Bucknell University
Bucknell Digital Commons

Honors Theses

Student Theses

Spring 2012

# Verifying Harder's Conjecture for Classical and Siegel Modular Forms

David Sulon
*Bucknell University*, dws031@bucknell.edu

Follow this and additional works at: https://digitalcommons.bucknell.edu/honors_theses

Part of the Logic and Foundations Commons

Recommended Citation
Sulon, David, "Verifying Harder's Conjecture for Classical and Siegel Modular Forms" (2012). *Honors Theses*. 98.
https://digitalcommons.bucknell.edu/honors_theses/98

This Honors Thesis is brought to you for free and open access by the Student Theses at Bucknell Digital Commons. It has been accepted for inclusion in Honors Theses by an authorized administrator of Bucknell Digital Commons. For more information, please contact dcadmin@bucknell.edu.

# VERIFYING HARDER'S CONJECTURE FOR CLASSICAL AND SIEGEL MODULAR FORMS

by

David Sulon

A Thesis
Presented to the Faculty of
Bucknell University
in Partial Fulfillment of the Requirements for the Degree of
Bachelor of Science with Honors in Mathematics
May 4, 2012

Approved: ______________________________
Nathan C. Ryan
Thesis Advisor

______________________________
Karl Voss
Chair, Department of Mathematics

## Acknowledgments

I would like to thank Nathan, my research and thesis advisor, for his incredible amount of help and collaboration with this project. From his advising during our initial work in the summer of 2011 to his careful reading and critiquing of numerous drafts of this text, his help has been integral to the completion of this thesis.

I would also like to thank the Bucknell Program for Undergraduate Research and the Bucknell Mathematics Department for supporting this project in the summer of 2011, and as it later grew into a thesis.

# Contents

# List of Tables

# Abstract

A conjecture by Harder shows a surprising congruence between the coefficients of "classical" modular forms and the Hecke eigenvalues of corresponding Siegel modular forms, contigent upon "large primes" dividing the critical values of the given classical modular form.

Harder's Conjecture has already been verified for one-dimensional spaces of classical and Siegel modular forms (along with some two-dimensional cases), and for primes $p \leq 37$. We verify the conjecture for higher-dimensional spaces, and up to a comparable prime $p$.

# Chapter 1

# Introduction

## 1.1 Motivation

Mathematics is often thought of as mechanistic and predictable - this, however, is not the case at all. Results in mathematics can, in fact, be quite surprising (even to mathematicians). Our story of Harder's Conjecture begins with a particularly surprising mathematician - Srinivasa Ramanujan.

Born to a poor family in Erode, India in 1887, Ramanujan worked largely independently until he was "discovered" by G.H. Hardy in 1913. He discovered many results independently (most of which have been proven correct to date). One of which regards the function $\Delta$:

$$\Delta(q) = q\prod_{n=0}^{\infty}(1-q^n)^{24}. \tag{1.1}$$

When expanded, $\Delta$ has coefficients

$$\Delta(q) = q - 24q^2 + 252q^3 - 1472q^4 + 4830q^5 - 6048q^6 - 16744q^7 + 84480q^8 + \dots, \tag{1.2}$$

which we can write as the sum

$$\sum_{n=1}^{\infty} \tau(n) q^n, \tag{1.3}$$

where $\tau(n)$ is the coefficient of the $q^n$ term of $\Delta$ (e.g. $\tau(1) = 1$, $\tau(4) = -1472$). We list the first 25 values of $\tau(n)$ in Table 1.1:

| $n$ | $\tau(n)$ |
|---|---:|
| 1 | 1 |
| 2 | -24 |
| 3 | 252 |
| 4 | -1472 |
| 5 | 4830 |
| 6 | -6048 |
| 7 | -16744 |
| 8 | 84480 |
| 9 | -113643 |
| 10 | -115920 |
| 11 | 534612 |
| 12 | -370944 |
| 13 | -577738 |
| 14 | 401856 |
| 15 | 1217160 |
| 16 | 987136 |
| 17 | -6905934 |
| 18 | 2727432 |
| 19 | 10661420 |
| 20 | -7109760 |
| 21 | -4219488 |
| 22 | -12830688 |
| 23 | 18643272 |
| 24 | 21288960 |
| 25 | -25499225 |

**Table 1.1:** The first 25 coefficients of $\Delta$.

At first glance, the values for $\tau(n)$ appear to be completely random, unrelated integers (yet their absolute value does appear to increase). Suppose, however, that we try to multiply them together:

$$\tau(2) \cdot \tau(3) = -24 \cdot -252 = -6048 \tag{1.4}$$

But, that's $\tau(6)$! Could it be that $\tau(m) \cdot \tau(n) = \tau(m \cdot n)$? Ramanujan conjectured (later, Louis Mordell proved) that for relatively prime $m, n$ (i.e. the greatest common divisor of $m$ and $n$ is 1), this is true:

**Surprising Result 1.1.1.** Let $m, n$ be positive integers. If $m, n$ are relatively prime, then $\tau(m) \cdot \tau(n) = \tau(m \cdot n)$. [3]

(We say that, given this above property, $\tau$ is a *multiplicative* function.)

Ramanujan found another, equally surprising relationship between the coefficents $\tau(n)$. Suppose we consider coefficents $\tau(p)$ for primes $p$, and the quantity $p^{11} + 1$. Ramanujan found that, if divided by 691, both $\tau(p)$ and $p^{11} + 1$ yield the same remainder!

| $p$ | $\tau(p)$ | $\tau(p) \mod 691$ | $p^{11}+1$ | $(p^{11}+1) \mod 691$ |
|---|---|---|---|---|
| 2 | -24 | 667 | 2049 | 667 |
| 3 | 252 | 252 | 177148 | 252 |
| 5 | 4830 | 684 | 48828126 | 684 |
| 7 | -16744 | 531 | 1977326744 | 531 |
| 11 | 534612 | 469 | 285311670612 | 469 |
| 13 | -577738 | 629 | 1792160394038 | 629 |
| 17 | -6905934 | 611 | 34271896307634 | 611 |
| 19 | 10661420 | 672 | 116490258898220 | 672 |
| 23 | 18643272 | 92 | 952809757913928 | 92 |
| 29 | 128406630 | 173 | 12200509765705830 | 173 |
| 31 | -52843168 | 366 | 25408476896404832 | 366 |
| 37 | -182213314 | 622 | 177917621779460414 | 622 |
| 41 | 308120442 | 87 | 550329031716248442 | 87 |
| 43 | -17125708 | 36 | 929293739471222708 | 36 |
| 47 | 2687348496 | 435 | 2472159215084012304 | 435 |

**Table 1.2:** $\tau(p) \mod 691$ and $(p^{11}+1) \mod 691$ for primes $p$.

G.N. Watson proved this relationship:

**Surprising Result 1.1.2.** Let $p$ be a prime. Then,

$$\tau(p) \equiv p^{11} + 1 \pmod{691} \tag{1.5}$$

[3]

Later, Mordell proved that $\Delta$ is a modular form (see Section 1.4). However, the study of $\Delta$ (and modular forms in general) became somewhat dormant following this. The last fifty years, however, have shown a resurgence of interest in modular forms. Since this resurgence, the general theory of modular forms (including the theory of $L$-functions and periods; see Section 2.2) has been greatly expanded upon. There has been considerable interest in modular forms in recent years; for example, Wiles/Taylor's proof of Fermat's Last Theorem relied heavily on the intimate relationship between modular forms and elliptic curves. They, in fact, proved this relationship, thus implying Fermat's Last Theorem.

Also, two of the seven Clay Mathematics Institute's Millenial Prize Problems (each of which include a $1,000,000 prize for a proof/solution) are related to modular forms and $L$-functions (i.e. the BSD Conjecture and the Riemann Hypothesis). In addition, a large number of Fields Medals have been awarded to mathematicians whose work regarded modular forms.

The original ideas behind modular forms have also been generalized in the past fifty years; for example, Siegel modular forms (see Section 1.5) represent a generalization of modular forms themselves. We can also generalize the congruence in (1.5):

**Surprising Result 1.1.3.** The congruence in (1.5) can actually be thought of as a congruence between modular forms.

But, we can generalize further:

**Surprising Result 1.1.4.** There exist analogous congruences between "classical" and Siegel modular forms.

In very general terms, this is the main idea of Harder's Conjecture.

## 1.2 The Conjecture

We will state Harder's Conjecture in full at this point, even though very little of its specifics have yet been explained (this is largely the purpose of the introduction to this thesis):

**Harder's Conjecture.** *Let $f = \sum_{n=1}^{\infty} a_n q^n \in S_r$ be a normalized eigenform with field of Fourier coefficients $\mathbb{Q}_f$. If a large prime $\ell$ of $\mathbb{Q}_f$ divides a critical value $\Lambda(f,t)$ then there exists a Siegel modular form $F \in S_{k,j}$ with $j = 2t - r - 2$ and $k = r - t + 2$ that is an eigenform with eigenvalue $\lambda_p$ for $T_p$, with field $\mathbb{Q}_F$ of eigenvalues $\lambda_p$ and such that there exists a prime $\ell'$ of the compositum of $\mathbb{Q}_F$ and $\mathbb{Q}_f$ dividing $\ell$ for which*

$$\lambda_p \equiv p^{k-2} + a_p + p^{j+k-1} \pmod{\ell'} \tag{1.6}$$

*for all primes $p \in \mathbb{Q}$.*

We can see, though, a similarity in the form of the congruence in (1.6) to the congruences that Ramanujan found. The concepts and notation of Harder's Conjecture, however, require much more explanation. We will start with a brief overview of necessary number theoretic background, and conclude the section with a discussion of the LLL Algorithm and algebraic dependence (which is specifically used in Section 2.3). We will then provide an introduction to the necessary theory of "classical" and Siegel modular forms.

Chapters 2 and 3 will discuss the specific calculations needed to verify Harder's Conjecture; i.e. the computations of the critical values of classical modular forms and the Hecke eigenvalues of spaces of Siegel modular forms.

Finally, we will discuss the actual verification of the Harder's Conjecture in Chapter 4.

## 1.3 Number Theoretic Background

At the heart of elementary number theory lies the notion of division:

**Definition 1.3.1.** Let $m, n \in \mathbb{N}$. If there exists a positive integer $l$ such that $lm = n$, then we say *m divides n*. We denote this as $m \mid n$.

**Remark 1.3.2.** We call $l$ and $m$ *divisors* of $n$.

We then define a *prime number*:

**Definition 1.3.3.** Let $n \in \mathbb{N}$. If $n$ has exactly two divisors (namely 1 and $n$ itself), we call $n$ *prime.*

In general, prime numbers act as "building blocks" of the integers $\mathbb{Z}$. Any number in $\mathbb{Z}$ can be written as a product of prime numbers. Moreover, this factorization is unique:

**Theorem 1.3.4** (Fundamental Theorem of Arithmetic)**.** *Let $n \in \mathbb{Z}$, then $n$ can be written uniquely as the product of positive integer powers $\delta_i$ of primes ${p_1}^{\delta_1}, \ldots, {p_i}^{\delta_i}$:*

$$n = \prod_{j=1}^{i} {p_j}^{\delta_j} \tag{1.7}$$

In the next section, we will see that the idea of prime numbers can be extended to other fields.

### 1.3.1 Basic Algebraic Number Thoery

Throughout this section, let $\mathbb{F} \in \mathbb{C}$ be a field. We first define what it means for a number to be algebraic:

**Definition 1.3.5.** Let $\alpha \in \mathbb{C}$. If $\alpha$ is the root of some irreducible, monic polynomial

$$f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0 \tag{1.8}$$

where each $a_i \in \mathbb{Q}$, then we say that $\alpha$ is an *algebraic number.*

**Definition 1.3.6.** We say that the irreducible, monic polynomial (1.8) *defines* $\alpha$, and that the *degree* of $\alpha$ is equal to the degree of (1.8).

**Remark 1.3.7.** We call the irreducible, monic polynomial which defines $\alpha$ the *minimal* polynomial of $\alpha$.

Also, we can define the *norm* of an algebraic number:

**Definition 1.3.8.** Let $\alpha_1$ be an algebraic number whose minimal polynomial $f$ has $n$ roots, each denoted $\alpha_i$ with $1 < i \leq n$. We define the *norm* of $\alpha_1$ $N(\alpha_1)$ as

$$N(\alpha_1) = \prod_{i=1}^{n} \alpha_i \tag{1.9}$$

We can adjoin an algebraic number $\alpha$ to a field $\mathbb{F}$:

**Definition 1.3.9.** Let $\alpha$ be an algebraic number, and let $\mathbb{F}$ be a field. Let $\mathbb{F}(\alpha)$ be the smallest field containing both $\mathbb{F}$ and $\alpha$. We call $\mathbb{F}(\alpha)$ a *simple extension* of $\mathbb{F}$ by $\alpha$.

**Example 1.3.10.** Consider the algebraic number $i = \sqrt{-1}$ (it is the root of the polynomial $f(x) = x^2 + 1$). We can see that $\mathbb{Q}(i) \subseteq \mathbb{C}$ is the field of numbers of the form $a + bi$, where $a, b \in \mathbb{Q}$.

**Remark 1.3.11.** We can see that, if $\alpha \in \mathbb{F}$, then $\mathbb{F}(\alpha)$ is a trivial extension, and $\mathbb{F}(\alpha) = \mathbb{F}$.

We can extend a field by multiple algebraic numbers:

**Definition 1.3.12.** Let $\{\alpha_1, \ldots, \alpha_i\}$ be a finite set of algebraic numbers, and let $\mathbb{F}$ be a field. Let $\mathbb{F}(\alpha_1, \ldots, \alpha_i)$ is the smallest field containing both $\mathbb{F}$ and $\{\alpha_1, \ldots, \alpha_i\}$. $\mathbb{F}(\alpha_1, \ldots, \alpha_i)$ is called a *finite extension* of $\mathbb{F}$.

However, there is an important theorem that allows us to simplify finite extensions into simple extensions:

**Theorem 1.3.13** ([7])**.** *Every finite extension of a field $\mathbb{F}$ is a simple extension. That is, given any finite extension $\mathbb{F}(\alpha_1, \ldots, \alpha_i)$, there exists an algebraic number $\alpha$ such that $\mathbb{F}(\alpha) = \mathbb{F}(\alpha_1, \ldots, \alpha_i)$.*

**Definition 1.3.14.** We call a finite extension of $\mathbb{Q}$ a *number field.*

**Definition 1.3.15.** Let $\alpha$ have degree $\delta$. The *degree* of the extension $\mathbb{Q}(\alpha)$ of $\mathbb{Q}$ (which we denote $[\mathbb{Q}(\alpha) : \mathbb{Q}]$) is $\delta$.

**Example 1.3.16.** Let $\alpha = \sqrt{2}$. The irreducible polynomial defining $\alpha$, which is $x^2 - 2$, has degree 2; thus, $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$.

**Definition 1.3.17.** We call a degree 2 extension (as in Example 1.3.16) a *quadratic extension.*

As one might recall, $\mathbb{Z}$ is a ring and $\mathbb{Z} \subseteq \mathbb{Q}$; here, $\mathbb{Z}$ is called the ring of rational integers. We can generalize this notion for any field:

**Definition 1.3.18.** Let $\alpha$ be an algebraic number. If $\alpha$ is the root of some irreducible, monic polynomial of the form

$$f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0 \tag{1.10}$$

where each $a_i \in \mathbb{Z}$, then $\alpha$ is an *algebraic integer.*

**Theorem 1.3.19.** *If $\alpha$ is an algebraic integer, then $N(\alpha) \in \mathbb{Z}$.*

There exists a special kind of algebraic integer, called a *unit*:

**Definition 1.3.20.** Let $\alpha$ be an algebraic integer. If its multiplicative inverse $\alpha^{-1}$ is also an algebraic integer, then $\alpha$ is called a *unit.*

**Example 1.3.21.** Both $i$ and $3-2\sqrt{2}$ are units, in $\mathbb{Q}(i)$ and $\mathbb{Q}(\sqrt{2})$, respectively. [7]

**Theorem 1.3.22.** *If $\alpha$ is a unit, then $N(\alpha) = 1$.*

**Definition 1.3.23.** Given a field $\mathbb{F}$, we denote the set of its algebraic integers as $\mathcal{O}_{\mathbb{F}}$.

