Some applications of singular moduli and complex multiplication

Kumulierte Habilitationsschrift

zur
Erlangung der Lehrbefähigung und Lehrbefugnis
der Mathematisch-Naturwissenschaftlichen Fakultät
der Universität zu Köln

vorgelegt von

Dr. rer. nat. Michael Helmut Mertens
aus
Viersen

Köln, September 2019

Für meine Eltern.

Kurzzusammenfassung

Die vorliegende kumulierte Habilitationsschrift fasst drei Originalarbeiten des Autors, die sich alle mit verschiedenen Aspekten und Anwendungen singulärer Werte von Modulfunktionen und komplexer Multiplikation befassen. Diese Arbeiten stehen einerseits im Zusammenhang mit der algebraischen Formel von Bruinier und Ono für die Partitionsfunktion, sowie Moonshine für die sporadisch einfachen Gruppen von Thompson bzw. O'Nan. Im Zusammenhang mit O'Nan-Moonshine führt der Zusammenhang mit Spuren singulärer Werte auf Resultate über die Arithmetik gewisser elliptischer Kurven.

Abstract

The present cumulative Habilitationsschrift combines three original works of the author, which all deal with various aspects and applications of singular moduli of modular functions and complex multiplication. These works are connected to the algebraic formula for the partition function due to Bruinier and Ono on the one hand and Moonshine for the sporadic groups of Thompson and O'Nan respectively on the other hand. In the context of O'Nan Moonshine, the connection to traces of singular moduli leads to results on the arithmetic of certain elliptic curves.

Contents

Chapter 1

Introduction

Complex multiplication and singular moduli are one of the most important subjects in the arithmetic theory of modular forms, originating from the study of elliptic functions of Gauß, Abel, Jacobi, and Eisenstein (among many others). Hermite [71] was first to observe and explain the fact that the number

$$e^{\pi\sqrt{163}} = 262537412640768743.99999999999250072597..., \tag{1.1}$$

even though (now) known to be transcendental by the Theorem of Gel'fond-Schneider [60, 95], is surprisingly close to an integer, using the theory of complex multiplication and singular moduli. Another historically famous appearance of this topic comes from the first letter the famous Indian mathematician Ramanujan wrote to Hardy, where Ramanujan gives the following formula,

$$\cfrac{1}{1+\cfrac{e^{-2\pi}}{1+\cfrac{e^{-4\pi}}{1+\dots}}} = e^{2\pi/5}\left(\sqrt{\frac{5+\sqrt{5}}{2}} - \frac{1+\sqrt{5}}{2}\right). \tag{1.2}$$

Hardy commented on this and similar formulas in Ramanujan's letter as follows [67, p. 9]:

> *"These formulas defeated me completely. I had never seen anything in the least like them before. A single look at them is enough to show that they could only be written down by a mathematician of the highest class. They must be true because, if they were not true, no one would have had the imagination to invent them."*

Both these observations are explained through the theory of *complex multiplication*, more concretely by the fact that the value of a modular function (with algebraic

Fourier coefficients) at a so-called CM point, i.e. a point in the upper half-plane $\mathfrak{H}$ belonging to an imaginary quadratic number field, is an algebraic number. Such values are called *singular moduli*. In Chapter 2, we give a brief account of some important aspects of this theory.

Singular moduli and especially their traces have been a very active field of study in the past and they are what connects the works comprising the main contents of this thesis. Before giving a summary of these works, we recall some standard notation which will be used throughout.

Notation

Throughout, let $\mathfrak{H}$ (in Appendix A, the symbol $\mathbb{H}$ is used instead) denote the complex upper half-plane

$$\mathfrak{H} := \{\tau \in \mathbb{C} \, : \, \mathrm{Im}(\tau) > 0\}.$$

The letter τ always denotes a variable in $\mathfrak{H}$, its real and imaginary parts are usually denoted by u and v.

The group $\mathrm{SL}_2(\mathbb{R})$ acts on $\mathfrak{H}$ from the left via *Möbius transformations*

$$(\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right), \tau) \mapsto \gamma.\tau := \frac{a\tau + b}{c\tau + d}, \tag{1.3}$$

inducing, together with a weight $k \in \mathbb{Z}$, a right action on the vector space of functions $f : \mathfrak{H} \to \mathbb{C}$ via the *Petersson slash operator*,

$$(f|_k\gamma)(\tau) := (c\tau + d)^{-k} f(\gamma.\tau), \qquad \gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{R}), \quad \tau \in \mathfrak{H}. \tag{1.4}$$

This action can be extended to half-integral weights by passing from the group $\mathrm{SL}_2(\mathbb{R})$ to the *metaplectic group* $\mathrm{Mp}_2(\mathbb{R})$, a double cover of $\mathrm{SL}_2(\mathbb{R})$.

A holomorphic function $f : \mathfrak{H} \to \mathbb{C}$ which is invariant under the weight k slash action of a discrete subgroup $\Gamma \leq \mathrm{SL}_2(\mathbb{R})$ of finite covolume and, in case Γ is not cocompact, moderate growth towards the *cusps* of Γ, is called a *modular form* of weight k for Γ. The space of such functions is denoted by $M_k(\Gamma)$.

In this thesis, all occurring groups Γ will be congruence subgroups of $\mathrm{SL}_2(\mathbb{Z})$ (or occasionally normalizers of such groups in $\mathrm{SL}_2(\mathbb{R})$). More precisely they will almost always be of the form

$$\Gamma_0(N) := \{\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z}) \, : \, c \equiv 0 \pmod{N}\} \tag{1.5}$$

for some positive integer N.

Occasionally, one relaxes the requirement of invariance under the slash action by allowing a *multiplier system* ψ of weight k, i.e. one has

$$(f|_k\gamma)(\tau) = \psi(\gamma)f(\tau), \qquad \tau \in \mathfrak{H}$$

for a function $\psi : \Gamma \to \mathbb{C}^*$ satisfying $|\psi(\gamma)| = 1$ and the cocycle condition

$$\psi(\gamma_3)(c_3\tau + d_3)^k = \psi(\gamma_1)(c_1(\gamma_2.\tau) + d_1)^k\psi(\gamma_2)(c_2\tau + d_2)^k, \tag{1.6}$$

where $\gamma_j = \left(\begin{smallmatrix} * & * \\ c_j & d_j \end{smallmatrix}\right) \in \Gamma$ and $\gamma_3 = \gamma_1\gamma_2$. Note that by fixing a branch of the logarithm and setting $z^k := e^{k\log z}$ for $k \in \mathbb{C}$, the above can be used to define multiplier systems, and therefore modular forms, of arbitrary real or even complex weights, while for $k \in \mathbb{Z}$, the condition in (1.6) reduces to the requirement that ψ be a homomorphism of groups.

The space of modular forms of weight k with multiplier system ψ for Γ is denoted by $M_k(\Gamma, \psi)$. If a modular form $f \in M_k(\Gamma, \psi)$ vanishes towards all the cusps (if there are any), we call it a *cusp form* and the subspace of cusp forms in $M_k(\Gamma, \psi)$ is denoted by $S_k(\Gamma, \psi)$. If instead one relaxes the growth condition at the boundary to allow poles at the cusps, one obtains the space of *weakly holomorphic modular forms*, denoted by $M_k^!(\Gamma, \psi)$. If ψ is trivial, we suppress it from the notation.

Suppose the weight k is half-integral, $\Gamma = \Gamma_0(4N)$ for some N, and the multiplier system ψ is compatible with the "trivial" multiplier system ψ_0 of weight k, i.e. the one corresponding to the embedding of $\Gamma_0(4)$ into the metaplectic group due to Shimura [97]. Explicitly, this multiplier system is given by

$$\psi_0\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}\right) = \left(\frac{c}{d}\right)\left(\frac{-4}{d}\right)^{-k}, \qquad c \equiv 0 \pmod 4,$$

where the corresponding branch of the square root is chosen which is positive for positive real arguments. Then there is an important subspace of the space $M_k^!(\Gamma, \psi)$, the *Kohnen plus space*, defined by

$$M_k^{!,+}(\Gamma, \psi) := \left\{ f(\tau) = \sum_{n \gg -\infty} a_f(n)q^n \ : \ a_f(n) = 0 \,\text{for}\, n \not\equiv 0, (-1)^{k-1/2} \pmod 4 \right\}. \tag{1.7}$$

The spaces $M_k^+(\Gamma, \psi)$ and $S_k^+(\Gamma, \psi)$ are defined analogously and we suppress the multiplier system from the notation if it is the aformentioned "trivial" one.

Various further relaxations of the concept of modular forms exist and are studied. One such relaxation which will occur frequently in this work is that of *harmonic (weak) Maaß forms*, which are invariant under the slash operator (possibly with a multiplier system) and grow at most exponentially towards the cusps of Γ, but instead of being holomorphic on $\mathfrak{H}$, they are merely required to be annihilated by the weight k *hyperbolic Laplacian*,

$$\Delta_k := -v^2 \left(\frac{\partial^2}{\partial u^2} + \frac{\partial^2}{\partial v^2} \right) + ikv \left(\frac{\partial}{\partial u} + i\frac{\partial}{\partial v} \right). \tag{1.8}$$

The space of these functions is denoted by $H_k(\Gamma, \psi)$, so that we have the inclusion of spaces

$$S_k(\Gamma, \psi) \subseteq M_k(\Gamma, \psi) \subseteq M_k^!(\Gamma, \psi) \subseteq H_k(\Gamma, \psi).$$

It is not hard to see that a harmonic Maaß form f of weight k for $\Gamma = \Gamma_0(N)$, say, naturally splits into a holomorphic part f^+ and a non-holomorphic part f^-. The holomorphic part of a harmonic Maaß form is called a *mock modular form*. The image of f under the so-called ξ-*operator*, a variation of the *Maaß lowering operator*, is called the *shadow* of the mock modular form f^+.

We now give a summary and some background of the results in the relevant papers [82, 62, 45]. The published versions (or in the case of [45] the version accepted for publication) are included in the appendix.

1.1 On class invariants for non-holomorphic modular functions and a question of Bruinier and Ono

Since the days of Euler, *partitions* have been an object of interest to number theorists, being one of the most fundamental concepts in Combinatorics. A partition of a positive integer n is a non-increasing sequence of positive integers summing to n. The number of partitions of n is commonly denoted $p(n)$, where one sets $p(0) := 1$ for convenience. For example, the partitions of 5 are given by

$$(5),\ (4,1),\ (3,2),\ (3,1,1),\ (2,2,1),\ (2,1,1,1),\ (1,1,1,1,1),$$

so that $p(5) = 7$. Despite its very simple definition, a closed formula to compute $p(n)$ has long been searched for. Euler [49] was able to give the following recursive formula for $p(n)$.

Theorem 1.1.1 (Euler, 1775). *For any integer $n > 0$ and $B := \lceil (1+\sqrt{24n+1})/6 \rceil$ one has the identity*

$$p(n) = \sum_{k=1}^{B} (-1)^{k+1} \left[p\left(n - \frac{1}{2}k(3k-1)\right) + p\left(n - \frac{1}{2}k(3k+1)\right)\right],$$

where we use the convention $p(n) = 0$ for $n < 0$.

This formula is indeed fairly efficient if n is not too large and was famously used by MacMahon around 1916 to compute $p(n)$ for all $n \leq 200$, see [68, Table IV]. It is a direct corollary of the product representation of the generating function of the partition function,

$$\sum_{n=0}^{\infty} p(n) q^n = \prod_{n=1}^{\infty} (1-q^n)^{-1}, \qquad |q| < 1, \tag{1.9}$$

and Euler's *Pentagonal Number Theorem*,

$$\prod_{n=1}^{\infty} (1-q^n) = \sum_{m \in \mathbb{Z}} (-1)^m q^{\frac{m(3m-1)}{2}}, \qquad |q| < 1. \tag{1.10}$$

In 1918, Hardy and Ramanujan [68] found a complete asymptotic expansion for $p(n)$, pioneering a now vital tool in Analytic Number Theory, the *Circle Method.* A simplified version of their result is given as follows.

Theorem 1.1.2 (Hardy-Ramanujan, 1918). *We have the asymptotic equality*

$$p(n) \sim \frac{1}{4n\sqrt{3}} e^{\pi \sqrt{2n/3}}, \qquad n \to \infty.$$

Some 20 years later, Rademacher [90] was able to refine the method of Hardy and Ramanujan to obtain a convergent infinite series representation for $p(n)$. A short proof has recently been given by Pribitkin and Williams [89].

