# Computing With Modular Forms

William Stein

October 24, 2005

# Contents


**Preface** **7**

**1 Modular Forms** **9**

1.1 Basic Definitions . . . 9
1.2 Modular Forms of Level 1 . . . 10
1.3 Modular Forms of Any Level . . . 12
1.4 Eisenstein Series and Delta . . . 13
1.5 Structure Theorem . . . 16
1.6 Hecke Operators . . . 18
1.7 The Victor Miller Basis . . . 22
1.8 The Complexity of Computing Fourier Coefficients . . . 24
1.9 Exercises . . . 25

**2 Dirichlet Characters** **27**

2.1 Decomposing Modular Forms Using Dirichlet Characters . . . 28
2.2 Representation and Arithmetic . . . 29
2.3 Algorithms . . . 34
2.4 Alternative Representations of Characters . . . 38
2.5 Exercises . . . 39

**3 Eisenstein Series** **41**

3.1 Generalized Bernoulli Numbers . . . 41
3.2 Explicit Basis for the Eisenstein Subspace . . . 43
3.3 Exercises . . . 45

**4 Dimensions Formulas** **47**

4.1 Modular Forms for $\Gamma_0(N)$ . . . 48
4.1.1 New and Old Subspaces . . . 49
4.2 Modular Forms for $\Gamma_1(N)$ . . . 52
4.3 Modular Forms with Character . . . 53
4.4 Exercises . . . 56

**5 Linear Algebra** **57**
5.1 Echelon Forms of Matrices . . . . . . . . . . . . . . . . . . . . . . . 57
5.2 Echelon Forms over $\mathbb{Q}$ . . . . . . . . . . . . . . . . . . . . . . . 60
5.3 Polynomials . . . . . . . . . . . . . . . . . . . . . . . . . . . . 65
5.4 Decomposing Spaces . . . . . . . . . . . . . . . . . . . . . . . . 65
5.4.1 Wiedemann's Minimal Polynomial Algorithm . . . . . . . 66
5.4.2 Polynomial Factorization . . . . . . . . . . . . . . . . . . . 70
5.4.3 Decomposition Using Kernels . . . . . . . . . . . . . . . . 70
5.4.4 Multi-Modular Decomposition Algorithm . . . . . . . . . 70

**6 Modular Symbols** **73**
6.1 Modular Symbols . . . . . . . . . . . . . . . . . . . . . . . . . . 74
6.2 Manin Symbols . . . . . . . . . . . . . . . . . . . . . . . . . . . 75
6.2.1 Coset Representatives and Manin Symbols . . . . . . . . 79
6.2.2 Modular Symbols With Character . . . . . . . . . . . . . 80
6.3 Hecke Operators . . . . . . . . . . . . . . . . . . . . . . . . . . 80
6.3.1 General Definition of Hecke Operators . . . . . . . . . . . 81
6.3.2 Hecke Operators on Manin Symbols . . . . . . . . . . . . 83
6.3.3 Remarks on Complexity . . . . . . . . . . . . . . . . . . . 84
6.4 Cuspidal Modular Symbols . . . . . . . . . . . . . . . . . . . . . 85
6.5 The Pairing Between Modular Symbols and Modular Forms . . . 86
6.6 Explicitly Computing $\mathbb{M}_k(\Gamma_0(N)$ . . . . . . . . . . . . . . . . 90
6.6.1 Computing $\mathbb{P}^1(\mathbb{Z}/N\mathbb{Z})$ . . . . . . . . . . . . . . . . . . 91
6.6.2 Examples of Computation of $\mathbb{M}_k(\Gamma_0(N))$ . . . . . . . . . 94
6.6.3 Refined Algorithm For Computing Presentation . . . . . . 102
6.7 Applications . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 105
6.7.1 Later in this Book . . . . . . . . . . . . . . . . . . . . . . 105
6.7.2 Discussion of the Literature and Research . . . . . . . . . 105
6.8 Exercises . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 106

**7 Computing Spaces of Modular Forms** **109**
7.1 Atkin-Lehner-Li Theory . . . . . . . . . . . . . . . . . . . . . . 109
7.2 Computing Cuspforms Using Modular Symbols . . . . . . . . . . . . . . . . . . . . . . . . . . 111
7.3 Computing Systems of Eigenvalues . . . . . . . . . . . . . . . . . 112
7.3.1 Computing Projection Onto a Subspace . . . . . . . . . . 113
7.3.2 Systems of Eigenvalues . . . . . . . . . . . . . . . . . . . . 113

**8 Periods and Special Values of $L$-functions** **117**
8.1 The Period Mapping and Complex Torus Attached to a Newform 117
8.2 Extended Modular Symbols . . . . . . . . . . . . . . . . . . . . . 119
8.3 Numerically Approximating Period Integrals . . . . . . . . . . . . 119
8.4 Speeding Convergence Using the Atkin-Lehner Operator . . . . . 123
8.4.1 Another Atkin-Lehner Trick . . . . . . . . . . . . . . . . . 124
8.5 Computing the Period Mapping . . . . . . . . . . . . . . . . . . . 125
8.6 Computing Elliptic Curves of Given Conductor . . . . . . . . . . 126

8.6.1 Using Modular Symbols . . . . . . . . . . . . . . . . . . . . 126
8.6.2 Finding Curves by Finding $S$-Integral Points . . . . . . . . 128
8.7 Examples . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 129
8.7.1 Jacobians of genus-two curves . . . . . . . . . . . . . . . . 129
8.7.2 Level one cusp forms . . . . . . . . . . . . . . . . . . . . . 130
8.7.3 CM elliptic curves of weight greater than two . . . . . . . 131
8.8 Exercises . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 131

**9 Congruences 133**
9.1 Congruences Between Modular Forms . . . . . . . . . . . . . . . 133
9.1.1 The $j$-invariant . . . . . . . . . . . . . . . . . . . . . . . 133
9.1.2 Congruences for Modular Forms . . . . . . . . . . . . . . . 134
9.1.3 Congruence for Newforms . . . . . . . . . . . . . . . . . . . 137
9.2 Generating the Hecke Algebra as a $\mathbb{Z}$-module . . . . . . . . . . . 138

# Preface

This is a book about algorithms for computing with modular forms that started as a series of notes for a graduate course at Harvard University in 2004. This book is meant to answer the question "How do *you* compute spaces of modular forms", by both providing a clear description of the specific algorithms that are used and explaining how to apply them using SAGE [SJ05].

I have spent many years trying to find good practical ways to compute with classical modular forms for congruence subgroups of $\mathrm{SL}_2(\mathbb{Z})$, and have implemented most of these algorithms several times, first in C++ [Ste99], then in MAGMA [BCP97], and most recently as part of SAGE. Much of this work has involved turning formulas and constructions burried in obscure research papers into precise computational recipes, then testing these in many cases and eliminating subtle inaccuracies (published theorems sometimes contain small mistakes that appear magnified when implemented and run on a computer). The goal of this book is to explain some of what I have learned along the way.

The author is aware of no other books on computing with modular forms, the closest work being Cremona's book [Cre97a], which is about computing with elliptic curves, and Cohen's book [Coh93] about algebraic number theory. The field is not yet mature, and there are missing details and potential improvements to many of the algorithms, which you the reader might fill in, and which would be greatly appreciated by other mathematicians.

