. By Lemma 1.5.1 this implies that V is asymptotically G-regular.

For simplicity let us first consider the case when the central charge of V is divisible by 24. Since V is holomorphic and C_2-cofinite, Theorem I of [DLN15] states that the character $Z_{e,e} = \mathrm{Ch}(V)$ is a modular function for $\mathrm{SL}_2(\mathbb{Z})$. It has a pole of order

$$m := \frac{c}{24} \in \mathbb{Z}$$

at the infinite cusp, and therefore we may write $Z_{e,e}$ as a polynomial in the j-function of degree m. This polynomial is monic because V is of CFT type. Using well-known asymptotics for the j-function (cf. [Rad38]) we get

$$\dim V_n = c_e(n) \sim \frac{m^{1/4} e^{4\pi\sqrt{mn}}}{\sqrt{2} n^{3/4}}.$$

Let us now look at the other graded trace functions. Let $h \in G$, $h \neq e$. Since V is a holomorphic C_2-cofinite vertex operator algebra of CFT type, Lemma 5.3.1 implies that

$$Z_{e,h}(\tau) = \sum_{n=0}^{\infty} c_h(n) q^{n-m}$$

is a weakly holomorphic modular function on some congruence subgroup $\Gamma_0(N)$. We may thus express $Z_{e,e}$ as a linear combination of Maass-Poincarè series—or, if one prefers, of Rademacher sums—plus a constant. (See Theorem 1.1 of [BO12] and also Theorem 8.9 of [DGO15a]).

Suppose that $Z_{e,h}$ has a pole at the cusp s of $\Gamma_0(N)$ of order m_s. Note that if $s = \frac{a}{c}$ with $(a, c) = 1$, and if $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$ then

$$Z_{e,h}(\gamma\tau) = \sigma(h, \gamma) Z_{h^c, h^d}(\tau) = \sigma(h, \gamma) \sum_{n=0}^{\infty} a(n) q^{\frac{n}{\mathrm{ord}(h^c)} + \rho(V(h^c)) - m}.$$

Since $\rho(V(h^c)) \geq 0$ by assumption, we find that $m_s = m - \rho(V(h^c)) \leq m$. As mentioned in the previous paragraph we can write $Z_{e,h}$ as

$$Z_{e,h}(\tau) = K + \sum_{s \in \mathcal{S}_N^*} (c_s P_{s,\Gamma_0(N)}^{[m_s]}(\tau) + \cdots)$$

where:

- $\mathcal{S}_N^*$ is the complete set of representatives for the cusps of $\Gamma_0(N)$ where $Z_{e,h}$ has a pole;
- $P_{s,\Gamma_0(N)}^{[m]}$ is the index m Maass-Poincaré series for $\Gamma_0(N)$ that is holomorphic at the cusps of $\Gamma_0(N)$, except for the cusp s where it has principal part q^m;
- c_s is a nonzero constant;
- the omitted terms are Maass-Poincaré series of lower indices;
- and K is a constant.

The exact formula for the coefficients of the Maass-Poincaré series $P_{s,\Gamma_0(N)}^{[m_s]}$, together with the asymptotics of the I-Bessel function, imply that

$$\begin{aligned} c_h(n) = & \left(K_\infty \frac{e^{4\pi\sqrt{mn}/N}}{n^{3/4}} + o\left(\frac{e^{4\pi\sqrt{mn}/N}}{n^{3/4}} \right) \right) \\ & + \sum_{s = \frac{a}{c} \in S_N^* \setminus \{\infty\}} \left(K_s \frac{e^{4\pi\sqrt{m_s n}/c}}{n^{3/4}} + o\left(\frac{e^{4\pi\sqrt{m_s n}/c}}{n^{3/4}} \right) \right) \end{aligned}$$

as $n \to \infty$, where the isolated term is the contribution coming from the infinite cusp, and K_s and K_∞ are constants (which my be zero).

If $Z_{e,h}$ is holomorphic at the zero cusp, i.e. if $0 \notin \mathcal{S}_N^*$, then $c_h(n) = o(c_e(n))$ since each term is $o(c_e(n))$. If $Z_{e,h}$ has a pole at the zero cusp then we claim that m_0 is strictly less than m, in which case $c_h(n)$ is also $o(c_e(n))$ since each term is $o(c_e(n))$.

Indeed let $S = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$. The expansion of $Z_{e,h}$ at the zero cusp of $\Gamma_0(N)$ is

$$Z_{e,h}(S\tau) = \sigma(h, S) Z_{h,e}(\tau) = \sigma(h, S) \sum_{n=0}^{\infty} \dim V(h)_n \, q^{\frac{n}{\operatorname{ord}(h)} + \rho - m} \tag{5.1}$$

where $\sigma(h, S)$ is a nonzero constant and ρ is the conformal weight of $V(h)$, which is positive by our assumption since $h \neq e$. Note that the order of the pole of $Z_{e,h}$ at the zero cusp is $0 < m_0 = m - \rho < m$ which proves the claim. This completes the proof when the central charge is divisible by 24.