**Example 1.3.24.** We can show that $\mathcal{O}_{\mathbb{Q}} = \mathbb{Z}$:

*Proof.* We can see that $n \in \mathbb{Z}$ is the root of the polynomial $f(x) = x - n$; thus, $n \in \mathcal{O}_{\mathbb{Q}}$.

Now, let $m \in \mathcal{O}_{\mathbb{Q}}$ be arbitrary. Thus, $m$ is the root of some irreducible monic polynomial $g$ with coefficients in $\mathbb{Z}$. Since $g$ is irreducible over $\mathbb{Q}$, this implies that $g(x) = x - m$. Thus, since the coefficients of $g$ are in $\mathbb{Z}$, this implies that $m \in \mathbb{Z}$. □

**Example 1.3.25.** For $\mathbb{Q}(i)$, $\mathcal{O}_{\mathbb{Q}(i)} = \{a+bi : a, b \in \mathbb{Z}\}$ (These are called the *Gaussian* integers $\mathbb{Z}[i]$).

We can see that the set of algebraic integers have a certain algebraic structure:

**Theorem 1.3.26** ([7])**.** *Given a field $\mathbb{F}$, the set $\mathcal{O}_{\mathbb{F}}$ forms a ring.*

**Definition 1.3.27.** Let $R$ be a ring, and $\mathfrak{A} \subseteq R$. $\mathfrak{A}$ is called an *ideal* of $R$ if:

(i) Given $a, b \in \mathfrak{A}$, $a + b \in \mathfrak{A}$.

(ii) Given $a \in \mathfrak{A}$ and $r \in R$, $ar \in \mathfrak{A}$.

We can generate ideals from algebraic integers:

**Theorem 1.3.28.** *Let $\alpha_1, \ldots, \alpha_n \in \mathcal{O}_{\mathbb{F}}$ for some field $\mathbb{F}$. The set $\mathfrak{A} \subseteq \mathcal{O}_{\mathbb{F}}$ of elements of the form*

$$\eta_1\alpha_1 + \cdots + \eta_n\alpha_n, \tag{1.11}$$

*where each $\eta_i \in \mathcal{O}_{\mathbb{F}}$, is an ideal of $\mathcal{O}_{\mathbb{F}}$.*

**Definition 1.3.29.** We say that the ideal $\mathfrak{A}$ of Theorem 1.3.28 is *generated* by $\alpha_1, \ldots, \alpha_n$; we use the notation $\mathfrak{A} = (\alpha_1, \ldots, \alpha_n)$.

**Definition 1.3.30.** An ideal $[\alpha]$ generated by a single algebraic integer $\alpha$ is called a *principal ideal.* [7]

**Definition 1.3.31.** Let $\mathbb{F}$ be a field with multiplicative identity 1. The principal ideal (1), denoted $\mathfrak{O}$, is called the *unit ideal* of $\mathbb{F}$.

**Remark 1.3.32.** One can see that $\mathfrak{O} = \mathcal{O}_{\mathbb{F}}$.

We can then define the product of two ideals:

**Definition 1.3.33.** Let $\mathfrak{A} = (\alpha_1, \ldots, \alpha_m)$ and $\mathfrak{B} = (\beta_1, \ldots, \beta_n)$ Let

$$\mathfrak{A} \cdot \mathfrak{B} = (\alpha_1\beta_1, \ldots, \alpha_1\beta_n, \ldots, \alpha_2\beta_1, \ldots, \alpha_2\beta_n, \ldots, \alpha_m\beta_n) \tag{1.12}$$

We can show that this product is commutative:

**Theorem 1.3.34.** *Let $\mathfrak{A}, \mathfrak{B}$ be ideals. Then, $\mathfrak{A} \cdot \mathfrak{B} = \mathfrak{B} \cdot \mathfrak{A}$.*

Then, we can generalize the idea of divisibility for ideals:

**Definition 1.3.35.** Let $\mathfrak{A}, \mathfrak{B}$ be ideals. If there exists an ideal $\mathfrak{C}$ such that $\mathfrak{A} = \mathfrak{B} \cdot \mathfrak{C}$, then we say $\mathfrak{B}$ *divides* $\mathfrak{A}$, and we write $\mathfrak{B} \mid \mathfrak{A}$. We call $\mathfrak{B}$ and $\mathfrak{C}$ the *divisors* of $\mathfrak{A}$. [7]

We introduce the following theorem [7]:

**Theorem 1.3.36.** *Let $\mathbb{F}$ be a field, and let $\mathfrak{A}$ be an ideal of $\mathbb{F}$. Then, there exists an ideal $\mathfrak{B} \subseteq \mathbb{F}$ and a natural number $a$ such that $\mathfrak{A} \cdot \mathfrak{B} = (a)$.*

The above notion of divisibility can be difficult to check through our definition of the product of ideals given in Definition 1.3.33. Fortunately, there exists an easier way to check divisibility of ideals:

**Theorem 1.3.37.** *Let $\mathfrak{A}, \mathfrak{B}$ be ideals of field $\mathbb{F}$. $\mathfrak{B} \mid \mathfrak{A}$ if and only if $\mathfrak{A} \subseteq \mathfrak{B}$.*

*Proof.* (i) Let $\mathfrak{B} \mid \mathfrak{A}$. Then, there exists $\mathfrak{C}$ such that $\mathfrak{A} = \mathfrak{B} \cdot \mathfrak{C}$. Let $\mathfrak{B} = (\beta_1, \dots, \beta_m)$ and $\mathfrak{C} = (\gamma_1, \dots, \gamma_n)$. We know each $\alpha \in \mathfrak{A}$ can be written as the sum

$$\alpha = \sum_{i=1}^{\infty} \sum_{j=1}^{\infty} \eta_{i,j} \beta_i \gamma_j, \tag{1.13}$$

where each $\eta_{i,j} \in \mathcal{O}_{\mathbb{F}}$. This sum is equivalent to

$$\alpha = \sum_{i=1}^{\infty} \left( \sum_{j=1}^{\infty} \eta_{i,j} \gamma_j \right) \beta_i, \tag{1.14}$$

and since each $\eta_{i,j}\gamma_j \in \mathcal{O}_{\mathbb{F}}$, we know $\alpha \in \mathfrak{B}$.

(ii) Now, let $\mathfrak{A} \subseteq \mathfrak{B}$. Using Theorem 1.3.36, we let $\mathfrak{C}$ and $b$ be such that $\mathfrak{C} \cdot \mathfrak{A} = (b)$. We can see that the ideal $\mathfrak{C} \cdot \mathfrak{A}$ is a subset of $(b) = \mathfrak{B} \cdot \mathfrak{C}$. Thus, we can write $\mathfrak{C} \cdot \mathfrak{A}$ as

$$(b\alpha_1, \dots, b\alpha_m) = (b)(\alpha_1, \dots, \alpha_m) = \mathfrak{B} \cdot \mathfrak{C} \cdot (\alpha_1, \dots, \alpha_m). \tag{1.15}$$

Thus, $\mathfrak{A} = \mathfrak{B} \cdot (\alpha_1, \dots, \alpha_m)$, and we have $\mathfrak{B} \mid \mathfrak{A}$.

□

**Example 1.3.38.** Consider $\mathbb{Z}$, and the ideals (3) and (6). We can see that $(3) = \{z \in \mathbb{Z} : 3 \mid z\}$, and that $(6) = \{z \in \mathbb{Z} : 6 \mid z\}$. Any element divisible by 6 must also be divisible by 3; thus, $(6) \subseteq (3)$. Also, $(6) = (3) \cdot (2)$.

Thus, the question of divisibility of ideals simply becomes a question of set-containment - Theorem 1.3.37 can be summarized as "to contain is to divide". As one might expect, this leads to a definition of "primeness" for ideals:

**Definition 1.3.39.** Let $\mathfrak{P}$ be an ideal with only two divisors, namely $\mathfrak{O}$ and $\mathfrak{P}$ itself. We call $\mathfrak{P}$ a *prime ideal.*

Alternatively, we can show the following:

**Theorem 1.3.40.** *Let $\mathfrak{P}$ be an ideal of a ring $R$. This ideal $\mathfrak{P}$ is prime if and only if the following are true:*

*(i) $\mathfrak{P} \neq R$.*

*(ii) Given $a, b \in R$ such that their product $ab \in \mathfrak{P}$, either $a \in \mathfrak{P}$ or $b \in \mathfrak{P}$.*

The following theorem holds for prime ideals:

**Theorem 1.3.41.** (Fundamental Theorem for Ideals) *Let $\mathfrak{A} \neq \mathfrak{O}$ be an ideal. Then $\mathfrak{A}$ can be uniquely expressed as the product of prime ideals:*

$$\mathfrak{A} = \mathfrak{P}_1 \cdot \mathfrak{P}_2 \cdot \cdots \cdot \mathfrak{P}_n, \tag{1.16}$$

*with multiplicity.*

We can then generalize the notion of "prime number" for fields other than $\mathbb{Q}$:

**Theorem 1.3.42.** *Let $\mathbb{F}$ be a field, and let $\mathcal{O}_{\mathbb{F}}$ be its ring of integers, with $m, n \in \mathcal{O}_{\mathbb{F}}$. If $(m) \mid (n)$, then $m \mid n$.*

**Definition 1.3.43.** Let $\mathbb{F}$ be a field, and let $\mathcal{O}_{\mathbb{F}}$ be its ring of integers. A positive integer $n \in \mathcal{O}_{\mathbb{F}}$ is *prime* if ideal $(n)$ of $\mathcal{O}_{\mathbb{F}}$ is a prime ideal.

**Example 1.3.44.** Consider $\mathbb{Q}$, and its ring of integers $\mathbb{Z}$. We know that $3\mathbb{Z}$ is an ideal of $\mathbb{Z}$, generated by 3. Also, $3\mathbb{Z}$ can be written alternatively as $\{z \in \mathbb{Z} : z \equiv 0 \mod 3\}$. Let $x = ab \in 3\mathbb{Z}$ be arbitrary, where $a, b \in \mathbb{Z}$. Then $3 \mid x$. We know that, since $x = ab$, either $3 \mid a$ or $3 \mid b$. This implies that either $a$ or $b$ are in $3\mathbb{Z}$. Since $3\mathbb{Z} \neq \mathbb{Z}$, then we have shown that $3\mathbb{Z}$ is a prime ideal of $\mathbb{Z}$. Thus, by Definition 1.3.43, 3 is a prime of $\mathbb{Q}$, which is as expected.

A prime $p$ of one field $\mathbb{F}$ may not necessarily be prime in an extension $\mathbb{F}(\alpha)$ of $\mathbb{F}$:

**Example 1.3.45.** Consider $\mathbb{Q}$, in which 2 is prime. However, if we extend $\mathbb{Q}$ to the Gaussian numbers $\mathbb{Q}(i)$ and consider the ideal $(2) = \{a + bi : 2 \mid a \text{ and } 2 \mid b\}$ of $\mathbb{Z}(i)$, we see that 2 (which is clearly in (2)) can be written as the product

$$2 = (1 + i)(1 - i), \tag{1.17}$$

yet neither $1 + i$ nor $1 - i$ are in (2). Thus, 2 is not prime in $\mathbb{Q}(i)$.

In fact, we have special terminology for what happened in Example 1.3.45:

**Definition 1.3.46.** Let $p \in \mathbb{F}$ be a prime, and let $\mathbb{F}(\alpha)$ be an extension of $\mathbb{F}$. If $[p] = \mathfrak{P}_1 \cdot \mathfrak{P}_2$, where $\mathfrak{P}_1$ and $\mathfrak{P}_2$ are distinct prime ideals of $\mathcal{O}_{\mathbb{F}(\alpha)}$, then we say $p$ *splits* in $\mathbb{F}(\alpha)$.

**Example 1.3.47.** Given Example 1.3.45, we can show that both $(2) \subseteq (1 + i)$ and $(2) \subseteq (1 - i)$. Then, by Theorem 1.3.37, we know that $(1 + i) \mid (2)$ and $(1 - i) \mid (2)$. Since $(1 + i)$ and $(1 - i)$ are prime ideals of $\mathbb{Z}(i)$, we can see that 2 splits in $\mathbb{Q}(i)$.

There is a special case of primes splitting:

**Definition 1.3.48.** Let $p \in \mathbb{F}$ be a prime, and let $\mathbb{F}(\alpha)$ be an extension of $\mathbb{F}$. If $[p] = \mathfrak{P} \cdot \mathfrak{P} = \mathfrak{P}^2$, where $\mathfrak{P}$ is a prime ideal of $\mathcal{O}_{\mathbb{F}(\alpha)}$, then we say $p$ *ramifies* in $\mathbb{F}(\alpha)$.

Finally, if splitting does not occur, we say that $p$ is inert:

**Definition 1.3.49.** Let $p \in \mathbb{F}$ be a prime, and let $\mathbb{F}(\alpha)$ be an extension of $\mathbb{F}$. If $[p]$ is a prime ideal of $\mathbb{F}(\alpha)$, then we say $p$ is *inert* in $\mathbb{F}(\alpha)$.

Given 2 and $1 + i$ of Example 1.3.45, it makes sense to say that $1 + i$ divides 2, even though both are primes (of $\mathbb{Q}$ and $\mathbb{Q}(i)$, respectively). We shall express this formally:

**Definition 1.3.50.** Let $\mathbb{F}$ be a field, and let $\mathbb{F}(\alpha)$ be an extension of $\mathbb{F}$. Let $p$ be a prime in $\mathbb{F}$, and assume that $(p)$ splits into prime ideals $(\pi_1)$ and $(\pi_2)$ of $\mathcal{O}_{\mathbb{F}(\alpha)}$. Then, we say that both $\pi_1$ and $\pi_2$ *divide* $p$, and write $\pi_1 \mid p$ and $\pi_2 \mid p$.

**Theorem 1.3.51.** *Let $\mathbb{F}$ be a field, and let $\mathbb{F}(\alpha)$ be an extension of $\mathbb{F}$. Suppose $p$ is a prime in $\mathbb{F}$ and $\pi_1$ are primes in $\mathbb{F}(\alpha)$. If $N(\pi_1) \ \mid \ N(p)$, then $\pi_1 \mid p$.*

The ideas behind Definition 1.3.50 are very important for understanding some of the terminology of Harder's Conjecture, specifically regarding "primes dividing primes." Additionally, the conjecture refers to the *compositum* of two field extensions:

**Definition 1.3.52.** Let $\mathbb{F}$ be a field, and let $\mathbb{K}$ and $\mathbb{L}$ be extensions of $\mathbb{F}$. The *compositum* of $\mathbb{K}$ and $\mathbb{L}$, denoted $\mathbb{K}+\mathbb{L}$, is the intersection of all fields containing both $\mathbb{K}$ and $\mathbb{L}$.

**Example 1.3.53.** If we consider $\mathbb{Q}$ and extensions $\mathbb{Q}(i)$ and $\mathbb{Q}(\sqrt{2})$, then the compositum of $\mathbb{Q}(i)$ and $\mathbb{Q}(\sqrt{2})$ is $\mathbb{Q}(i, \sqrt{2}) = \mathbb{Q}(i+\sqrt{2})$.

## 1.3.2 The LLL Algorithm and Algebraic Dependence

As explained later in Section 2.3, we will be calculating ratios of critical values of modular forms. These critical value ratios are known to be algebraic (see [10]), but can sometimes only be presented as floating-point decimals. We can use a process called "algebraic dependence" (which itself uses the LLL Algorithm) to find exact expressions for these critical value ratios. We begin this section with a discussion of the LLL Algorithm.

### The LLL Algorithm

Recall from elementary linear algebra the definition of linear independence:

**Definition 1.3.54.** Let $\{\mathbf{b}_1, \ldots, \mathbf{b}_m\}$ be a set of vectors in $\mathbb{R}^n$. The set of vectors $\{\mathbf{b}_1, \ldots, \mathbf{b}_m\}$ is linearly independent if the only solution to the equation

$$c_1\mathbf{b}_1 + c_2\mathbf{b}_2 + \cdots + c_m\mathbf{b}_m = \mathbf{0} \tag{1.18}$$

is the trivial solution $c_1 = c_2 = \cdots = c_m = 0$, where each $c_i \in \mathbb{R}$.