This book focuses on how best to compute the spaces $M_k(N, \varepsilon)$ of modular forms, where $k \geq 2$ is an integer and $\varepsilon$ is a Dirichlet character modulo $N$. I will spend the most effort explaining the algorithms that appear so far to be the best (in practice!) for such computations. I will not discuss computing half-integral weight forms, weight one forms, forms for non-congruence subgroups or groups other than $\mathrm{GL}_2$, Hilbert and Siegel modular forms, trace formulas, $p$-adic modular forms, and modular abelian varieties, all of which are topics for another book.

The reader is not assumed to have prior exposure to modular forms, but should be familiar with abstract algebra, basic algebraic number theory, Riemann surfaces, and complex analysis.

**Acknowledgement.** Kevin Buzzard made many helpful remarks which were helpful in finding the algorithms in Chapter 2. Noam Elkies made many remarks about chapters 1 and 2. The students in the Harvard course made helpful remark; in particular, Abhinav Kumar made observations about computing widths of cusps, Thomas James Barnet-Lamb about how to represent Dirichlet characters, and Tseno V. Tselkov, Jennifer Balakrishnan and Jesse Kass made other remarks.

Parts of Chapter 7 follow [Ser73, Ch. VII] closely, though we adjust the notation, definitions, and order of presentation to be consistent with the rest of this book. (For example, Serre writes $2k$ for the weight instead of $k$.)

**Grant Information.** This material is based upon work supported by the National Science Foundation under Grant No. 0400386.

# Chapter 1

# Modular Forms

## 1.1 Basic Definitions

Modular forms are certain types of functions on the *complex upper half plane*

$$\mathfrak{h} = \{z \in \mathbb{C} : \mathrm{Im}(z) > 0\}.$$

The group

$$\mathrm{SL}_2(\mathbb{R}) = \left\{ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) : ad - bc = 1, \text{ and } a, b, c, d \in \mathbb{R} \right\}$$

acts on $\mathfrak{h}$ via linear fractional transformations, as follows. If $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{R})$ and $z \in \mathfrak{h}$, then (see Exercise 7.1)

$$\gamma(z) = \frac{az + b}{cz + d} \in \mathfrak{h}. \tag{1.1.1}$$

**Definition 1.1.1** (Modular Group)**.** The *modular group* is the subgroup $\mathrm{SL}_2(\mathbb{Z})$ of $\mathrm{SL}_2(\mathbb{R})$ of matrices with integer entries. Thus is is the group of all matrices $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ with $a, b, c, d \in \mathbb{Z}$ and $ad - bc = 1$.

For example, the matrices

$$S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \qquad \text{and} \qquad T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \tag{1.1.2}$$

are both elements of $\mathrm{SL}_2(\mathbb{Z})$; the matrix $S$ defines the function $z \mapsto -1/z$, and $T$ the function $z \mapsto z + 1$.

**Theorem 1.1.2.** *The group* $\mathrm{SL}_2(\mathbb{Z})$ *is generated by* $S$ *and* $T$*.*

*Proof.* See e.g. [Ser73, §VII.1], which uses the fundamental domain $\mathcal{F}$ consisting of all elements of $\mathfrak{h}$ that satisfy $|z| \geq 1$ and $\mathrm{Re}(z) \leq 1/2$. $\square$

In SAGE we compute the group $\mathrm{SL}_2(\mathbb{Z})$ and its generators as follows:

```
sage: G = SL(2,Z)
sage: print G
The modular group SL(2,Z)
sage: S, T = G.gens()
sage: S
[ 0 -1]
[ 1  0]
sage: T
[1 1]
[0 1]
```

**Definition 1.1.3** (Holomorphic and Meromorphic)**.** A function $f : \mathfrak{h} \to \mathbb{C}$ is *holomorphic* if $f$ is complex differentiable at every point $z \in \mathfrak{h}$, i.e., for each $z \in \mathfrak{h}$ the limit $\lim_{h\to 0}(f(z+h) - f(z))/h$ exists, where $h$ may approach 0 along any path. The function $f$ is *meromorphic* if it is holomorphic except (possibly) at a discrete set of points in $\mathfrak{h}$.

The function $f(z) = e^z$ is a holomorphic function on $\mathfrak{h}$ (in fact on all of $\mathbb{C}$). The function $1/(z-i)$ is meromorphic on $\mathfrak{h}$, and fails to be analytic at $i$.

Modular forms are holomorphic functions on $\mathfrak{h}$ that transform in a particular way under a subgroup of $\mathrm{SL}_2(\mathbb{Z})$. Before definining general modular forms, we define modular forms of level 1.

## 1.2 Modular Forms of Level 1

**Definition 1.2.1** (Weakly Modular Function)**.** A *weakly modular function* of weight $k \in \mathbb{Z}$ is a meromorphic function $f$ on $\mathfrak{h}$ such that for all $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$ and all $z \in \mathfrak{h}$ we have

$$f(z) = (cz+d)^{-k} f(\gamma(z)). \tag{1.2.1}$$

The constant functions are weakly modular of weight 0. There are no nonzero weakly modular functions of odd weight (see Exercise 7.4), and it is by no means obvious that there are any weakly modular functions of even weight $k \geq 2$. The product of two weakly modular functions of weights $k_1$ and $k_2$ is a weakly modular function of weight $k_1 + k_2$ (see Exercise 7.3), so once we find some nonconstant weakly modular functions, we'll find many of them.

When $k$ is even (1.2.1) has a possibly more conceptual interpretation; namely (1.2.1) is the same as

$$f(\gamma(z))d(\gamma(z))^{k/2} = f(z)dz^{k/2}.$$

Thus (1.2.1) simply says that the weight $k$ "differential form" $f(z)dz^{k/2}$ is fixed under the action of every element of $\mathrm{SL}_2(\mathbb{Z})$.

Since $\mathrm{SL}_2(\mathbb{Z})$ is generated by the matrices $S$ and $T$ of (1.1.2), to show that a meromorphic function $f$ on $\mathfrak{h}$ is a weakly modular function all we have to do is show that for all $z \in \mathfrak{h}$ we have

$$f(z+1) = f(z) \qquad \text{and} \qquad f(-1/z) = z^k f(z). \tag{1.2.2}$$

Suppose that $f$ is a weakly modular function of some weight $k$. Then $f$ might have a *Fourier expansion*, which we try to obtain as follows. Let $q = q(z) = e^{2\pi i z}$, which we view as a holomorphic function $\mathbb{C} \cup \infty \to D$, where $D$ is the closed unit disk. Let $D'$ be the punctured unit disk, i.e., $D$ with the origin removed, and note that $q : \mathbb{C} \to D'$. By (1.2.2) we have $f(z+1) = f(z)$, so there is a set-theoretic map $F : D' \to \mathbb{C}$ such that for every $z \in \mathfrak{h}$ we have $F(q(z)) = f(z)$. This function $F$ is thus a complex-valued function on the open unit disk. It may or may not be well behaved at 0.

Suppose that $F$ is well-behaved at 0, namely that for some $m \in \mathbb{Z}$ and all $q$ in a neighborhood of 0 we have the equality

$$F(q) = \sum_{n=m}^{\infty} a_n q^n.$$

If this is the case, we say that $f$ is *meromorphic at* $\infty$. If, moreover, $m \geq 0$, then we say that $f$ is *holomorphic at* $\infty$.

**Definition 1.2.2** (Modular Function)**.** A *modular function* of weight $k$ is a weakly modular function of weight $k$ that is meromorphic at $\infty$.

**Definition 1.2.3** (Modular Form)**.** A *modular form* of weight $k$ (and level 1) is a modular function of weight $k$ that is holomorphic on $\mathfrak{h}$ and at $\infty$.