If the central charge is not divisible by 24, the character $Z_{e,e}$ is still a modular function for $\mathrm{SL}_2(\mathbb{Z})$ but possibly with a multiplier system. This still gives $c_e(n) \sim K \frac{e^{4\pi\sqrt{mn}}}{n^{3/4}}$ as $n \to \infty$ for some constant K. The same proof as before holds. □

5.5 Positivity condition on twisted sectors

Let V be a holomorphic C_2-cofinite vertex operator algebra of CFT type, and let G be a finite group of automorphisms of V. Recall the following definition: the pair (V, G) satisfies the positivity condition on twisted sectors if the conformal weight $\rho(V(g))$ of the twisted sector $V(g)$ is positive for all $g \in G \setminus \{e\}$. In this section we give examples where it is known to hold. The results in this section are due to Möller (cf. Section 4 of [Möl18]).

The first class of examples are given by tensor products of holomorphic vertex operator algebras. Let W be a holomorphic C_2-cofinite vertex operator algebra of CFT type. Then the vertex operator algebra $V = W^{\otimes k}$ is also a holomorphic C_2-cofinite vertex operator algebra of CFT type, and any subgroup G of the symmetric group S_k acts on V in an obvious way. Proposition 4.1 of [Möl18] says that the pair (V, G) satisfies the positivity condition on twisted sectors.

Another class of examples come from lattice vertex operator algebras. Let L be an even, unimodular and positive-definite lattice, and let $V = V_L$ be the vertex operator algebra associated to L. Then V is a holomorphic C_2-cofinite vertex operator algebra of CFT type. The full group of automorphism of a lattice vertex operator algebra is known; it is given by

$$\mathrm{Aut}(V) = K \cdot O(\hat{L})$$

where $K := \langle \{e^{v(0)} | v \in V_1\} \rangle$ is the inner automorphism group of V, $O(\hat{L})$ is the group of automorphisms of V induced by the group $O(L)$ of isometries of L, and the notation $S \cdot T$ means the product of group subsets which is given by $\{st : s \in S, t \in T\}$. Let G be a subgroup of $K_0 \cdot O(\hat{L})$ where $K_0 := \langle \{e^{(2\pi i)h(0)} | h \in L \otimes_{\mathbb{Z}} \mathbb{Q}\} \rangle \leq K$. Proposition 4.2 of [Möl18] says that the pair (V, G) satisfies the positivity condition on twisted sectors.

From these examples we have the following corollary to Theorem 1.5.4.

Corollary 5.5.1 (Corollary 1.5.5)**.** *Let (V, G) be either of the following:*

- *$V = W^{\otimes k}$ ($k \in \mathbb{Z}_{\geq 0}$) where W is a holomorphic C_2-cofinite vertex operator algebra of CFT type, and $G \leq S_k$;*
- *V is a vertex algebra associated to an even, unimodular and positive-definite lattice, and $G \leq K_0 \cdot O(\hat{L})$.*

Then the G-module V has dominant identity trace. Consequently V is asymptotically G-regular.

Appendix A

Appendices for Chapter 3

A.1 Primes that have the rationality property

In the following table we use the notation $N{+}e, f, \ldots$ for the modular curve $X_0(N){+}e, f, \ldots$. Moreover we use the notation $N+$ when all the exact divisors of N are included, and the notation $N-$ when no exact divisors are included. The following table lists the primes that have the rationality property for the genus zero modular curves of the form $N{+}e, f, \ldots$. There are no primes that have the rationality property for the genus zero modular curves of the form $N{+}e, f, \ldots$ not listed in this table.

X	primes that have the rationality property for X
2+	3, 5, 7, 11, 13, 17, 19, 23, 31, 47
2−	3, 5, 7, 11, 23
3+	2, 5, 7, 11, 13, 17, 23, 29
3−	2, 5, 11
4+	3, 5, 7, 11, 23
4−	3, 7
5+	2, 3, 7, 11, 19
5−	2

X	primes that have the rationality property for X
6+	5, 7, 11, 13
6+6	5, 11
6+3	5
7+	2, 3, 5, 17
7−	3
8+	3, 7
9+	2, 5
9−	2
10+	3, 7, 11
10+5	3
11+	2, 3, 5
12+	5
13+	2, 3
14+	3, 5
14+14	3
15+	2, 7
15+15	2
17+	2, 3, 7
19+	2, 5
20+	3
21+	2, 5
22+	3, 5
23+	2, 3
25+	2
26+	3
27+	2
29+	3
31+	2
33+	2
35+	2, 3
47+	2
55+	2

A.2 Principal moduli for $\Gamma_0(N)$

Let $\eta(\tau)$ be the Dedekind eta function. In this table we employ the following notation for an eta-product:

$$n_1^{d_1} \cdots n_l^{d_l} := \eta(n_1\tau)^{d_1} \cdots \eta(n_l\tau)^{d_l}.$$

The following table shows the principal moduli T_N, up to an additive constant, for all $\Gamma_0(N)$ of genus zero.