We now define a lattice:

**Definition 1.3.55.** A *lattice* $L$ is a subset of $\mathbb{R}^n$, generated by all integer combinations of a set $B = \{\mathbf{b}_1, \ldots, \mathbf{b}_m\}$ of linearly independent vectors:

$$L = \sum_{i=1}^{m} z_i\mathbf{b}_i \tag{1.19}$$

where each $z_i \in \mathbb{Z}$. We call $B$ the *basis* of $F$.

**Remark 1.3.56.** We can express $B$ as an $n \times m$ matrix:

$$M_B = \begin{pmatrix} \vdots & \vdots & \vdots & \vdots \\ \mathbf{b}_1 & \mathbf{b}_2 & \dots & \mathbf{b}_m \\ \vdots & \vdots & \vdots & \vdots \end{pmatrix} \tag{1.20}$$

The basis for a given lattice is not unique:

**Example 1.3.57.** Consider lattice $L = \mathbb{Z} \times \mathbb{Z}$. We can see that both

$$B_1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \tag{1.21}$$

and

$$B_2 = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \tag{1.22}$$

each form a basis for $L$.

Given a lattice $L$, we are interested in finding an orthogonal basis for $L$:

**Definition 1.3.58.** Let $B$ be a basis. If, for each pair $\mathbf{b}_i, \mathbf{b}_j \in B$, the dot product $\mathbf{b}_i \cdot \mathbf{b}_j = 0$, then we say $B$ is *orthogonal.*

**Remark 1.3.59.** We can see that $B_1$ of Example 1.3.57 is orthogonal, while $B_2$ is not.

Through the Gram-Schmidt Orthogonalization Method, we can find an orthogonal basis $B^*$, given basis $B$ of $L$:

**Algorithm 1.3.60** (Gram-Schmidt Orthogonalization Method)**.** Let $B = \{\mathbf{b}_1, \mathbf{b}_2, \dots, \mathbf{b}_m\}$ be a basis of lattice $L$.

1. Set ${\mathbf{b}_1}^* = -\mathbf{b}_1$.

2. For each $2 \leq i \leq m$ in succession, set

$$\mathbf{b}_i{}^* = \mathbf{b}_i - \sum_{k=1}^{i-1} \frac{\mathbf{b}_i \cdot \mathbf{b}_k{}^*}{\mathbf{b}_k{}^* \cdot \mathbf{b}_k{}^*} \mathbf{b}_k{}^* \tag{1.23}$$

3. $B^* = \{\mathbf{b}_1{}^*, \mathbf{b}_2{}^*, \ldots, \mathbf{b}_m{}^*\}$ is an orthogonal basis for $L$.

**Remark 1.3.61.** Performing Step 2 of the Gram-Schmidt Orthogonalization Method once, for a single $i$, is called *incremental Gram-Schmidt.*

We can also reduce a basis $B$ for lattice $L$:

**Definition 1.3.62.** Let $B$ be a basis for lattice $L$. We say $B$ is *reduced* if, for each $\mathbf{b}_i{}^* \in B^*$,

$$\|\mathbf{b}_i{}^*\|^2 \geq \left(\frac{3}{4} - (\mu_{i,i-1})^2\right) \|\mathbf{b}_{i-1}{}^*\|^2, \tag{1.24}$$

for $1 < i \leq m$, where

$$\mu_{i,j} = \frac{\mathbf{b}_i \cdot \mathbf{b}_j{}^*}{\mathbf{b}_j{}^* \cdot \mathbf{b}_j{}^*} \tag{1.25}$$

(see [4]).

We can think of a reduced basis as one which includes the shortest possible vector elements. The Lenstra-Lenstra-Lovász (or LLL) Algorithm, named by *Computing and Science and Engineering* in 2000 as one of the top ten algorithms of the last century [2], allows us to find a reduced basis $B'$ for a basis $B$ of a lattice $L$. The specifics of the algorithm are beyond the scope of this text; however, we will outline it below in very broad terms (see [4] p. 87 for a more detailed description):

**LLL Algorithm.** *1. Perform Incremental Gram-Schmidt on vectors in $B$.*

*2. Test whether the resulting basis is reduced; if it is, then the algorithm terminates. If not, continue to the next step.*

*3. If $\mu_i, j > .5$, round $\mu_{i,j}$ to the nearest integer. Then, swap vectors in a specified way discussed in [4]*

*4. Return to step 2.*

**Theorem 1.3.63** (Lenstra-Lenstra-Lovász)**.** *The LLL Algorithm produces a reduced basis for a lattice $L$ in polynomial time. [4]*

### Algebraic Dependence

Given a real number $\alpha$, which may be presented as a floating-point decimal, we often want to find a polynomial $f(x)$ (with coefficients in $\mathbb{Z}$) such that $f(\alpha)$ is close to zero. This is known as *algebraic dependence*. The LLL Algorithm gives a method for finding this polynomial:

**Algorithm 1.3.64** (Algebraic Dependence)**.** Let $\alpha \in \mathbb{R}$, and let $n$ be such that $n-1$ is the desired degree of the polynomial $f$ for which $f(\alpha)$ is as close to zero as possible.

1. Consider the quadratic form $Q(\mathbf{a})$; given a vector $\mathbf{a} = (a_1, a_2, \ldots, a_n)$ and sufficiently large $N \in \mathbb{Z}$:

$$Q(\mathbf{a}) = {a_2}^2 + {a_3}^2 + \cdots + {a_n}^2 + N(a_1 + a_2\alpha + a_3\alpha^2 + \cdots + a_n\alpha^{n-1}) \qquad (1.26)$$

2. Let $A$ be the Gram matrix defining $Q(\mathbf{a})$, i.e. $Q(\mathbf{a}) = \mathbf{a}^{\mathrm{T}}A\mathbf{a}$.

3. Using the LLL Algorithm, reduce $A$; call this reduced matrix $A'$.

4. Let $\mathbf{a}'$ be the first vector of $A'$.

5. Let $Q'(\mathbf{a}')$ be the quadratic form defined by $\mathbf{a}'$;

$$Q'(\mathbf{a}') = {a_2}'^2 + {a_3}'^2 + \cdots + {a_n}'^2 + N({a_1}' + {a_2}'\alpha + {a_3}'\alpha^2 + \cdots + {a_n}'\alpha^{n-1}). \qquad (1.27)$$

Since $A'$ is LLL-reduced, this implies that the vector $\mathbf{a}'$ is small, and that both $\sum_{i=1}^{n} {a_i}^2$ and

$$N({a_1}' + {a_2}'\alpha + {a_3}'\alpha^2 + \cdots + {a_n}'\alpha^{n-1}) \qquad (1.28)$$

are small. Thus, if $N$ is large, we know $\sum_{i=1}^{n} {a_1}'\alpha^{i-1}$ is extremely small.

6. We then use the polynomial

$$f(x) = {a_1}' + {a_2}'x + {a_3}'x^2 + \cdots + {a_n}'x^{n-1}, \qquad (1.29)$$

for which $\alpha$ is approximately a root (i.e. $f(\alpha)$ is close to zero).

In Sage [15], the function `algdep` (which itself is actually a GP/PARI [1] function) takes three parameters: the real number $\alpha$ for which $f$ is approximated, a precision parameter, and the maximum degree of $f$. When we compute critical values (see Section 2.3), we are sometimes presented with floating-point decimals. However, we know which field these critical value ratios are in; thus, we know which degree to specify for `algdep`.

## 1.4 "Classical" Modular Forms

Modular forms are important structures in modern number theory, as introduced in Section 1.1. They are intimately connected with elliptic curves, and their study heavily contributed to Andrew Wiles' proof of Fermat's Last Theorem. [14]

In Section 1.5, we will encounter generalizations of modular forms, called "Siegel" modular forms. In order to alleviate confusion between the two, we will later refer to the modular forms discussed in this section as "classical" modular forms. However, since Siegel modular forms have not yet been introduced, we will simply refer to "classical" modular forms as "modular forms" throughout this section.

### 1.4.1 Preliminaries

Before we formally define modular forms, we must first define some of their preliminary aspects. First, we define their domain - the upper-half plane $\mathbb{H}_1$:

**Definition 1.4.1.** Let

$$\mathbb{H}_1 = \{z \in \mathbb{C} : \mathrm{Im}(z) > 0\}. \tag{1.30}$$

The criteria for defining modular forms are linked to the modular group $\mathrm{SL}_2(\mathbb{Z})$:

**Definition 1.4.2.** Let $\mathrm{SL}_2(\mathbb{Z})$ be the group of 2-by-2 integer-valued matrices with determinant 1; i.e.

$$\mathrm{SL}_2(\mathbb{Z}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, c, d \in \mathbb{Z}, ad - bc = 1 \right\}. \tag{1.31}$$

One can easily show that $\mathrm{SL}_2(\mathbb{Z})$ is a group, with standard matrix multiplication as its operation. For the purposes of this paper, however, we are primarily concerned with its connection to fractional linear transformations of the Riemann sphere $\hat{\mathbb{C}} = \mathbb{C} \cup \infty$: [5]

**Definition 1.4.3.** Let $M = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$, and let $\tau \in \hat{\mathbb{C}}$. We define the fractional linear transformation $\gamma_M$ of $M$ on $\tau$ as such:

$$\gamma_M(\tau) = \frac{a\tau + b}{c\tau + d}. \tag{1.32}$$

**Example 1.4.4.** Consider $M = \left(\begin{smallmatrix} 1 & -2 \\ -1 & 3 \end{smallmatrix}\right)$. We can see that $M$ corresponds to the fractional linear transformation

$$\gamma_M(\tau) = \frac{\tau - 2}{-\tau + 3} \tag{1.33}$$

**Proposition 1.4.5.** $\mathrm{SL}_2(\mathbb{Z})$ *is generated by the elements*

$$A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \tag{1.34}$$

*and*

$$B = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}. \tag{1.35}$$

**Remark 1.4.6.** We can see that $A$ and $B$ correspond to the transformations $\gamma_A(\tau) = \tau + 1$ and $\gamma_B(\tau) \;=\; -1/\tau$, respectively. Also, both $I$ and $-I$ correspond to the identity transformation $\gamma_I(\tau) = \tau$. [5]

The upper-half plane $\mathbb{H}_1 \in \hat{\mathbb{C}}$ is actually mapped to itself by elements of $\mathrm{SL}_2(\mathbb{Z})$:

**Theorem 1.4.7.** *Let $M \in \mathrm{SL}_2(\mathbb{Z})$, and let $\tau \in \mathbb{H}_1$. Then, $\gamma_M(\tau) \in \mathbb{H}_1$.*

*Proof.* Let $M \in \mathrm{SL}_2(\mathbb{Z})$, and let $\tau \in \mathbb{H}_1$. We know $\tau$ is of the form $x + yi$, where $x, y \in \mathbb{R}$ and $y > 0$. Thus,

$$\gamma_M(\tau) = \frac{ax + b + ayi}{cx + d + cyi}. \tag{1.36}$$

If we then multiply by the conjugate of the denominator, we get

$$\gamma_M(\tau) = \frac{acx^2 + adx + acy^2 + bcx + bd}{c^2y^2 + (cx + d)^2} + \frac{(ad - bc)y}{c^2y^2 + (cx + d)^2} i. \tag{1.37}$$

Since $ad - bc = 1$ and $y > 0$, we know the imaginary part of $\gamma_M(\tau)$ is positive. Thus, $\gamma_M(\tau) \in \mathbb{H}_1$. □

We now require some definitions from complex analysis:

**Definition 1.4.8.** Let $z = x + iy$ and let $U$ be some open neighborhood of $z$. Let $f$ be a complex-valued function of $z$, i.e. $f(x, y) = u(x, y) + iv(x, y)$ for some functions $u, v$ of $x$ and $y$. If $\frac{\partial u}{\partial x} = \frac{\partial v}{\partial y}$ and $\frac{\partial v}{\partial x} = -\frac{\partial u}{\partial y}$ and these partial derivatives of $z$ are continuous on $U$, then $f$ is complex differentiable.

**Definition 1.4.9.** A function $f : A \to B$ is *holomorphic* on $A$ if, for every point $z \in A$, $f$ is complex differentiable at $z$.

**Definition 1.4.10.** A function $f : \mathbb{H}_1 \to \mathbb{C}$ is *holomorphic at* $\infty$ if $\lim_{\mathrm{Im}(\tau)\to\infty} f(\tau)$ exists.

### 1.4.2 Modular Forms

We can now define modular forms:

**Definition 1.4.11.** Let $r > 0$ be an integer, and $f : \mathbb{H}_1 \to \mathbb{C}$. $f$ is a modular form of weight $r$ if

(i) $f$ is holomorphic on $\mathbb{H}_1$,

(ii) $f$ is holomorphic at $\infty$,

(iii) $f$ satisfies the functional equation

$$f(\gamma_M(\tau)) = (c\tau + d)^r f(\tau),\ \forall \tau \in \mathbb{H}_1 \tag{1.38}$$

and for all fractional linear transformations $\gamma_M$ defined by $M = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$.

**Remark 1.4.12.** If a function $f$ satisfies Conditions (i) and (iii) of Def. 1.4.11, then it is said to be "weakly" modular of weight $r$. [5]

We can see that condition (iii) of 1.4.11 yields an infinite number of symmetries which must be checked in order to determine whether a function $f$ is a modular form. Fortunately, since $\mathrm{SL}_2(\mathbb{Z})$ is generated by $A = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ and $B = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$, we only need to check whether 1.4.11 (iii) holds for $A$ and $B$:

**Theorem 1.4.13.** *Let $r$ be an integer and $\tau \in \mathbb{H}_1$. If $f$ satisfies*

$$f(\tau + 1) = f(\tau) \tag{1.39}$$

*and*

$$f(-1/\tau) = \tau^r f(\tau), \tag{1.40}$$

*then $f$ satisfies*

$$f(\gamma_M(\tau)) = (c\tau + d)^r f(\tau). \tag{1.41}$$

*for all $M \in \mathrm{SL}_2(\mathbb{Z})$.*

We can define spaces of modular forms:

**Definition 1.4.14.** We denote the set of modular forms of weight $r$ as $M_r(\mathrm{SL}_2(\mathbb{Z}))$.

However, for simplicity's sake, we will refer to this set as $M_r$. We can easily check that $M_r$ forms a vector space over $\mathbb{C}$ [5]. Furthermore,

**Theorem 1.4.15.** *Let $f \in M_{r_1}$ and $g \in M_{r_2}$. The product $fg$ is a modular form of weight $r_1 + r_2$.*

Then, we can define the direct sum $M_*$ of spaces of modular forms, which itself has a certain algebraic structure:

**Theorem 1.4.16.** *Let*

$$M_* = \bigoplus_{r \in \mathbb{Z}} M_r. \tag{1.42}$$

*Then, $M_*$ is a ring.*

In addition, given (1.39), modular forms are $\mathbb{Z}$-periodic. [5] Thus, they have Fourier expansions:

**Theorem 1.4.17.** *Let $f$ be a modular form. The form $f$ has a Fourier expansion*

$$f(q) = \sum_{n=0}^{\infty} a_n q^n \text{ where } q = e^{2\pi i \tau}. \tag{1.43}$$

**Remark 1.4.18.** If the leading coefficient $a_n$ (i.e. the smallest $n$ such that $a_n \neq 0$) of a modular form $f$ is equal to 1, we say $f$ is *normalized.*

For the purposes of this paper, we are primarily concerned with the above Fourier series representations of modular forms, and the coefficients $a_n$ of such series. We will not be explicitly evaluating any modular form for $\tau$; thus, for the purposes of simplicity, we can think of them as functions of $q$.

**Remark 1.4.19.** A theorem by Shimura [10] tells us that the coefficients $a_n$ of a normalized modular form are algebraic.

Thus, given a form $f$, we define the number field of its coefficients:

**Definition 1.4.20.** Let $f = \sum_{n=0}^{\infty} a_n q^n$ be a modular form. We denote the smallest field which contains all of $a_n$ as $\mathbb{Q}_f$.

**Remark 1.4.21.** Shimura [10] also tells us that the degree of the extension $[\mathbb{Q}_f : \mathbb{Q}]$ is finite.

We will now explore some examples of modular forms:

**Example 1.4.22.** The zero function $f(q) = 0$ is a modular form of any weight.

**Example 1.4.23.** The constant function $g(q) = k$, $k \neq 0$ is a modular form of weight 0.

**Example 1.4.24.** A very famous modular form is $\Delta$ (see Section 1.1):

$$\Delta(q) = q\prod_{n=0}^{\infty}(1-q^n)^{24} = q-24q^2+252q^3-1472q^4+4830q^5-\ldots = \sum_{n=1}^{\infty}\tau(n)q^n, \quad (1.44)$$

where $\tau$ is the Ramanujan $\tau$-function. $\Delta$ has weight 12.