Theorem 1.1.3 (Rademacher, 1937). *For any integer $n \geq 1$ we have that*

$$p(n) = \frac{1}{\pi\sqrt{2}} \sum_{k=1}^{\infty} A_k(n) \sqrt{k} \frac{\mathrm{d}}{\mathrm{d}n} \left(\frac{\sinh\left(\frac{\pi}{k}\sqrt{\frac{2}{3}(n-\frac{1}{24})}\right)}{\sqrt{n-1/24}} \right),$$

where

$$A_k(n) = \sum_{h\,(k)^*} \exp\left(\pi i s(h,k) + 2\pi i h/k\right),$$

the notation $h\,(k)^*$ signifying that the sum runs over all h modulo k coprime to k, and

$$s(h,k) = \frac{1}{4k}\sum_{\mu=1}^{k-1}\cot(\pi\mu/k)\cot(\pi h\mu/k)$$

denotes the classical Dedekind sum[1].

Rademacher's formula is essentially what is used in many modern computer algebra systems such as Pari/Gp, Sage, or Magma [65, 104, 12] to compute $p(n)$. However, the formula is an infinite series which needs to be truncated somewhere for practical computations. This may be not quite satisfactory as $p(n)$ can intrisically be obtained from a finite process.

In 2013, Bruinier and Ono [23] found a representation of $p(n)$ as a finite sum of algebraic numbers, more precisely as the trace of the singular moduli of a specific non-holomorphic modular function. Their result is a consequence of the general properties of a certain *theta lift* they introduce [23, Equation (3.1)] which maps *harmonic Maaß forms* of weight -2 for $\Gamma_0(N)$ to vector-valued harmonic Maaß forms of weight $-1/2$ with respect to the Weil representation associated to the lattice

$$L = \left\{ \begin{pmatrix} b & a/N \\ c & -b \end{pmatrix} \;:\; a,b,c \in \mathbb{Z} \right\}$$

in the quadratic space of rational 2×2-matrices with trace 0 endowed with the quadratic form $X \mapsto N \det X$. A similar theta lift had been studied previously by Bruinier and Funke [21, 55] and it has been extended to general weights and its properties have been studied further by Alfes [1].

In order to state the formula of Bruinier and Ono, we first recall the definition of the *Eisenstein series* of weight $k \in 2\mathbb{Z}_{>0}$ for the full modular group $\mathrm{SL}_2(\mathbb{Z})$,

$$E_k(\tau) = 1 - \frac{2k}{B_k}\sum_{n=1}^{\infty}\sigma_{k-1}(n)q^n, \qquad \tau \in \mathfrak{H},\ q := e^{2\pi i\tau}. \tag{1.11}$$

For $k \geq 4$, these are modular forms for $\mathrm{SL}_2(\mathbb{Z})$, while E_2 is a so-called *quasimodular form*. In particular, it is not modular, but the non-holomorphic function

$$E_2^*(\tau) := E_2(\tau) - \frac{3}{\pi v}$$

with $v = \mathrm{Im}(\tau)$ transforms like a modular form of weight 2. Also recall the *Dedekind eta function*

$$\eta(\tau) := q^{1/24}\prod_{n=1}^{\infty}(1-q^n), \tag{1.12}$$

[1] This is not the standard defnition of the Dedekind sum, but usually an identity that has to be proven, see e.g. [92, Equation (26)]

which is a cusp form of weight 1/2 for $\mathrm{SL}_2(\mathbb{Z})$ with respect to a certain multiplier system involving the Dedekind sums that appear in Theorem 1.1.3. The 24th power of this multiplier system is trivial, so that

$$\Delta(\tau) := \eta(\tau)^{24} = \frac{E_4(\tau)^3 - E_6(\tau)^2}{1728}$$

is a cusp form of weight 12 for $\mathrm{SL}_2(\mathbb{Z})$.

Using these functions, we define the weakly holomorphic modular form

$$F(\tau) := \frac{E_2(\tau) - 2E_2(2\tau) - 3E_2(3\tau) + 6E_2(6\tau)}{2\eta(\tau)^2\eta(2\tau)^2\eta(3\tau)^2\eta(6\tau)^2} \in M^!_{-2}(\Gamma_0(6)) \tag{1.13}$$

and apply the *Maaß raising operator* to it. This operator is defined by

$$R_k := \frac{1}{2\pi i}\frac{\partial}{\partial\tau} - \frac{k}{4\pi v} \tag{1.14}$$

and maps modular forms of weight k to modular forms of weight $k+2$ (without preserving holomorphicity of course). Thus we obtain a non-holomorphic modular function

$$P(\tau) := R_{-2}F(\tau). \tag{1.15}$$

The formula of Bruinier and Ono is then given as follows [23, Theorem 1.1].

Theorem 1.1.4 (Bruinier-Ono, 2013). *For $n \in \mathbb{N}$ let $\delta := 1 - 24n$ and $\overline{\mathcal{Q}}_\delta$ denote a set of representatitives of positive definite quadratic forms $Q(X,Y) = aX^2 + bXY + cY^2$ with $a, b, c \in \mathbb{Z}$, $a \equiv 0 \pmod 6$, and $b \equiv 1 \pmod{12}$ of discriminant δ, modulo the action of $\Gamma_0(6)$. Then we have*

$$p(n) = \frac{1}{24n-1}\sum_{Q\in\overline{\mathcal{Q}}_\delta} P(\tau_Q),$$

where for any positive definite binary quadratic form Q we write τ_Q for the unique point in $\mathfrak{H}$ satisfying $Q(\tau_Q, 1) = 0$.

Thus $p(n)$ can be written as a trace of singular moduli (see Section 2.4). It can be shown [79] that $(24n-1)P(\tau_Q)$ is an algebraic integer for all $Q \in \overline{\mathcal{Q}}_\delta$. The formula in Theorem 1.1.4 has also essentially been derived from Rademacher's formula in Theorem 1.1.3 by Bringmann and Ono [16] (the function P there is given as a Poincaré series, so less explicitly than in [23]). Folsom and Masri [50] used the formula to derive a new asymptotic and error term for the partition function. A derivation of the Hardy-Ramanujan formula in Theorem 1.1.2 from Theorem 1.1.4 has been given by Dewar and Murty [36].

Bruinier and Ono also show that the polynomial

$$H_\delta(X) = \prod_{Q\in\overline{\mathcal{Q}}_\delta} (X - P(\tau_Q)), \tag{1.16}$$

whose roots are the singular values $P(\tau_Q)$ is defined over $\mathbb{Q}$. It is however not in general irreducible over $\mathbb{Q}$ [24, Lemma 3.7]. In loc. cit., Bruinier, Ono, and Sutherland find an efficient algorithm using CM elliptic curves and what is called *isogeny volcanos* to compute H_δ and therefore $p(n)$, as well as the related polynomial

$$\widehat{H}_\delta(X) = \prod_{Q\in\overline{\mathcal{P}}_\delta} (X - P(\tau_Q)) \in \mathbb{Q}[X], \tag{1.17}$$

where $\overline{\mathcal{P}}_\delta$ denotes the set of *primitive* forms in $\mathcal{Q}_\delta$, i.e. those whose coefficients are relatively prime. We note here that this construction is analogous to the class polynomial considered in Equation (2.4). They use their algorithm to compute $\widehat{H}_\delta$ for many values of δ and always find that it is irreducible over $\mathbb{Q}$, leading them to ask (see [23, Section 5]) if this is always the case. In [82], reproduced in Appendix A, Rolen and the author show that this is indeed true.

Theorem 1.1.5 (M.-Rolen, 2015)**.** *The polynomial $\widehat{H}_\delta$ is irreducible over $\mathbb{Q}$. Moreover we have that*

$$\Omega_t \cong K[X]/\widehat{H}_\delta(X),$$

where we write $\delta = t^2 d$ for a fundamental discriminant $d < 0$ and $K := \mathbb{Q}(\sqrt{d})$, is the ring class field of the order of conductor t in K.

The proof of this has two main parts: First we show that $\widehat{H}_\delta$ is the power of an irreducible polynomial, i.e. the sets

$$\{P(\tau_Q) \,:\, Q \in \overline{\mathcal{P}}_\delta\} \quad \text{and} \quad \{P(\tau_{Q_0})^\sigma \,:\, \sigma \in \mathrm{Gal}(\Omega_t/K)\}$$

are equal for all $Q_0 \in \overline{\mathcal{P}}_\delta$ (see [82, Proposition 3.2]). This follows essentially from a convenient formulation of *Shimura reciprocity* due to Schertz [94] in combination with a formula of Masser [80, Appendix I]. The second part of the proof relies on explicitly bounding the value $P(\gamma\tau)$ for all γ in a fixed set of representatives of $\mathrm{SL}_2(\mathbb{Z})/\Gamma_0(6)$ and τ in the standard fundamental domain for $\mathrm{SL}_2(\mathbb{Z})$ ([82, Lemma 3.3]). This explicit (but actually rather crude) bound is enough to show that all the values $P(\tau_Q)$ for $Q \in \overline{\mathcal{P}}_\delta$ are distinct for all $n \geq 54$ (i.e. $\delta \leq 1 - 24 \cdot 54 = -1295$). Using the data computed by Sutherland[2], it can be verified directly by computer that $\widehat{H}_\delta$ is irreducible for the remaining n, completing the proof.

Building on the same kind of ideas, Braun, Buck, and Girsch [13] showed the following more general result.

[2] available online at `http://math.mit.edu/~drew/Pfiles/`

Theorem 1.1.6 (Braun-Buck-Girsch, 2015). *Let $F \in M_{-2k}(\mathrm{SL}_2(\mathbb{Z}))$ with rational Fourier coefficients and let $P := R_{-2} \circ \ldots \circ R_{-2k+2} \circ R_{-2k}F$. Then for each sufficiently small negative discriminant $D < 0$, the polynomial*

$$\widehat{H}_{D,P}(X) = \prod_{Q} (X - P(\tau_Q)) \in \mathbb{Q}[X],$$

where Q ranges over a set of representatives of primitive, positive definite, integral binary quadratic forms modulo $\mathrm{SL}_2(\mathbb{Z})$, is irreducible over $\mathbb{Q}$.

It should be pointed out that in [13], an explicit bound on the discriminant D, from which on the above theorem holds, is given in terms of the weight and principal part of F.

1.2 A proof of the Thompson Moonshine Conjecture

The subject of Moonshine is, very broadly speaking, concerned with surprising and sometimes strange connections between different areas of Mathematics, e.g. Representation Theory of finite groups and modular forms. The most well-studied example of this is *Monstrous Moonshine* which we describe now.

According to the classification theorem of finite simple groups [6], a finite simple group is isomorphic to either

1. a cyclic group of prime order,
2. an alternating group of degree ≥ 5,
3. a finite group of Lie type (or the Tits group),
4. one of 26 *sporadic simple groups.*

The largest of the sporadic simple groups is the so-called *Monster group* $\mathbb{M}$ of order

$$\#\mathbb{M} = 2^{46} \cdot 3^{20} \cdot 5^{9} \cdot 7^{6} \cdot 11^{2} \cdot 13^{3} \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 41 \cdot 47 \cdot 59 \cdot 71 \approx 8.08 \cdot 10^{53}.$$

Its character table was first computed in 1976, assuming its existence, by Fischer, Livingstone, and Thorne (see [33]) and it was first constructed in 1982 by Griess [61] as the automorphism group of a certain 196884-dimensional commutative, but non-associative $\mathbb{R}$-algebra, called the *Griess algebra.* Even before the existence of the Monster had been established, some people noted some seemingly coincidental connections between the monster and the realm of modular forms. The first such observation was made by Ogg [86] who showed the following.

Theorem 1.2.1 (Ogg, 1975)**.** *Let p be prime. The modular curve $X_0(p)^+$, i.e. the compactified quotient $\overline{\Gamma_0(p)^+ \backslash \mathfrak{H}}$, has genus 0 if and only if*

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

Ogg remarks in [86] that these primes are precisely the prime divisors of the order of the Monster group and offers a bottle of Jack Daniels whiskey to the first person to offer an explanation for this coincidence. For a relatively recent discussion of this question as well as a partial solution to the *Jack Daniels Problem*, we refer to [47]. An analogue of this phenomenon in the context of so-called *Umbral Moonshine* (see below) has recently been found by Aricheta [5].