N	T_N
2	$1^{24}/2^{24}$
3	$1^{12}/3^{12}$
4	$1^{8}/4^{8}$
5	$1^{6}/5^{6}$
6	$2^{8}3^{4}/1^{4}6^{8}$
7	$1^{4}/7^{4}$
8	$1^{4}4^{2}/2^{2}8^{4}$

N	T_N
9	$1^{3}/9^{3}$
10	$2^{4}5^{2}/1^{2}10^{4}$
12	$3^{3}4^{1}/1^{1}12^{3}$
13	$1^{2}/13^{2}$
16	$1^{2}8^{1}/2^{1}16^{2}$
18	$2^{2}9^{1}/1^{1}18^{2}$
25	$1/25$

A.3 Higher level analogues of Δ.

We again use the following notation for an eta-product:

$$n_1^{d_1} \cdots n_l^{d_l} := \eta(n_1\tau)^{d_1} \cdots \eta(n_l\tau)^{d_l}.$$

The following table lists the modular (non-cuspidal) forms $\Delta^{(N)} \in M_{12}(\Gamma_0(N))$ that vanish only at the infinite cusp of $\Gamma_0(N)$ and nowhere else.

N	$\Delta^{(N)}$
2	$2^{48}/1^{24}$
3	$3^{36}/1^{12}$
4	$4^{48}/2^{24}$
5	$5^{30}/1^{6}$
6	$1^{12}6^{72}/2^{24}3^{36}$
7	$7^{28}/1^{4}$
8	$8^{48}/4^{24}$

N	$\Delta^{(N)}$
9	$9^{36}/3^{12}$
10	$1^{6}10^{60}/2^{12}5^{30}$
12	$2^{12}12^{72}/4^{24}6^{36}$
13	$13^{26}/1^{2}$
16	$16^{48}/8^{24}$
18	$3^{12}18^{72}/6^{24}9^{36}$
25	$25^{30}/5^{6}$

A.4 The polynomials $g_p^{(N)}$

In the following table we list the polynomials $g_p^{(N)}$ whose roots are the T_N-invariants of the characteristic p supersingular elliptic curves with level N structure, such that the j-invariant is 0 or 1728.

N	$g_p^{(N)}$ where $p - 1 = 12m + 4\delta + 6\epsilon$
2	$(x+256)^\delta(x-512)^\epsilon(x+64)^\epsilon$
3	$(x+27)^\delta(x+243)^\delta(x^2-486x-19683)^\epsilon$
4	$(x^2+256x+4096)^\delta(x+32)^\epsilon(x^2-512x-8192)^\epsilon$
5	$(x^2+250x+3125)^\delta(x^2-500x-15625)^\epsilon(x^2+22x+125)^\epsilon$
6	$(x+3)^\delta(x^3+225x^2-405x+243)^\delta(x^2+18x-27)^\epsilon(x^4-540x^3+270x^2-972x+729)^\epsilon$
7	$(x^2+13x+49)^\delta(x^2+245x+2401)^\delta(x^4-490x^3-21609x^2-235298x-823543)^\epsilon$
8	$(x^4+256x^3+5120x^2+32768x+65536)^\delta(x^2+32x+128)^\epsilon(x^4-512x^3-10240x^2-65536x-131072)^\epsilon$
9	$(x+9)^\delta(x^3+243x^2+2187x+6561)^\delta(x^6-486x^5-24057x^4-367416x^3-2657205x^2-9565938x-14348907)^\epsilon$

N	$g_p^{(N)}$ where $p-1=12m+4\delta+6\epsilon$
10	$(x^6+230x^5+275x^4-1500x^3+4375x^2-6250x+3125)^\delta(x^2+2x+5)^\epsilon(x^2+20x-25)^\epsilon$ $(x^4-540x^3+1350x^2-1500x+625)^\epsilon(x^2-2x+5)^\epsilon$
12	$(x^2+4x-8)^\delta(x^6+228x^5-408x^4-128x^3-192x^2+768x-512)^\delta$ $(x^4+20x^3-48x^2+32x-32)^\epsilon(x^8-536x^7-272x^6+3328x^5+6400x^4-20480x^3+4096x^2+16384x-8192)^\epsilon$
13	$(x^2+5x+13)^\delta(x^4+247x^3+3380x^2+15379x+28561)^\delta$ $(x^6-494x^5-20618x^4-237276x^3-1313806x^2-3712930x-4826809)^\epsilon(x^2+6x+13)^\epsilon$
16	$(x^8+256x^7+5632x^6+53248x^5+282624x^4+917504x^3+1835008x^2+2097152x+1048576)^\delta(x^4+32x^3+192x^2+512x+512)^\epsilon$ $(x^8-512x^7-11264x^6-106496x^5-565248x^4-1835008x^3-3670016x^2-4194304x-2097152)^\epsilon$
18	$(x^3+3x^2-9x+9)^\delta(x^9+225x^8-1080x^7+3348x^6-8262x^5+16038x^4-23328x^3+26244x^2-19683x+6561)^\delta$ $(x^6+18x^5-81x^4+216x^3-405x^2+486x-243)^\epsilon$ $(x^{12}-540x^{11}+1890x^{10}-4212x^9+13527x^8-48600x^7+129276x^6-262440x^5$ $+413343x^4-498636x^3+433026x^2-236196x+59049)^\epsilon$
25	$(x^{10}+250x^9+4375x^8+35000x^7+178125x^6+631250x^5+1640625x^4+3125000x^3+4296875x^2+3906250x+1953125)^\delta$ $(x^4+10x^3+45x^2+100x+125)^\epsilon(x^2+2x+5)^\epsilon$ $(x^{10}-500x^9-18125x^8-163750x^7-871875x^6-3137500x^5-8203125x^4-15625000x^3-21484375x^2-19531250x-9765625)^\epsilon$