Another important class of modular forms are the Eisenstein series:

**Definition 1.4.25.** Let $r > 2$ be an even integer. We define the Eisenstein series of weight $r$ as:

$$e_r(\tau) = \sum_{\{(c,d)\in\mathbb{Z}^2-\{(0,0)\}\}} \frac{1}{(c\tau+d)^r}, \ \tau \in \mathbb{H}_1. \quad (1.45)$$

Mordell [5] shows us that we can write each $e_r$ in terms of the arithmetic function $\sigma_k$:

**Theorem 1.4.26.** *Let $e_r$ denote the Eisenstein series of weight $r$, for even $r > 2$. Then*

$$e_r(q) = 2\zeta(r)\left(1 - \frac{4r}{B_r}\sum_{n=1}^{\infty}\sigma_{r-1}(n)q^n\right) \quad (1.46)$$

*where $\zeta$ denotes the Riemann zeta function, $\sigma_{r-1}(n)$ is the function*

$$\sigma_{r-1}(n) = \sum_{\substack{m|n \\ m>0}} m^{r-1}, \quad (1.47)$$

*and $B_r$ denotes the $r$th Bernoulli number (see Section 4.2).*

We can "build" any modular form by multiplying and adding together various $e_r$. Specifically, we can "build" the space $M_r$ with $e_4$ and $e_6$:

**Theorem 1.4.27.** *The space $M_r$ can be written as a linear combination of ${e_4}^a {e_6}^b$ for positive integers $a, b$ that satisfy $4a + 6b = r$. The dimension of $M_r$ is equal to the number of solutions to $4a + 6b = r$.*

We found the dimensions of certain $M_r$ using Sage code in the Appendices (see 5.1).

**Example 1.4.28.** $\Delta$ (see 1.4.24) is a linear combination of ${e_4}^3$ and ${e_6}^2$:

$$\Delta(q) = \frac{{e_4}^3 - {e_6}^2}{\zeta(12)1728} \in M_{12} \tag{1.48}$$

**Example 1.4.29.** $\Delta_{22}$, a modular form of weight 22, is a linear combination of ${e_4}^4 e_6$ and $e_4 {e_6}^3$:

$$\Delta_{22}(q) = \frac{288}{\zeta(22)497664}\left({e_4}^4 e_6 - e_4 {e_6}^3\right) \in M_{22} \tag{1.49}$$

We can verify that the coefficients of $\Delta_{22}$ display the Ramanujan congruence shown in Section 1.1.

### 1.4.3 Cuspidal Forms

For the verification of Harder's Conjecture, we are interested in a specific type of modular form, called a "cuspidal" form:

**Definition 1.4.30.** Let $f$ be a modular form of weight $r$. If the Fourier expansion of $f$ has leading coefficient $a_0 = 0$, then $f$ is said to be a cuspidal, or "cusp" form.

Equivalently, given $q = e^{2\pi i\tau}$, we can define cusp forms as such:

**Definition 1.4.31.** Let $f$ be a modular form. If $\lim_{\mathrm{Im}(\tau)\to\infty} f(\tau) = 0$, then $f$ is a cusp form [5].

Given 1.4.30, we can see that a cusp form $f$ can be written as:

$$f(q) = \sum_{n=1}^{\infty} a_n q^n. \tag{1.50}$$

Some examples of cusp forms include:

**Example 1.4.32.** The zero function $f(q) = 0$ is trivially a cusp form.

**Example 1.4.33.** The modular form $\Delta$ is also a cusp form (note how the first term of the Fourier expansion $\Delta$ in (1.44) is $q$).

Cusp forms of weight $r$ have an associated vector space:

**Definition 1.4.34.** The space of cusp forms of weight $r$ is denoted $S_r$.

We can find the dimension of $S_r$ given the following theorem [5]:

**Theorem 1.4.35.** *Let $S_r$ be the space of cusp forms of weight $r$. Then,*

$$\dim S_r = \dim M_{r-12} \tag{1.51}$$

## 1.5 Siegel Modular Forms

We can generalize the ideas behind modular forms; $\mathrm{SL}_2(\mathbb{Z})$, $\mathbb{H}_1$, and the Eisenstein series all have analogues in the properties in Siegel modular forms. First, we must define

**Definition 1.5.1.** Let $\mathrm{Sp}(4, \mathbb{Q})$ be the group of matrices $M \in \mathrm{M}(4, \mathbb{Q})$ such that

$$M^T J M = J, \tag{1.52}$$

where $J = \begin{pmatrix} & I_2 \\ -I_2 & \end{pmatrix}$ represents the standard symplectic form, and $M^T$ denotes the transpose of $M$. We can see a similarity to $\mathrm{SL}_2(\mathbb{Z})$, as discussed in Section 1.4.

We can then define the full Siegel modular group $\Gamma^{(2)}$:

**Definition 1.5.2.** Let $\Gamma^{(2)} = \mathrm{Sp}(4, \mathbb{Z}) = \mathrm{Sp}(4, \mathbb{Q}) \cap \mathrm{M}(4, \mathbb{Z})$.

We now consider a generalization of the upper-half plane $\mathbb{H}_1$ (recall 1.4.1):

**Definition 1.5.3.** Let

$$\mathbb{H}_2 := \{Z \in \mathrm{M}(2,\mathbb{C}) \ : \ {}^tZ = Z, \mathrm{Im}(Z) > 0\}. \tag{1.53}$$

This is called the Siegel upper-half space of degree 2.

The coefficients of vector-valued Siegel modular forms are homogenous polynomials:

**Definition 1.5.4.** Let $p(X,Y) = \sum_{i=0}^{n} X^{a_i}Y^{b_i}$ be a polynomial of $X$ and $Y$. If, for all $i$, $j = a_i + b_i$ remains constant, then we say that $p$ is a homogenous polynomial of degree $j$.

**Example 1.5.5.** Both $p_1(X,Y) = X^2 + 2XY - Y^2$ and $p_2(X,Y) = 4X^3 - 6XY^2$ are homogenous. We can see that $p_1$ has degree 2 and that $p_2$ has degree 3.

**Definition 1.5.6.** $\mathbb{C}[X,Y]_j$ is the space of homogeneous polynomials of degree $j$ with coefficients in $\mathbb{C}$.

Now we can define Siegel modular forms:

**Definition 1.5.7.** Let $k, j$ be non-negative integers. A Siegel modular form of genus 2 and weight $(k,j)$ is a complex analytic function $F\colon \mathbb{H}_2 \to \mathbb{C}[X,Y]_j$ such that

$$F(gZ) := F\big((AZ+B)(CZ+D)^{-1}\big) = \det(CZ+D)^k\,(CZ+D)\cdot F(Z) \tag{1.54}$$

for all $g = \left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right) \in \Gamma^{(2)}$, where $\Gamma^{(2)}$ is as in Definition 1.5.2.

We can observe that such an $F$ is a function of three complex variables, given $g \in \Gamma^(2)$.

**Definition 1.5.8.** Given $k, j$, we denote the space of all Siegel modular forms with weight $(k,j)$ as $M_{k,j}^{(2)}$; we suppress $j$ if it is 0.

**Definition 1.5.9.** If $j$ is positive $F$ is called *vector-valued*; if $j = 0$, $F$ is *scalar-valued.*

We write $M_*^{(2)} := \bigoplus_k M_k^{(2)}$ for the ring of (scalar-valued) Siegel modular forms of degree 2.

**Theorem 1.5.10.** *Let*

$$Q := \left\{ f = [a,b,c] \ : \ a,b,c \in \mathbb{Z},\ b^2 - 4ac \le 0,\ a \ge 0 \right\}.$$

*A Siegel modular form $F$ has a Fourier expansion of the form*

$$F(Z) = \sum_{f=[a,b,c] \in Q} C_F(f)\, e\left(a\tau + bz + c\tau'\right).$$

*Here $Z := \left(\begin{smallmatrix} \tau & z \\ z & \tau' \end{smallmatrix}\right)$ ($\tau, \tau' \in \mathbb{H}_1$ and $z \in \mathbb{C}$) and $e(x) = e^{2\pi i x}$.*

Spaces of Siegel modular forms have subspaces analogous to the classical $S_r$:

**Definition 1.5.11.** A Siegel modular form $F$ is called a *cusp form* if its Fourier expansion is supported on positive-definite elements of $Q$; i.e. $[a,b,c] \in Q$ such that $aX^2 + bXY + cY^2 > 0$ for all $X, Y \neq 0$.

**Definition 1.5.12.** The subspace of cusp forms in $M^{(2)}_{k,j}$ is denoted $S^{(2)}_{k,j}$.

The ring of all vector-valued Siegel modular forms $\bigoplus_{k,j} M^{(2)}_{k,j}$ is not finitely generated [3]. For this reason, we usually fix the coefficient degree $j$. We are specifically interested in the case of weight $(k,2)$; we have a concrete way to calculate these spaces thanks to the work of Satoh.

### 1.5.1 Satoh's Theorem

Given Siegel modular forms in $M^{(2)}_{k,0}$, we can compute Siegel modular forms in $M^{(2)}_{k,2}$ using the Satoh bracket [13]:

**Definition 1.5.13.** Suppose $F \in M^{(2)}_k$ and $G \in M^{(2)}_{k'}$ are two scalar-valued Siegel modular forms. We define the Satoh bracket by

$$[F,G]_2 = \frac{1}{2\pi i}\left(\frac{1}{k} G\,\partial_Z F - \frac{1}{k'} F\,\partial_Z G\right) \in M^{(2)}_{k+k',2}, \tag{1.55}$$

where $\partial_Z = \left(\begin{smallmatrix} \partial_\tau & 1/2\,\partial_z \\ 1/2\,\partial_z & \partial_{\tau'} \end{smallmatrix}\right)$.

The weight of the resulting Siegel modular form is given explicitly:

**Theorem 1.5.14.** *Let $F \in M_k^{(2)}$ and $G \in M_{k'}^{(2)}$. Then, $[F, G] \in M_{k+k',2}^{(2)}$.*

In the same paper, Satoh showed that $\bigoplus_k M_{k,2}^{(2)}$ is generated by Satoh brackets of scalar-valued elements. More precisely, he shows that

$$\begin{aligned} M_{k,2}^{(2)} =& [E_4, E_6]_2 M_{k-10}^{(2)} \oplus [E_4, \chi_{10}]_2 M_{k-14}^{(2)} \oplus \\ & [E_4, \chi_{12}]_2 M_{k-16}^{(2)} \oplus [E_6, \chi_{10}]_2 \mathbb{C}[E_6, \chi_{10}, \chi_{12}]_{k-16} \oplus \\ & [E_6, \chi_{12}]_2 \mathbb{C}[E_6, \chi_{10}, \chi_{12}]_{k-18} \oplus [\chi_{10}, \chi_{12}]_2 \mathbb{C}[\chi_{10}, \chi_{12}]_{k-22}. \end{aligned}$$

Here, the forms $E_4, E_6, \chi_{10}, \chi_{12}$ are the generators of the ring of scalar-valued Siegel modular forms, as described by Igusa [9]. $\mathbb{C}[A_1, \ldots, A_n]_k$ refers to the module of weight $k$ modular forms that can be expressed in terms of generators $A_1, \ldots, A_n$.

We can compute a basis for the space $M_{k,2}^{(2)}$ through a Sage [15] implementation in [11] of an algorithm found in [12].

## 1.6 Notation

This section will serve primarily as a reference for the (often abundant) notation used in this text. See Table 1.3.

| Notation | Meaning | Section |
|---:|---:|---:|
| $\Delta$ | A modular form of weight 12 | 1.1 |
| $\tau(n)$ | Ramanujan $\tau$-function | 1.1 |
| $m \mid n$ | "$m$ divides $n$" | 1.3 |
| $N(\alpha)$ | The norm of $\alpha$ | 1.3.1 |
| $\mathbb{F}(\alpha)$ | An extension of field $\mathbb{F}$ by $\alpha$ | 1.3.1 |
| $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ | The degree of the extension of $\mathbb{Q}(\alpha)$ by $\alpha$ | 1.3.1 |
| $\mathcal{O}_{\mathbb{F}}$ | The ring of algebraic integers in field $\mathbb{F}$ | 1.3.1 |
| $(a)$ | The ideal generated by element $a$ | 1.3.1 |
| $\mathfrak{O}$ | The unit ideal of field $\mathbb{F}$ | 1.3.1 |
| $\mathfrak{P}$ | A prime ideal | 1.3.1 |
| $\mathbb{K} + \mathbb{L}$ | The compositum of $\mathbb{K}$ and $\mathbb{L}$ | 1.3.1 |
| $\mu_{i,j}$ | Used for Gram-Schmidt Orthogonalization | 1.3.2 |
| $A'$ | The LLL-reduced basis of the lattice defined by $A$ | 1.3.2 |
| $Q(\mathbf{a})$ | A quadratic form, defined by **a**, used for algebraic dependence | 1.3.2 |
| $\mathbb{H}_1$ | The upper-half plane | 1.4 |
| $\mathrm{SL}_2(\mathbb{Z})$ | The group of 2-by-2 integer-valued matrices with determinant 1 | 1.4 |
| $M_r$ | The space of modular forms of weight $r$ | 1.4 |
| $\mathbb{Q}_f$ | The coefficient field of a classical modular form $f$ | 1.4 |
| $e_r$ | The Eisenstein series of weight $r$ | 1.4 |
| $\sigma_{r-1}(n)$ | The $\sigma$ function | 1.4 |
| $S_r$ | The space of cusp forms of weight $r$ | 1.4 |
| $\mathrm{Sp}(4, \mathbb{Q})$ | Analogous to $\mathrm{SL}_2(\mathbb{Z})$ for classical modular forms | 1.5 |
| $\Gamma^{(2)}$ | The full Siegel modular group | 1.5 |
| $\mathbb{H}_2$ | The Siegel upper-half space of degree 2 | 1.5 |
| $\mathbb{C}[X, Y]_j$ | The space of homogenous polynomials of degree $j$ | 1.5 |
| $S_{k,j}$ | The space of Siegel modular forms of weight $(k, j)$ | 1.5 |
| $\mathbb{Q}_F$ | The coefficient field of a Siegel modular form $F$ | 1.5 |
| $[F, G]_2$ | The Satoh bracket of $F$ and $G$ | 1.5.1 |
| $L_f(s)$ | The $L$-series of $f$ | 2.1 |
| $\Lambda(f, s)$ | The $L$-function of $f$ | 2.1 |
| $\Lambda(f, t)$ | The critical value of $f$ at integer $t$ | 2.2 |
| $\mathbb{R}_t(f)$ | The $t$-th period of $f$ | 2.4 |
| $T_p$ | Hecke operator for prime $p$ | 3.1 |
| $\lambda_p$ | Hecke eigenvalue for $T_p$ | 3.2 |
| $\ell$ | Large prime | 4.2 |
| $B_k$ | The $k$th Bernoulli number | 4.2 |

**Table 1.3:** Notation used in this text.

# Chapter 2

# L-functions, Critical Values and Periods

As discussed in Chapter 1, Harder's Conjecture relates large primes (i.e. primes larger than the form's weight $r$) dividing the ratios of critical values of cusp forms. In this chapter, we will define $L$-functions for modular forms, as well as their critical values. Then, we will discuss methods for calculating these critical values.

## 2.1 L-functions

We can, for $f(q) = \sum_{n=1}^{\infty} a_n q^n \in S_r$, define the Dirichlet series

$$L_f(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s} = a_1 + \frac{a_2}{2^s} + \frac{a_3}{3^s} + \dots. \tag{2.1}$$

Given the Ramanujan bound on the coefficients of the modular form (i.e. $|a_n| \leq n^{(r-1)/2}$), we can show that this series converges when $\Re s > (1+r)/2$. However, this series has an analytic continuation

$$\Lambda(f,s) = \frac{\Gamma(s)}{(2\pi)^s} L_f(s), \tag{2.2}$$

which represents the associated $L$-function for $f$, defined over the entire complex plane. One can show that there is a certain symmetry to this function; for example, it satisfies the functional equation

$$\Lambda(f,s) = (-1)^{r/2}\Lambda(f,k-s). \tag{2.3}$$

Also, given that the Mellin transform of $f$ [5] is

$$g(s) = \int_0^\infty f(y)y^{s-1}dy, \tag{2.4}$$

we can show that [6] this $L$-function is equal to the integral

$$\int_0^\infty f(iy)y^{s-1}dy = \Lambda(f,s). \tag{2.5}$$

The specifics of Mellin transforms are beyond the scope of this text; however, we will note their connection to the calculation of sums like $L_f(s)$ (these are called "Dirichlet series"). More on the derivation of can be found in [5].