If $f$ is a modular form, then there are complex numbers $a_n$ such that for all $z \in \mathfrak{h}$,

$$f(z) = \sum_{n=0}^{\infty} a_n q^n = \sum_{n=0}^{\infty} a_n e^{2\pi i n z}.$$

**Proposition 1.2.4.** *The above series converges for all $z \in \mathfrak{h}$.*

*Proof.* n The function $f(q)$ is holomorphic on $D$, so its Taylor series converges absolutely in $D$. See also [Ser73, §VII.4] for an explicit bound on the $|a_n|$. $\square$

We set $f(\infty) = a_0$, since $q^{2\pi i z} \to 0$ as $z \to i\infty$, and the value of $f$ at $\infty$ should be the value of $F$ at 0, which is $a_0$ from the power series.

**Definition 1.2.5** (Cusp Form)**.** A *cusp form* of weight $k$ (and level 1) is a modular form of weight $k$ such that $f(\infty) = 0$, i.e., $a_0 = 0$.

## 1.3 Modular Forms of Any Level

We next define spaces of modular forms of level possibly bigger than 1. When $k = 2$ these are closely related to elliptic curves and abelian varieties.

For each positive integer $N$, define a subgroup of $\mathrm{SL}_2(\mathbb{Z})$ as follows:

$$\Gamma_1(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \pmod{N} \right\}.$$

This is a "congruence subgroup", since it is given by congruence conditions. We are now in a position to define $M_k(\Gamma_1(N))$.

**Definition 1.3.1** (Modular Forms)**.** Let $M_k(\Gamma_1(N))$ be the complex vector space of holomorphic functions $f : \mathfrak{h}^* \to \mathbb{C}$ such that $f|[\gamma]_k = f$ for all $\gamma \in \Gamma_1(N)$.

What it means for $f$ to be holomorphic at the elements of $\mathbb{Q} \cup \{i\infty\}$ is subtle. We say $f$ is *holomorphic* at $i\infty$ if its $q$-expansion $\sum a_n q^n$ has no nonzero coefficient $a_n$ for $n < 0$. To make sense of holomorphicity of $f$ at $\alpha \in \mathbb{Q}$, let $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ be such that $\gamma(\infty) = \alpha$. We say $f$ is holomorphic at $\alpha$ if $f|[\gamma]_k$ is holomorphic at infinity. Note that formally

$$f|[\gamma]_k(\infty) = (cz + d)^{-k} f(\alpha),$$

where $(c, d)$ is the bottom row of $\gamma$ and the factor $(cz + d)^{-k}$ does not affect holomorphicity at $\alpha$.

Another subtlety hidden in this definition is that $f|[\gamma]_k$ is a modular form for the conjugate group $G = \gamma^{-1}\Gamma_1(N)\gamma$, which need not equal $\Gamma_1(N)$. In particular, the matrix $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ need not be in $G$, so $f|[\gamma]_k$ need not even have a power series expansion $\sum_{n\in\mathbb{Z}} b_n q^n$ at infinity! Fortunately (see Exercise 3.1) there is some positive integer $h$ such that $\left(\begin{smallmatrix} 1 & h \\ 0 & 1 \end{smallmatrix}\right) \in G$, so $f|[\gamma]_k$ has a power series expansion $\sum_{n\in\mathbb{Z}} b_{n/h} q^{n/h}$ in powers of $q^{1/h}$, and we again say $f|[\gamma]_k$ is holomorphic at infinity if $b_{n/h} = 0$ for all $n < 0$. (The reason we obtain a power series in $q^{1/h}$ is that $f|[\gamma]_k(hz)$ is invariant under $z \mapsto z + 1$, so $f|[\gamma]_k(hz)$ has an expansion in powers of $q$.)

A *congruence subgroup* is a subgroup $\Gamma$ of $\mathrm{SL}_2(\mathbb{Z})$ that contains the kernel $\Gamma(N) = \ker(\mathrm{SL}_2(\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z}))$ for some $N$. The smallest such $N$ is the *level* of $\Gamma$.

**Definition 1.3.2** (Width of Cusp)**.** The minimal $h$ such that $\left(\begin{smallmatrix} 1 & h \\ 0 & 1 \end{smallmatrix}\right) \in \gamma^{-1}\Gamma\gamma$ is called the *width of the cusp* $\gamma(\infty)$ for the group $\Gamma$.

**Algorithm 1.3.3** (Width of Cusp)**.**
Given a congruence subgroup $\Gamma$ of level $N$ and a cusp $\alpha$ for $\Gamma$, this algorithm computes the width $h$ of $\alpha$. We assume that $\Gamma$ is given by congruence conditions, e.g., $\Gamma = \Gamma_0(N)$ or $\Gamma_1(N)$.

1. [Find $\gamma$] Using the extended Euclidean algorithm, find $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ such that $\gamma(\infty) = \alpha$. If $\alpha = \infty$ set $\gamma \leftarrow 1$; otherwise, write $\alpha = a/b$, find $c, d$ such that $ad - bc = 1$, and set $\gamma \leftarrow \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$.

2. [Generic Conjugate Matrix] Compute the following matrix in $M_2(\mathbb{Z}[x])$:

$$\delta(x) \leftarrow \gamma \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \gamma^{-1}.$$

   Note that $\delta(x)$ matrix whose entries are constant or linear in $x$.

3. [Solve] The congruence conditions that define $\Gamma$ give rise to four linear congruence conditions on $x$. Use techniques from elementary number theory to find the smallest simultaneous positive solution $h$ to these four equations.

**Example 1.3.4.**

1. Suppose $\alpha = 0$ and $\Gamma = \Gamma_0(N)$ or $\Gamma_1(N)$. Then $\gamma = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$ has the property that $\gamma(\infty) = \alpha$. Next, the congruence condition is

$$\delta(x) = \gamma \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \gamma^{-1} = \begin{pmatrix} 1 & 0 \\ x & 1 \end{pmatrix} \equiv \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \pmod{N}.$$

   Thus the smallest positive solution is $h = N$, so the width of 0 is $N$.

2. Suppose $N = pq$ where $p, q$ are distinct primes, and let $\alpha = 1/p$. Then $\gamma = \left(\begin{smallmatrix} 1 & 0 \\ p & 1 \end{smallmatrix}\right)$ sends $\infty$ to $\alpha$. The congruence condition for $\Gamma_0(pq)$ is

$$\delta(x) = \gamma \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \gamma^{-1} = \begin{pmatrix} 1 - px & x \\ -p^2x & px + 1 \end{pmatrix} \equiv \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \pmod{pq}.$$

   Since $p^2x \equiv 0 \pmod{pq}$, we see that $x = q$ is the smallest solution. Thus $1/p$ has width $q$, and likewise $1/q$ has width $p$.

**Remark 1.3.5.** For $\Gamma_0(N)$, once we enforce that the bottom left entry is 0 (mod $N$), and use that the determinant is 1, the coprimeness that one gets from the other two congruences is automatic. So there is one congruence to solve for $\Gamma_0(N)$. There are 2 congruences in the $\Gamma_1(N)$ case (the bottom left entry and top left entry).

## 1.4 Eisenstein Series and Delta

For an even integer $k \geq 4$, define the (non-normalized) *weight $k$ Eisenstein series* to be

$$G_k(z) = \sum_{m,n\in\mathbb{Z}}^{*} \frac{1}{(mz+n)^k},$$

where the sum is over all $m, n \in \mathbb{Z}$ such that $mz + n \neq 0$.