A.5 Modular relations

The following table gives j as rational functions of T_N.

N	modular relation between j and $T = T_N$
2	$j = \dfrac{(T+256)^3}{T^2}$
3	$j = \dfrac{(T+27)(T+243)^3}{T^3}$
4	$j = \dfrac{(T^2+256T+4096)^3}{(T+16)T^4}$
5	$j = \dfrac{(T^2+250T+3125)^3}{T^5}$
6	$j = \dfrac{(T+3)^3(T^3+225T^2-405T+243)^3}{(T-1)^2(T-9)^6T^3}$
7	$j = \dfrac{(T^2+13T+49)(T^2+245T+2401)^3}{T^7}$
8	$j = \dfrac{(T^4+256T^3+5120T^2+32768T+65536)^3}{(T+4)(T+8)^2T^8}$
9	$j = \dfrac{(T+9)^3(T^3+243T^2+2187T+6561)^3}{(T^2+9T+27)T^9}$

N	modular relation between j and $T = T_N$
10	$j = \dfrac{(T^6 + 230T^5 + 275T^4 - 1500T^3 + 4375T^2 - 6250T + 3125)^3}{(T-1)^2(T-5)^{10}T^5}$
12	$j = \dfrac{(T^2 + 4T - 8)^3(T^6 + 228T^5 - 408T^4 - 128T^3 - 192T^2 + 768T - 512)^3}{(T-2)(T-1)^3(T+2)^3(T-4)^{12}T^4}$
13	$\dfrac{(T^2 + 5T + 13)(T^4 + 247T^3 + 3380T^2 + 15379T + 28561)^3}{T^{13}}$
16	$j = \dfrac{(T^8 + 256T^7 + 5632T^6 + 53248T^5 + 282624T^4 + 917504T^3 + 1835008T^2 + 2097152T + 1048576)^3}{(T+2)(T+4)^4(T^2+4T+8)T^{16}}$
18	$j = \dfrac{(T^3 + 3T^2 - 9T + 9)^3(T^9 + 225T^8 - 1080T^7 + 3348T^6 - 8262T^5 + 16038T^4 - 23328T^3 + 26244T^2 - 19683T + 6561)^3}{(T-1)^2T^9(T-3)^{18}(T^2-3T+3)(T^2+3)^2}$
25	$j = \dfrac{(T^{10} + 250T^9 + 4375T^8 + 35000T^7 + 178125T^6 + 631250T^5 + 1640625T^4 + 3125000T^3 + 4296875T^2 + 3906250T + 1953125)^3}{(T^4 + 5T^3 + 15T^2 + 25T + 25)T^{25}}$

Appendix B

Appendices for Chapter 4

B.1 Genus one modular curves

The following is the complete list of all modular curves of the form $X_0(N)+e, f, \ldots$ of genus one, using the notations of Appendix A.1, where N is squarefree.

11−; 14−; 14+2; 15−; 15+3; 17−; 19−; 21−; 21+7; 22+2; 22+22; 26+2; 26+13; 30+5; 30+6; 30+30; 30+2, 3, 6; 30+2, 5, 10; 30+3, 10, 30; 33+33; 34+2; 34+17; 34+34; 35+5; 37+; 38+19; 38+38; 39+3; 42+14; 42+2, 3, 6; 42+2, 7, 14; 42+3, 7, 21; 42+6, 7, 42; 43+; 51+17; 51+51; 53+; 55+11; 55+55; 57+; 58+; 61+; 62+31; 65+65; 65+; 66+2, 11, 22; 66+2, 33, 66; 66+3, 11, 33; 69+23; 70+2, 35, 70; 70+5, 7, 35; 70+5, 14, 70; 74+; 77+; 78+2, 39, 78; 78+3, 13, 39; 78+3, 26, 78; 79+; 82+; 83+; 86+; 89+; 91+; 94+47; 95+95; 101+; 102+; 105+3, 35, 105; 105+5, 7, 35; 105+15, 21, 35; 105+5, 21, 105; 110+5, 11, 55; 110+2, 55, 110; 110+10, 11, 110; 111+; 114+; 118+; 119+119; 123+; 130+; 131+; 138+; 141+; 142+; 143+; 145+; 155+; 159+; 174+; 182+; 190+; 195+; 210+; 222+; 231+; 238+