In general, we are only concerned with the values of this $L$-function evaluated at specific $s$, called "critical" values.

## 2.2 Critical Values

We now define the critical values of the $L$-function associated to $f$:

**Definition 2.2.1.** Let $f \in S_r$ and let $t$ be an integer such that $1 \leq t \leq r-1$. Then $\Lambda(f,t)$ is the critical value of the $L$-function $\Lambda(f,t)$ at $t$. Moreover, if $t$ is odd, we call $\Lambda(f,t)$ an odd critical value, and if $t$ is even, we call $\Lambda(f,t)$ an even critical value.

Each $\Lambda(f,t)$ is likely to be transcendental [10]; however, they can be divided by a specific real number (which depends on the parity of $t$) such that the result is algebraic. We can make this more precise through the following theorem: [10]:

**Theorem 2.2.2.** *Let $f \in S_r$. Then there exists a number $\omega_+$ such that for even critical values $\Lambda(f,t)$, $\Lambda(f,t)/\omega_+$ is in $\mathbb{Q}_f$. Similarly, there exists a number $\omega_-$ such that for odd critical values $\Lambda(f,t)$, $\Lambda(f,t)/\omega_-$ is in $\mathbb{Q}_f$.*

By Theorem 2.2.2, each of the terms of the ratio of even critical values

$$\Lambda(f,2) : \Lambda(f,4) : \cdots : \Lambda(f,r-2) \tag{2.6}$$

is in $\mathbb{Q}_f$, since dividing each $\Lambda(f,t)$ by $\Lambda(f,2)$ will cancel the $\omega_+$ term, and each $\Lambda(f,t)/\omega_+$ is in $\mathbb{Q}_f$. Similarly, each of the terms of the ratio of odd critical values

$$\Lambda(f,1) : \Lambda(f,3) : \cdots : \Lambda(f,r-1) \tag{2.7}$$

is also rational in $\mathbb{Q}_f$. In order to verify Harder's Conjecture, we need to examine these above ratios of critical values (see Chapter 4). In the next two sections, we discuss two methods for computing these critical values; one method uses the functionality of Sage to directly calculate each critical value $\Lambda(f,t)$ (see Section 2.3, while the other uses Manin's theory of periods [10] (see Section 2.4).

## 2.3 Calculating Critical Values

We can calculate each critical value $\Lambda(f,t)$ in Sage [15] via an implementation of (2.2). This process yields a number which is approximated in Sage as a floating-point decimal. As stated above, we can take the ratios of even critical values (e.g. divide each by $\Lambda(f,2)$).

$$\Lambda(f,2) : \Lambda(f,4) : \cdots : \Lambda(f,r-2). \tag{2.8}$$

and odd critical values (e.g. divide each by $\Lambda(f,1)$)

$$\Lambda(f,1) : \Lambda(f,3) : \cdots : \Lambda(f,r-1). \tag{2.9}$$

For simplicity, we introduce the following notation:

**Definition 2.3.1.** Fix a modular form $f$. Let

$$x_t = \begin{cases} \Lambda(f,t)/\Lambda(f,2) & \text{if t is even,} \\ \Lambda(f,t)/\Lambda(f,1) & \text{if t is odd.} \end{cases} \tag{2.10}$$

We can see that each $x_t$ is now in $\mathbb{Q}_f$. However, each $x_t$ is still represented in Sage as a floating-point decimal. Thus, we can use PARI/GP's [1] algebraic dependence (i.e., `algdep`) function (recall Section 1.3.2). For each floating-point $x_t$, `algdep` yields (given certain inputted precision and degree parameters) a polynomial $p(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$ such that $x_t$ is a zero of $p$. Given the dimension of the $\mathbb{Q}_f$, we know what degree $p$ should be, and thus specify this in the appropriate parameter of `algdep`.

**Example 2.3.2.** For $f \in S_r$ such that $\dim S_r = 1$, `algdep` provides a linear equation $p(x) = a_0 + a_1x$ which has a solution that is a ratio of integers $-a_0/a_1$. Let $f \in S_{20}$, a one-dimensional space of cusp forms. Using Sage, we can directly calculate

$$\Lambda(f,2) \ = \ -1.529819475\ldots, \tag{2.11}$$

$$\Lambda(f,4) \ = \ 0.2234111365\ldots, \tag{2.12}$$

and

$$\Lambda(f,6) \ = \ -0.043209186\ldots. \tag{2.13}$$

We then calculate the ratio

$$\Lambda(f,2) : \Lambda(f,4) : \Lambda(f,6), \tag{2.14}$$

or, equivalently,

$$1 : \frac{\Lambda(f,4)}{\Lambda(f,2)} : \frac{\Lambda(f,6)}{\Lambda(f,2)} \approx 1 : -0.1460375816\cdots : 0.02824463118\ldots. \tag{2.15}$$

Using `algdep`, we find that $\frac{\Lambda(f,6)}{\Lambda(f,2)}$ is a solution to the linear equation $p(x) = 4896x + 715$, and that $\frac{\Lambda(f,6)}{\Lambda(f,2)}$ is a solution to the equation $q(x) = 4284x - 121$. If we solve these equations, we can express (2.14) as a ratio of integers:

$$\Lambda(f,2) : \Lambda(f,4) : \Lambda(f,6) = 1 : -\frac{715}{4896} : \frac{121}{4284} = 34272 : -5005 : 968 \tag{2.16}$$

**Example 2.3.3.** If $f$ is in a two-dimensional space of cusp forms, then `algdep` gives us quadratic polynomials, which have roots in $\mathbb{Q}_f$ (in this case, a quadratic field). Let $g \in S_{24}$, a two-dimensional space of cusp forms. As in 2.3.2, we can directly calculate each $\Lambda(g,t)$ in Sage. For this example, we will calculate the ratio of odd critical values

$$\Lambda(g,1) : \Lambda(g,3) : \Lambda(g,5) \simeq 1 : -0.0853312994 : 0.0088169890. \tag{2.17}$$

Using `algdep`, we find that $\frac{\Lambda(g,3)}{\Lambda(g,1)}$ is a solution to

$$p(x) = 129427105500x^2 + 22124013945x + 945456364, \tag{2.18}$$

and that $\frac{\Lambda(g,5)}{\Lambda(g,1)}$ is a solution to

$$q(x) = 218446060140000x^2 - 3883006019340x + 17254578643. \tag{2.19}$$

Using Sage, we can solve these equations, and find that

$$\frac{\Lambda(g,3)}{\Lambda(g,1)} = -\frac{134084933}{1568813400} \pm \frac{569}{1568813400}\sqrt{144169}, \tag{2.20}$$

and that

$$\frac{\Lambda(g,5)}{\Lambda(g,1)} = \frac{162197411}{18249462000} \pm \frac{3403}{18249462000}\sqrt{144169}. \tag{2.21}$$

We can verify whether to use the positve or negative root by comparing to the original floating-point value of $x_t$.

This above method for finding critical works well (given enough precision). However, it is slow, and is still inexact (as it relies upon `algdep` to convert floating-point decimals into algebraic numbers). Fortunately, there exists another way to calculate at least some of these critical values, through purely algebraic means. This method requires Manin's equations, which we describe in the next section.

## 2.4 Manin's Equations and Calculating Periods

We can alternatively calculate the critical values of a modular form through the calculation of its periods [10]. We first make the following definition:

**Definition 2.4.1.** Let $f \in S_r$ and let $t$ be an integer $0 \leq t \leq r-2$. Then define

$$R_t(f) = \int_0^{i\infty} z^t f(z)\ dz. \tag{2.22}$$

If $t$ is even, we call $R_t(f)$ an even period and if $t$ is odd, we call it an odd period [6].

We can see that, given (2.1), a modular form's periods $R_0, R_1, \dots R_\omega$ (where $\omega = r-2$) are intimately related to its critical values:

**Proposition 2.4.2.** *Let $f \in S_r$ and $t$ be an integer $1 \le t \le r-1$.*

$$\Lambda(f,t) = R_{t-1}(f). \tag{2.23}$$

It is clear that the even periods of $f$ correspond to its odd critical values, and that the odd periods of $f$ correspond to its even critical values. We can use Manin's Coefficient Theorem to calculate algebraically the exact ratio of even periods (and therefore find the ratio of odd critical values without using `algdep` to convert floating-point decimals). His theorem is as follows [10]:

**Manin's Coefficient Theorem.** *Let $f \in S_r$ be written as $f(q) = \sum_{n=1}^{\infty} a_n q^n$. Then, for $n \ge 2$:*

$$(\sigma_{\omega+1}(n) - a_n)R_0 = \sum_{D} \sum_{l=1}^{\frac{\omega-2}{4}} 2\binom{\omega}{2l} R_{2l}\left(\Delta^{2l}\delta^{\omega-2l} - \Delta^{\omega-2l}\delta^{2l}\right) \tag{2.24}$$

*where $a_n$ is the $n$th coefficient of $f$, and the outer summation is taken over the set $D$ of integer solutions of the equation $n = \Delta\Delta' + \delta\delta'$ which satisfy $\Delta > \delta > 0$ and either*

$$\Delta' > \delta' > 0 \tag{2.25}$$

*or*

$$\Delta | n,\ \Delta' = n/\Delta,\ \delta' = 0,\ 0 < \delta/\Delta \le 1/2 \tag{2.26}$$

*with a coefficient of $1/2$ included if $\delta/\Delta = 1/2$.*

**Example 2.4.3.** If $n = 4$, then there are three possible integer solutions $\Delta, \Delta', \delta, \delta'$ to the equation $n = \Delta\Delta' + \delta\delta'$ that satisfy the conditions of (2.25) and (2.26); here, each solution is written as a vector $(\Delta, \Delta', \delta, \delta')$:

$$\begin{pmatrix} \Delta \\ \Delta' \\ \delta \\ \delta' \end{pmatrix} = \begin{pmatrix} 2 \\ 2 \\ 1 \\ 0 \end{pmatrix} \text{ or } \begin{pmatrix} 4 \\ 1 \\ 1 \\ 0 \end{pmatrix} \text{ or } \begin{pmatrix} 4 \\ 1 \\ 2 \\ 0 \end{pmatrix} \tag{2.27}$$

We can then see that, for $n = 4$, the outer sum of (2.24) has three terms. We can then rewrite (2.24) for the $n = 4$ case (note the coefficient of $1/2$, which is included whenever $\delta/\Delta = 1/2$):

$$(\sigma_{\omega+1}(4) - a_4)R_0 = \frac{1}{2}\sum_{l=1}^{\frac{\omega-2}{4}} 2\binom{\omega}{2l} R_{2l}\,(2^{2l} - 2^{\omega-2l}) \;+\; \sum_{l=1}^{\frac{\omega-2}{4}} 2\binom{\omega}{2l} R_{2l}\,(4^{2l} - 4^{\omega-2l}) \;+$$
$$\frac{1}{2}\sum_{l=1}^{\frac{\omega-2}{4}} 2\binom{\omega}{2l} R_{2l}\,(4^{2l}2^{\omega-2l} - 4^{\omega-2l}2^{2l})$$

**Remark 2.4.4.** As in Section 1.4, $\sigma_{\omega+1}(n)$ is the sum of the $\omega + 1$ powers of the divisors of $n$. Thus, one can see that since $\sigma_{\omega+1}(n) \in \mathbb{Z}$ and so the coefficient of $R_0$ is in $\mathbb{Q}_f$ (since $a_n \in \mathbb{Q}_f$).

For each $n \geq 2$, (2.24) yields a linear equation of the form

$$b_0R_0 + \cdots + b_{(\omega-2)/2}R_{(\omega-2)/4} = 0. \tag{2.28}$$

We can then use Sage to build an matrix $M$ of coefficients for each $r_k$, where each row of $M$ corresponds to the linear equation given by (2.24) evaluated at some $n \geq 2$. We can see that this matrix has a width equal to the number of even periods in $R_0 \ldots R_{(\omega-2)/4}$. Given enough choices of $n$ (specifically, if we evaluate (2.24) for $2 \leq n \leq (\omega - 2)/4$), we can always ensure that $M$ has enough rows to solve it for ratios $1 : R_2/R_0 : R_4/R_0 : \cdots : R_{(\omega-2)/4}/R_0$.

**Example 2.4.5.** Let $f \in S_{16}$. Thus, $\omega = 14$. We can use (2.24) for $n = 2$, $n = 3$ and $n = 4$ to produce a $3 \times 4$ matrix $M$ of coefficients of even periods $R_0, \ldots R_6$:

$$M = \begin{pmatrix} -32553 & -372372 & -1009008 & -576576 \\ -14352256 & -96720624 & -118053936 & -35026992 \\ -1073760705 & -9154765620 & -18631332720 & -9816206400 \end{pmatrix}. \tag{2.29}$$

We want to solve $M\mathbf{r} = \mathbf{0}$, where $\mathbf{r}$ is the vector of even periods $(R_0, R_2, R_4, R_6)$. Thus, we row-reduce $M$:

$$M = \begin{pmatrix} 1 & 0 & 0 & \frac{98280}{3617} \\ 0 & 1 & 0 & -6 \\ 0 & 0 & 1 & \frac{21}{11} \end{pmatrix}. \tag{2.30}$$

Now, we can see that the ratio of even periods $R_0 : \cdots : R_6$ is

$$R_0 : R_2 : R_4 : R_6 = -\frac{98280}{3617} : 6 : -\frac{21}{11} : 1, \tag{2.31}$$

or, equivalently,

$$R_0 : R_2 : R_4 : R_6 = 1 : -\frac{3617}{16380} : \frac{3617}{51480} : -\frac{3617}{98280}. \tag{2.32}$$

One can see that Manin's equation (2.24) only yields half of the even period ratios. However, there exists a certain symmetry between these periods, given by one of the Shimura-Eichler relation [10]

**Theorem 2.4.6.** (Shimura-Eichler Relation I) *Let $f \in S_r$, and let $R_k$ denote the kth period of $f$. Then*

$$R_k + (-1)^k R_{\omega-k} = 0. \tag{2.33}$$

Thus, using (2.33), we can find the ratio of all the even periods of a given modular form exactly. One can see, though, that for $S_r$ with dimension greater than one, (2.24) yields a coefficient of $R_0$ that may not be a ratio of integers in $\mathbb{Q}$ (this is due to the contribution of $a_n$, which, for $f \in S_r$ such that $\dim S_r > 1$, is rational $\mathbb{Q}_f$).

One might ask whether a similar algebraic method exists for finding odd periods. Theorem 2.4 can only be used for calculating the ratio of even periods; however, Manin cites the other Shimura-Eichler relations, which allow for some information to be gathered about the ratios of odd periods [10]:

**Theorem 2.4.7.** (Shimura-Eichler Relations II and III) *Let $f \in S_r$, and let $R_k$ denote the kth period of $f$. Then*

$$R_k + (-1)^k \sum_{0 \le i \le k \ , \ i \equiv 0(2)} \binom{k}{i} R_{\omega-k+i} + (-1)^k \sum_{0 \le i \le \omega-k \ , \ i \equiv k(2)} \binom{\omega-k}{i} r_i = 0 \tag{2.34}$$

*and*

$$\sum_{1 \le i \le k \ , \ i \equiv 1(2)} \binom{k}{i} R_{\omega-k+i} + \sum_{1 \le i \le \omega-k \ , \ i \not\equiv k(2)} \binom{\omega-k}{i} R_i = 0 \tag{2.35}$$

Like with Theorem 2.4, we can use (2.33), (2.34), and (2.35) (given different choices of $k$) to produce a matrix $M$ of coefficents for $R_0 \dots R_\omega$. Specifically, we can use these equations to attempt to find the ratios of odd periods (since the Coefficents Theorem cannot be used to calculate these). For modular forms in one-dimensional spaces, $M\mathbf{r} = \mathbf{0}$ can be solved projectively for the odd periods (i.e. we can find the ratio $R_1 : R_3 : \ldots$; however, for higher-dimensional spaces, we need additional ratios $R_3/R_1$, $R_5/R_1$, etc. to solve projectively $M\mathbf{r} = \mathbf{0}$. Specifically, for $\dim S_r = 2$, we need one additional ratio of periods, while for $\dim S_r = 3$, we need two more such ratios (it seems as though for $\dim S_r = d$, we require $d - 1$ additional ratios to solve projectively $M\mathbf{r} = \mathbf{0}$).