Another observation of a different sort of connection between the Monster and modular forms was made in 1978 by McKay who noticed that the first few coefficients of the modular j-function

$$j(\tau) = \frac{E_4(\tau)^3}{\Delta(\tau)} = q^{-1} + 744 + 196884q + 21493760q^2 + ... \tag{1.18}$$

or rather the so-called *Hauptmodul*, i.e. a (suitably normalized) generator of the field of modular functions, for the group $\mathrm{SL}_2(\mathbb{Z})$ given by $J = j - 744$, can be written in terms of dimensions of irreducible representations of $\mathbb{M}$,

$$196884 = 1 + 196883, \qquad 21493760 = 1 + 196883 + 21296876, ...$$

This led Thompson [107, 108] to conjecture the existence of an infinite-dimensional graded representation of the Monster, where the dimension of the nth graded component is the nth coefficient of J. The observations of McKay and Thompson were much extended by Conway and Norton [33] who managed to associate to each of the 194 conjugacy classes of $\mathbb{M}$ a Hauptmodul for a genus 0 subgroup of $\mathrm{SL}_2(\mathbb{R})$ whose coefficients agree, like those of J, with character values of the Monster. Note here that the dimension of a representation is simply the value of its associated character at the neutral element of the group. Their findings led Conway and Norton to conjecture that there should be an infinite-dimensional graded representation of $\mathbb{M}$ whose *McKay-Thompson series* coincide with the Hauptmoduln specified in [33], refining Thompson's original conjecture. For a graded G-module $V = \bigoplus_n V_n$ for a finite group G and a conjugacy class $[g] \subseteq G$, the associated McKay-Thompson series is defined by

$$\mathcal{T}_{[g]}(\tau) := \sum_n \mathrm{trace}(g|V_n)q^n. \tag{1.19}$$

The conjecture of Conway and Norton is usually referred to as the *Monstrous Moonshine Conjecture*. Following a suggestion of Thompson, an abstract proof for the existence of the Moonshine module was sketched by Atkin, Fong, and Smith [103]. As pointed out in [57, 62], this proof contains at least one and possibly two gaps, but the proof strategy is sound and has been used several times, for instance in the works just referenced. Frenkel, Lepowsky, and Meurman [53, 54] constructed a so-called *vertex operator algebra* $V^\natural$, i.e. a graded vector space endowed with an infinite collection of products, with an action of the Monster and showed that the associated McKay-Thompson series of the neutral element is indeed the function J, therefore confirming Thompson's original conjecture. The first non-trivial graded component of $V^\natural$ is exactly the Griess algebra mentioned above. In subsequent work, Borcherds [8] was able to verify that the McKay-Thompson series of the other conjugacy classes of the Monster agree with the Hauptmoduln found by Conway and Norton, therefore proving the full Monstrous Moonshine Conjecture.

Theorem 1.2.2 (Frenkel-Lepowsky-Meurman, 1988, and R. Borcherds, 1992)**.** *The Monstrous Moonshine Conjecture is true, i.e. there is an infinite-dimensional* $\mathbb{M}$*-module* $V^\natural$ *whose McKay-Thompson series are given by the Hauptmoduln specified by Conway and Norton. Moreover,* $V^\natural$ *carries the structure of a vertex operator algebra, on which* $\mathbb{M}$ *acts via automorphisms.*

Borcherds's proof of this result employed a variety of deep ideas from both Mathematics and Mathematical Physics, among them a new axiomatic description of vertex operator algebras, Borcherds-Kac-Moody algebras, and bosonic string theories. The work related to Monstrous Moonshine was one of the reasons to award him the Fields Medal in 1998.

Other kinds of Moonshine have been observed over the years, such as Generalized Moonshine as conjectured by Norton [85] and proven by Carnahan [25], Mathieu Moonshine as conjectured by Eguchi, Ooguri, and Tachikawa [48] and proven abstractly by Gannon [57], and more generally, Umbral Moonshine as conjectured by Cheng, Duncan, and Harvey [29] and proven abstractly by Duncan, Griffin, and Ono [42]. For a fairly recent and more detailed survey on the subject of Moonshine, the reader may consult [41] and for further information on the background and details the book [56].

In 2015, Harvey and Rayhaun [69] found evidence for moonshine for the finite sporadic *Thompson group Th*, which was first discovered and constructed by Thompson and Smith [102, 106] as the automorphism group of the 248-dimensional *Thompson lattice.* Their first observation was that the first few coefficients of the function f_3 in Zagier's basis of the space $M^{!,+}_{1/2}(\Gamma_0(4))$ of weakly holomorphic modular forms of weight 1/2 for $\Gamma_0(4)$ satisfying the Kohnen plus space condition (see (2.8)) are closely related to dimensions of irreducible representations of the

Thompson group: We have

$$\begin{aligned} f_3(\tau) &= q^{-3} + \sum_{n=1}^{\infty} A(n,3)q^n \\ &= q^{-3} - 248q + 26752q^4 - 85995q^5 + 1707264q^8 - 4096248q^9 + O(q^{12}) \end{aligned}$$

Comparing to the character table of Th [32, 59], one sees that 248, 85995, 1707264 occur as dimensions of irreducible representations of Th and we can decompose $26752 = 27000 - 248$ and $4096248 = 4096000 + 248$, where again, 27000 and 4096000 are dimensions of irreducible representations of Th. The function f_3 is connected to the Thompson group via the aforementioned Generalized Moonshine: The Thompson group (or rather $Th \times C_3$) is the centralizer of the conjugacy class $3C$ in the Monster group, so that Generalized Moonshine predicts a natural action of Th on the so-called *$3C$-twisted module* of the Monstrous Moonshine module $V^\natural$. The associated graded dimension function is given by the unique cube-root of the j-function which is real-valued on the imaginary axis

$$j(\tau)^{1/3} = q^{-1/3} + 248q^{2/3} + 4124q^{5/3} + 34752q^{8/3} + ...,$$

which is the *Borcherds lift* of the function f_3, i.e.

$$j(\tau)^{1/3} = q^{-1/3} \prod_{n=1}^{\infty} (1-q^n)^{A(n^2,3)},$$

see also Theorem 2.4.4. Harvey and Rayhaun modify the function f_3 slightly by adding a weight 1/2 theta function called a *theta correction* and define

$$\begin{aligned} \mathcal{F}_3(\tau) = 2f_3(\tau) + 248\vartheta(\tau) = 2q^{-3} + 248 + 2 \cdot 27000q^4 \\ - 2 \cdot 85995q^5 + 2 \cdot 1707264q^8 - ..., \quad (1.20) \end{aligned}$$

with $\vartheta(\tau) = \sum_{n\in\mathbb{Z}} q^{n^2}$ and we see that the first few coefficients are now all (two times)[3] dimensions of irreducible representations of Th with alternating signs. This is in flavour related to Umbral Moonshine and a first case of so-called *Penumbral Moonshine*, on which there is ongoing work of Duncan, Harvey, and Rayhaun. Because of these observations Harvey and Rayhaun conjecture that $\mathcal{F}_3$ is the graded dimension function of a graded *Th-supermodule W*. This means that each graded component decomposes as $W_m = W_m^0 \oplus W_m^1$, a direct sum of an even and odd part. In this case, W_m^i is trivial whenever $m \not\equiv i \pmod 2$. The *supertrace* of an element is defined as

$$\operatorname{strace}(g|W_m) = \operatorname{trace}(g|W_m^0) - \operatorname{trace}(g|W_m^1) \quad (1.21)$$

[3] Actually, they are rather the sum of the dimensions of two Galois conjugate representations, which necessarily have the same dimension, see Theorem 1.2.3.

and the McKay-Thompson series for a supermodule are defined as for usual modules but with the trace replaced by the supertrace.

The coefficients of f_3 are in fact twisted traces of singular moduli of the J-function (see Theorem 2.4.3). Using twisted traces of singular moduli of Hauptmoduln for the groups $\Gamma_0(N)$ for $N \in \{2, ..., 10, 12, 13, 16, 18, 25\}$ with appropriate theta corrections, Harvey and Rayhaun are able to obtain further tentative McKay-Thompson series of the Th-supermodule W.

All of these can also be realized in terms of *Rademacher sums*, essentially a low-weight analogue of Poincaré series, projected to the plus space: A Poincaré series is obtained by averaging a 1-periodic seed function over a set of representatives $\Gamma_\infty \setminus \Gamma_0(N)$, say, and, provided that the thus defined series converges absolutely, the function defined in this manner will transform like a modular form of the desired weight. For the most common types of Poincaré series, the convergence solely depends the weight, see for instance [15, 19, 31, 84, 88] and the references therein for details. Rademacher sums and series were first devised by Rademacher [91] in his study of the coefficients of the j-function. Their theory was developed systematically, with applications to moonshine in mind, mainly by Duncan and Frenkel [40] as well as Cheng and Duncan [27, 28]. Instead of averaging over the whole group, one only averages over a certain "rectangle" and lets this rectangle grow. This procedure improves the convergence properties of the sum compared to those of a Poincaré series. However, the resulting series is in general not modular but rather mock modular. Employing the approach via Rademacher sums with certain multiplier systems similar to those occuring in Umbral Moonshine enabled Harvey and Rayhaun to (numerically) compute candidates for all the tentative McKay-Thompson series $\mathcal{T}_{[g]}$, supporting their conjecture.

Together with Griffin, we showed in [62], which is reproduced in Appendix B, that the conjecture of Harvey and Rayhaun is indeed true.

Theorem 1.2.3 (Griffin-M., 2016)**.** *The Thompson-Moonshine Conjecture of Harvey and Rayhaun is true. Moreover, the McKay-Thompson series $\mathcal{T}_{[g]}$ are the unique modular forms in the space $M^{!,+}_{1/2}(4o(g), \psi_{[g]})$, where $o(g)$ denotes the order of a group element g and $\psi_{[g]}$ is the multiplier system associated to $[g]$, satisfying the following conditions:*

- *The Fourier expansion at ∞ is given by*

$$2q^{-3} + \chi_2(g) - (\chi_4(g) + \chi_5(g))q^4 + O(q^5),$$

where $\chi_1, ..., \chi_{48}$ denote the irreducible characters of Th as in [62, Tables 1–4],

- *Apart from the pole at ∞, there is a pole of order $3/4$ at the cusp $1/2o(g)$ in* *case $o(g)$ is odd; otherwise, the only pole is at ∞. The function vanishes at all other cusps of* $\Gamma_0(4o(g))$.

Remark. 1. For an element g with $o(g) \neq 36$, it suffices to specify that the function $\mathcal{T}_{[g]}$ should have an expansion $2q^{-3} + \chi_2(g) + O(q^4)$ in addition to the second condition in Theorem 1.2.3 in order to determine it uniquely.

2. In the statement of Theorem 1.2.3 in the original publication (see Theorem 1.2 in Appendix B), the conjugacy classes $12A$ and $12B$ of Th are excluded. The reason for this is that according to [62, Remark 3.3], the multpliers of the Rademacher sums and the corresponding theta corrections were not identical. While this is true at first glance when one computes the multiplier system of the given theta correction directly, the two multipliers actually agree on the group $\Gamma_0(48)$ as was pointed out to the author by Maryam Khaqan and John Duncan. Hence there is no reason to exclude the two conjugacy classes from the statement of the theorem.

The proof of this result follows similar lines as Gannon's proof of Mathieu Moonshine [57] and Duncan-Griffin-Ono's proof of Umbral Moonshine in general [42]. As first step it is necessary to verify that all the functions provided by Harvey and Rayhaun are indeed weakly holomorphic modular forms rather than mock modular forms, as Rademacher sums generically would be. This follows from the fact that the space of possible shadows is either trivial or has a basis such that the *Bruinier-Funke pairing* (see e.g. [20, Proposition 3.5]) allows to show that the shadow must be 0. Through the *Schur orthogonality relations*, one can write down the generating function for the (tentative) multiplicities of each irreducible character in the graded supermodule whose existence one wants to prove. The claim follows if all these multiplicities are integers whose signs are exactly alternating (or 0). The integrality of these multiplicities can be verified by showing that the McKay-Thompson series satisfy sufficiently many congruences. An idea of Thompson [108] allows to compute the required congruences from the character table, however it is also possible, as done in [62], to find all congruences modulo powers of primes dividing the order of Th and check a posteriori that these suffice to deduce integrality of the multiplicities. For the "positivity", i.e. the fact the signs alternate as conjectured by Harvey and Rayhaun, requires the representation of the McKay-Thompson series as Rademacher sums. Their Fourier coefficients can be represented as infinite sums of Kloosterman sums weighted by Bessel functions. Through explicit estimates on Kloosterman zeta functions, mimicking and extending the procedure established in [57] and building essentially on work by Kohnen [76], one finds that from a certain point on, the coefficients of $\mathcal{T}_{[1A]}$ dominate all the other coefficients, which allows to deduce the expected sign behaviour of all the multiplicities from an explicit point on. The rest can be checked directly by inspection.

One important feature of the Hauptmoduln in Monstrous Moonshine is that they are *replicable*, which means for example that their Fourier coefficients can be computed recursively from the first 23 of them (see for instance [52]). This is reminiscent of the VOA structure of the Moonshine module $V^\natural$. IN [42], a mock modular anaolgue of replicability is established for the McKay-Thompson series in Umbral Moonshine using work of Imamoğlu, Raum, and Richter [73] and the author [81] on holomorphic projection (see also [35]). In [62], we connect some of the McKay-Thompson series of Thompson Moonshine to such replicable functions via their associated weak Jacobi forms.