B.2 Function field generators for genus one modular curves

The following table compiles the values of A, and the relationship between B and C, for the generators $x = q^{-2} + Aq^{-1} + \cdots$ and $y = q^{-3} + Bq^{-2} + Cq^{-1} + \cdots$ of the function field of genus one modular curves. We group these modular curves into compatible collections. We use the notations of Appendix A.1.

1. Base $X = 11-$

X	A	relationship between B and C
$11-$	2	$C - 2B = 1$
$22+2$	0	$C = 1$, B is any constant
$22+22$	4	$C - 4B = 1$
$33+33$	2	$C - 2B = 4$
$55+55$	2	$C - 2B = 1$
$66+2, 33, 66$	0	$C = 4$, B is any constant
$110+2, 55, 110$	0	$C = 1$, B is any constant

2. Base $X = 14+2$

X	A	relationship between B and C
$14+2$	1	$C - B = 2$
$42+2, 3, 6$	1	$C - B = -1$
$70+2, 35, 70$	1	$C - B = 2$

3. Base $X = 15-$

X	A	relationship between B and C
$15-$	1	$C - B = 1$
$30+6$	-1	$C + B = 1$
$30+30$	3	$C - 3B = 1$

4. Base $X = 15{+}3$

X	A	relationship between B and C
$15{+}3$	1	$C - B = 1$
$30{+}2, 3, 6$	-1	$C + B = 1$
$30{+}3, 10, 30$	3	$C - 3B = 1$
$105{+}3, 35, 105$	1	$C - B = 1$

5. Base $X = 17-$

X	A	relationship between B and C
$17-$	1	$C - B = 0$
$34{+}2$	-1	$C + B = 0$
$34{+}34$	3	$C - 3B = 0$
$51{+}51$	1	$C - B = 3$
$119{+}119$	1	$C - B = 0$

6. Base $X = 19-$

X	A	relationship between B and C
$19-$	0	$C = 2$, B is any constant
$38{+}38$	2	$C - 2B = 2$
$95{+}95$	0	$C = 2$, B is any constant

7. Base $X = 21-$

X	A	relationship between B and C
$21-$	1	$C - B = -1$
$42{+}14$	-1	$C + B = -1$

8. Base $X = 21{+}7$

X	A	relationship between B and C
21+7	1	$C - B = -1$
$42{+}2, 7, 14$	-1	$C + B = -1$
$105{+}5, 7, 35$	1	$C - B = -1$

9. Base $X = 26{+}2$

X	A	relationship between B and C
26+2	1	$C - B = -1$
$78{+}2, 39, 78$	1	$C - B = 2$

10. Base $X = 26{+}13$

X	A	relationship between B and C
26+13	-1	$C + B = 3$
$78{+}3, 13, 39$	-1	$C + B = 0$

11. Base $X = 35{+}5$

X	A	relationship between B and C
35+5	0	$C = -1$, B is any constant
$70{+}5, 14, 70$	2	$C - 2B = 1$
$105{+}5, 21, 105$	0	$C = 2$, B is any constant

12. Base $X = 37{+}$

X	A	relationship between B and C
37+	2	$C - 2B = 3$
74+	0	$C = 3$, B is any constant
111+	2	$C - 2B = 0$
222+	0	$C = 0$, B is any constant

13. Base $X = 39+3$

X	A	relationship between B and C
39+3	-1	$C + B = 1$
$78+3, 26, 78$	1	$C - B = 1$

14. Base $X = 43+$

X	A	relationship between B and C
43+	2	$C - 2B = 2$
86+	0	$C = 2$

15. Base $X = 53+$

X	A	relationship between B and C
53+	1	$C - B = 3$
159+	1	$C - B = 0$

16. Base $X = 55+11$

X	A	relationship between B and C
55+11	-1	$C + B = 0$
$110+10, 11, 110$	1	$C - B = 0$

17. Base $X = 57+$

X	A	relationship between B and C
57+	2	$C - 2B = 1$
114+	0	$C = 1$, B is any constant

18. Base $X = 58+$

X	A	relationship between B and C
58+	1	$C - B = 3$
174+	1	$C - B = 0$

19. Base $X = 65+$

X	A	relationship between B and C
65+	1	$C - B = 2$
130+	-1	$C + B = 2$
195+	1	$C - B = -1$

20. Base $X = 77+$

X	A	relationship between B and C
77+	0	$C = 3$, B is any constant
231+	0	$C = 0$, B is any constant

21. Base $X = 91+$

X	A	relationship between B and C
91+	2	$C - 2B = 0$
182+	0	$C = 0$, B is any constant

Bibliography

[AB16] Victor Manuel Aricheta and Lea Beneish. Moonshine modules and a question of Griess. *arXiv preprint arXiv:1610.01689*, 2016.