**Proposition 1.4.1.** *The function $G_k(z)$ is a modular form of weight $k$.*

See [Ser73, § VII.2.3], where he proves that $G_k(z)$ defines a holomorphic function on $\mathfrak{h} \cup \{\infty\}$. To see that $G_k$ is modular, note that

$$G_k(z+1) = \sum^{*} \frac{1}{(m(z+1)+n)^k} = \sum^{*} \frac{1}{(mz+(n+m))^k} = \sum^{*} \frac{1}{(mz+n)^k},$$

and

$$G_k(-1/z) = \sum^{*} \frac{1}{(-m/z+n)^k} = \sum^{*} \frac{z^k}{(-m+nz)^k} = z^k \sum^{*} \frac{1}{(mz+n)^k} = z^k G_k(z).$$

**Proposition 1.4.2.** *$G_k(\infty) = 2\zeta(k)$, where $\zeta$ is the Riemann zeta function.*

*Proof.* Taking the limit as $z \to i\infty$ in the definition of $G_k(z)$, we obtain $\sum^{*}_{n\in\mathbb{Z}} \frac{1}{n^k}$, since the terms involving $z$ all go to 0 as $z \mapsto i\infty$. This sum is twice $\zeta(k) = \sum_{n\geq 1} \frac{1}{n^k}$. □

For example, one can show that

$$G_4(\infty) = 2\zeta(4) = \frac{1}{3^2 \cdot 5}\pi^4$$

and

$$G_6(\infty) = 2\zeta(6) = \frac{2}{3^3 \cdot 5 \cdot 7}\pi^6.$$

Suppose $E = \mathbb{C}/\Lambda$ is an elliptic curve over $\mathbb{C}$, viewed as a quotient of $\mathbb{C}$ by a lattice $\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$, with $\omega_1/\omega_2 \in \mathfrak{h}$. Then

$$\wp_\Lambda(u) = \frac{1}{u^2} + \sum_{k=4,\ \text{even}}^{\infty} (k-1)G_k(\omega_1/\omega_2)u^{k-2},$$

and

$$(\wp')^2 = 4\wp^3 - 60G_4(\omega_1/\omega_2)\wp - 140G_6(\omega_1/\omega_2).$$

The discriminant of the cubic $4x^3 - 60G_4(\omega_1/\omega_2)x - 140G_6(\omega_1/\omega_2)$ is $16\Delta(\omega_1/\omega_2)$, where

$$\Delta = (60G_4)^3 - 27(140G_6)^2$$

is a cusp form of weight 12. Since $E$ is an elliptic curve, $\Delta(\omega_1/\omega_2) \neq 0$.

**Proposition 1.4.3.** *For every even integer $k \geq 4$, we have*

$$G_k(z) = 2\zeta(k) + 2 \cdot \frac{(2\pi i)^k}{(k-1)!} \cdot \sum_{n=1}^{\infty} \sigma_{k-1}(n)q^n,$$

*where $\sigma_d(n)$ is the sum of the $d$th powers of the divisors of $n$.*

For the proof, see [Ser73, §VII.4], which uses clever manipulations of various series, starting with the identity

$$\pi\cot(\pi z) = \frac{1}{z} + \sum_{m=1}^{\infty}\left(\frac{1}{z+m} + \frac{1}{z-m}\right).$$

From a computational point of view, the $q$-expansion for $G_k$ from Proposition 1.4.3 is unsatisfactory, because it involves transcendental numbers. To understand more clearly what is going on, we introduce the *Bernoulli numbers* $B_n$ for $n \geq 0$ *defined* by the following equality of formal power series:

$$\frac{x}{e^x - 1} = \sum_{n=0}^{\infty} B_n \frac{x^n}{n!}. \tag{1.4.1}$$

Expanding the power series on the left we have

$$\frac{x}{e^x-1} = 1 - \frac{x}{2} + \frac{x^2}{12} - \frac{x^4}{720} + \frac{x^6}{30240} - \frac{x^8}{1209600} + \cdots$$

As this expansion suggests, the Bernoulli numbers $B_n$ with $n > 1$ odd are 0 (see Exercise 7.6). Expanding the series further, we obtain the following table:

$$B_0 = 1, \quad B_1 = -\frac{1}{2}, \quad B_2 = \frac{1}{6}, \quad B_4 = -\frac{1}{30}, \quad B_6 = \frac{1}{42}, \quad B_8 = -\frac{1}{30},$$

$$B_{10} = \frac{5}{66}, \quad B_{12} = -\frac{691}{2730}, \quad B_{14} = \frac{7}{6}, \quad B_{16} = -\frac{3617}{510}, \quad B_{18} = \frac{43867}{798},$$

$$B_{20} = -\frac{174611}{330}, \quad B_{22} = \frac{854513}{138}, \quad B_{24} = -\frac{236364091}{2730}, \quad B_{26} = \frac{8553103}{6}.$$

For us the significance of the Bernoulli numbers is their connection with values of $\zeta$ at positive even integers.

**Proposition 1.4.4.** *If $k \geq 2$ is an* **even** *integer, then*

$$\zeta(k) = -\frac{(2\pi i)^k}{2\cdot k!}\cdot B_k.$$

The proof involves manipulating a power series expansion for $z\cot(z)$ (see [Ser73, §VII.4]).

**Definition 1.4.5** (Normalized Eisenstein Series)**.** The *normalized Eisenstein series* of even weight $k \geq 4$ is

$$E_k = \frac{(k-1)!}{2\cdot(2\pi i)^k}\cdot G_k$$

Combining Propositions 1.4.3 and 1.4.4 we see that

$$E_k = -\frac{B_k}{2k} + q + \sum_{n=2}^{\infty}\sigma_{k-1}(n)q^n. \tag{1.4.2}$$

**Remark 1.4.6. Warning:** Our series $E_k$ is normalized so that the coefficient of $q$ is 1, but most books normalize $E_k$ so that the constant coefficient is 1. We use the normalization with the coefficient of $q$ equal to 1, because then the eigenvalue of the $n$th Hecke operator (see Section 1.6) is the coefficient of $q^n$. Our normalization will also be convenient when we consider congruences between cusp forms and Eisenstein series.

## 1.5 Structure Theorem

If $f$ is a nonzero meromorphic function on $\mathfrak{h}$ and $w \in \mathfrak{h}$, let $\mathrm{ord}_w(f)$ be the largest integer $n$ such that $f/(w-z)^n$ is holomorphic at $w$. If $f = \sum_{n=m}^{\infty} a_n q^n$ with $a_m \neq 0$, let $\mathrm{ord}_\infty(f) = m$. We will use the following theorem to give a presentation for the vector space of modular forms of weight $k$; this presentation will allow us to obtain an algorithm to compute a basis for this space.