It remains to be remarked that unlike in the case of Monstrous Moonshine, no construction of the Th-supermodule whose existence is asserted in Theorem 1.2.3 is available to date. For several cases of Umbral Moonshine, a module has been constructed [4, 26, 46, 43], but in particular not yet for the case of Mathieu Moonshine. We hope to be able to construct the Thompson-supermodule in the future in order to complete the picture.

1.3 O'Nan Moonshine and Arithmetic

The 26 sporadic groups may be subdivided into two collections, the *Happy Family*, consisting of those 20 sporadic simple groups which are quotients of subgroups of the Monster, and the six so-called *Pariahs* or *non-monstrous sporadic groups*: the *Lyons group Ly*, the three[4] *Janko groups* J_1, J_3, and J_4, the *Rudvalis group Ru*, and the *O'Nan group O'N*. It has long been an open question in Moonshine, asked already by Conway and Norton [33], whether these groups, which have nothing to do with the Monster, are in any way connected to Moonshine (see also [11]).

In [45], which is reproduced in Appendix C, we show together with Duncan and Ono that the O'Nan group indeed has a connection to Moonshine (see also [44, 58]). Evidence for the existence of this group was first found in 1976 by O'Nan [87] and according to loc. cit., it was first constructed by Sims. The fact that it is a Pariah, i.e. not a subquotient of the Monster, was first shown by Griess [61].

A first observation leading to Moonshine for the O'Nan group comes from inspecting Zagier's basis of the space $M_{3/2}^{!,+}(\Gamma_0(4))$, see (2.10). The function g_4 in this basis has Fourier expansion

$$g_4(\tau) = q^{-4} - 2 - 26752q^3 - 143376q^4 - 8288256q^7 - 26124256q^8 + O(q^{11})$$

and one notices that 26752 is a dimension of an irreducible representation of the O'Nan group, and one can write 143376 = 1+58311+85064, where 1, 58311, 85064 are also dimensions of irreducible represenations of *O'N*. Similar decompositions can be observed for higher level analogues of g_4.

[4] The second Janko group J_2 is a member of the Happy Family.

Using essentially the same approach as described above in the context of Thompson Moonshine, the existence of a module for the O'Nan group is established, whose McKay-Thompson series are special modular forms [45, Theorem 1.1, Theorem 3.1].

Theorem 1.3.1 (Duncan-M.-Ono, 2017)**.** *There exists an infinite-dimensional graded O'N-module $W = \bigoplus_{0<m\equiv 0,3\,(4)} W_m$ whose McKay-Thompson series*

$$F_{[g]}(\tau) = -q^{-4} + 2 + \sum_{0<m\equiv 0,3\,(4)} a_{[g]}(m)q^m$$

for each conjugacy class $[g] \subseteq O'N$ are weakly holomorphic modular forms of weight $3/2$ of level $4o(g)$ in the Kohnen plus space with trivial multipliers for $o(g) \neq 16$. Moreover, these forms are uniquely determined by the following conditions:

(a) $F_{[g]} \in M^{!,+}_{3/2}(\Gamma_0(4o(g)), \psi_{[g]})$,

(b) $F_{[g]}(\tau)$ *has the principal part at infinity specified above and additionally a pole of order $1/4$ at $1/o(g)$ as forced by the plus space condition and vanishes at all other cusps,*

(c) we have $a_{[g]}(3) = \chi_7(g)$, $a_{[g]}(4) = \chi_1(g)+\chi_{12}(g)+\chi_{18}(g)$ *and* $a_{[g]}(7)$ *as specified in [45, Tables B.1–B.3], where* $\chi_1, ..., \chi_{30}$ *denote the irreducible characters of O'N as in [45, Table A.1].*

Note that the conditions (a) and (b) inTheorem 1.3.1 determine a weakly holomorphic modular form up to the addition of cusp forms. This leaves a choice for the contribution from cusp forms which is fixed by condition (c). A reason for choosing this particular contribution from cusp forms comes from the required congruences that the McKay-Thompson series, see the remark following [45, Theorem 3.1].

Remark. It should be pointed out that the module W whose existence is asserted in Theorem 1.3.1 is slightly virtual, i.e. finitely many (four to be precise) graded components can only be decomposed into irreducible *O'N*-modules using negative multiplicities (see [45, Table B.1-B.2]. This could be remedied by adding weight 3/2 unary theta functions to some of the McKay-Thompson series, but at the expense of the classifying properties (see the second remark following [45, Theorem 1.1]).

Remark. In an earlier version of [45], a variation of Theorem 1.3.1 was considered where we required all multiplier systems to be trivial and instead allowed mock modular forms with the properties given. These mock modular forms automatically have trivial shadows unless $o(g) = 16$. The multipliers occurring in Theorem 1.3.1 are connected to the cohomology of *O'N* (cf. [45, p. 15f]), while the existence of non-trivial shadows is not known to be.

Returning to the Zagier basis in weight 3/2, Zagier showed (see Theorem 2.4.2) that the coefficients of the first element

$$g_1(\tau) = q^{-1} - 2 + 248q^3 - 492q^4 + 4119q^7 - 7256q^8 + 33512q^{11} - 53008q^{12} + O(q^{15})$$

in this basis are the negatives of the traces of the singular moduli of the J-function in (1.18). It also follows from his work on the action of Hecke operators on these traces [114] as well as the work of Miller and Pixton [83] that one can write the coefficients of the McKay-Thompson series $F_{[g]}$ of the $O'N$-module in Theorem 1.3.1 in terms of traces of singular moduli of explicit modular functions of level $o(g)$ (see [45, Proposition 5.1 and Appendix D], *generalized Hurwitz class numbers* (which are the traces of the constant function 1 as studied in detail in [55]), as well as coefficients of weight 3/2 cusp forms.

By important work of Waldspurger [110] and Kohnen [76] we know that coefficients of weight 3/2 cusp forms (or more precisely newforms) in the plus space are closely connected to L-values of weight 2 cusp forms.

Theorem 1.3.2 (Waldspurger, 1981, Kohnen, 1985). *Let $N \in \mathbb{N}$ be odd and square-free, $f \in S^+_{k+\frac{1}{2}}(\Gamma_0(4N))$ be a newform with Fourier expansion $f(\tau) = \sum_{n=1}^{\infty} b_f(n)q^n$. Further let $F \in S_{2k}(\Gamma_0(N))$ the image of f under the* Shimura correspondence. *For a prime $\ell | N$, let w_ℓ be the eigenvalue of F under the Atkin–Lehner involution W_ℓ and choose a fundamental discriminant D with $(-1)^k D > 0$ and $\left(\frac{D}{\ell}\right) = w_\ell$ for all ℓ. Then we have*

$$\langle f, f \rangle = \frac{\langle F, F \rangle \pi^k}{2^{\omega(N)}(k-1)!|D|^{k-\frac{1}{2}} L(F, D; k)} \cdot |b_f(|D|)|^2,$$

where $L(F, D; s)$ denotes the twist of the newform F by the quadratic character $\left(\frac{D}{\bullet}\right)$ and $\omega(N)$ denotes the number of distinct prime divisors of N.

The Conjecture of Birch and Swinnerton-Dyer [7, 113] together with the Modularity Theorem [14, 105, 112] asserts that the L-values in Theorem 1.3.2 contain arithmetic information about the associated elliptic curve in case the weight 2 newform has rational coefficients.

Conjecture 1.3.3 (Birch and Swinnerton-Dyer, 1964). *Let $E/\mathbb{Q}$ be an elliptic curve. Then we have that*

$$\frac{L^{(r)}(E, 1)}{r!\Omega_E} = \frac{\#\text{Ш}(E) \cdot \mathrm{Reg}(E) \prod_\ell c_\ell(E)}{(\#E(\mathbb{Q})_{tors})^2}, \tag{1.22}$$

where r denotes the analytic rank, *i.e. the order of vanishing of $L(E, s)$ at $s = 1$, which equals the Mordell–Weil rank of E, Ω_E is the real period of E, $\#\text{Ш}(E)$ and*

Reg(E) *denote the order of the Tate-Shafarevich group and the regulator of* E, *respectively, the* $c_\ell(E)$ *for prime* ℓ *are the Tamagawa numbers of* E, *and* $\#E(\mathbb{Q})_{tors}$ *is the order of the torsion subgroup of the* $\mathbb{Q}$*-rational points of* E.

Using these results and conjectures together with the work of Kolyvagin [77] and Gross and Zagier [64] on the Birch and Swinnerton-Dyer Conjecture we can obtain non-trivial information on p-divisibility of class groups of imaginary quadratic number fields for small primes p as well as on p-torsion of Selmer- and Tate-Shafarevich groups of quadratic twists of certain elliptic curves. The precise results are as follows (see [45, Theorems 1.2-1.4]).

Theorem 1.3.4 (Duncan-M.-Ono, 2017)**.** *Suppose that* $-D<0$ *is a fundamental discriminant. Then the following are true:*

1. *If* $-D<-8$ *is even and* $g_2\in O'N$ *has order 2, then*

$$\dim W_D \equiv \mathrm{trace}(g_2|W_D) \equiv -24H(D) \equiv 0 \pmod{2^4}.$$

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

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

In what follows, let E_N denote the strong Weil curve of conductor N, i.e. in the cases under consideration here, where the genus of the modular curve $X_0(N)$ equals 1, a model of said modular curve.

Theorem 1.3.5 (Duncan-M.-Ono, 2017)**.** *Assume the Birch and Swinnerton-Dyer Conjecture 1.3.3. If* $p=11$ *or* 19 *and* $-D<0$ *is a fundamental discriminant for which* $\left(\frac{-D}{p}\right)=-1$, *and* $g_p\in O'N$ *has order* p, *then the following are true.*

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

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

2. *Suppose that* $L(E_p(-D),1)\neq 0$. *Then we have that* $\mathrm{rk}(E(-D))=0$. *Moreover, we have* $p|\#\text{Ш}(E_p(-D))$ *if and only if*

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

Note that due to the work of Kolyvagin [77] as well as Gross and Zagier [64], part (2) of Theorem 1.3.5 is in fact unconditionally true.

Thanks to work of Skinner and Urban on the Iwasawa main conjectures for GL_2 [100, 101], we have the following completely unconditional result.

Theorem 1.3.6 (Duncan-M.-Ono, 2017). *Suppose that $N \in \{14, 15\}$. If p is the unique prime ≥ 5 dividing N, then let $\delta_p := \frac{p-1}{2}$ and let $p' := N/p$. If $-D < 0$ is a fundamental discriminant for which $\left(\frac{-D}{p}\right) = -1$ and $\left(\frac{-D}{p'}\right) = 1$, then the following are true.*

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

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

2. *Suppose that $L(E_N(-D), 1) \neq 0$. Then we have that* $\mathrm{rk}(E(-D)) = 0$. *Moreover, we have $p|\#Ш(E_N(-D))$ if and only if*

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

The proofs of Theorems 1.3.4 to 1.3.6 all rely heavily on the fact that one can write all the graded characters for the *O'N*-module W essentially in terms of traces of singular moduli (and coefficients of cusp forms). This allows to control very easily when certain constituents of the McKay-Thompson series are forced to vanish, allowing to examine the remaining constituents (i.e. class numbers or coefficients of cusp forms) directly.

Arithmetic implications of this sort have not been noticed in the context of Moonshine prior to [45]. Similar results are the subject of ongoing work of the author with Cheng and Duncan as well as with Duncan, Griffin, and Rolen. The former of these for instance involves mock modular McKay-Thompson series without poles but satisfying certain optimality requirements. The coefficients there can essentially be written down in terms of generalized class numbers and coefficients of cusp forms. These yield infinitely many virtual modules for example for the group $2.M_{12}$ which also appears in Umbral Moonshine, to which that work is directly connected. The there obtained modules yield an amusing criterion to decide if a given odd discriminant is a congruent number, depending on the decomposition of the corresponding graded component into irreducibles. The latter work in progress concerns Moonshine of a similar flavour as O'Nan Moonshine for some of the Janko groups, which allow us to obtain statements like Theorems 1.3.5 and 1.3.6 for other elliptic curves.

At the current stage, it is not clear how the Arithmetic can be linked directly to the O'Nan group, say, without using strong results on modular forms. In particular, there is no known group action of *O'N* on the arithmetic quantities to date. One future goal would be to find a construction of the module in Theorem 1.3.1, hoping that it admits a group theoretic explanation for the results in Theorems 1.3.4 to 1.3.6.