[ABD04] Toshiyuki Abe, Geoffrey Buhl, and Chongying Dong. Rationality, regularity, and C_2-cofiniteness. *Transactions of the American Mathematical Society*, 356(8):3391–3402, 2004.

[AC18] Vassilis Anagiannis and Miranda Cheng. TASI lectures on moonshine. *arXiv preprint arXiv:1807.00723*, 2018.

[Apo12] Tom Apostol. *Modular functions and Dirichlet series in number theory*, volume 41. Springer Science & Business Media, 2012.

[Ari19] Victor Manuel Aricheta. Supersingular elliptic curves and moonshine. *Symmetry, Integrability and Geometry: Methods and Applications*, 15:007–17, 2019.

[BFOR17] Kathrin Bringmann, Amanda Folsom, Ken Ono, and Larry Rolen. *Harmonic Maass forms and mock modular forms: theory and applications*, volume 64. American Mathematical Soc., 2017.

[BO12] Kathrin Bringmann and Ken Ono. Coefficients of harmonic Maass forms. In *Partitions, q-series, and modular forms*, pages 23–38. Springer, 2012.

[Bor86] Richard Borcherds. Vertex algebras, Kac-Moody algebras, and the Monster. *Proceedings of the National Academy of Sciences*, 83(10):3068–3071, 1986.

[Bor92] Richard Borcherds. Monstrous moonshine and monstrous Lie superalgebras. *Inventiones mathematicae*, 109(1):405–444, 1992.

[CCN$^+$85] John Horton Conway, Robert Curtis, Simon Norton, Richard Parker, Robert Wilson, and J. G. Thackray. *Atlas of finite groups: maximal subgroups and ordinary characters for simple groups.* Clarendon Press, 1985.

[CD12] Miranda Cheng and John Duncan. On Rademacher sums, the largest Mathieu group and the holographic modularity of moonshine. *Communications in Number Theory and Physics*, 6(3):697–758, 2012.

[CD14] Miranda Cheng and John Duncan. Rademacher sums and Rademacher series. In *Conformal field theory, automorphic forms and related topics*, pages 143–182. Springer, 2014.

[CD16] Miranda Cheng and John Duncan. Optimal mock Jacobi theta functions. *arXiv preprint arXiv:1605.04480*, 2016.

[CDH14a] Miranda Cheng, John Duncan, and Jeffrey Harvey. Umbral moonshine. *Communications in Number Theory and Physics*, 8(2):101–242, 2014.

[CDH14b] Miranda Cheng, John Duncan, and Jeffrey Harvey. Umbral moonshine and the Niemeier lattices. *Research in the Mathematical Sciences*, 1(1):3, 2014.

[CDH18] Miranda Cheng, John Duncan, and Jeffrey Harvey. Weight one Jacobi forms and umbral moonshine. *Journal of Physics A: Mathematical and Theoretical*, 2018.

[Che10] Miranda Cheng. K3 surfaces, $\mathcal{N} = 4$ dyons and the Mathieu group M_{24}. *Communications in Number Theory and Physics*, 4(4):623–657, 2010.

[CM16] Scott Carnahan and Masahiko Miyamoto. Regularity of fixed-point vertex operator subalgebras. *arXiv preprint arXiv:1603.05645*, 2016.

[CN79] John Horton Conway and Simon Norton. Monstrous moonshine. *Bulletin of the London Mathematical Society*, 11(3):308–339, 1979.

[Cum04] C.J. Cummins. Congruence subgroups of groups commensurable with PSL(2,$\mathbb{Z}$) of genus 0 and 1. *Experimental Mathematics*, 13(3):361–382, 2004.

[Deu41] Max Deuring. Die typen der multiplikatorenringe elliptischer funktionenkörper. In *Abhandlungen aus dem mathematischen Seminar der Universität Hamburg*, volume 14, pages 197–272. Springer, 1941.

[Dev16] TS Developers. Sagemath, 2016.

[DF11] John Duncan and Igor Frenkel. Rademacher sums, moonshine and gravity. *Communications in Number Theory and Physics*, 5(4):849–976, 2011.

[DGO15a] John Duncan, Michael Griffin, and Ken Ono. Moonshine. *Research in the Mathematical Sciences*, 2(11):57, 2015.

[DGO15b] John Duncan, Michael Griffin, and Ken Ono. Proof of the umbral moonshine conjecture. *Research in the Mathematical Sciences*, 2(1):26, 2015.

[DHVW85] Lance Dixon, Jeffrey A Harvey, Cumrun Vafa, and Edward Witten. Strings on orbifolds. *Nuclear Physics B*, 261:678–686, 1985.