Thus, for higher-dimensional $S_r$, we cannot find the ratio of odd periods (and, therefore, even critical values) through exclusively algebraic means. However, these above methods are faster than the methods outlined in Section 2.3. We can then choose to use these methods only to find the ratios that Manin's Coefficient Theorem and Theorems 2.4.6 and 2.4.7 do not provide for higher-dimensional $S_r$; and therefore find the ratios of even critical values in the most efficient manner possible.

In short, we can use Theorem 2.4 to find the ratios of all the odd critical values, and use a sort of "hybridization" of the Shimura-Eichler relations (i.e. Theorems 2.4.6 and 2.4.7) and the equations of Section 2.3 to find the ratios of all the even critical values. Therefore, given any cusp form $f$, we are able to find the ratios of all its critical values.

# Chapter 3

# Hecke Operators and Eigenvalues

## 3.1 Hecke Operators

In order to verify the conjecture, we also need to compute Hecke eigenforms. First, however, we need to describe the Hecke action on Siegel modular forms. We can give formulas for the image of a Siegel modular form of weight $(k, j)$ under the operator $T(p^\delta)$. Because the Hecke operators are multiplicative, we can understand them by understanding their image. The formulas for the image of $F$ under $T(p^\delta)$ can be found in [8]; however, we present them here for completeness.

**Theorem 3.1.1.** *Let $F$ be a Siegel modular form as above and let the image of $F$ under $T(p^\delta)$ have coefficients $C'([a,b,c])$. Then*

$$C'([a,b,c]) = \sum_{\alpha+\beta+\gamma=\delta} p^{\beta(k+j-2)+\gamma(2k+j-3)} \times \sum_{\substack{U\in R(p^\beta)\\ a_U\equiv 0\,(p^{\beta+\gamma})\\ b_U\equiv c_U\equiv 0\,(p^\gamma)}} \rho_j(d_{0,\beta}U) C\left(p^\alpha\left[\frac{a_U}{p^{\beta+\gamma}}, \frac{b_U}{p^\gamma}, \frac{c_U}{p^{\gamma-\beta}}\right]\right)$$

*where*

*(i) $R(p^\beta)$ is a complete set of representatives for $\mathrm{SL}(2,\mathbb{Z})/\Gamma_0^{(1)}(p^\beta)$; i.e. each element of $R(p^\beta)$ represents an equivalence class in $\mathrm{SL}(2,\mathbb{Z})/\Gamma_0^{(1)}(p^\beta)$;*

*(ii)* *for* $f = [a, b, c]$, $[a_U, b_U, c_U] = f_U := f\left((X, Y)U^T\right)$*;*

*(iii)* $d_{0,\beta} = \left(\begin{smallmatrix} 1 & \\ & p^\beta \end{smallmatrix}\right)$*;*

*(iv)* *for* $g \in \mathrm{GL}_2$*, the* $(j+1) \times (j+1)$ *matrix* $\rho_j(g)$*, which can interpreted as a homogeneous polynomial of degree* $j$*, is determined as such: Given pairs* $u_1, u_2$ *and* $v_1, v_2$ *of variables and for* $g \in \mathrm{GL}_2$*, we set* $(v_1, v_2) = (u_1, u_2)g$*. Then, the matrix* $\rho_j(g)$ *is given by*

$$(v_1^j, v_1^{j-1}v_2, \ldots, v_1 v_2^{j-1}, v_2^j) = (u_1^j, u_1^{j-1}u_2, \ldots, u_1 u_2^{j-1}, u_2^j)\rho_j(g).$$

Since $T$ is multiplicative, we can write $T(n) = T(p^{\delta_1}) \cdot T(p^{\delta_2}) \cdot \cdots \cdot T(p^{\delta_m})$, where $p^{\delta_1} \cdot p^{\delta_2} \cdot \cdots \cdot p^{\delta_m}$ is the prime decomposition of $n$.

**Definition 3.1.2.** We denote the Hecke eigenvalue of a Siegel modular $F$ under the operator $T(n)$ by $\lambda_n(F)$, or just $\lambda_n$ if $F$ is fixed.

**Remark 3.1.3.** If $T(n)(F) = \lambda_n \cdot F\ F$, then $F$ is an *eigenform.*

## 3.2 Computing Hecke Eigenforms

Fix $S_{k,2}$ with basis $\{F_1, \ldots, F_n\}$ (we know that each $F_i$ is an algebraic combination of the Igusa generators and Satoh brackets). Given that the Hecke operators are a commuting family of linear operators, we know that there exists a basis $\{G_1, \ldots, G_n\}$ for the $S_{k,2}$ for which each $G_i$ is an eigenform of any Hecke operator.

We can compute the forms $G_i$ as follows:

**Algorithm 3.2.1.** Consider $S_{k,2}$ with basis $\{F_1, \ldots, F_n\}$.

1. Determine the matrix representation for the Hecke operator $T(2)$ by computing the image under $T(2)$ of each basis element $F_i$.

2. Build an invertible matrix $N$ whose $j$th row consists of the coefficients of $F_j$ at certain indices $Q_1, \ldots, Q_n$. To ensure that $N$ is invertible we pick the indices one at time, making sure that each choice of index $Q_i$ increases the rank of the matrix.

3. Construct a matrix $M$ whose $j$th row consists of coefficients of the image of $F_j$ under $T(2)$ indexed by $Q_1, \ldots, Q_n$.

4. Then, the matrix representation of $T(2)$ is $M \cdot N^{-1}$.

Using $T(2)$, we compute the Hecke eigenforms, then express them as a linear combination of the basis $\{F_1, \ldots, F_n\}$. Then, in order to compute the Hecke eigenvalues $\lambda_{p^\delta}$, we compute these expressions to high precision, and finally compute their image under the Hecke operator $T(p^\delta)$.

# Chapter 4

# Verifying Harder's Conjecture

## 4.1 The Conjecture

We re-state Harder's Conjecture:

**Harder's Conjecture.** *Let $f = \sum_{n=1}^{\infty} a_n q^n \in S_r$ be a normalized eigenform with field of Fourier coefficients $\mathbb{Q}_f$. If a large prime $\ell$ of $\mathbb{Q}_f$ divides a critical value $\Lambda(f,t)$ then there exists a Siegel modular form $F \in S_{k,j}$ with $j = 2t-r-2$ and $k = r-t+2$ that is an eigenform with eigenvalue $\lambda_p$ for $T_p$, with field $\mathbb{Q}_F$ of eigenvalues $\lambda_p$ and such that there exists a prime $\ell'$ of the compositum of $\mathbb{Q}_F$ and $\mathbb{Q}_f$ dividing $\ell$ for which*

$$\lambda_p \equiv p^{k-2} + a_p + p^{j+k-1} \pmod{\ell'} \tag{4.1}$$

*for all primes $p \in \mathbb{Q}$.*

The congruence in (4.1) shows a surprising relationship between the critical values $\Lambda(f,t)$ and coefficients $a_p$ of a classical modular form, and the Hecke eigenvalues $\lambda_p$ of a corresponding Siegel modular form.

At this point, however, we still require the definition of "large prime," $\ell$, and what it means for $\ell$ to divide a critical value $\Lambda(f,t)$; this is discussed in the next section.

## 4.2 Large Primes

We first define the Bernoulli numbers:

**Definition 4.2.1.** The *Bernoulli numbers* $B_k$ are the coefficients of the formal power series expansion

$$\frac{t}{e^t - 1} = \sum_{k=0}^{\infty} B_k \frac{t^k}{k!}. \tag{4.2}$$

Given the power-series expansion for $e^t$, $B_k$ can be calculated in succession by matching coefficients in the equation

$$t = \sum_{n=1}^{\infty} \left( \sum_{k=0}^{n-1} \binom{n}{k} B_k \right) \frac{t^n}{n!} \tag{4.3}$$

(see [5], p. 9). We can show that, given (4.3), each $B_k$ is rational.

We list the first few Bernoulli numbers below, expressed in lowest terms (note that, for each odd $k > 1$, $B_k = 0$):

| $k$ | $B_k$ |
|---|---|
| 0 | 1 |
| 1 | $-1/2$ |
| 2 | $1/6$ |
| 4 | $-1/30$ |
| 6 | $1/42$ |
| 8 | $-1/30$ |
| 10 | $5/66$ |
| 12 | $-691/2730$ |
| 14 | $7/6$ |
| 16 | $-3617/510$ |
| 18 | $43867/798$ |
| 20 | $-174611/330$ |
| 22 | $854513/138$ |

**Table 4.1:** Bernoulli numbers $B_k$ for $k = 1$ and even $2 \leq k \leq 22$.

For the purpose of simplicity in describing Harder's definition of "large primes," we will introduce the following terminology:

**Definition 4.2.2.** Let $p$ be a prime in $\mathbb{Q}$. If $p$ divides the numerator of the Bernoulli number $B_k$ expressed in lowest terms, then we say $p$ is a *Bernoulli prime of weight* $k$. If $p$ does not divide the numerator of the Bernoulli number $B_k$ expressed in lowest terms, then we say $p$ is a *non-Bernoulli prime of weight* $k$.

**Example 4.2.3.** 691 is a Bernoulli prime of weight 12 (as can bee seen in Table 4.1).

**Definition 4.2.4.** Let $f$ be a classical modular form with weight $r$, with coefficient field $\mathbb{Q}_f$ (see Definition 1.4.20). Let $\ell$ be a prime in $\mathbb{Q}_f$ such that $N(\ell)$ is a non-Bernoulli prime of weight $r$, and

$$N(\ell) > r, \tag{4.4}$$

where $N(\ell)$ denotes the norm of $\ell$ (see Definition 1.3.8). We call $\ell$ a *large prime* (with respect to the weight of $f$).

Using the methods outlined in Section 2.4, we can find the ratios of critical values $\Lambda(f, t)$ of a given classical modular form $f$. The hypothesis of Harder's Conjecture requires us to determine whether a large prime $\ell$ divides one of these critical values. Since the critical values themselves are likely not algebraic (they contain the likely transcendental numbers $\omega_+$ and $\omega_-$, see Theorem 2.2.2), Harder uses a broader definition of "divides" in the statement of his conjecture:

**Definition 4.2.5.** Let $f$ be a classical modular form, and let $\pi$ be prime in $\mathbb{Q}_f$. We say $\pi$ *divides* a critical value $\Lambda(f, t)$ if, for even $t$:

$$\pi \mid \Lambda(f, t)/\omega_+, \tag{4.5}$$

or, for odd $t$,

$$\pi \mid \Lambda(f, t)/\omega_-. \tag{4.6}$$

Thus, we examine the ratios of even and odd critical values:

$$\Lambda(f, 2) : \Lambda(f, 4) : \cdots : \Lambda(f, r-2) \tag{4.7}$$

and

$$\Lambda(f, 1) : \Lambda(f, 3) : \cdots : \Lambda(f, r-1), \tag{4.8}$$

in order to eliminate the $\omega_{\pm}$, and check whether $p$ divides each term of the above ratios. We can easily check this using Theorem 1.3.51, i.e. if $N(p)$ divides one of the terms of

$$N(\Lambda(f,2)) : N(\Lambda(f,4)) : \cdots : N(\Lambda(f,r-2)) \tag{4.9}$$

or

$$N(\Lambda(f,1)) : N(\Lambda(f,3)) : \cdots : N(\Lambda(f,r-1)), \tag{4.10}$$

then by Theorem 1.3.51, $p$ divides the corresponding term of (4.7) or (4.8), and we say that $p$ divides the corresponding critical value $\Lambda(f,t)$ itself (by Definition 4.2.5).

Thus, after we find the critical values of a modular form $f$, we check the prime decomposition of each of the terms of (4.9) and (4.10) for any primes $\ell$ larger than the weight of $f$. By Definition 4.2.4, $\ell$ is a large prime; thus, Harder's Conjecture should apply for $f$ and $\ell$.

This procedure can be summarized in the following algorithm:

**Algorithm 4.2.6.** Let $f$ be a classical modular form of weight $r$.

1. Compute the even and odd ratios of critical values $\Lambda(f,1),\ldots,\Lambda(f,r-1)$ of $f$, using the methods in Section 2.4.
2. If these ratios are given exactly (i.e. Manin's equations were used solely), we skip to the next step. Otherwise, (i.e. if these ratios were computed using the equations of Section 2.2), we use `algdep` to provide a polynomial $p$ (which has degree equal to $[\mathbb{Q}(f):\mathbb{Q}]$) for which each ratio term is a root.
3. Find the norms of $N(\Lambda(f,t))$ of each ratio term.
4. Clear all of the denominators of the even and odd ratios, such that each ratio term is in $\mathbb{Z}$.
5. Factor each of the terms of the ratios

   $$N(\Lambda(f,2)) : N(\Lambda(f,4)) : \cdots : N(\Lambda(f,r-2)) \tag{4.11}$$

   and

   $$N(\Lambda(f,1)) : N(\Lambda(f,3)) : \cdots : N(\Lambda(f,r-1)). \tag{4.12}$$

6. Determine whether any primes in the terms of the above ratios are larger than $r$.

7. If such a prime exists, and is not a Bernoulli prime of weight $r$, then we know a large prime $\ell$ divides the corresponding critical value of $f$.

**Example 4.2.7.** Let $f \in S_{22}$. We compute $N(\Lambda(f,2)) : N(\Lambda(f,4)) : \cdots : N(\Lambda(f,20))$, using Sage:

$$\begin{gathered} -82080 : -97100640 : 7469280 : -3365280 : 574560 : \\ 574560 : -3365280 : 7469280 : -97100640 : -82080 \end{gathered}$$

Similarly, we compute $N(\Lambda(f,1)) : N(\Lambda(f,3)) : \cdots : N(\Lambda(f,21))$:

$$\begin{gathered} 15872220000 : -1648122528 : 212074590 : -34335886 : 6603055 : 0 : \\ -6603055 : 34335886 : -212074590 : 164812252 : -15872220000 \end{gathered}$$

Since $S_{22}$ is a one-dimensional space, we know that $\mathbb{Q}_f = \mathbb{Q}$. Thus, for each $\Lambda(f,t)$, $N(\Lambda(f,t)) = \Lambda(f,t)$. If we then factor each ratio term, we get

$$\begin{aligned} N(\Lambda(f,2)) : N(\Lambda(f,4)) : \cdots : N(\Lambda(f,10)) = \\ 2^5 \cdot 3^3 \cdot 5^4 \cdot 7 \cdot 13 \cdot 17 \cdot 19 : \\ -1 \cdot 2^5 \cdot 3 \cdot 13 \cdot 17 \cdot 131 \cdot 593 : \\ 2 \cdot 3 \cdot 5 \cdot 7 \cdot 13 \cdot 131 \cdot 593 : \\ -1 \cdot 2 \cdot 13 \cdot 17 \cdot 131 \cdot 593 : \\ 5 \cdot 17 \cdot 131 \cdot 593 \end{aligned}$$

and

$$\begin{aligned} N(\Lambda(f,1)) : N(\Lambda(f,3)) : \cdots : N(\Lambda(f,11)) = \\ -1 \cdot 2^5 \cdot 3^3 \cdot 5 \cdot 19 : \\ -1 \cdot 2^5 \cdot 3^3 \cdot 5 \cdot 7 \cdot 13^2 \cdot 19 : \\ 2^5 \cdot 3^3 \cdot 5 \cdot 7 \cdot 13 : \\ -1 \cdot 2^5 \cdot 3^3 \cdot 5 \cdot 19 \cdot 41 : \\ 2^5 \cdot 3^3 \cdot 5 \cdot 7 \cdot 19 : \\ 2^5 \cdot 3^3 \cdot 5 \cdot 7 \cdot 19 : \\ -1 \cdot 2^5 \cdot 3^3 \cdot 5 \cdot 19 \cdot 41 : 2^5 \cdot 3^3 \cdot 5 \cdot 7 \cdot 13 \cdot 19 : \\ 0. \end{aligned}$$

Both 131 and 594 are Bernoulli numbers of weight 22; thus, despite the fact that they are larger than 22, they are not large primes. The prime 41, however, is not a Bernoulli number, and is therefore a large prime.