1.4 Summary

As we have seen in Sections 1.1 to 1.3, the connecting feature of the results in this thesis are singular moduli and especially their traces. In [82], we investigated algebraic properties of a class polynomial built from singular moduli of a non-holomorphic function, where the traces of these singular moduli are the partition numbers $p(n)$. We show that, similar to the classical case of the class polynomial in (2.4) associated to the j-function, this polynomial is irreducible over $\mathbb{Q}$ and that its roots generate the ring class field of the order of conductor t in $\mathbb{Q}(\sqrt{d})$, where we write $1-24n=t^2d$ with $d<0$ a fundamental discriminant.

In [45, 62], we show that traces of singular moduli of various modular functions essetially yield character values of certain representations of the finite sporadic Thompson group and the pariah group *O'N*. More precisely we show the existence of an infinite-dimensional graded module for the respective groups whose McKay-Thompson series are essentially given as generating functions of(twisted) traces of singular moduli plus some appropriate corrections (weight 1/2 theta functions for the Thompson group and generalized class numbers and cusp forms in the case of *O'N*). For the O'Nan group, this description in terms of traces allows us to deduce information for example on arithmetic properties of quadratic twists of certain elliptic curves.

Acknowledgements

The articles [45, 62, 82] contained in the appendix and providing the main contents of this thesis have all been written with collaborators, namely Larry Rolen [82], Michael J. Griffin [62], as well as John F. R. Duncan and Ken Ono [45]. Each one of the results has been a joint project of the people involved, everyone contributing essentially equal shares of ideas and work. I would like to take this opportunity to thank all the aformentioned collaborators for a great work atmosphere and all their brilliant ideas contributing to the success of the projects.

The works were written while I was employed as a wissenschaftlicher Mitarbeiter/Postdoctoral Fellow at (in chronological order) the Universität zu Köln (partially funded by the European Research Council under the European Union's Seventh Framework Programme (FP/2007-2013) / ERC Grant agreement n. 335220 - AQSER, awarded to Kathrin Bringmann), at Emory University in Atlanta, GA, and at the Max-Planck-Institut für Mathematik in Bonn. I express my gratitude to all these institutions for their support and hospitality.

Special thanks go to Kathrin Bringmann for her advice and encouragement during the past years and especially in the endeavour to obtain the Habilitation at the Universität zu Köln. I would also like to thank the (prospective) members of the Habilitationskommission and the referees for this thesis for agreeing to act in their respective roles in the process.

Zu guter Letzt möchte ich meiner Familie, insbesondere meinen Eltern, denen diese Arbeit gewidmet ist, danken für alles, was sie für mich getan haben.

Chapter 2

Complex multiplication and singular moduli

As mentioned in the introduction, we now give a very brief overview of some of concepts and classical applications of complex multiplication and singular moduli. All of the material presented here can be found in many places, including numerous textbooks. This account is mainly based on [115, Section 6] and [34, Chapters 2 and 3].

2.1 Complex multiplication and elliptic curves

It is a standard result from the theory of elliptic functions that an *elliptic curve*

$$E:\ y^2 = 4x^3 - g_2x - g_3, \qquad g_2^3 - 27g_3^2 \neq 0 \tag{2.1}$$

over $\mathbb{C}$ are isomorphic to a flat torus $\mathbb{C}/\Lambda$, where $\Lambda = \mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2 \subset \mathbb{C}$ is a two-dimensional lattice in $\mathbb{C}$. This isomorphism is such that if we have $\lambda \in \mathbb{C}$ and a lattice Λ' with $\lambda\Lambda \subseteq \Lambda'$, we obtain an algebraic map, called an *isogeny*, from E to $E' \cong \mathbb{C}/\Lambda'$. Indeed all isogenies, i.e. morphisms $E \to E'$ sending the point at infinity to the point at infinity, are of this form [99, Theorem VI.4.1 (b)]. This is of particular interest when we can choose $\Lambda' = \Lambda$, in which case one also calls the isogenies *endomorphisms* of E. For $\lambda = m \in \mathbb{Z}$ one clearly always has $m\Lambda \subseteq \Lambda$ and for a generic lattice Λ, these are the only $\lambda \in \mathbb{C}$ satisfying $\lambda\Lambda \subseteq \Lambda$. On the elliptic curve E, this corresponds to the isogeny

$$[m]:\ E \to E, \quad P \to mP.$$

If we have $\lambda\Lambda \subseteq \Lambda$ for some $\lambda \notin \mathbb{Z}$, this automatically implies that λ lies in an order $\mathcal{O}$ in some imaginary quadratic number field K and Λ is then of the form

$\alpha\mathfrak{a}$ for some $\alpha \in \mathbb{C}^\times$ and a proper fractional $\mathcal{O}$-ideal $\mathfrak{a}$ in K. In this case, we say that the elliptic curve $E = \mathbb{C}/\Lambda$ has *complex multiplication* (or *CM* for short) by the order $\mathcal{O}$. Note that we can write the associated lattice of E as $\lambda(\mathbb{Z} \oplus \mathbb{Z}\tau)$ for some $\tau \in \mathfrak{H}$, which is unique up to $\mathrm{SL}_2(\mathbb{Z})$-equivalence. If E has CM, then the corresponding τ satisfies a quadratic equation $a\tau^2 + b\tau + c = 0$ for some (coprime) $a, b, c \in \mathbb{Z}$ and vice versa. Such points τ are called *CM points* and the discriminant of the corresponding equation is called the discriminant of τ.

We note that an equivalent characterization of elliptic curves or rather lattices with complex multiplication can be given using the Weierstrass $\wp$-function.

Lemma 2.1.1. *Let Λ be a lattice in $\mathbb{C}$ and $\wp$ its associated Weierstrass $\wp$-function. The a number $\lambda \in \mathbb{C}\setminus\mathbb{Z}$ satisfies $\lambda\Lambda \subseteq \Lambda$ if and only if $\wp(\lambda z)$ is a rational function in $\wp(z)$.*

2.2 Algebraicity of singular moduli

An important invariant of an elliptic curve $E \cong \mathbb{C}/\Lambda$ as given in (2.1) is its j-invariant

$$j(E) = 1728\frac{g_2^3}{g_2^3 - 27g_3^2}.$$

Note that we have $j(E) = j(\tau)$ for $j(\tau)$ as in (1.18) and $\tau \in \mathfrak{H}$ such that $\Lambda = \lambda(\mathbb{Z} \oplus \mathbb{Z}\tau)$. Note again that this τ is unique up to action of $\mathrm{SL}_2(\mathbb{Z})$. Two elliptic curves are isomorphic (over $\mathbb{C}$) if and only if they have the same j-invariant and one can show that if $j(E)$ is contained in a subfield K of $\mathbb{C}$, then there is an elliptic curve defined over K with the same j-invariant [99, Proposition III.1.4].

It can be inferred essentially from Lemma 2.1.1 that if E has complex multiplication, then the *singular modulus* $j(E)$ is an algebraic number. In particular, elliptic curves with *CM* can always be defined over a number field.

However, using the theory of modular forms, one can prove a much stronger result.

Theorem 2.2.1. *For a CM point τ of discriminant $D < 0$ the value $j(\tau)$ is an algebraic integer of degree $h(D)$, where $h(D)$ denotes the* class number *of D, i.e. the number of equivalence classes of positive definite binary primitive integral quadratic forms modulo* $\mathrm{SL}_2(\mathbb{Z})$.

Proof outline. We sketch a proof based on modular forms for the fact that $j(\tau)$ is an algebraic integer. For this, we consider the mth *modular polynomial* $\Psi_m(X, Y)$ for $m \geq 2$ defined by

$$\Psi_m(X, j(\tau)) := \prod_{M \in \mathrm{SL}_2(\mathbb{Z})\backslash\Gamma_m} (X - j(M.\tau)), \tag{2.2}$$

where Γ_m denotes the set of 2×2 matrices over $\mathbb{Z}$ with determinant m. This is a polynomial in X of degree $\sigma_1(m) = \sum_{d|m} d$, because the set

$$\left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in \mathbb{Z}^{2\times 2} \;:\; ad = m,\ 0 \leq b < d \right\}$$

is a full set of representatives of $\mathrm{SL}_2(\mathbb{Z}) \setminus \Gamma_m$ and has cardinality $\sigma_1(m)$. The coefficients are holomorphic functions in τ. The function $\Psi(X, j(\tau))$ also doesn't depend on the choice of representatives due to the modular invariance of $j(\tau)$. Replacing τ by $\gamma.\tau$ for some $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ only changes the system of representatives, hence the coefficients of $\Psi(X, j(\tau))$ as a polynomial in X are all modular functions for $\mathrm{SL}_2(\mathbb{Z})$ without poles in $\mathfrak{H}$, hence polynomials in $j(\tau)$. Since $j(\tau)$ is a transcendental function, we may replace a formal variable Y for it and obtain a polynomial $\Psi_m(X, Y) \in \mathbb{C}[X, Y]$. By using the explicit system of representatives, the fact that $j(\tau)$ has integer Fourier coefficients, as well as Galois conjugation, one sees that the coefficients are indeed integers, so that $\Psi_m(X, Y) \in \mathbb{Z}[X, Y]$.

Assuming for simplicity that m is not a perfect square[1], one can in fact also show with a similar argument that the restriction to the diagonal $\Psi_m(X, X)$ is monic (up to sign) and of degree $\sigma_1^+(m) = \sum_{d|m} \max(d, m/d)$.

Now let $\tau \in \mathfrak{H}$ be a CM point satisfying $a\tau^2 + b\tau + c = 0$ for coprime $a, b, c \in \mathbb{Z}$, $a > 0$. An equivalent way of saying this is that τ is a fixed point of the matrix $M = \left(\begin{smallmatrix} 0 & -c \\ a & b \end{smallmatrix}\right)$ of determinant $m = ac$. Assuming for simplicity that m is not a perfect square[2], we have by construction

$$0 = \Psi_m(j(M.\tau), j(\tau)) = \Psi_m(j(\tau), j(\tau)),$$

whence $j(\tau)$ is the root of a non-zero polynomial with integer coefficients and leading coefficient ±1 and therfore an algebraic integer. □

Since any modular function for any finite index subgroup of $\mathrm{SL}_2(\mathbb{Z})$ is an algebraic function in the j-function, which can be seen using a construction similar to the modular polynomial in (2.2), it follows directly from Theorem 2.2.1 that the singular moduli of any modular function with algebraic Fourier coefficients are algebraic numbers. For example, the *Rogers-Ramanujan continued fraction*

$$r(\tau) := \cfrac{q^{1/5}}{1 + \cfrac{q}{1 + \cfrac{q^2}{\ddots}}} = q^{1/5} \prod_{n=0}^{\infty} \frac{(1 - q^{5n+1})(1 - q^{5n+4})}{(1 - q^{5n+2})(1 - q^{5n+3})} \tag{2.3}$$

[1] If m is a perfect square, then $\Psi(X, Y)$ is divisible by $(X - Y)$, so that the diagonal restriction is identically zero.

[2] If it is, we may factor out the factor $(X - Y)$ in $\Psi_m(X, Y)$ without affecting the other basic properties of the polynomial.

is a modular function (in fact a generator for the field of modular functions) for the principal congruence subgroup

$$\Gamma(5) = \{\gamma \in \mathrm{SL}_2(\mathbb{Z}) \,:\, \gamma \equiv \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right) \pmod 5\}$$

and one can show that

$$j(\tau) = -\frac{(r(\tau)^{20} - 228r(\tau)^{15} + 494r(\tau)^{10} + 228r(\tau)^5 + 1)^3}{r(\tau)^5(r(\tau)^{10} + 11r(\tau)^5 - 1)^5},$$

an identity that essentially goes back to Klein [74, 75], see also [37]. Using the well-known evaluation $j(i) = 1728$, one arrives at Ramanujan's evaluation of the continued fraction given in (1.2).

Returning to the singular moduli of the j-function, one can determine their degrees over $\mathbb{Q}$ and their minimal polynomials explicitly. For this let $\mathcal{Q}_D$ for a discriminant $D < 0$ denote the set of all positive definite binary primitive integral quadratic forms $Q(x, y) = ax^2 + bxy + cy^2$, $a, b, c \in \mathbb{Z}$, $a > 0$, $\gcd(a, b, c) = 1$, of discriminant $D = b^2 - 4ac$. Every such quadratic form has an associated CM point $\tau_Q \in \mathfrak{H}$, namely the unique root in $\mathfrak{H}$ of the quadratic polynomial $Q(\tau_Q, 1)$. With this we define the *class polynomial*

$$H_D(X) := \prod_{\mathcal{Q}_D/\,\mathrm{SL}_2(\mathbb{Z})} (X - j(\tau_Q)). \tag{2.4}$$

Then we have the following result.