**Theorem 1.5.1** (Valence Formula)**.** *Suppose $f$ is a modular form. Then*

$$\mathrm{ord}_\infty(f) + \frac{1}{2}\mathrm{ord}_i(f) + \frac{1}{3}\mathrm{ord}_\rho(f) + \sum_{w\in D}^{*} \mathrm{ord}_w(f) = \frac{k}{12},$$

*where $\sum_{w\in D}^{*}$ is the sum over elements of $\mathcal{F}$ other than $i$ or $\rho$.*

*Proof.* Serre proves this theorem in [Ser73, §VII.3] using the residue theorem from complex analysis. □

Let $M_k$ denote the complex vector space of modular forms of weight $k$, and let $S_k$ denote the subspace of cusp forms. We have an exact sequence

$$0 \to S_k \to M_k \to \mathbb{C}$$

that sends $f \in M_k$ to $f(\infty)$. When $k \geq 4$ is even, the space $M_k$ contains $G_k$ and $G_k(\infty) = 2\zeta(k) \neq 0$, so the map $M_k \to \mathbb{C}$ is surjective, and $\dim(S_k) = \dim(M_k) - 1$, so

$$M_k = S_k \oplus \mathbb{C}G_k.$$

**Proposition 1.5.2.** *For $k < 0$ and $k = 2$, we have $M_k = 0$.*

*Proof.* Suppose $f \in M_k$ is nonzero yet $k = 2$ or $k < 0$. By Theorem 1.5.1,

$$\mathrm{ord}_\infty(f) + \frac{1}{2}\mathrm{ord}_i(f) + \frac{1}{3}\mathrm{ord}_\rho(f) + \sum_{w\in D}^{*} \mathrm{ord}_w(f) = \frac{k}{12} \leq 1/6.$$

This is impossible because each quantity on the left-hand side is nonnegative so whatever the sum is, it is too big (or 0, in which $k = 0$). □

**Theorem 1.5.3.** *Multiplication by $\Delta$ defines an isomorphism $M_{k-12} \to S_k$.*

*Proof.* (We follow [Ser73, §VII.3.2] closely.) We apply Theorem 1.5.1 to $G_4$ and $G_6$. If $f = G_4$, then

$$\mathrm{ord}_\infty(f) + \frac{1}{2}\,\mathrm{ord}_i(f) + \frac{1}{3}\,\mathrm{ord}_\rho(f) + \sum_{w\in D}^{*} \mathrm{ord}_w(f) = \frac{4}{12} = \frac{1}{3},$$

with the ords all nonnegative, so $\mathrm{ord}_\rho(G_4) = 1$ and $\mathrm{ord}_w(G_4) = 0$ for all $w \neq \rho$. Likewise $\mathrm{ord}_i(G_6) = 1$ and $\mathrm{ord}_w(G_6) = 0$ for all $w \neq i$. Thus $\Delta(i) \neq 0$, so $\Delta$ is not identically 0 (we also saw this above using the Weierstrass $\wp$ function). Since $\Delta$ has weight 12 and $\mathrm{ord}_\infty(\Delta) \geq 1$, Theorem 1.5.1 implies that $\Delta$ has a simple zero at $\infty$ and does not vanish on $\mathfrak{h}$. Thus if $f \in S_k$ and we let $g = f/\Delta$, then $g$ is holomorphic and satisfies the appropriate transformation formula, so $g$ is a modular form of weight $k - 12$. □

**Corollary 1.5.4.** *For $k = 0, 4, 6, 8, 10, 14$, the vector space $M_k$ has dimension 1, with basis 1, $G_4$, $G_6$, $E_8$, $E_{10}$, and $E_{14}$, respectively, and $S_k = 0$.*

*Proof.* Combining Proposition 1.5.2 with Theorem 1.5.3 we see that the spaces $M_k$ for $k \leq 10$ can not have dimension bigger than 1, since then $M_{k'} \neq 0$ for some $k' < 0$. Also $M_{14}$ has dimension at most 1, since $M_2$ has dimension 0. Each of the indicated spaces of weight $\geq 4$ contains the indicated Eisenstein series, so has dimension 1, as claimed. □

**Corollary 1.5.5.** $\dim M_k = \begin{cases} 0 & \textit{if } k \textit{ is odd}, \\ \lfloor k/12 \rfloor & \textit{if } k \equiv 2 \pmod{12}, \\ \lfloor k/12 \rfloor + 1 & \textit{if } k \not\equiv 2 \pmod{12}, \end{cases}$ *where $\lfloor x \rfloor$ is the biggest integer $\leq x$.*

*Proof.* As we have seen above, the formula is true when $k \leq 12$. By Theorem 1.5.3, the dimension increases by 1 when $k$ is replaced by $k + 12$. □

**Theorem 1.5.6.** *The space $M_k$ has as basis the modular forms $G_4^a G_6^b$, where $a, b$ are all pairs of nonnegative integers such that $4a + 6b = k$.*

*Proof.* We first prove by induction that the modular forms $G_4^a G_6^b$ generate $M_k$, the cases $k \leq 12$ being clear (e.g., when $k = 0$ we have $a = b = 0$ and basis 1). Choose some pair of integers $a, b$ such that $4a + 6b = k$ (it is an elementary exercise to show these exist). The form $g = G_4^a G_6^b$ is not a cusp form, since it is nonzero at $\infty$. Now suppose $f \in M_k$ is arbitrary. Since $M_k = S_k \oplus \mathbb{C}G_k$, there is $\alpha \in \mathbb{C}$ such that $f - \alpha g \in S_k$. Then by Theorem 1.5.3, there is $h \in M_{k-12}$ such that $f - \alpha g = \Delta h$. By induction, $h$ is a polynomial in $G_4$ and $G_6$ of the required type, and so is $\Delta$, so $f$ is as well.

Suppose there is a nontrivial linear relation between the $G_4^a G_6^b$ for a given $k$. By multiplying the linear relation by a suitable power of $G_4$ and $G_6$, we may assume that that we have such a nontrivial relation with $k \equiv 0 \pmod{12}$. Now divide the linear relation by $G_6^{k/12}$ to see that $G_4^3/G_6^2$ satisfies a polynomial with coefficients in $\mathbb{C}$. Hence $G_4^3/G_6^2$ is a root of a polynomial, hence a constant, which is a contradiction since the $q$-expansion of $G_4^3/G_6^2$ is not constant. □

**Algorithm 1.5.7** (Basis).
Given integers $n$ and $k$, this algorithm computes a basis of $q$-expansions for the complex vector space $M_k$ mod $q^n$. The $q$-expansions output by this algorithm have coefficients in $\mathbb{Q}$.

1. [Simple Case] If $k = 0$ output the basis with just $1$ in it, and terminate; otherwise if $k < 4$ or $k$ is odd, output the empty basis and terminate.
2. [Power Series] Compute $E_4$ and $E_6$ mod $q^n$ using the formula from (1.4.2) and the definition (1.4.1) of Bernoulli numbers.
3. [Initialize] Set $b \leftarrow 0$.
4. [Enumerate Basis] For each integer $b$ between $0$ and $\lfloor k/6 \rfloor$, compute $a = (k-6b)/4$. If $a$ is an integer, compute and output the basis element $E_4^a E_6^b \bmod q^n$. When we compute, e.g., $E_4^a$, do the computation by finding $E_4^m \pmod{q^n}$ for each $m \leq a$, and save these intermediate powers, so they can be reused later, and likewise for powers of $E_6$.

*Proof.* This is simply a translation of Theorem 1.5.6 into an algorithm, since $E_k$ is a nonzero scalar multiple of $G_k$. That the $q$-expansions have coefficients in $\mathbb{Q}$ is Equation 1.4.2. □

**Example 1.5.8.** We compute a basis for $M_{24}$, which is the space with smallest weight whose dimension is bigger than 1. It has as basis $E_4^6$, $E_4^3E_6^2$, and $E_6^4$, whose explicit expansions are

$$\begin{aligned}
E_4^6 &= \frac{1}{191102976000000} + \frac{1}{132710400000}q + \frac{203}{44236800000}q^2 + \cdots \\
E_4^3E_6^2 &= \frac{1}{3511517184000} - \frac{1}{12192768000}q - \frac{377}{4064256000}q^2 + \cdots \\
E_6^4 &= \frac{1}{64524128256} - \frac{1}{32006016}q + \frac{241}{10668672}q^2 + \cdots
\end{aligned}$$

In Section 1.7, we will discuss properties of the reduced row echelon form of any basis for $M_k$, which have better properties than the above basis.

