CLASSICAL AND p-ADIC MODULAR FORMS ARISING FROM THE BORCHERDS EXPONENTS OF OTHER MODULAR FORMS

JAYCE GETZ
SENIOR THESIS

ABSTRACT. Let $f(z) = q^h \prod_{n=1}^{\infty}(1-q^n)^{c(n)}$ be a modular form on $\mathrm{SL}_2(\mathbb{Z})$. Formal logarithmic differentiation of f yields a q-series $g(z) := h - \sum_{n=1}^{\infty}\sum_{d|n} c(d)dq^n$ whose coefficients are uniquely determined by the exponents of the original form. We provide a formula, due to Bruinier, Kohnen, and Ono for $g(z)$ in terms of the values of the classical j-function at the zeros and poles of $f(z)$. Further, we give a variety of cases in which $g(z)$ is additionally a p-adic modular form in the classical sense of Serre. As an application, we derive some p-adic formulae, due to Bruinier, Ono, and Papanikolas, in which the class numbers of a family of imaginary quadratic fields are written in terms of special values of the j-function at imaginary quadratic arguments.

1. INTRODUCTION

Suppose f is a function on the upper half plane $\mathbb{H}$. For each positive integer k, define an action $|_k$ of $\mathrm{GL}_2^+(\mathbb{Q})$ on the set of such f by

$$f(z)|_k\gamma = \det(\gamma)^{k/2}(cz+d)^{-k} f\left(\frac{az+b}{cz+d}\right). \tag{1.1}$$

Here $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2^+(\mathbb{Q})$ (with the exception of the proof of Theorem 2, in this thesis we always use the symbol γ in this sense). Suppose $\Gamma' \subset \Gamma := \mathrm{SL}_2(\mathbb{Z})$ is a congruence subgroup. Let $\mathcal{M}_k^{\infty}(\Gamma')$ (resp., $\mathcal{M}_k^{\mathrm{mero}}(\Gamma')$) denote the space of holomorphic (resp., meromorphic) functions on the upper half plane $\mathbb{H}$ that satisfy the functional equation

$$f(z)|_k\gamma := f(z) \tag{1.2}$$

for all $\gamma \in \Gamma'$ and additionally are meromorphic at the cusps of Γ' (for a precise description of this "meromorphic at the cusps" condition, see [18, §III.3, p. 125]). Such a function will be called a *weakly modular form of weight k* (resp., *meromorphic modular form of weight k*) following J-P. Serre's convention [28, §VII.2]. We further define $M_k(\Gamma') \subset \mathcal{M}_k^{\infty}(\Gamma')$ to be the space of weakly modular forms that, additionally, are holomorphic at the cusps of Γ'. Such a form will be called a *holomorphic modular form*, or, simply, a *modular form*. For any congruence subgroup Γ' containing the element $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$, meromorphicity of f at the cusps of Γ' implies that f can be identified with a Fourier, or q-series, expansion

$$f(z) := \sum_{n=n_0}^{\infty} a_n q^n \tag{1.3}$$

Date: June 3, 2004.

The author would like to thank his family for their constant personal and financial support, Particular thanks go to his little brother Joel, who is the coolest person in the world. This thesis is dedicated to them.

where here, and throughout this thesis, $q := e^{2\pi i z}$. In the case $\Gamma' = \Gamma$, this is in fact equivalent to meromorphicity at the cusps. Holomorphicity at the cusps in the case of $\Gamma' = \Gamma$ (which are all in the same orbit as ∞ under the action of Γ) is equivalent to the statement that $n_0 \geq 0$. Finally, a holomorphic modular form over Γ' is said to be a *cusp form* if it vanishes at the cusps of Γ'; we denote the space of cusp forms of weight k over Γ' by $S_k(\Gamma')$. In the case $f \in M_k(\Gamma)$, this is simply the assertion that in the expansion (1.3) we have $n_0 > 0$. For convenience we define $\mathcal{M}_k^{\text{mero}} := \mathcal{M}_k^{\text{mero}}(\Gamma)$, $\mathcal{M}_k^{\infty} := \mathcal{M}_k^{\infty}(\Gamma)$ and $M_k := M_k(\Gamma)$.