Theorem 2.2.2. *The polynomial $H_D(X)$ has integer coefficients and is irreducible over $\mathbb{Q}$. In particular, the singular modulus $j(\tau_Q)$ is an algebraic integer of degree exactly $h(D) = \#\mathcal{Q}_D/\,\mathrm{SL}_2(\mathbb{Z})$ and its Galois conjugates are given by $j(\tau_{Q'})$, $Q' \in \mathcal{Q}_D/\,\mathrm{SL}_2(\mathbb{Z})$.*

It is well-known that $h(-163) = 1$, in fact -163 is the smallest discriminant with this property, so that by Theorem 2.2.2 we find that $j((1 + \sqrt{-163})/2)$ is a rational integer. Furthermore, $\exp(-\pi\sqrt{163}) \approx 3.809 \cdot 10^{-18}$ and the coefficients c_n of the j-function can be bounded from above by $\exp(4\pi\sqrt{n})/(\sqrt{2}n^{3/4})$ (see [18, Section 5.3]), showing that the integer

$$j((1 + \sqrt{-163})/2) = -e^{\pi\sqrt{163}} + 744 + \sum_{n=1}^{\infty} c_n(-1)^n e^{-\pi\sqrt{163}n} = -e^{\pi\sqrt{163}} + 744 + \varepsilon$$

for some small error ε with $|\varepsilon| < 7.724 \cdot 10^{-13}$. This explains Hermite's original observation that $e^{\pi\sqrt{163}}$ is so surprisingly close to an integer (see (1.1)).

2.3 Explicit class field theory

One of the most important applications of the theory of complex multiplication lies in explicit *class field theory.* This theory aims to describe relatively abelian extensions of algebraic number fields whose Galois group is isomorphic to a class group in some sense. To state the main theorem of class field theory, we need to introduce some notation. Let K be a number field with ring of integers $\mathcal{O}_K$ and $\mathfrak{m}$ a *modulus* of K, i.e. a formal product of finitely many finite primes of K, denoted by $\mathfrak{m}_0$, and distinct real infinite primes, whose product we denote by $\mathfrak{m}_\infty$. Further denote by $I_K(\mathfrak{m})$ the group of fractional ideals coprime to the finite primes dividing $\mathfrak{m}$ and let

$$P_{K,1}(\mathfrak{m}) := \{\alpha\mathcal{O}_K \in I_K(\mathfrak{m}) \,:\, \alpha \in \mathcal{O}_K,\, \alpha \equiv 1 \pmod{\mathfrak{m}_0},\, \sigma(\alpha) > 0 \text{ for all } \sigma \mid \mathfrak{m}_\infty\}.$$

A subgroup $H \leq I_K(\mathfrak{m})$ containing $P_{K,1}(\mathfrak{m})$ is called a *congruence subgroup* and the (finite) quotient $I_K(\mathfrak{m})/H$ is called *generalized class group* for $\mathfrak{m}$.

Theorem 2.3.1 (Main theorem of class field theory). *Let K be a number field. Then the following are true.*

(i) If L/K is a finite abelian extension, then there exists a modulus $\mathfrak{m}$ of K, divisible by all finite and infinite primes which ramify in L, such that the Galois group $\mathrm{Gal}(L/K)$ *is canonically isomorphic to a generalized class group for $\mathfrak{m}$ via the so-called* Artin map.

(ii) Let $\mathfrak{m}$ be a modulus of K and H a congruence subgroup for $\mathfrak{m}$. Then there exists a unique abelian extension L/K whose Galois group is canonically isomorphic to the generalized class group $I_K(\mathfrak{m})/H$ via the Artin map.

Remark. There is a choice for the modulus $\mathfrak{m}$ in (i) of Theorem 2.3.1, in fact there are always infinitely many eligible moduli. The so-called *conductor* $\mathfrak{f} = \mathfrak{f}(L/K)$ provides a unique "minimal" choice in the sense that any eligible modulus is divisible by $\mathfrak{f}$.

In many textbooks, the first application of the main theorem of class field theory 2.3.1 one encounters is the proof of the celebrated Theorem of Kronecker-Weber [78, 111], whose first complete proof was found by Hilbert [72] in 1896.

Theorem 2.3.2 (Kronecker, 1853, Weber, 1886). *Let $K/\mathbb{Q}$ be a finite abelian extension of $\mathbb{Q}$. Then there is some $N \in \mathbb{N}$ such that $K \subseteq \mathbb{Q}(\exp(2\pi i/N))$.*

One reason why this result is so remarkable is that abelian extensions of $\mathbb{Q}$ can be generated by special values of a single transcendental function, namely the exponential function. The 12th of Hilbert's famous 23 problems asks for a generalization of this result to arbitrary number fields, in particular for an appropriate analogue for the roots of unity occuring in Theorem 2.3.2. *Kronecker's Jugendtraum* gives a (at the time conjectural) generalization of Theorem 2.3.2 to the case of imaginary quadratic number fields. This result was first proven by Takagi, later important contributions are due to Fueter and Hasse (see for instance [109, pp. 89 ff.] for an account of the history). It is to date the only fully resolved generalization of the theorem of Kronecker-Weber.

Theorem 2.3.3 (Second main theorem of class field theory)**.** *Kronecker's Jugendtraum is true. More precisely, any finite abelian extension L/K of an imaginary quadratic number field K with ring of integers $\mathcal{O}_K = \mathbb{Z} \oplus \mathbb{Z}\tau$ for some $\tau \in \mathfrak{H}$ is contained in the* ray class field $K_{\mathfrak{m}}$ *for the modulus $\mathfrak{m} = N\mathcal{O}_K$ for some positive integer N. Furthermore, we have that*

$$K_{\mathfrak{m}} = K(j(\tau), h^{(s)}(1/N))$$

where

$$h^{(1)}(z) := (g_2 g_3/\Delta)\wp(\tau, z),\ h^{(2)}(z) := (g_2^2/\Delta)\wp(\tau, z)^2,\ h^{(3)}(z) := (g_3/\Delta)\wp(\tau, z)^3 \tag{2.5}$$

with $g_k = g_k(\mathcal{O}_K)$ and $\Delta = g_2^3 - 27g_3^2$ denote the elliptic Weber functions *and s is half the number of roots of unity in $\mathcal{O}_K$.*

Special abelian extensions of imaginary quadratic fields can be generated just by singular moduli. For this consider the *Hilbert class field* of an imaginary quadratic number field, i.e. the maximal unramified abelian extension of K, which has the property that its Galois group over K is canonically isomorphic to the ideal class group of K, i.e. the corresponding modulus is simply $\mathcal{O}_K$.

Theorem 2.3.4. *Let $K/\mathbb{Q}$ be an imaginary quadratic number field of discriminant D. Then the class polynomial $H_D(X)$ defined in* (2.4) *is irreducible over K. The Hilbert class field H/K is generated by any one value $j(\tau_Q)$, $Q \in \mathcal{Q}_D$, i.e.*

$$H = K(j(\tau_Q)) \cong K[X]/(H_D(X)).$$

The same result is true if one considers an order $\mathcal{O}$ of conductor f in K and the singular moduli $j(\tau_Q)$ for $Q \in \mathcal{Q}_{f^2D}$. The field generated over K by any one these values is the so-called *ring class field* of $\mathcal{O}$.

We remark that the general case of Hilbert's 12th problem is still open. Shimura and Taniyama [96, 98] were able to construct abelian extensions of so-called *CM-fields*, i.e. imaginary-quadratic extensions of totally real number fields, using an approach through abelian varieties rather than that of modular functions, which had been used for instance by Hecke [70].

2.4 Norms and traces of singular moduli

Since singular moduli are algebraic numbers, it makes sense to study their norms and traces. As indicated in the introduction, their traces are of greater importance in the context of this thesis, but nevertheless we start by discussing norms of singular moduli. These were studied by Gross and Zagier [63] and the methods used in the proof gave rise to their seminal work on heights of Heegner points and derivatives of L-functions [64]. As it turns out, it is more natural to study norms of differences of singular moduli (note that $j((1+\sqrt{-3})/2)=0$, so that one doesn't lose the information about the singular moduli themselves). For coprime discriminants $D_1, D_2 < 0$ let

$$J(D_1,D_2) = \prod_{Q_1 \in \mathcal{Q}_{D_1}/\operatorname{SL}_2(\mathbb{Z})} \prod_{Q_2 \in \mathcal{Q}_{D_2}/\operatorname{SL}_2(\mathbb{Z})} (j(\tau_{Q_1}) - j(\tau_{Q_2})). \tag{2.6}$$

Up to sign, this is the resultant of the two polynomials $H_{D_1}(X)$ and $H_{D_2}(X)$.

Theorem 2.4.1 (Gross-Zagier, 1985). *For coprime discriminants $D_1, D_2 < 0$, every prime divisor of $J(D_1,D_2)$ must divide $\frac{1}{4}(D_1D_2 - x^2)$ for some $x \in \mathbb{Z}$ satisfying $|x| \leq \sqrt{D_1D_2}$ and $x^2 \equiv D_1D_2 \pmod 4$. In particular, all prime factors of $J(D_1,D_2)$ are at most $D_1D_2/4$.*

If we choose for example the discriminants $D_1 = -163$ and $D_2 = -3$, the primes satisfying the conditions in Theorem 2.4.1 are 2, 3, 5, 11, 17, 23, 29, 61, and indeed we have

$$J(-163,-3) = j\left(\frac{1+\sqrt{-163}}{2}\right) = -262537412640768000 = -2^{18}\cdot 3^3 \cdot 5^3 \cdot 23^3 \cdot 29^3.$$

The fact that this number is a perfect cube is connected to the fact that the function

$$\gamma_2(\tau) := \frac{E_4(\tau)}{\eta(\tau)^8} = q^{-1/3} + 248q^{2/3} + 4124q^{5/3} + 34752q^{8/3} + \ldots$$

is a cube root of the j-function and $\gamma_2(3\tau)$ is a modular function for $\Gamma_0(9)$. These facts combined with Theorem 2.3.4 can be used to show that γ_2 takes algebraic integer values at certain CM points of discriminants not divisble by 3.

We note that there is actually a completely explicit formula for the prime factorization of the number $J(D_1,D_2)$, at least for fundamental discriminants D_1, D_2.

Now we take a look at traces of singular moduli. We begin by summarizing the main results in Zagier's influential paper [114] on the subject, focussing on traces of singular moduli for the j-function.

We begin by defining the functions $f_d(\tau) \in M^{!,+}_{1/2}(\Gamma_0(4))$, where $-d \leq 0$ is a discriminant, by the property

$$f_d(\tau) := q^{-d} + \sum_{\substack{D=1 \\ D\equiv 0,1\ (4)}}^{\infty} A(D,d)q^D \in M^{!,+}_{1/2}(\Gamma_0(4)). \tag{2.7}$$

This condition suffices to determine the functions uniquely and they form a basis of the space $M^{!,+}_{1/2}(\Gamma_0(4))$. Explicitly, we have

$$\begin{aligned}
f_0(\tau) &= 1 + 2q + 2q^4 + 2q^9 + 2q^{16} + O(q^{25}),\\
f_3(\tau) &= q^{-3} - 248q + 26752q^4 - 85995q^5 + 1707264q^8 - 4096248q^9 + O(q^{12}),\\
f_4(\tau) &= q^{-4} + 492q + 143376q^4 + 565760q^5 + 18473000q^8 + 51180012q^9 + O(q^{12}),\\
f_7(\tau) &= q^{-7} - 4119q + 8288256q^4 - 52756480q^5 + 5734772736q^8 + O(q^9),\\
f_8(\tau) &= q^{-8} + 7256q + 26124256q^4 + 190356480q^5 + 29071392966q^8 + O(q^9).
\end{aligned} \tag{2.8}$$

Similarly, we define a basis of the space $M^{!,+}_{3/2}(\Gamma_0(4))$ given by the functions g_D indexed by discriminants $D > 0$, which are determined by the property

$$g_D(\tau) := q^{-D} + \sum_{\substack{d=0 \\ d\equiv 0,3\ (4)}}^{\infty} B(D,d)q^d \in M^{!,+}_{3/2}(\Gamma_0(4)). \tag{2.9}$$

Explicitly, we have

$$\begin{aligned}
g_1(\tau) &= q^{-1} - 2 + 248q^3 - 492q^4 + 4119q^7 - 7256q^8 + 33512q^{11} + O(q^{12}),\\
g_4(\tau) &= q^{-4} - 2 - 26752q^3 - 143376q^4 - 8288256q^7 - 26124256q^8 + O(q^{11}),\\
g_5(\tau) &= q^{-5} + 0 + 85995q^3 - 565760q^4 + 52756480q^7 - 190356480q^8 + O(q^{11}),\\
g_8(\tau) &= q^{-8} + 0 - 1707264q^3 - 18473000q^4 - 5734772736q^7 + O(q^8),\\
g_9(\tau) &= q^{-9} - 2 + 4096248q^3 - 51180012q^4 + 22505066244q^7 + O(q^8).
\end{aligned} \tag{2.10}$$

Looking at the coefficients $A(D,d)$ and $B(D,d)$, one observes that they seem to agree up to sign. This is indeed true in general [114, Theorem 4] and is now usually called *Zagier duality*, a phenomenon which has inspired a flurry of subsequent works generalizing this observation to different contexts (see for instance [17, 30, 39, 51, 66, 93] and the references therein).