## 1.6 Hecke Operators

Let $k$ be an integer. Define the weight $k$ right action of $\mathrm{GL}_2(\mathbb{Q})$ on functions $f$ on $\mathfrak{h}$ as follows. If $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{Q})$, let

$$f|[\gamma]_k = \det(\gamma)^{k-1}(cz+d)^{-k} f(\gamma(z)).$$

One checks as an exercise that

$$f|[\gamma_1\gamma_2]_k = (f|[\gamma_1]_k)|[\gamma_2]_k,$$

i.e., that this is a right group action. Also $f$ is a weakly modular function if $f$ is meromorphic and $f|[\gamma]_k = f$ for all $\gamma \in \mathrm{SL}_2(\mathbb{Z})$.

For any positive integer $n$, let

$$S_n = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in M_2(\mathbb{Z}) \;:\; a \geq 1,\; ad = n,\; \text{and } 0 \leq b < d \right\}.$$

Note that the set $S_n$ is in bijection with the set of sublattices of $\mathbb{Z}^2$ of index $n$, where $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ corresponds to $L = \mathbb{Z} \cdot (a, b) + \mathbb{Z} \cdot (0, d)$, as one can see, e.g., by using Hermite normal form (the analogue of reduced row echelon form over $\mathbb{Z}$).

**Definition 1.6.1** (Hecke Operator $T_{n,k}$)**.** The $n$th Hecke operator $T_{n,k}$ of weight $k$ is the operator on functions on $\mathfrak{h}$ defined by

$$T_{n,k}(f) = \sum_{\gamma \in S_n} f|[\gamma]_k.$$

**Remark 1.6.2.** It would make more sense to write $T_{n,k}$ on the right, e.g., $f|T_{n,k}$, since $T_{n,k}$ is defined using a right group action. However, if $n, m$ are integers, then $T_{n,k}$ and $T_{m,k}$ commute, so it doesn't matter whether we consider the Hecke operators as acting on the right or left.

**Proposition 1.6.3.** *If $f$ is a weakly modular function of weight $k$, so is $T_{n,k}(f)$, and if $f$ is also a modular function, then so is $T_{n,k}(f)$.*

*Proof.* Suppose $\gamma \in \mathrm{SL}_2(\mathbb{Z})$. Since $\gamma$ induces an automorphism of $\mathbb{Z}^2$, the set

$$S_n \cdot \gamma = \{\delta\gamma : \delta \in S_n\}$$

is also in bijection with the sublattices of $\mathbb{Z}^2$ of index $n$. Then for each element $\delta\gamma \in S_n \cdot \gamma$, there is $\sigma \in \mathrm{SL}_2(\mathbb{Z})$ such that $\sigma\delta\gamma \in S_n$ (the element $\sigma$ is the transformation of $\delta\gamma$ to Hermite normal form), and the set of elements $\sigma\delta\gamma$ is equal to $S_n$. Thus

$$T_{n,k}(f) = \sum_{\sigma\delta\gamma \in S_n} f|[\sigma\delta\gamma]_k = \sum_{\delta \in S_n} f|[\delta\gamma]_k = T_{n,k}(f)|[\gamma]_k.$$

That $f$ being holomorphic on $\mathfrak{h}$ implies $T_{n,k}(f)$ is holomorphic on $\mathfrak{h}$ follows because each $f|[\gamma]_k$ is holomorphic on $\mathfrak{h}$, and a finite sum of holomorphic functions is holomorphic. □

We will frequently drop $k$ from the notation in $T_{n,k}$, since the weight $k$ is implicit in the modular function to which we apply the Hecke operator. Thus we henceforth make the convention that if we write $T_n(f)$ and $f$ is modular, then we mean $T_{n,k}(f)$, where $k$ is the weight of $f$.

**Proposition 1.6.4.** *On weight $k$ modular functions we have*

$$T_{mn} = T_n T_m \qquad \text{if } (n, m) = 1, \tag{1.6.1}$$

*and*

$$T_{p^n} = T_{p^{n-1}} T_p \,-\, p^{k-1} T_{p^{n-2}}, \qquad \text{if } p \text{ is prime.} \tag{1.6.2}$$

*Proof.* Let $L$ be a lattice of index $mn$. The quotient $\mathbb{Z}^2/L$ is an abelian group of order $mn$, and $(m,n)=1$, so $\mathbb{Z}^2/L$ decomposes uniquely as a direct sum of a subgroup order $m$ with a subgroup of order $n$. Thus there exists a unique lattice $L'$ such that $L \subset L' \subset \mathbb{Z}^2$, and $L'$ has index $m$ in $\mathbb{Z}^2$. Thus $L'$ corresponds to an element of $S_m$, and the index $n$ subgroup $L \subset L'$ corresponds to multiplying that element on the right by some uniquely determined element of $S_n$. We thus have

$$\mathrm{SL}_2(\mathbb{Z}) \cdot S_m \cdot S_n = \mathrm{SL}_2(\mathbb{Z}) \cdot S_{mn}$$

i.e., the set products of elements in $S_m$ with elements of $S_n$ equal the elements of $S_{mn}$, up to $\mathrm{SL}_2(\mathbb{Z})$-equivalence. It then follows from the definitions that for any $f$, we have $T_{mn}(f) = T_n(T_m(f))$.

We will show that $T_{p^n} + p^{k-1}T_{p^{n-2}} = T_p T_{p^{n-1}}$. Suppose $f$ is a weight $k$ weakly modular function. Using that $f|[p]_k = (p^2)^{k-1}p^{-k}f = p^{k-2}f$, we have

$$\sum_{x\in S_{p^n}} f|[x]_k \;+\; p^{k-1}\sum_{x\in S_{p^{n-2}}} f|[x]_k = \sum_{x\in S_{p^n}} f|[x]_k \;+ p \sum_{x\in pS_{p^{n-2}}} f|[x]_k.$$

Also

$$T_pT_{p^{n-1}}(f) = \sum_{y\in S_p}\sum_{x\in S_{p^{n-1}}} f|[x]_k|[y]_k = \sum_{x\in S_{p^{n-1}}\cdot S_p} f|[x]_k.$$

Thus it suffices to show that $S_{p^n}$ union $p$ copies of $pS_{p^{n-2}}$ is equal to $S_{p^{n-1}} \cdot S_p$, where we consider elements up to $\mathrm{SL}_2(\mathbb{Z})$-equivalence.

Suppose $L$ is a sublattice of $\mathbb{Z}^2$ of index $p^n$, so $L$ corresponds to an element of $S_{p^n}$. First suppose $L$ is not contained in $p\mathbb{Z}^2$. Then the image of $L$ in $\mathbb{Z}^2/p\mathbb{Z}^2 = (\mathbb{Z}/p\mathbb{Z})^2$ is of order $p$, so if $L' = p\mathbb{Z}^2 + L$, then $[\mathbb{Z}^2 : L'] = p$ and $[L : L'] = p^{n-1}$, and $L'$ is the only lattice with this property. Second suppose that $L \subset p\mathbb{Z}^2$ if of index $p^n$, and that $x \in S_{p^n}$ corresponds to $L$. Then every one of the $p+1$ lattices $L' \subset \mathbb{Z}^2$ of index $p$ contains $L$. Thus there are $p+1$ chains $L \subset L' \subset \mathbb{Z}^2$ with $[\mathbb{Z}^2 : L'] = p$.