We take the opportunity now to introduce the only congruence subgroup we will explicitly use in this thesis, namely the following level N subgroup:

$$\Gamma_0(N) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma : c \equiv 0 \pmod{N} \right\}.$$

By convention, $\Gamma_0(1) = \Gamma$.

Remark. If $\left(\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right) \in \Gamma'$, then from (1.2) we have $(-1)^k f(z) = f(z)$ for all $f \in \mathcal{M}_k^{\text{mero}}(\Gamma')$, from which it follows that $\mathcal{M}_{2m+1}^{\text{mero}}(\Gamma') = 0$ for all integers m. Thus, in particular, $\mathcal{M}_{2m+1}^{\text{mero}} = 0$.

For examples of modular forms on M_k for even $k \geq 4$, we may take the classical Eisenstein series of weight k:

$$E_k(z) := 1 - \frac{2k}{B_k} \sum_{n=1}^{\infty} \sigma_{k-1}(n) q^n \tag{1.4}$$

where B_k is the kth Bernoulli number and $\sigma_{k-1}(n) := \sum_{d|n} d^{k-1}$. We can formally define E_2 using (1.4), and though it is not a modular form, it satisfies the following transformation law for $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma$:

$$E_2\left(\frac{az+b}{cz+d}\right)(cz+d)^{-2} = E_2(z) + \frac{12c}{2\pi i(cz+d)}. \tag{1.5}$$

This transformation law turns out to play a role in many arguments; a proof of it in this form is given in [27, p. 68].

Other useful examples of modular forms are the discriminant function

$$\Delta(z) := \frac{E_4(z)^3 - E_6(z)^2}{1728} = q \prod_{n=1}^{\infty} (1-q^n)^{24} \tag{1.6}$$

which is of weight 12, and the j-function, which is a weakly modular form of weight zero:

$$j(z) := \frac{E_4(z)^3}{\Delta(z)} = q^{-1} + 744 + 196884q + 21493760q^2 + \cdots. \tag{1.7}$$

We note that any element of $\mathcal{M}_0^{\infty}$ is a polynomial in $j(z)$. If we wish to emphasize for a proof that we are regarding E_k, Δ, j as q-series (which can be either viewed formally or as functions holomorphic in the punctured disc $0 < |q| < 1$), we write them as $E_k(q)$, $\Delta(q)$, and $J(q)$, respectively.

It is easy to see that $\mathcal{M}_k^{\infty}(\Gamma')$ is a vector space over $\mathbb{C}$ for all congruence subgroups Γ'. There exists an important class of linear operators on these spaces, namely, the Hecke operators $T_{k,n}$. These can be defined (in an admittedly ad-hoc manner) by

$$f(z)|T_{k,n} = n^{k-1} \sum_{\substack{ad=n,\ d>0 \\ 0 \leq b \leq d-1}} f\left(\frac{az+b}{d}\right) \tag{1.8}$$

or, equivalently,

$$f(z)|T_{k,n} := \sum_{n\in\mathbb{Z}} \left(\sum_{0<d|(m,n)} d^{k-1} a\left(\frac{mn}{d^2}\right) \right) q^n. \tag{1.9}$$

If we define, for positive integers d, the V- and U-operators $V(d)$ and $U(d)$ on formal q-series in $\mathbb{C}[[q]]$ by

$$\left(\sum_{n\geq n_0} c(n)q^n \right) |V(d) := \sum_{n\geq n_0} c(n)q^{dn} \tag{1.10}$$

and

$$\left(\sum_{n\geq n_0} c(n)q^n \right) |U(d) := \sum_{n\geq n_0} c(dn)q^n \tag{1.11}$$

then we may write

$$T_{k,n} = \sum_{d|n} d^{k-1} V(d) \circ U(n/d). \tag{1.12}$$

Note that if we identify a meromorphic modular form f with its q-expansion, we have

$$d^{k/2} f|V(d) = f|_k \left(\begin{smallmatrix} d & 0 \\ 0 & 1 \end{smallmatrix}\right). \tag{1.13}$$

For more natural definitions of these operators and a discussion of their basic properties, see, for example, [18, §III.5] or [28, §VII].