[DLM98] Chongying Dong, Haisheng Li, and Geoffrey Mason. Twisted representations of vertex operator algebras. *Mathematische Annalen*, 310(3):571–600, 1998.

[DLM00] Chongying Dong, Haisheng Li, and Geoffrey Mason. Modular-invariance of trace functions in orbifold theory and generalized moonshine. *Communications in Mathematical Physics*, 214(1):1–56, 2000.

[DLN15] Chongying Dong, Xingjun Lin, and Siu-Hung Ng. Congruence property in conformal field theory. *Algebra & Number Theory*, 9(9):2121–2166, 2015.

[DMC15] John Duncan and Sander Mack-Crane. The moonshine module for Conway's group. In *Forum of Mathematics, Sigma*, volume 3. Cambridge University Press, 2015.

[Don93] Chongying Dong. Vertex algebras associated with even lattices. *J. Algebra*, 161(1):245–265, 1993.

[Don94] Chongying Dong. Representations of the moonshine module vertex operator algebra. *Contemporary Mathematics*, 175:27–27, 1994.

[DR73] Pierre Deligne and Michael Rapoport. Les schémas de modules de courbes elliptiques. In *Modular functions of one variable II*, pages 143–316. Springer, 1973.

[DR18] Chongying Dong and Li Ren. Congruence property in orbifold theory. *Proceedings of the American Mathematical Society*, 146(2):497–506, 2018.

[DRX17] Chongying Dong, Li Ren, and Feng Xu. On orbifold theory. *Advances in Mathematics*, 321:1–30, 2017.

[Duk14] W Duke. Almost a century of answering the question: what is a mock theta function? *Notices of the AMS*, 61(11), 2014.

[Dun07] John Duncan. Super-moonshine for Conway's largest sporadic group. *Duke Mathematical Journal*, 139(2):255–315, 2007.

[EH11] Tohru Eguchi and Kazuhiro Hikami. Note on twisted elliptic genus of K3 surface. *Physics Letters B*, 694(4-5):446–455, 2011.

[EOT11] Tohru Eguchi, Hirosi Ooguri, and Yuji Tachikawa. Notes on the K3 surface and the Mathieu group M_{24}. *Experimental Mathematics*, 20(1):91–96, 2011.

[FBZ04] Edward Frenkel and David Ben-Zvi. *Vertex algebras and algebraic curves.* Number 88. American Mathematical Soc., 2004.

[Fer93] Charles Ferenbaugh. The genus-zero problem for $n|h$-type groups. *Duke Mathematical Journal*, 72(1):31–63, 1993.

[FH99] Masahiro Furumoto and Yuji Hasegawa. Hyperelliptic quotients of modular curves $X_0(N)$. *Tokyo Journal of Mathematics*, 22(1):105–125, 1999.

[FHL93] Igor Frenkel, Yi-Zhi Huang, and James Lepowsky. *On axiomatic approaches to vertex operator algebras and modules*, volume 494. American Mathematical Soc., 1993.

[FLM84] Igor Frenkel, James Lepowsky, and Arne Meurman. A natural representation of the Fischer-Griess monster with the modular function J as character. *Proceedings of the National Academy of Sciences*, 81(10):3256–3260, 1984.

[FLM89] Igor Frenkel, James Lepowsky, and Arne Meurman. *Vertex operator algebras and the Monster*, volume 134. Academic press, 1989.

[Fol17] Amanda Folsom. Perspectives on mock modular forms. *Journal of Number Theory*, 176:500–540, 2017.

[Fon80] Paul Fong. Characters arising in the monster-modular connection. In *Proceedings of Symposia in Pure Mathematics*, volume 37, pages 557–559. Amer Mathematical Soc 201 Charles St, Providence, RI 02940-2213, 1980.

[FZ92] Igor Frenkel and Yongchang Zhu. Vertex operator algebras associated to representations of affine and Virasoro algebras. *Duke Mathematical Journal*, 66(1):123–168, 1992.

[G^+] PARI Group et al. Bordeaux, pari/gp, version 2.5. 0, 2011.

[Gab00] Matthias Gaberdiel. An introduction to conformal field theory. *Reports on Progress in Physics*, 63(4):607, 2000.

[Gan06] Terry Gannon. *Moonshine beyond the Monster: The bridge connecting algebra, modular forms and physics.* Cambridge University Press, 2006.

[Gan16] Terry Gannon. Much ado about Mathieu. *Advances in Mathematics*, 301:322–358, 2016.

[GAP18] The GAP Group. *GAP – Groups, Algorithms, and Programming, Version 4.9.1*, 2018.

[GHV10a] Matthias Gaberdiel, Stefan Hohenegger, and Roberto Volpato. Mathieu moonshine in the elliptic genus of K3. *Journal of High Energy Physics*, 2010(10):62, 2010.

[GHV10b] Matthias Gaberdiel, Stefan Hohenegger, and Roberto Volpato. Mathieu twining characters for K3. *Journal of High Energy Physics*, 2010(9):58, 2010.