The chains $L \subset L' \subset \mathbb{Z}^2$ with $[\mathbb{Z}^2 : L'] = p$ and $[\mathbb{Z}^2 : L] = p^{n-1}$ are in bijection with the elements of $S_{p^{n-1}} \cdot S_p$. On the other hand the union of $S_{p^n}$ with $p$ copies of $pS_{p^{n-2}}$ corresponds to the lattices $L$ of index $p^n$, but with those that contain $p\mathbb{Z}^2$ counted $p+1$ times. The structure of the set of chains $L \subset L' \subset \mathbb{Z}^2$ that we derived in the previous paragraph gives the result. □

**Corollary 1.6.5.** *The Hecke operator $T_{p^n}$, for prime $p$, is a polynomial in $T_p$. If $n, m$ are any integers then $T_nT_m = T_mT_n$.*

*Proof.* The first statement is clear from (1.6.2), and this gives commutativity when $m$ and $n$ are both powers of $p$. Combining this with (1.6.1) gives the second statement in general. □

**Remark 1.6.6.** Emmanuel Kowalski made the following remark on the number theory lists in June 2004 when asked about the polynomials $f_n(X)$ such that $T_{p^n} = f_n(T_p)$.

If you normalize the Hecke operators by considering

$$S_{n,k} = n^{-(k-1)/2} T_{n,k}$$

then the recursion on the polynomials $P_r(X)$ such that $S_{p^r,k} = P_r(S_{p,k})$ becomes

$$XP_r = P_{r+1} + P_{r-1},$$

which is the recursion satisfied by the Chebychev polynomials $U_r$ such that

$$U_r(2\cos t) = \frac{\sin((r+1)t)}{\sin(t)}.$$

Alternatively, those give the characters of the symmetric powers of the standard representation of $\mathrm{SL}_2(\mathbb{R})$, evaluated on a rotation matrix

$$\begin{pmatrix} \cos(t) & -\sin(t) \\ \sin(t) & \cos(t) \end{pmatrix}.$$

For references, see for instance [Iwa97, p. 97] or [Ser97, p. 78, p. 81], and there are certainly many others.

**Proposition 1.6.7.** *Suppose $f = \sum_{n\in\mathbb{Z}} a_n q^n$ is a modular function of weight $k$. Then*

$$T_n(f) = \sum_{m\in\mathbb{Z}} \left( \sum_{1\leq c \,|\, (n,m)} c^{k-1} a_{mn/c^2} \right) q^m.$$

*In particular, if $n = p$ is prime, then*

$$T_p(f) = \sum_{m\in\mathbb{Z}} \left(a_{mp} + p^{k-1} a_{m/p}\right) q^m,$$

*where $a_{m/p} = 0$ if $m/p \notin \mathbb{Z}$.*

The proposition is not that difficult to prove (or at least the proof is easy to follow), and is proved in [Ser73, §VII.5.3] by writing out $T_n(f)$ explicitly and using that $\sum_{0\leq b<d} e^{2\pi i bm/d}$ is $d$ if $d \mid m$ and 0 otherwise. A corollary of Proposition 1.6.7 is that $T_n$ preserves $M_k$ and $S_k$.

**Corollary 1.6.8.** *The Hecke operators preserve $M_k$ and $S_k$.*

**Remark 1.6.9.** (Elkies) We knew this already—for $M_k$ it's Proposition 1.6.3, and for $S_k$ it's easy to show directly that if $f(i\infty) = 0$ then $T_n f$ also vanishes at $i\infty$.

**Example 1.6.10.** Recall that

$$E_4 = \frac{1}{240} + q + 9q^2 + 28q^3 + 73q^4 + 126q^5 + 252q^6 + 344q^7 + \cdots.$$

Using the formula of Proposition 1.6.7, we see that

$$T_2(E_4) = (1/240 + 2^3 \cdot (1/240)) + 9q + (73 + 2^3 \cdot 1)q^2 + \cdots = 9E_4.$$

Since $M_k$ has dimension 1, and we have proved that $T_2$ preserves $M_k$, we know that $T_2$ acts as a scalar. Thus we know just from the constant coefficient of $T_2(E_4)$ that $T_2(E_4) = 9E_4$. More generally, $T_p(E_4) = (1 + p^3)E_4$, and even more generally

$$T_n(E_k) = \sigma_{k-1}(n)E_k,$$

for any integer $n \geq 1$ and even weight $k \geq 4$.

**Example 1.6.11.** The Hecke operators $T_n$ also preserve the subspace $S_k$ of $M_k$. Since $S_{12}$ has dimension 1, this means that $\Delta$ is an eigenvector for all $T_n$. Since the coefficient of $q$ in the $q$-expansion of $\Delta$ is 1, the eigenvalue of $T_n$ on $\Delta$ is the $n$th coefficient of $\Delta$. Moreover the function $\tau(n)$ that gives the $n$th coefficient of $\Delta$ is a multiplicative function. Likewise, one can show that the series $E_k$ are eigenvectors for all $T_n$, and because in this book we normalize $E_k$ so that the coefficient of $q$ is 1, the eigenvalue of $T_n$ on $E_k$ is the coefficient $\sigma_{k-1}(n)$ of $q^n$.

## 1.7 The Victor Miller Basis

**Lemma 1.7.1** (Victor Miller)**.** *The space $S_k$ has a basis $f_1, \ldots, f_d$ such that if $a_i(f_j)$ is the ith coefficient of $f_j$, then $a_i(f_j) = \delta_{i,j}$ for $i = 1, \ldots, d$. Moreover the $f_j$ all lie in $\mathbb{Z}[[q]]$.*

This is a straightforward construction involving $E_4$, $E_6$ and $\Delta$. The following proof is copied almost verbatim from [Lan95, Ch. X, Thm. 4.4], which is in turn presumably copied from the first lemma of Victor Miller's thesis.

*Proof.* Let $d = \dim S_k$. Since $B_4 = -1/30$ and $B_6 = 1/42$, we note that

$$F_4 = -8/B_4 \cdot E_4 = 1 + 240q + 2160q^2 + 6720q^3 + 17520q^4 + \cdots$$

and

$$F_6 = -12/B_6 \cdot E_6 = 1 - 504q - 16632q^2 - 122976q^3 - 532728q^4 + \cdots$$

have $q$-expansions in $\mathbb{Z}[[q]]$ with leading coefficient 1. Choose integers $a, b \geq 0$ such that

$$4a + 6b \leq 14 \qquad \text{and} \qquad 4a + 6b \equiv k \pmod{12},$$

with $a = b = 0$ when $k \equiv 0 \pmod{12}$, and let

$$g_j = \Delta^j F_6^{2(d-j)+a} F_4^b, \qquad \text{for } j = 1, \ldots, d.$$

Then

$$a_j(g_j) = 1, \qquad \text{and} \qquad a_i(g_j) = 0 \qquad \text{when} \qquad i < j.$$

Hence the $g_j$ are linearly independent over $\mathbb{C}$, and thus form a basis for $S_k$. Since $F_4, F_6$, and $\Delta$ are all in $\mathbb{Z}[[q]]$, so are the $g_j$. The $f_i$ may then be constructed from the $g_j$ by Gauss elimination. The coefficients of the resulting power series lie in $\mathbb{Z}$ because each time we clear a column we use the power series $g_j$ whose leading coefficient is 1 (so no denominators are introduced). $\square$

**Remark 1.7.2.** The basis coming from Victor Miller's lemma is canonical, since it is just the reduced row echelon form of any basis. Also the *integral* linear combinations are precisely the modular forms of level 1 with integral $q$-expansion.