Connecting these functions to singular moduli, Zagier shows the following [114, Theorems 1 and 5].

Theorem 2.4.2 (Zagier, 2002). *For an* $\mathrm{SL}_2(\mathbb{Z})$*-invariant function* f *and a discriminant* $D < 0$ *let*

$$\mathrm{Tr}_D(f) = \sum_{Q \in \mathcal{Q}_D / \mathrm{SL}_2(\mathbb{Z})} \frac{1}{w_Q} f(\tau_Q), \tag{2.11}$$

where $w_Q := \#\,\mathrm{Stab}_{\mathrm{SL}_2(\mathbb{Z})}(Q)/2$.

1. *We have for any discriminant* $-d < 0$ *that*

$$B(1,d) = \mathrm{Tr}_{-d}(J).$$

2. *Letting* $B_m(D,d)$ *denote the dth coefficient of the function* $g_D|T_{m^2}$*, where* T_{m^2} *denotes the mth Hecke operator acting on* $M^{!,+}_{3/2}(\Gamma_0(4))$*, we have for any discriminant* $-d < 0$ *and* $m \geq 1$*,*

$$B_m(1,d) = \mathrm{Tr}_{-d}(mJ|T_m).$$

Note that $mJ|T_m$ is the unique modular function for $\mathrm{SL}_2(\mathbb{Z})$ with Fourier expansion $q^{-m} + O(q)$ at ∞ and no poles anywhere else.

Another way to state Theorem 2.4.2 is that the so-called *Zagier lift*, i.e. the map $M^!_0(\mathrm{SL}_2(\mathbb{Z})) \to M^{!,+}_{3/2}(\Gamma_0(4))$ defined through the trace operator Tr in (2.11), is well-defined and Hecke-equivariant. Generalizations of this lift have been studied more systematically in level 1 by Duke and Jenkins [38] and generalized to arbitrary level (but without action of Hecke operators) by Miller and Pixton [83]. The image of the constant function, which in level 1 yields the mock modular Hurwitz class number generating function, has been studied by Funke [55] as a theta lift, which was generalized by Bruinier and Funke [21] to lifts of arbitrary modular functions for the groups $\Gamma_0(N)$, which then map to mock modular forms of weight 3/2.

Theorem 2.4.2 interprets the coefficients $B(m^2,d)$ and therefore by Zagier duality also $A(m^2,d)$ as traces of singular moduli of distinct modular functions. For discriminants $D > 0$ which are not squares, Zagier proves [114, Theorem 6] that we can realize the coefficients $A(D,d)$ as *twisted traces* of singular moduli.

Theorem 2.4.3 (Zagier, 2002). *Let* $D > 0$ *and* $-d < 0$ *be coprime fundamental discriminants and* $\chi = \chi_{D,-d}$ *denote the associated* genus character*, defined on* $\mathcal{Q}_{-Dd}$ *by* $\chi(Q) = \left(\frac{-d}{p}\right)$ *for any prime* $p \nmid Dd$ *which is represented by* Q*. Then we have*

$$A(D,d) = \frac{1}{\sqrt{D}} \sum_{Q \in \mathcal{Q}_{-Dd}/\,\mathrm{SL}_2(\mathbb{Z})} \chi(Q) j(\tau_Q).$$

Later works generalizing this and the results mentioned above include for instance [1, 2, 3, 22], just to name a few.

An important application of Zagier's work, specifically Theorem 2.4.2, is an almost elementary proof of the following result due to Borcherds [9, Theorem 14.1].

Theorem 2.4.4 (Borcherds, 1995). *Let $-d \leq 0$ be a disciminant, then the modular function*

$$\mathscr{H}_d(j(\tau)) = \prod_{Q \in \mathcal{Q}_{-d}/\operatorname{SL}_2(\mathbb{Z})} (j(\tau) - j(\tau_Q))^{1/w_Q}$$

with w_Q as in Theorem 2.4.2 has a product expansion

$$\mathscr{H}_d(j(\tau)) = q^{-H(d)} \prod_{n=1}^{\infty} (1 - q^n)^{A(n^2,d)}.$$

This is the easiest case of the so-called *Borcherds lift* established in [9, 10], which in general enables one to construct automorphic forms on orthogonal groups whose divisors have a special shape.

Bibliography

[1] C. Alfes. Formulas for the coefficients of half-integral weight harmonic Maaß forms. *Math. Z.*, 277(3-4):769–795, 2014.

[2] C. Alfes and S. Ehlen. Twisted traces of CM values of weak Maass forms. *J. Number Theory*, 133(6):1827–1845, 2013.

[3] C. Alfes-Neumann and M. Schwagenscheidt. On a theta lift related to the Shintani lift. *Adv. Math.*, 328:858–889, 2018.

[4] V. Anagiannis, M. C. N. Cheng, and S. M. Harrison. $K3$ elliptic genus and an umbral moonshine module. *Comm. Math. Phys.*, 366(2):647–680, 2019.

[5] V. M. Aricheta. Supersingular elliptic curves and moonshine. *SIGMA Symmetry Integrability Geom. Methods Appl.*, 15:Paper No. 007, 17, 2019.

[6] M. Aschbacher. The status of the classification of the finite simple groups. *Notices Amer. Math. Soc.*, 51(7):736–740, 2004.

[7] B. J. Birch and H. P. F. Swinnerton-Dyer. Notes on elliptic curves. II. *J. Reine Angew. Math.*, 218:79–108, 1965.

[8] R. E. Borcherds. Monstrous moonshine and monstrous Lie superalgebras. *Invent. Math.*, 109(2):405–444, 1992.

[9] R. E. Borcherds. Automorphic forms on $\mathrm{O}_{s+2,2}(\mathbf{R})$ and infinite products. *Invent. Math.*, 120(1):161–213, 1995.

[10] R. E. Borcherds. Automorphic forms with singularities on Grassmannians. *Invent. Math.*, 132(3):491–562, 1998.

[11] R. E. Borcherds. Problems in Moonshine. In *First International Congress of Chinese Mathematicians (Beijing, 1998)*, volume 20 of *AMS/IP Stud. Adv. Math.*, pages 3–10. Amer. Math. Soc., Providence, RI, 2001.

[12] W. Bosma, J. Cannon, and C. Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993).

[13] J. Braun, J. Buck, and J. Girsch. Class invariants for certain non-holomorphic modular functions. *Res. Number Theory*, 1:Art. 21, 13, 2015.

[14] C. Breuil, B. Conrad, F. Diamond, and R. Taylor. On the modularity of elliptic curves over $\mathbf{Q}$: wild 3-adic exercises. *J. Amer. Math. Soc.*, 14(4):843–939, 2001.

[15] K. Bringmann, A. Folsom, K. Ono, and L. Rolen. *Harmonic Maass forms and mock modular forms: theory and applications*, volume 64 of *American Mathematical Society Colloquium Publications*. American Mathematical Society, Providence, RI, 2017.

[16] K. Bringmann and K. Ono. Arithmetic properties of coefficients of half-integral weight Maass-Poincaré series. *Math. Ann.*, 337(3):591–612, 2007.

[17] K. Bringmann and K. Ono. Arithmetic properties of coefficients of half-integral weight Maass-Poincaré series. *Math. Ann.*, 337(3):591–612, 2007.

[18] N. Brisebarre and G. Philibert. Effective lower and upper bounds for the Fourier coefficients of powers of the modular invariant j. *J. Ramanujan Math. Soc.*, 20(4):255–282, 2005.

[19] J. H. Bruinier. *Borcherds products on O(2, l) and Chern classes of Heegner divisors*, volume 1780 of *Lecture Notes in Mathematics*. Springer-Verlag, Berlin, 2002.

[20] J. H. Bruinier and J. Funke. On two geometric theta lifts. *Duke Math. J.*, 1(125):45–90, 2004.

[21] J. H. Bruinier and J. Funke. Traces of CM values of modular functions. *J. Reine Angew. Math.*, 594:1–33, 2006.

[22] J. H. Bruinier and Y. Li. Heegner divisors in generalized Jacobians and traces of singular moduli. *Algebra Number Theory*, 10(6):1277–1300, 2016.

[23] J. H. Bruinier and K. Ono. Algebraic formulas for the coefficients of half-integral weight harmonic weak Maass forms. *Adv. Math.*, 246:198–219, 2013.

[24] J. H. Bruinier, K. Ono, and A. V. Sutherland. Class polynomials for non-holomorphic modular functions. *J. Number Theory*, 161:204–229, 2016.

[25] S. Carnahan. Generalized Moonshine IV: Monstrous Lie algebras. preprint, available at `https://arxiv.org/abs/1208.6254`.

[26] M. C. N. Cheng and J. F. R. Duncan. Meromorphic Jacobi Forms of Half-Integral Index and Umbral Moonshine Modules. preprint, available at `https://arxiv.org/abs/1707.01336`.

[27] M. C. N. Cheng and J. F. R. Duncan. On Rademacher sums, the largest Mathieu group and the holographic modularity of moonshine. *Commun. Number Theory Phys.*, 6(3):697–758, 2012.

[28] M. C. N. Cheng and J. F. R. Duncan. Rademacher Sums and Rademacher Series. In *Conformal Field Theory, Automorphic Forms and Related Topics*, volume 8 of *Contributions in Mathematical and Computational Sciences*, pages 143–182. Springer-Verlag, 2014.

[29] M. C. N. Cheng, J. F. R. Duncan, and J. A. Harvey. Umbral moonshine. *Commun. Number Theory Phys.*, 8(2):101–242, 2014.

[30] B. Cho and Y. Choie. Zagier duality for harmonic weak Maass forms of integral weight. *Proc. Amer. Math. Soc.*, 139(3):787–797, 2011.

[31] H. Cohen and F. Strömberg. *Modular forms*, volume 179 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, 2017. A classical approach.

[32] J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker, and R. A. Wilson. *Atlas of finite groups*. Oxford University Press, Eynsham, 1985. Maximal subgroups and ordinary characters for simple groups, With computational assistance from J. G. Thackray.

[33] J. H. Conway and S. P. Norton. Monstrous moonshine. *Bull. London Math. Soc.*, 11(3):308–339, 1979.

[34] D. A. Cox. *Primes of the form $x^2 + ny^2$*. Pure and Applied Mathematics (Hoboken). John Wiley & Sons, Inc., Hoboken, NJ, second edition, 2013.

[35] A. Dabholkar, S. Murthy, and D. Zagier. Quantum Black Holes, Wall Crossing, and Mock Modular Forms. Cambridge Monographs in Mathematical Physics, to appear.

[36] M. Dewar and M. Ram Murty. A derivation of the Hardy-Ramanujan formula from an arithmetic formula. *Proc. Amer. Math. Soc.*, 141(6):1903–1911, 2013.

[37] W. Duke. Continued fractions and modular functions. *Bull. Amer. Math. Soc. (N.S.)*, 42(2):137–162, 2005.

[38] W. Duke and P. Jenkins. Integral traces of singular values of weak Maass forms. *Algebra Number Theory*, 2(5):573–593, 2008.

[39] W. Duke and P. Jenkins. On the zeros and coefficients of certain weakly holomorphic modular forms. *Pure Appl. Math. Q.*, 4(4, Special Issue: In honor of Jean-Pierre Serre. Part 1):1327–1340, 2008.

[40] J. F. R. Duncan and I. B. Frenkel. Rademacher sums, moonshine and gravity. *Commun. Number Theory Phys.*, 5(4):849–976, 2011.

[41] J. F. R. Duncan, M. J. Griffin, and K. Ono. Moonshine. *Res. Math. Sci.*, 2:Art. 11, 57, 2015.

[42] J. F. R. Duncan, M. J. Griffin, and K. Ono. Proof of the Umbral Moonshine Conjecture. *Research Math. Sci.*, 2(26), 2015.

[43] J. F. R. Duncan and J. A. Harvey. The umbral moonshine module for the unique unimodular Niemeier root system. *Algebra Number Theory*, 11(3):505–535, 2017.