[Gri76] Robert Griess. The structure of the "monster" simple group. In *Proceedings of the Conference on Finite Groups*, pages 113–118. Elsevier, 1976.

[Gri82] Robert Griess. The friendly giant. *Inventiones mathematicae*, 69(1):1–102, 1982.

[Has35] Helmut Hasse. Existenz separabler zyklischer unverzweigter erweiterungskörper vom primzahlgrade p über elliptischen funktionenkörpern der charakteristik p. *Journal für die reine und angewandte Mathematik*, 172:77–85, 1935.

[Has97] Yuji Hasegawa. Hyperelliptic modular curves $X_0^*(N)$. *Acta Arithmetica*, 81(4):369–385, 1997.

[Hum12] James Humphreys. *Introduction to Lie algebras and representation theory*, volume 9. Springer Science & Business Media, 2012.

[Igu59] Jun-ichi Igusa. Kroneckerian model of fields of elliptic modular functions. *American Journal of Mathematics*, 81(3):561–577, 1959.

[JST16] Jay Jorgenson, Lejla Smajlović, and Holger Then. Kroneckers limit formula, holomorphic modular functions, and q-expansions on certain arithmetic groups. *Experimental Mathematics*, 25(3):295–319, 2016.

[KZ98] Masanobu Kaneko and Don Zagier. Supersingular j-invariants, hypergeometric series, and Atkin's orthogonal polynomials. *AMS/IP Studies in Advanced Mathematics*, 7:97–126, 1998.

[LL12] James Lepowsky and Haisheng Li. *Introduction to vertex operator algebras and their representations*, volume 227. Springer Science & Business Media, 2012.

[Miy15] Masahiko Miyamoto. C_2-cofiniteness of cyclic-orbifold models. *Communications in Mathematical Physics*, 335(3):1279–1286, 2015.

[Miy18] Masahiko Miyamoto. C_2-cofiniteness of orbifold models for finite groups. *arXiv preprint arXiv:1812.00570*, 2018.

[Möl18] Sven Möller. Orbifold vertex operator algebras and the positivity condition. *arXiv preprint arXiv:1803.03702*, 2018.

[Nak18] Tomoaki Nakaya. The number of linear factors of supersingular polynomials and sporadic simple groups. *arXiv preprint arXiv:1809.02363*, 2018.

[Ogg74] Andrew Ogg. Automorphismes de courbes modulaires. *Seminaire Delange-Pisot, Poitou*, 7, 1974.

[Ogg75] Andrew Ogg. On the reduction modulo p of $X_0(pM)$. In *US-Japan Seminar on Applications of Automorphic Forms to Number Theory. Ann Arbor*, 1975.

[Ono04] Ken Ono. *The web of modularity: arithmetic of the coefficients of modular forms and q-series.* Number 102. American Mathematical Soc., 2004.

[Rad38] Hans Rademacher. The Fourier coefficients of the modular invariant $J(\tau)$. *American Journal of Mathematics*, 60(2):501–512, 1938.

[Sak11] Yuichi Sakai. The Atkin orthogonal polynomials for the low-level Fricke groups and their application. *International Journal of Number Theory*, 7(06):1637–1661, 2011.

[Sak15] Yuichi Sakai. On modular solutions of fractional weights for the Kaneko–Zagier equation for $\Gamma_0^*(2)$ and $\Gamma_0^*(3)$. *The Ramanujan Journal*, 37(3):461–467, 2015.

[Shi71] Goro Shimura. *Introduction to the arithmetic theory of automorphic functions*, volume 1. Princeton university press, 1971.

[Sil09] Joseph Silverman. *The arithmetic of elliptic curves*, volume 106. Springer Science & Business Media, 2009.

[Sin] Interview with Richard Borcherds. `https://simonsingh.net/media/articles/maths-and-science/interview-with-richard-borcherds/`. Accessed: 2019-03-26.

[Sol01] Ronald Solomon. A brief history of the classification of the finite simple groups. *Bulletin of the American Mathematical Society*, 38(3):315–352, 2001.

[Stu87] Jacob Sturm. On the congruence of modular forms. In *Number theory*, pages 275–280. Springer, 1987.

[Tho79] John Thompson. Some numerology between the Fischer-Griess monster and the elliptic modular function. *Bulletin of the London Mathematical Society*, 11(3):352–353, 1979.

[Tsu07] Hiroyuki Tsutsumi. The Atkin orthogonal polynomials for congruence subgroups of low levels. *The Ramanujan Journal*, 14(2):223–247, 2007.

[Zag07] Don Zagier. Ramanujan's mock theta functions and their applications. *Séminaire BOUR*, 2007.

[Zhu96] Yongchang Zhu. Modular invariance of characters of vertex operator algebras. *Journal of the American Mathematical Society*, 9(1):237–302, 1996.

[Zwe08] Sander Zwegers. Mock theta functions. *arXiv preprint arXiv:0807.4834*, 2008.