If we consider $M := \bigoplus_{k=0}^{\infty} M_k$ it is straightforward to see that we have something better than a collection of vector spaces, we have a graded algebra, where the grading is given by weight and the multiplication operation is multiplication of functions (for proof of this, see [28, §VII]). A question naturally suggests itself: are there natural operators on this algebra? As one possible answer to this question, we define Ramanujan's theta operator:

$$\Theta := \frac{1}{2\pi i}\frac{d}{dz} = q\frac{d}{dq}.$$

It is perhaps speaking loosely to call Θ an operator, but

$$f(z) \mapsto \Theta f(z) - f(z)\frac{k}{12}E_2(z)$$

is a derivation on M. In particular, we have the following:

Proposition 1. *If f is in $\mathcal{M}_k^{mero}(\Gamma')$ then*

$$g(z) = \Theta f - f(z)\frac{k}{12}E_2 \in \mathcal{M}_{k+2}^{mero}(\Gamma'). \tag{1.14}$$

The same statement is true with $\mathcal{M}_k^{mero}(\Gamma')$ replaced by $\mathcal{M}_k^{\infty}(\Gamma')$ or $M_k(\Gamma')$ throughout.

Proof. By noting its affect on q-expansions, we see that applying the Θ operator does not affect meromorphicity (resp., holomorphicity) at the cusps. Thus we need only check the

functional equation. For $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma$, upon differentiating the functional equation (1.2) we have

$$\begin{aligned} \Theta f(\gamma z)(cz+d)^{-k-2} &= \Theta f(z) + \frac{ck}{2\pi i} f(\gamma z)(cz+d)^{-k-1} \\ &= \Theta f(z) + \frac{ck}{2\pi i} f(z)(cz+d)^{-1}. \end{aligned}$$

Using (1.5), for $\gamma \in \Gamma' \subset \Gamma$ we have

$$\begin{aligned} \Theta f(z)|_{k+2}\gamma &- \frac{k}{12}\left(E_2(z)|_2\gamma\right)\left(f(z)|_k\gamma\right) \\ &= \Theta f(z) + \frac{ck}{2\pi i} f(\gamma z)(cz+d)^{-k-1} - \frac{k}{12} E_2(z) f(z) - \left(\frac{k}{12}\right)\frac{12c}{2\pi i(cz+d)} f(z) \\ &= \Theta f(z) - \frac{k}{12} E_2(z) f(z). \end{aligned}$$

□

Remark. It is worth mentioning that there exists a family of "Rankin-Cohen" brackets on $\bigoplus_{k=0}^{\infty} M_k$ (defined using Θ), one of which gives this algebra the structure of a graded Lie algebra. For their definition and basic properties see [33], and for references to recent work, see [5].

Now, given a modular form $f \in \mathcal{M}_k^{\text{mero}}(\Gamma')$, normalized so that its first nonzero q-expansion coefficient is 1, we can write

$$f(z) = q^h \prod_{n=1}^{\infty} (1-q^n)^{c(n)}$$

for some complex numbers $c(n)$, in some neighborhood of ∞. Ignoring convergence issues for a moment (which will be dealt with carefully in Lemma 8), some easy manipulations with q-series yield

$$\frac{\Theta f}{f} = h - \sum_{n \geq 1} \sum_{d|n} c(d) d q^n \tag{1.15}$$

In the next section, we will prove the following characterization of this logarithmic derivative:

Theorem 2 (Bruinier, Kohnen, Ono, [7], [24])**.** *If $f(z) = \sum_{n=h}^{\infty} a(n) q^n \in \mathcal{M}_k^{mero}$ is normalized so that $a(h) = 1$, then*

$$\frac{\Theta f(z)}{f(z)} = \frac{k}{12} E_2(z) - \frac{E_4(z)^2 E_6(z)}{\Delta(z)} \sum_{\tau_i \in \mathfrak{F}} \frac{e_\tau \operatorname{ord}_\tau(f)}{j(z) - j(\tau)}.$$

Remark. This formula has been generalized to several genus zero congruence subgroups in [1] (see §2 of this thesis) and Hecke subgroups of $\mathrm{SL}_2(\mathbb{R})$ (see [10]). The author has also received a preprint [9] giving a generalization to $\Gamma_0(N)$ for squarefree N.

This formula alone is of interest in that it explicitly relates, via equation (1.15), the product expansion exponents of f to special values of j, namely, $j(\tau)$ where τ is a zero or pole of f. Further, it has been used to provide recursive formulas for the coefficients of any modular form over Γ (see [7]), to provide infinite families of systems of orthogonal polynomials divisible by the supersingular locus as polynomials over $\mathbb{F}_p$ (see [4]), (generalizing work of Atkin

described in [16]), and also to provide a characterization of the characteristic polynomials of the Hecke operators over Γ (again in [7]). We will not discuss these applications in this thesis. We will, however, give one additional application, which we defer for a moment in order to introduce the concept of a p-adic modular form.

Following Serre, we define a p-adic modular form to be the p-adic limit of a sequence of elements of $\oplus_{k=0}^{\infty} M_k$ (a precise definition is given in §3). It turns out that in many cases of interest, the logarithmic derivative of a modular form is a p-adic modular form of weight 2. In particular, we have the following theorem of Bruinier and Ono:

Theorem 3 ([8])**.** *Let $f(z) = q^h(1 + \sum_{n=1}^{\infty} a(n)q^n) \in q^h\mathcal{O}_K[[q]] \cap \mathcal{M}_k^{mero}(\Gamma_0(1))$, where $\mathcal{O}_K$ is the ring of integers of a number field K. Moreover, let $c(n) \in K$ denote the algebraic numbers defined by the formal infinite product*

$$f(z) = q^h \prod_{n=1}^{\infty} (1 - q^n)^{c(n)}. \tag{1.16}$$

If $f(z)$ is good at a prime p, then the formal power series

$$\frac{\Theta(f)}{f} = h - \sum_{n=1}^{\infty} \sum_{d|n} c(d) d q^n$$

is a weight two p-adic modular form.

We offer a brief proof of this result, mainly as motivation for the following generalization:

Theorem 4. *Suppose $p \geq 5$ is prime. Let $f(z) = q^h(1 + \sum_{n=1}^{\infty} a(n)q^n) \in q^h\mathcal{O}_K[[q]] \cap \mathcal{M}_k^{mero}(\Gamma_0(p))$ where $\mathcal{O}_K$ is the ring of integers of a number field K. Moreover, let $c(n) \in K$ denote the algebraic numbers defined by the formal infinite product (1.16) for f. If f is good at p, then the formal power series*

$$\frac{\Theta(f)}{f} = h - \sum_{n=1}^{\infty} \sum_{d|n} c(d) d q^n$$

is a weight two p-adic modular form.

The proofs of both of these theorems appear in §5.

Remark. In theorems 3 and 4, we allow h to be negative. The fact that the $c(n)$ are elements of K (implicitly identified with an embedding $K \hookrightarrow \mathbb{C}$) will be obvious from the proof of Lemma 8.