**Example 4.2.8.** Let $f \in S_{28}$. $S_{28}$ is a two-dimensional space; thus, $[\mathbb{Q}(f) : \mathbb{Q}] = 2$. We compute the even and odd critical value ratios, using Sage (we only list critical values up to $t = r/2$, due to the symmetries discussed in Section 2.3):

$$\begin{aligned} &\Lambda(f,2) : \Lambda(f,4) : \cdots : \Lambda(f,14) \approx \\ &1 : -0.0657416395 : 0.0051115803 : -0.0004736837 : \\ &5.14533 \times 10^{-5} : -5.6821 \times 10^{-6} : 6.558 \times 10^{-7} \end{aligned}$$

$$\begin{aligned} &\Lambda(f,1) : \Lambda(f,3) : \cdots : \Lambda(f,13) \approx \\ &1 : -0.0607104106 : 0.0043345433 : -0.000367817 : \\ &3.71113 \times 10^{-5} : -4.2118 \times 10^{-6} : 3.966 \times 10^{-7}. \end{aligned}$$

Then, using `algdep`, we can find polynomials for which each of these critical value ratio terms is a root (see Tables 4.2 and 4.3).

| $t$ | $p_t(x)$ |
|---:|---:|
| 2 | $x - 1$ |
| 4 | $82555200000x^2 + 10861798608x + 357271915$ |
| 6 | $9398909520000x^2 - 96408856260x + 247224523$ |
| 8 | $9765100800000x^2 + 9386773668x + 2255305$ |
| 10 | $324689601600000x^2 - 35628539580x + 973609$ |
| 12 | $519503362560000x^2 + 8156801628x + 29575$ |
| 14 | $49952246400000x^2 - 250818660x + 143$ |

**Table 4.2:** For $f \in S_{28}$ and for even $t$, the polynomial $p_t$ for which the ratio term corresponding to $\Lambda(f, t)$ is a root.

| $t$ | $p_t(x)$ |
|---:|---:|
| 1 | $x - 1$ |
| 3 | $177542052187500x^2 + 21564388652625x + 654806568371$ |
| 5 | $66053447460000000x^2 - 573573698051400x + 1245150313949$ |
| 7 | $1003070421793440000000x^2 + 74316802008695400x + 13764509056379$ |
| 9 | $4702706782693920000000x^2 - 3598354508458374000x + 6877165357969$ |
| 11 | $1469350323080640000000x^2 + 1424400418960200x + 3392780147$ |
| 13 | $6435282965791680000000x^2 - 11106335140828200x + 3392780147$ |

**Table 4.3:** For $f \in S_{28}$ and for odd $t$, the polynomial $p_t$ for which the ratio term corresponding to $\Lambda(f, t)$ is a root.

We can then compute the norms of these ratio terms, and express them as a ratio of integers:

$$\begin{aligned}
N(\Lambda(f,2)) : N(\Lambda(f,4)) : \cdots : N(\Lambda(f,14)) = \\
-1 \cdot 2^12 \cdot 3^6 \cdot 5^5 \cdot 7^2 \cdot 11 \cdot 13 \cdot 19 \cdot 23 : \\
2^{12} \cdot 3^6 \cdot 5^6 \cdot 7^3 \cdot 11^2 \cdot 13^3 \cdot 17^2 \cdot 19^2 \cdot 23 : \\
2^{12} \cdot 3^6 \cdot 5^5 \cdot 7^3 \cdot 11 \cdot 13^3 \cdot 17 \cdot 19^2 \cdot 23 \cdot 647 : \\
2^{12} \cdot 3^6 \cdot 5^6 \cdot 7^2 \cdot 11 \cdot 13^3 \cdot 17 \cdot 19 \cdot 23 \cdot 157 : \\
2^{12} \cdot 3^6 \cdot 5^5 \cdot 7^3 \cdot 11 \cdot 13^3 \cdot 19 \cdot 23 \cdot 823 : \\
2^{12} \cdot 3^6 \cdot 5^7 \cdot 7^3 \cdot 11 \cdot 13^3 \cdot 19 \cdot 23 : \\
2^{12} \cdot 3^6 \cdot 5^5 \cdot 7^2 \cdot 11^2 \cdot 13^2 \cdot 19 \cdot 23
\end{aligned}$$

$$\begin{aligned}
N(\Lambda(f,1)) : N(\Lambda(f,3)) : \cdots : N(\Lambda(f,13)) = \\
2^{12}\cdot 3^{8}\cdot 5^{7}\cdot 7^{4}\cdot 11^{3}\cdot 13^{2}\cdot 17\cdot 19^{2}\cdot 23^{2} : \\
2^{10}\cdot 3^{4}\cdot 7\cdot 11\cdot 17\cdot 19^{2}\cdot 23^{2}\cdot 193\cdot 9349\cdot 362903 : \\
2^{4}\cdot 3^{4}\cdot 7^{2}\cdot 11\cdot 13\cdot 17\cdot 19^{2}\cdot 367\cdot 9349\cdot 362903 : \\
2^{2}\cdot 5\cdot 13\cdot 17\cdot 19^{2}\cdot 23\cdot 4057\cdot 9349\cdot 362903 : \\
2\cdot 7\cdot 11\cdot 13\cdot 17\cdot 23\cdot 2027\cdot 9349\cdot 362903 : \\
2\cdot 3^{2}\cdot 5\cdot 7^{2}\cdot 13\cdot 19\cdot 23\cdot 9349\cdot 362903 : \\
7\cdot 11\cdot 17\cdot 19\cdot 23\cdot 9349\cdot 362903.
\end{aligned}$$

Both 9349 and 362903 are Bernoulli numbers of weight 8; thus, they are not large primes. However, we find large primes in the factorizations in the following critical values (see Table 4.4):

| $t$ | $\ell \mid \Lambda(f,t)$ |
|---:|---:|
| 3 | 193 |
| 5 | 367 |
| 6 | 647 |
| 7 | 4057 |
| 8 | 157 |
| 9 | 2027 |
| 10 | 823 |
| 18 | 823 |
| 19 | 2027 |
| 20 | 157 |
| 21 | 4057 |
| 22 | 647 |
| 23 | 367 |
| 25 | 193 |

**Table 4.4:** Large primes dividing the critical values of $f \in S_{28}$.

**Example 4.2.9.** Let $f \in S_{32}$. Like $S_{28}$ in Example 4.2.8, $S_{32}$ is a two-dimensional space. Using similar methods to Example 4.2.8, we can compute the ratios

$$
\begin{gathered}
N(\Lambda(f,2)) : N(\Lambda(f,4)) : \cdots : N(\Lambda(f,16)) = \\
-1 \cdot 2^{11} \cdot 3^{11} \cdot 5^{4} \cdot 7^{4} \cdot 11 \cdot 13 \cdot 23 \cdot 29^{2} : \\
2^{11} \cdot 3^{11} \cdot 5^{6} \cdot 7^{4} \cdot 11 \cdot 13^{2} \cdot 17 \cdot 19 \cdot 23^{2} \cdot 29^{2} \cdot 7687 : \\
2^{11} \cdot 3^{11} \cdot 5^{5} \cdot 7^{4} \cdot 11 \cdot 13 \cdot 17 \cdot 19^{2} \cdot 23^{2} \cdot 29^{2} \cdot 751 : \\
2^{11} \cdot 3^{11} \cdot 5^{6} \cdot 7^{4} \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23 \cdot 29^{2} \cdot 31 \cdot 173 : \\
2^{11} \cdot 3^{11} \cdot 5^{5} \cdot 7^{4} \cdot 11 \cdot 13^{2} \cdot 17 \cdot 19 \cdot 23 \cdot 29^{2} \cdot 1307 : \\
2^{11} \cdot 3^{11} \cdot 5^{6} \cdot 7^{4} \cdot 11 \cdot 13 \cdot 17^{2} \cdot 23 \cdot 29^{2} : \\
2^{11} \cdot 3^{11} \cdot 5^{5} \cdot 7^{4} \cdot 11 \cdot 13 \cdot 23 \cdot 29^{2} \cdot 211 : \\
2^{11} \cdot 3^{11} \cdot 5^{6} \cdot 7^{4} \cdot 11 \cdot 13^{2} \cdot 23 \cdot 29^{2}
\end{gathered}
$$

$$
\begin{gathered}
N(\Lambda(f,1)) : N(\Lambda(f,3)) : \cdots : N(\Lambda(f,15)) = \\
-1 \cdot 2^{10} \cdot 3^{13} \cdot 5^{6} \cdot 7^{7} \cdot 11^{2} \cdot 13^{3} \cdot 17 \cdot 19^{2} \cdot 23^{2} \cdot 29^{2} : \\
2^{11} \cdot 3^{13} \cdot 5^{6} \cdot 7^{7} \cdot 11^{2} \cdot 13^{3} \cdot 17 \cdot 19^{2} \cdot 23^{2} \cdot 29^{2} \cdot 37 \cdot 683 \cdot 3119 \cdot 305065927 : \\
2^{10} \cdot 3^{13} \cdot 5^{6} \cdot 7^{7} \cdot 11^{2} \cdot 13^{3} \cdot 17 \cdot 19^{2} \cdot 23^{2} \cdot 29^{2} \cdot 37^{2} \cdot 683 \cdot 51199 \cdot 305065927 : \\
2^{10} \cdot 3^{13} \cdot 5^{6} \cdot 7^{7} \cdot 11^{2} \cdot 13^{3} \cdot 17 \cdot 19^{2} \cdot 23^{2} \cdot 29^{2} \cdot 37 \cdot 47 \cdot 67 \cdot 683 \cdot 305065927 : \\
2^{10} \cdot 3^{13} \cdot 5^{6} \cdot 7^{7} \cdot 11^{2} \cdot 13^{3} \cdot 17 \cdot 19^{2} \cdot 23^{2} \cdot 29^{2} \cdot 37 \cdot 503 \cdot 683 \cdot 14243 \cdot 305065927 : \\
2^{10} \cdot 3^{13} \cdot 5^{6} \cdot 7^{7} \cdot 11^{3} \cdot 13^{3} \cdot 17 \cdot 19^{2} \cdot 23^{2} \cdot 29^{2} \cdot 37 \cdot 683 \cdot 305065927 : \\
2^{10} \cdot 3^{13} \cdot 5^{6} \cdot 7^{7} \cdot 11^{2} \cdot 13^{3} \cdot 17 \cdot 19^{2} \cdot 23^{2} \cdot 29^{2} \cdot 37 \cdot 61 \cdot 683 \cdot 305065927 : \\
2^{10} \cdot 3^{13} \cdot 5^{6} \cdot 7^{7} \cdot 11^{2} \cdot 13^{3} \cdot 17 \cdot 19^{2} \cdot 23^{2} \cdot 29^{2} \cdot 37 \cdot 683 \cdot 305065927.
\end{gathered}
$$

After we disregard the Bernoulli numbers of weight 32, we list the large primes dividing the critical values of $f$ (see Table 4.5):

| $t$ | $\ell \mid \Lambda(f,t)$ |
|---:|---:|
| 3 | 3119 |
| 4 | 7687 |
| 5 | 51199 |
| 6 | 751 |
| 7 | 47 |
| 8 | 173 |
| 9 | 503 |
| 10 | 1307 |
| 13 | 61 |
| 14 | 211 |
| 18 | 211 |
| 19 | 61 |
| 22 | 1307 |
| 23 | 503 |
| 24 | 173 |
| 25 | 47 |
| 26 | 751 |
| 27 | 51199 |
| 28 | 7687 |
| 29 | 3119 |

**Table 4.5:** Large primes dividing the critical values of $f \in S_{32}$.

If a large prime $\ell$ divides the critical value $\Lambda(f,t)$ at $t$, then Harder's Conjecture should apply for $f$. This means that there should exist a Siegel modular form that is a Hecke eigenform of $S_{k,j}$ (see Section 1.5), with

$$j = 2t - r - 2 \tag{4.13}$$

and

$$k = r - t + 2, \tag{4.14}$$

for which the congruence in (4.1) should hold.

Even though they contain large primes, not all of the critical values listed in Tables 4.4 and 4.4 correspond to Siegel modular forms that we can calculate using the methods outlined in this text (we are able to calculate $S_{k,j}$ for even $k$ and $j = 0$

or $j = 2$). For example, if $r = 22$, the critical values $\Lambda(f, 8)$ and $\Lambda(f, 14)$ contain the large prime 41, yet we find that given 4.13 and 4.14, the conjecture should apply for $S_{16,-8}$ and $S_{10,4}$. The "space" $S_{16,-8}$ has $j < 0$, and thus is not a space of vector-valued Siegel modular forms. $S_{10,4}$ is a legitimate space of Siegel modular forms, yet we have not implemented methods for computing spaces of weight $(k, 4)$.

In fact, of the $f \in S_r$ with at least one large prime dividing a critical value of $f$, the least $r$ for which there exists a corresponding "legitimate," calculable (by our methods) $S_{k,j}$ is $r = 32$. We see that $\Lambda(f, 18)$ contains the large prime 211, and thus, given 4.13 and 4.14, $S_{32}$ should correspond with $S_{16,2}$ through the congruence in Harder's Conjecture.

Once we are given $S_{k,j}$, we then compute the Hecke eigenforms $F$ of the space (see Section 3.2). Then, for each eigenform $F$ and for each prime $p$, we compute the Hecke eigenvalue $\lambda_p$ corresponding to the Hecke operator $T_p$, using the methods outlined in Section 3.1.

After computing $\lambda_p$ and $a_p$, We then check the congruence in (4.1) through simple calculations in Sage:

**Algorithm 4.2.10.** Let $r, k, j, \ell, p, a_p$, and $\lambda_p$ be as defined in the hypothesis of Harder's Conjecture. We verify the congruence of the conjecture through the following process:

1. We construct the field $\mathbb{K} = \mathbb{Z}/\ell\mathbb{Z}$.
2. Let $A$ be the polynomial for which the $a_p$ are roots, and let $L$ be the polynomial for which the $\lambda_p$ are roots.
3. Let $\alpha_1, \ldots, \alpha_m$ denote the roots of $A$ in $\mathbb{K}$, and let $\nu_1, \ldots, \nu_n$ denote the roots of $L$ in $K$.
4. If some $\alpha_i$ is congruent to some $\nu_i$ in $\mathbb{K}$, then the conjecture is verified.

## 4.3 Results

We list the spaces of classical and Siegel modular forms for which Harder's Conjecture has been verified in Table 4.6:

| $(k, j)$ | $r$ | $\dim S_{k,j}^{(2)}$ | $\dim S_r^{(1)}$ | $t$ | ordinary $\ell \mid \mathrm{Norm}(\Lambda(f,t)/\omega_\pm)$ | $p$ |
|---|---|---|---|---|---|---|
| $(14, 2)$ | 28 | 1 | 2 | 16 | NONE | |
| $(16, 2)$ | 32 | 2 | 2 | 18 | 211 | $p \leq 31$ |
| $(18, 2)$ | 36 | 2 | 3 | 20 | 269741 | $p \leq 31$ |
| $(20, 2)$ | 40 | 3 | 3 | 22 | 509 | $p \leq 31$ |
| | | | | | 1447 | $p \leq 31$ |
| $(22, 2)$ | 44 | 5 | 3 | 24 | 205157 | $p \leq 31$ |
| $(24, 2)$ | 48 | 5 | 4 | 26 | 168943 | $p \leq 31$ |
| $(26, 2)$ | 52 | 8 | 4 | 28 | 173 | $p \leq 31$ |
| | | | | | 929 | $p \leq 31$ |
| | | | | | 4261 | $p \leq 31$ |
| | | | | | 434167 | $p \leq 31$ |
| $(28, 2)$ | 56 | 10 | 4 | 30 | 173 | $p \leq 31$ |
| | | | | | 1721 | $p \leq 31$ |
| | | | | | 38053 | $p \leq 31$ |
| | | | | | 1547453 | $p \leq 31$ |
| $(30, 2)$ | 60 | 11 | 5 | 32 | 325187 | $p \leq 31$ |
| | | | | | 32210303 | $p \leq 31$ |
| | | | | | 427092920047 | $p \leq 31$ |

**Table 4.6:** A summary of the cases for which Harder's Conjecture has been verified.

## 4.4 Conclusion

Since it is a fairly simple congruence calculation, the final verification of Harder's Conjecture is a relatively fast and easy computation. However, computing the components of the congruence can be much less trivial. Yet, with the exception of $S_{60}$, the computation of each critical value (using a hybridization of Manin's equations and direct periods calculations) is also relatively fast (usually taking on the order of minutes to complete). Since $S_{60}$ is a five-dimensional space, it is possible that the calculation of its critical values is slowed by `algdep` straining to produce a quintic polynomial.