**Remark 1.7.3.** (Elkies)

1. If you have just a single form $f$ in $M_k$ to write as a polynomial in $E_4$ and $E_6$, then it is wasteful to compute the Victor Miller basis. Instead, use the upper triangular basis $\Delta^j F_6^{2(d-j)+a} F_4^b$, and match coefficients from $q^0$ to $q^d$. (Or use "my" recursion if $f$ happens to be the Eisenstein series.)

2. When $4 \mid k$, the zeroth form $f_0$ in the Miller basis is also the theta function of an extremal self-dual even lattice of dimension $2k$ (if one exists). More generally, if a lattice is with $c$ of extremality then its theta function differs from $f_0$ by a linear combination of $f_d, f_{d-1}, ..., f_{d+1-c}$.

We extend the Victor Miller basis to all $M_k$ by taking a multiple of $G_k$ with constant term 1, and subtracting off the $f_i$ from the Victor Miller basis so that the coefficients of $q, q^2, \ldots q^d$ of the resulting expansion are 0. We call the extra basis element $f_0$.

**Example 1.7.4.** If $k = 24$, then $d = 2$. Choose $a = b = 0$, since $k \equiv 0 \pmod{12}$. Then

$$g_1 = \Delta F_6^2 = q - 1032q^2 + 245196q^3 + 10965568q^4 + 60177390q^5 - \cdots$$

and

$$g_2 = \Delta^2 = q^2 - 48q^3 + 1080q^4 - 15040q^5 + \cdots$$

We let $f_2 = g_2$ and

$$f_1 = g_1 + 1032g_2 = q + 195660q^3 + 12080128q^4 + 44656110q^5 - \cdots .$$

**Example 1.7.5.** When $k = 36$, the Victor Miller basis, including $f_0$, is

$$\begin{aligned}
f_0 &= 1 + \quad 6218175600q^4 + 15281788354560q^5 + \cdots \\
f_1 &= \quad q + \quad 57093088q^4 + 37927345230q^5 + \cdots \\
f_2 &= \quad q^2 + \quad 194184q^4 + \quad 7442432q^5 + \cdots \\
f_3 &= \quad q^3 - \quad 72q^4 + \quad 2484q^5 + \cdots
\end{aligned}$$

**Algorithm 1.7.6** (Hecke Operator)**.**
This algorithm computes a matrix for the Hecke operator $T_n$ on the Victor Miller basis for $M_k$.

1. [Compute dimension] Set $d \leftarrow \dim(S_k)$, which we compute using Corollary 1.5.5.
2. [Compute basis] Using the algorithm implicit in Lemma 1.7.1, compute a basis $f_0, \ldots, f_d$ for $M_k$ modulo $q^{dn+1}$.

3. [Compute Hecke operator] Using the formula from Proposition 1.6.7, compute $T_n(f_i) \pmod{q^{d+1}}$ for each $i$.
4. [Write in terms of basis] The elements $T_n(f_i) \pmod{q^{d+1}}$ uniquely determine linear combinations of $f_0, f_1, \ldots, f_d \pmod{q^d}$. These linear combinations are trivial to find, since the basis of $f_i$ are in reduced row echelon form. I.e., the combinations are just the first few coefficients of the power series $T_n(f_i)$.
5. [Write down matrix] The matrix of $T_n$ acting from the left is the matrix whose rows are the linear combinations found in the previous step, i.e., whose rows are the coefficients of $T_n(f_i)$.

*Proof.* First note that we only have to compute a modular form $f$ modulo $q^{dn+1}$ in order to compute $T_n(f)$ modulo $q^{d+1}$. This follows from Proposition 1.6.7, since in the formula the $d$th coefficient of $T_n(f)$ involves only $a_{dn}$, and smaller-indexed coefficients of $f$. The uniqueness assertion of Step 4 follows from Lemma 1.7.1 above. $\square$

**Example 1.7.7.** This is the Hecke operator $T_2$ on $M_{36}$:

$$\begin{pmatrix} 34359738369 & 0 & 6218175600 & 9026867482214400 \\ 0 & 0 & 34416831456 & 5681332472832 \\ 0 & 1 & 194184 & -197264484 \\ 0 & 0 & -72 & -54528 \end{pmatrix}$$

It has characteristic polynomial

$$(x - 34359738369) \cdot (x^3 - 139656x^2 - 59208339456x - 1467625047588864),$$

where the cubic factor is irreducible.

**Conjecture 1.7.8** (Maeda)**.** *The characteristic polynomial of $T_2$ on $S_k$ is irreducible for any $k$.*

Kevin Buzzard even observed that in many specific cases the Galois group of the characteristic polynomial of $T_2$ is the full symmetric group (see [Buz96]). See also [FJ02] for more evidence for Maeda's conjecture.

## 1.8 The Complexity of Computing Fourier Coefficients

Let

$$\begin{aligned}\Delta &= \sum_{n=1}^{\infty} \tau(n) q^n \\ &= q - 24q^2 + 252q^3 - 1472q^4 + 4830q^5 - 6048q^6 - 16744q^7 \\ &\quad + 84480q^8 - 113643q^9 - 115920q^{10} + 534612q^{11} - \\ &\quad 370944q^{12} - 577738q^{13} + 401856q^{14} + 1217160q^{15} + \\ &\quad 987136q^{16} - 6905934q^{17} + 2727432q^{18} + 10661420q^{19} + \cdots\end{aligned}$$

be the $\Delta$-function.

**Conjecture 1.8.1** (Edixhoven, et al.). *There is an algorithm to compute $\tau(p)$, for prime $p$, that is polynomial-time in $\log(p)$. More generally, suppose $f = \sum a_n q^n$ is an eigenform in some space $M_k(N,\varepsilon)$, where $k \geq 2$. Then there is an algoirthm to compute $a_p$, for $p$ prime, in time polynomial in $\log(p)$.*

Bas Edixhoven and his students have been working for years to apply sophisticated techniques from arithmetic geometry (e.g., étale cohomology, motives, Arakelov theory) in order to prove that such an algorithm exists (among other things), and he believes they are almost there. There is evidently a significant gap between proving *existence* of an algorithm that shold be polynomial time, and actually writing down such an algorithm with explicitly bounded running times. The ideas Edixhoven uses are very similar to the ones used for counting points on elliptic curves in polynomial time (the algorithm of Schoof, with refinements by Atkins and Elkies).

## 1.9 Exercises

1.1 Suppose $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ is a matrix with real entries and positive determinant. Prove that if $z \in \mathbb{C}$ is a complex number with positive imaginary part, then the imaginary part of $\gamma(z) = (az+b)/(cz+d)$ is also positive.

1.2 (a) Prove that a polynomial is an analytic function on $\mathbb{C}$.

(b) Prove that a rational function (quotient of two polynomials) is a meromorphic function on $\mathbb{C}$.

1.3 Suppose $f$ and $g$ are weakly modular functions with $f \neq 0$.

(a) Prove that the product $fg$ is a weakly modular function.

(b) Prove that $1/f$ is a weakly modular function.

(c) If $f$ and $g$ are modular functions, show that $fg$ is a modular function.

(d) If $f$ and $g$ are modular forms, show that $fg$ is a modular form.

1.4 Suppose $f$ is a weakly modular function of odd weight $k$. Show that $f = 0$.

1.5 (a) Prove that $\Gamma_1(N)$ is a group.

(b) Prove that $\Gamma_1(N)$ has finite index in $\mathrm{SL}_2(\mathbb{Z})$ (Hint: it contains the kernel of the homomorphism $\mathrm{SL}_2(\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$.)