[44] J. F. R. Duncan, M. H. Mertens, and K. Ono. Pariah moonshine. *Nat. Commun.*, 8(670), 2017.

[45] J. F. R. Duncan, M. H. Mertens, and K. Ono. O'Nan moonshine and arithmetic. *Amer. J. Math.*, to appear. preprint available at `https://arxiv.org/abs/1702.03516`.

[46] J. F. R. Duncan and A. O'Desky. Super vertex algebras, meromorphic Jacobi forms and umbral moonshine. *J. Algebra*, 515:389–407, 2018.

[47] J. F. R. Duncan and K. Ono. The Jack Daniels problem. *J. Number Theory*, 161:230–239, 2016.

[48] T. Eguchi, H. Ooguri, and Y. Tachikawa. Notes on the $K3$ Surface and the Mathieu group M_{24}. *Exper. Math.*, 20:91–96, 2011.

[49] L. Euler. Evolutio producti infiniti $(1-x)(1-xx)(1-x^3)(1-x^4)(1-x^5)(1-x^6)$ etc. in seriem simplicem. In *Opera Omnia.*, volume 3 of *1*, pages 472–479. 1780.

[50] A. Folsom and R. Masri. Equidistribution of Heegner points and the partition function. *Math. Ann.*, 348(2):289–317, 2010.

[51] A. Folsom and K. Ono. Duality involving the mock theta function $f(q)$. *J. Lond. Math. Soc. (2)*, 77(2):320–334, 2008.

[52] D Ford, J. McKay, and S. Norton. More on replicable functions. *Comm. Algebra*, 22(13):5175–5193, 1994.

[53] I. Frenkel, J. Lepowsky, and A. Meurman. A natural representation of the Fischer-Griess monster with the modular function J as character. *Proc. Nat. Acad. Sci. U.S.A.*, 81(10):3256–3260, 1984.

[54] I. Frenkel, J. Lepowsky, and A. Meurman. *Vertex operator algebras and the Monster*, volume 134 of *Pure and Applied Mathematics*. Academic Press, Inc., Boston, MA, 1988.

[55] J. Funke. Heegner divisors and nonholomorphic modular forms. *Compositio Math.*, 133(3):289–321, 2002.

[56] T. Gannon. *Moonshine beyond the Monster*. Cambridge Monographs on Mathematical Physics. Cambridge University Press, Cambridge, 2006. The bridge connecting algebra, modular forms and physics.

[57] T. Gannon. Much ado about Mathieu. *Adv. Math.*, 301:322–358, 2016.

[58] T. Gannon. A pariah finds a home. *Nature*, 550:191–192, 2017.

[59] The GAP Group. *GAP – Groups, Algorithms, and Programming, Version 4.10.2*, 2019.

[60] A. Gel'fond. Sur le septième problème de Hilbert. *Bulletin de l'Académie des Sciences de l'URSS. Classe des sciences mathématiques et na.*, (4):623–634, 1934.

[61] R. L. Griess, Jr. The friendly giant. *Invent. Math.*, 69(1):1–102, 1982.

[62] M. J. Griffin and M. H. Mertens. A proof of the Thompson Moonshine Conjecture. *Research Math. Sci.*, 3(36), 2016.

[63] B. H. Gross and D. B. Zagier. On singular moduli. *J. Reine Angew. Math.*, 355:191–220, 1985.

[64] B. H. Gross and D. B. Zagier. Heegner points and derivatives of L-series. *Invent. Math.*, 84:225–320, 1986.

[65] The PARI Group. *User's Guide to Pari/Gp (version 2.11.1)*, 2018. available at `https://pari.math.u-bordeaux.fr/pub/pari/manuals/2.11.1/users.pdf`.

[66] P. Guerzhoy. On weak harmonic Maass-modular grids of even integral weights. *Math. Res. Lett.*, 16(1):59–65, 2009.

[67] G. H. Hardy. *Ramanujan. Twelve lectures on subjects suggested by his life and work.* Chelsea Publishing Company, New York, 3rd (corrected) edition, 1978.

[68] G. H. Hardy and S. Ramanujan. Asymptotic formulae in combinatory analysis. *Proc. London Math. Soc.*, 17(2):75–115, 1918.

[69] J. A. Harvey and B. C. Rayhaun. Traces of Singular Moduli and Moonshine for the Thompson Group. *Commun. Number Theory Phys.*, 10(1):23–62, 2016.

[70] E. Hecke. *Zur Theorie der Modulfunktionen von zwei Variablen und ihrer Anwendung auf die Zahlentheorie.* PhD thesis, Georg-August-Universität Göttingen, 1910.

[71] C. Hermite. Sur la théorie des équations modulaires. In É. Picard, editor, *Œuvres de Charles Hermite*, volume 2, pages 38–82. Cambridge university Press, reprint of the 1908 original edition, 2009.

[72] D. Hilbert. Ein neuer Beweis des Kroneckerschen Fundamentalsatzes über Abelsche Zahlkörper. *Nachrichten der Gesellschaft der Wissenschaften zu Göttingen*, pages 29–39, 1896. in D. Hilbert, Gesammelte Abhandlungen, vol. I, Springer-Verlag, 2nd ed. (1970), pp. 53–62.

[73] Ö. Imamoğlu, M. Raum, and O. Richter. Holomorphic projections and Ramanujan's mock theta functions. *Proc. Nat. Acad. Sci. U.S.A.*, 111(11):3961–3967, 2014.

[74] F. Klein. Weitere Untersuchungen über des Ikosaeder. *Math. Ann.*, 12(4):503–560, 1877.

[75] F. Klein. Über die Transformation der elliptischen Functionen und die Auflösung der Gleichungen fünften Grades. *Math. Ann.*, 14:111–172, 1878.

[76] W. Kohnen. Fourier coefficients of modular forms of half-integral weight. *Math. Ann.*, 271(2):237–268, 1985.

[77] V. A. Kolyvagin. Finiteness of $E(\mathbf{Q})$ and $\mathrm{CH}(E,\mathbf{Q})$ for a subclass of Weil curves. *Izv. Akad. Nauk SSSR Ser. Mat.*, 52(3):522–540, 670–671, 1988.

[78] L. Kronecker. Über die algebraisch auflösbaren Gleichungen (I. Abhandlung. *Monatsberichte der Kgl. Preuss. Akad. Wiss. Berlin*, pages 365–374, 1853. in L. Kronecker (ed. K. Hensel), Mathematische Werke, vol. 4, Chelsea Publishing (Reprint) (1968), p. 1–12.

[79] E. Larson and L. Rolen. Integrality properties of the CM-values of certain weak Maass forms. *Forum Math.*, 27(2):961–972, 2015.

[80] D. Masser. *Elliptic functions and transcendence.* Lecture Notes in Mathematics, Vol. 437. Springer-Verlag, Berlin-New York, 1975.

[81] M. H. Mertens. Eichler-Selberg Type Identities for Mixed Mock Modular Forms. *Adv. Math.*, 301:359–382, 2016.

[82] M. H. Mertens and L. Rolen. On class invariants for non-holomorphic modular functions and a question of Bruinier and Ono. *Res. Number Theory*, 1(4):13 pp., 2015.

[83] A. Miller and A. Pixton. Arithmetic traces of non-holomorphic modular invariants. *Int. J. Number Theory*, 6(1):69–87, 2010.

[84] D. Niebur. A class of nonanalytic automorphic functions. *Nagoya Math. J.*, 52:133–145, 1973.

[85] S. P. Norton. More on moonshine. In *Computational group theory (Durham, 1982)*, pages 185–193. Academic Press, London, 1984.

[86] A. P. Ogg. Automorphismes de courbes modulaires. In *Séminaire Delange-PisotPoitou (16e année: 1974/75), Théorie des nombres, Fasc. 1, Exp. No. 7*, page 8. 1975.

[87] M. E. O'Nan. Some evidence for the existence of a new simple group. *Proc. London Math. Soc. (3)*, 32(3):421–479, 1976.

[88] K. Ono. Unearthing the visions of a master: harmonic Maass forms and number theory. In *Current developments in mathematics, 2008*, pages 347–454. Int. Press, Somerville, MA, 2009.

[89] W. de Azevedo Pribitkin and B. Williams. Short proof of Rademacher's formula for partitions. *Res. Number Theory*, 5(2):Art. 17, 6, 2019.

[90] H. Rademacher. On the Partition Function $p(n)$. *Proc. London Math. Soc. (2)*, 43(4):241–254, 1937.

[91] H. Rademacher. The Fourier Coefficients of the Modular Invariant $J(\tau)$. *Amer. J. Math.*, 60(2):501–512, 1938.

[92] H. Rademacher and E. Grosswald. *Dedekind sums.* The Mathematical Association of America, Washington, D.C., 1972. The Carus Mathematical Monographs, No. 16.

[93] J. Rouse. Zagier duality for the exponents of Borcherds products for Hilbert modular forms. *J. London Math. Soc. (2)*, 73(2):339–354, 2006.

[94] R. Schertz. Weber's class invariants revisited. *J. Théor. Nombres Bordeaux*, 14(1):325–343, 2002.

[95] T. Schneider. Transzendenzuntersuchungen periodischer Funktionen I. Transzendenz von Potenzen. *J. Reine Angew. Math.*, 172:65–69, 1935.

[96] G. Shimura. Construction of class fields and zeta functions of algebraic curves. *Ann. of Math. (2)*, 85:58–159, 1967.

[97] G. Shimura. Modular Forms of Half Integral Weight. *Ann. of Math. (2)*, 97(3):440–481, 1973.

[98] G. Shimura and Y. Taniyama. *Complex multiplication of abelian varieties and its applications to number theory*, volume 6 of *Publications of the Mathematical Society of Japan.* The Mathematical Society of Japan, Tokyo, 1961.

[99] J. H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics.* Springer, Dordrecht, second edition, 2009.

[100] C. Skinner. Multiplicative reduction and the cyclotomic main conjecture for GL_2. *Pacific J. Math.*, 283(1):171–200, 2016.

[101] C. Skinner and E. Urban. The Iwasawa main conjectures for GL_2. *Invent. Math.*, 195(1):1–277, 2014.

[102] P. E. Smith. A simple subgroup of $M?$ and $E_8(3)$. *Bull. London Math. Soc.*, 8(2):161–165, 1976.

[103] S. D. Smith. On the head characters of the Monster simple group. In *Finite groups—coming of age (Montreal, Que., 1982)*, volume 45 of *Contemp. Math.*, pages 303–313. Amer. Math. Soc., Providence, RI, 1985.

[104] W. A. Stein et al. *Sage Mathematics Software (Version 8.8).* The Sage Development Team, 2019. `http://www.sagemath.org`.

[105] R. Taylor and A. Wiles. Ring-theoretic properties of certain Hecke algebras. *Ann. of Math. (2)*, 141(3):553–572, 1995.

[106] J. G. Thompson. A conjugacy theorem for E_8. *J. Algebra*, 38(2):525–530, 1976.

[107] J. G. Thompson. Finite groups and modular functions. *Bull. London Math. Soc.*, 11(3):347–351, 1979.

[108] J. G. Thompson. Some numerology between the Fischer-Griess Monster and the elliptic modular function. *Bull. London Math. Soc.*, 11(3):352–353, 1979.

[109] S. G. Vlăduţ. *Kronecker's Jugendtraum and modular functions*, volume 2 of *Studies in the Development of Modern Mathematics*. Gordon and Breach Science Publishers, New York, 1991. Translated from the Russian by M. Tsfasman.

[110] J.-L. Waldspurger. Sur les coefficients de Fourier des formes modulaires de poids demi-entier. *J. Math. Pures Appl. (9)*, 60(4):375–484, 1981.

[111] H. Weber. Theorie der Abel'schen Zahlkörper. *Acta Math.*, 8:193–263, 1886.

[112] A. Wiles. Modular elliptic curves and Fermat's last theorem. *Ann. of Math. (2)*, 141(3):443–551, 1995.

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

[114] D. Zagier. Traces of singular moduli. In *Motives, polylogarithms and Hodge theory, Part I (Irvine, CA, 1998)*, volume 3 of *Int. Press Lect. Ser.*, pages 211–244. Int. Press, Somerville, MA, 2002.

[115] D. Zagier. Elliptic modular forms and their applications. In *The 1-2-3 of modular forms*, Universitext, pages 1–103. Springer, Berlin, 2008.

Appendix A

On class invariants for non-holomorphicmodular functions and a question of Bruinier and Ono

See [82].

Appendix B

A proof of the Thompson Moonshine conjecture

See [62].

Appendix C

O'Nan Moonshine and Arithmetic

See [45].