However, what required the most computational resources, and what limited our range of primes $p$, was the calculation of the Hecke eigenvalues. The Hecke operators themselves do not require much time to complete; yet, they do require the computation of Siegel eigenforms to a certain number of coefficients (which increases as $p$

increases). For $k \leq 20$, the computation of the eigenforms of $S_{k,2}$ was relatively easy, as it requires only one or two Satoh bracket calculations. However, for higher $k$, the number of Satoh brackets (and multiplications of Satoh brackets) that are required drastically increases; for the these cases, the calculation of eigenforms to the required number of coefficients was often taxing to our systems.

Harder's Conjecture has previously been verified, but in limited cases. Most notably, Van der Geer verified it for one-dimensional spaces of classical and Siegel modular forms, and for $p \leq 37$. We therefore extend the work of these previous attempts by including higher-dimensional classical and Siegel spaces, and checking the congruence up to a comparable prime $p$.

# Chapter 5

# Appendices

## 5.1 Sage Code

Calling `classical_dim()` allows one to compute the dimension of a given space of modular forms of weight `weight`:

```
def mod_dim(x,y,k):
#returns how many integer solutions a,b solve x*a + y*b
#= k, thus, lets you find the dimension of a space of weight-k cuspidal
#forms using "dim = mod_dim(4,6,weight - 12)"

     no_solutions = 0
     for a in [0..k]:
     for b in [0..k]:
     if (x*a + y*b) == k:
          no_solutions += 1
     return no_solutions

def classical_dim(weight):
     dim = mod_dim(4,6,weight - 12)
     return dim
```

The following code lets us directly calculate periods:

```
def r(j,f,prec):
#Nathan Ryan’s Code:  Explicitly calculates a given period
#r_j, up to a certain precision.  This calls the below function

   if f.base_ring() == QQ:
       return (factorial(j)*I^(j+1)/2^(j+1)/pi^(j+1)*
f.cuspform_lseries(prec)(j+1)).n(prec)
   else:
       return (factorial(j)*I^(j+1)/2^(j+1)/pi^(j+1)*
my_cuspform_lseries(f,prec)(j+1)).n(prec)

def my_cuspform_lseries(f, prec=53, max_imaginary_part=0,
max_asymp_coeffs=40):
#Nathan Ryan’s Code:

   if f.q_expansion().list()[0] !=0:
       raise TypeError,"f = %s is not a cusp form"%self
   from sage.lfunctions.all import Dokchitser
   key = (prec, max_imaginary_part, max_asymp_coeffs)
   l = f.weight()
   N = f.level()
   w = f.atkin_lehner_eigenvalue()
   if w is None:
       raise ValueError, "Form is not an eigenform for Atkin-Lehner"
   e = (-1)**(l/2)*w
   L = Dokchitser(conductor = N,
                      gammaV = [0,1],
                      weight = l,
                      eps = e,
                      prec = prec)
   phi = f.hecke_eigenvalue_field().complex_embeddings(prec)[0]
   my_qexp = [ phi(a) for a in f.q_expansion(prec).list() ]
   s = ’coeff = %s;’%my_qexp#f.q_expansion(prec).list()
   #print s
   L.init_coeffs(’coeff[k+1]’,pari_precode = s,
                     max_imaginary_part=max_imaginary_part,
                     max_asymp_coeffs=max_asymp_coeffs)
   L.check_functional_equation()
   L.rename(’L-series associated to the cusp form %s’%f)
   return L
```

The following code is an implementation of Manin's equations:

```
def delta_solutions(n):
#Used for the outer sum of Manin's Coefficient Theorem; the sum is
#taken over special solutions to "n = D1*D2 + d1*d2"
     d1_list = [1..n]
     d2_list = [0..n]
     D1_list = [1..n]
     D2_list = [0..n]

     output_list = []
     for d1 in d1_list:  #"Brute-force" method - tries every
#possible delta-value to see if they satisfy Manin's criteria
          for d2 in d2_list:
               for D1 in D1_list:
                    for D2 in D2_list:
                         if (n == D1*D2 + d1*d2) and (D1 > d1):
                              if (D2 > d2) and (d2 > 0):
                                   output_list.append([D1,D2,d1,d2])
                              elif (n % D1 == 0) and (D2 == n/D1)
and (d2 == 0) and (d1/D1 <= (1/2)):
                                   output_list.append([D1,D2,d1,d2])

     return output_list

def inner_coeffs(omega,deltas):
#returns r_2, r_4, r_6 . . . given the weight omega
#and the list [D,D',d,d']

     l_list = [1..((omega - 2)/4)]
     return [2*binomial(omega,2*l)*(deltas[0]^(2*l)*deltas[2]^(omega-2*l) -
deltas[0]^(omega-2*l)*deltas[2]^(2*l)) for l in l_list]

def sigma(x,n): #returns sigma_n (x)
     running_sum = 0
     d_list = divisors(n)
     for d in d_list:
```

```
     running_sum += d^(x)

     return running_sum

def lamb(f,n):  #returns the nth coefficent of the modular form f
     return f[n]

def outer_sum(omega,n):  #Actually computes the outer sum of
#Manin's Coefficient Theorem

     running_sum = [0*i for i in [1..((omega - 2)/4)]]
     for deltas in delta_solutions(n):
          if (deltas[2]/deltas[0] == 1/2) and (deltas[3] == 0):
               leading_term = 1/2
          else:
               leading_term = 1
          for j in [0..(len(running_sum) - 1)]:
               running_sum[j] += leading_term * inner_coeffs(omega,deltas)[j]
     return running_sum


def coeffs_matrix(f,n):
#returns a matrix of coefficients to r_2l with n number of rows,
#with the r_0 term at the leftmost end of the matrix
     omega = f.weight() - 2
     F = f.hecke_eigenvalue_field() #makes sure the matrix
# is in the correct field
     output_list = []
     for m in [2..n]:  #n = 2 is the base case for
#Manin's Coefficient Theorem
          row_next = [-(sigma(omega + 1,m) - lamb(f,m))]
          for i in outer_sum(omega,m):
               row_next.append(i)
  output_list.append(row_next)
     output_matrix = matrix(F,output_list)
     return output_matrix

def coeffs_matrix_solve(f,n):
#puts the matrix produced by the Coefficient Theorem
```

```
#in row-reduced echelon form, and solves it.  The
#final row of the matrix is, therefore, the vector
#(1, r2 / r0, r4 / r0, . . .)

     M = coeffs_matrix(f,n)
     no_cols = M.ncols()
     N = M.rref()
     last_col = N.column(no_cols - 1).list()
     output_list = []
     for i in [0..(no_cols - 2)]:
          output_list.append(-last_col[i])
     output_list.append(1)
     output_vector = vector(output_list)
     return output_vector / output_list[0]

def periods_ratio(f):
#automatically calculates how how many rows of the
#above matrix are needed to solve the matrix
     omega = f.weight() - 2
     return coeffs_matrix_solve(f,ceil((omega - 2) / 4) + 2)

def even_periods(f):
     return periods_ratio(f)
```

Then, using a combination of Manin's equations and direct calculations, we can calculate the norms of the even and odd ratios of periods:

```
def odd_norms2(g, prec = 1200):
#Allows us to calculate all of the odd period ratios.
#Manin 5k, 6k, 7k do not provide enough information to
#calculate periods of modular forms in spaces of
#dimenion two or higher.  For dimension 2 spaces, the
#ratios r3 / r1 and r5 / r1 are needed, and are
#calculated explicitly.

 #For higher dimenions, it is necessary to calculate more of such ratios explicitl
    A = full_odd_matrix(g).rref()
    omega = g.weight() - 2
    weight = g.weight()
    dim = mod_dim(4,6,weight - 12) #the dimension of g
    if (dim > 1):
#If the dimension is one, then Manin 5k, 6k, and 7k are
#enough information to calculate all of the period ratios.
        r_one = r(1,g,prec)
    r_list = []
    for i in [0..(dim - 1)]:
        if (dim > 1):
    r_list.append(r(2*i + 1,g,prec) / r_one)
        else:
            r_list.append(1)

    for j in [dim..(omega/2 - dim)]:
        jth_row = A.row(j)
        next_period = sum([r_list[i - 1]*jth_row[-i] for i in [1..dim]])
        r_list.append(next_period)

    poly_list = [algdep(xx,dim) for xx in r_list]
    denom_list = [pp.coeffs()[-1] for pp in poly_list]
    ll = lcm(denom_list)
    odd_norm_list = [factor(ll*pp(x=0)) for pp in poly_list[:-2]]

    return odd_norm_list

def even_norms2(g):
#Uses Manin's equations (specifically the Coefficient Theorem,
#as shown above, to calculate the ratio of even periods)

    even_periods_list = even_periods(g)
    pre_norm_list = [norm(x) for x in even_periods_list]
    denom_list = [x.denominator() for x in pre_norm_list]
    ll = lcm(denom_list)
    int_list = (vector(pre_norm_list)*ll).list()
    even_norm_list = [factor(i) for i in int_list]

    return even_norm_list
```

Or, we can directly calculate each period, and then calculate the norms of each ratio term:

```
def odd_norms_nathans_method(f,prec = 1200):
#Directly calculates all of the odd periods
#(using none of Manin’s equations)

    r1 = r(1,f,prec)
    k = f.weight()
    dim = mod_dim(4,6,k - 12)
    omega = k - 2
    period_list = [r(j,f,prec)/r1 for j in range(1,omega,2)]
    period_list.append(-r(k - 3,f,prec)/r1)
    poly_list = [algdep(xx,dim) for xx in period_list]
    denom_list = [pp.coeffs()[-1] for pp in poly_list]
    ll = lcm(denom_list)
    odd_norm_list = [factor(ll*pp(x=0)) for pp in poly_list[:-1]]
    return odd_norm_list

def even_norms_nathans_method(f,prec = 1200):
#Directly calculates all of the even periods
#(using none of Manin’s equations)

    k = f.weight()
    r0 = r(0,f,prec)
    omega = k - 2
    dim = mod_dim(4,6,k - 12)
    period_list = [r(j,f,prec)/r0 for j in range(0,omega+1,2)]
    period_list.append(r(k - 2,f,prec)/r0)
    poly_list = [algdep(xx,dim) for xx in period_list]
    if x in poly_list:
        poly_list.remove(x)
    denom_list = [pp.coeffs()[-1] for pp in poly_list]
    ll = lcm(denom_list)
    even_norm_list = [factor(ll*pp(x=0)) for pp in poly_list[:-1]]
    return even_norm_list
```

Then, we use the following code to compute the ratios of critical value norms, given one of the above two methods of periods calculations (`lambda_ratios_full()` automatically removes the Bernoulli primes from each critical value prime decomposition):

```
def lambda_ratios_even(g,davidsMethod = True,prec = 1200):
    if davidsMethod:
        return odd_norms2(g,prec)
    else:
    return odd_norms_nathans_method(g,prec)

def lambda_ratios_odd(g,davidsMethod = True,prec = 1200):
    if davidsMethod:
        return even_norms2(g)
    else:
        return even_norms_nathans_method(g,prec)

def lambda_ratios_full(f,davidsMethod = True,prec = 1200):
    k = f.weight()
    c = k/2
    start_list_even = lambda_ratios_even(f,davidsMethod,prec)
    start_list_odd = lambda_ratios_odd(f,davidsMethod,prec)
    true_final_output = []
    bern_list = factor(bernoulli(k).numerator())
    for t in [1..(k - 1)]:
        if (t % 2 == 0):
            start_list = start_list_even
            odd = false
        else:
            start_list = start_list_odd
            odd = true

        if (t < c):
            output = start_list[ceil(t/2) - 1]
        if (t == c):
            if (c % 2 == 0):
                output = start_list[ceil(t/2) - 1]
            else:
                output = [(0,0)]
        if (t > c):
                u = k - t
                output = -start_list[ceil(u/2) - 1]

        final_output = []
        for (p,e) in output:
            add_p_e = true
                for (b_p,b_e) in bern_list:  #bernoulli primes
                    if (abs(p) == abs(b_p)):
                        add_p_e = false
                    if add_p_e:
                        final_output.append((p,e))

            true_final_output.append(final_output)

    return true_final_output
```

We can then check which large primes divide the critical values of a certain modular form. The following code outputs a list, where each entry is itself a list, including the weight of the given modular form, any large primes and the critical values that they divide, and the corresponding space of Siegel modular forms for which the conjecture should hold:

```
def large_prime_check(weight,loadFromFile = False,
davidsMethod = True,prec = 1200):
    f = create_form(weight)
    k = weight
    if loadFromFile:
        filename = ’CRIT_VALS/crit_vals’ + str(k)
        loaded_tuple = load(filename)
        full_list = [i for i in loaded_tuple]
    else:
        full_list = lambda_ratios_full(f,davidsMethod,prec)
    output_list = []
    for t in [1..(k - 1)]:
        current_row = [weight]
        current_row.append(t)
        L = full_list[t - 1]
        large_primes = false
        prime_list = []
        for (p,e) in L:
            if p > k:
                large_primes = true
                prime_list.append(p)
            current_row.append(prime_list)
if large_primes:
    current_row.append((k - t + 2,2*t - k - 2))
    output_list.append(current_row)

    return output_list
```

# References

[1] C. Batut, K. Belabas, D. Benardi, H. Cohen, and M. Olivier, *User's guide to PARI-GP*, 1998, `http://pari.home.ml.org`.

[2] J.P. Borwein, *Experimental and computational mathematics: Selected writings*, Perfectly Scientific Press, 2010.

[3] J.H. Bruinier, *The 1-2-3 of modular forms: lectures at a summer school in nordfjordeid, norway*, Universitext (1979), Springer, 2008.

[4] H. Cohen, *A course in computational algebraic number theory*, Graduate texts in mathematics, Springer-Verlag, 1993.

[5] F. Diamond and J.M. Shurman, *A first course in modular forms*, Graduate texts in mathematics, Springer, 2005.

[6] Neil Dummigan, *Period ratios of modular forms*, Math. Ann. **318** (2000), no. 3, 621–636. MR 1800772 (2002a:11049)

[7] Loo Keng Hua, *Introduction to number theory*, Springer-Verlag, 1982.

[8] Tomoyoshi Ibukiyama, *A conjecture on a Shimura type correspondence for Siegel modular forms, and Harder's conjecture on congruences*, Modular forms on Schiermonnikoog, Cambridge Univ. Press, Cambridge, 2008, pp. 107–144. MR 2512360 (2010j:11075)

[9] Jun-ichi Igusa, *On Siegel modular forms of genus two*, Amer. J. Math. **84** (1962), 175–200. MR 0141643 (25 #5040)

[10] Ju. I. Manin, *Periods of cusp forms, and $p$-adic Hecke series*, Mat. Sb. (N.S.) **92(134)** (1973), 378–401, 503. MR 0345909 (49 #10638)

[11] Martin Raum, Nathan C. Ryan, Nils-Peter Skoruppa, and Gonzalo Tornaría, *Siegel modular form package*, `http://hg.countnumber.de`, 2009.

[12] Martin Raum, Nathan C. Ryan, Nils-Peter Skoruppa, and Gonzalo Tornaría, *Explicit Computations of degree 2 Siegel modular forms*, (Preprint).

[13] Takakazu Satoh, *Construction of certain vector valued Siegel modular forms of degree two*, Proc. Japan Acad. Ser. A Math. Sci. **61** (1985), no. 7, 225–227. MR 816719 (87b:11041)

[14] W.A. Stein, *Modular forms, a computational approach*, Graduate studies in mathematics, American Mathematical Society, 2007.

[15] W. A. Stein et al., *Sage Mathematics Software (Version 4.7.2)*, The Sage Development Team, 2011, `http://www.sagemath.org`.