The definition of "good" in the preceding two theorems is given in §5 and discussed in some detail in §7. As one example, the form E_{p-1} is good at p. In general, whether or not a form is good at p is intimately related to the question of whether or not the value of the j-function at the zeros and poles of the form reduces to a supersingular j-invariant in characteristic p (which should come as no surprise to those familiar with overconvergent p-adic modular forms). Through this connection we are able to relate these p-adic modular forms to class numbers of imaginary quadratic fields. In particular, for small primes, we obtain p-adic class number formulae involving sums of special values of the j-function.

Before we can state this result, we must recall the notion of a Heegner point. A complex number τ of the form $\tau = \frac{-b+\sqrt{b^2-4ac}}{2a}$ with $a, b, c \in \mathbb{Z}$, $\gcd(a, b, c) = 1$ and $b^2 - 4ac < 0$ is known as a *Heegner point* of discriminant $d_\tau := b^2 - 4ac$. Heegner points are discussed at

some length in §6. Denote by h_K the class number of the number field K. We have the following:

Corollary 5 (Ono and Papanikolas, [25])**.** *Suppose that $d < -4$ is a fundamental discriminant of an imaginary quadratic field and that τ is a Heegner point of discriminant d. If $K = \mathbb{Q}(j(\tau))$, then the following are true:*

(1) *If $d \equiv 5 \pmod 8$, then as 2-adic numbers we have*

$$h_{\mathbb{Q}(\sqrt{d})} = -\frac{1}{720} \lim_{n\to\infty} \mathrm{Tr}_{K/\mathbb{Q}} \left(\sum_{a=0}^{n} \sum_{b=0}^{2^a-1} j\left(\frac{2^{n-a}\tau + b}{2^a} \right) \right).$$

(2) *If $d \equiv 2 \pmod 3$, then as 3-adic numbers we have*

$$h_{\mathbb{Q}(\sqrt{d})} = -\frac{1}{360} \lim_{n\to\infty} \mathrm{Tr}_{K/\mathbb{Q}} \left(\sum_{a=0}^{n} \sum_{b=0}^{3^a-1} j\left(\frac{3^{n-a}\tau + b}{3^a} \right) \right).$$

(3) *If $d \equiv 2, 3 \pmod 5$, then as 5-adic numbers we have*

$$h_{\mathbb{Q}(\sqrt{d})} = -\frac{1}{180} \lim_{n\to\infty} \mathrm{Tr}_{K/\mathbb{Q}} \left(\sum_{a=0}^{n} \sum_{b=0}^{5^a-1} j\left(\frac{5^{n-a}\tau + b}{5^a} \right) \right).$$

(4) *If $d \equiv 3, 5, 6 \pmod 7$, then as 7-adic numbers we have*

$$h_{\mathbb{Q}(\sqrt{d})} = -\frac{1}{120} \lim_{n\to\infty} \mathrm{Tr}_{K/\mathbb{Q}} \left(\sum_{a=0}^{n} \sum_{b=0}^{7^a-1} j\left(\frac{7^{n-a}\tau + b}{7^a} \right) \right).$$

In §7, we also use Theorem 4 to provide formulae of the same general form of those in Corollary 5, with a weight zero modular form in $\Gamma_0(p)$ taking the place of the j-function (see Theorem 33).

Before we begin the body of this work, we make a few remarks about its structure. Sections 2, 5, and 7 contain results that have only been published recently, if at all, and the primary purpose of this thesis is to collect their content into one place. Sections 3 and 4, on the other hand, are mostly derived from two well-known papers ([29] and [3], respectively). The author has provided proofs of most of the results in these sections that are necessary for the proof of theorems 2, 3, and 4. The notable exceptions are theorems 12 and 16 which are proven in [32] and [21], respectively.

In contrast, providing applications of theorems 2, 3 and 4, including Corollary 5 and Theorem 33, requires results for which we will not provide proofs; it would simply take us too far afield. In particular, §6 is intended to give a brief survey of the relevant definitions and theorems in the theory of complex multiplication, but we omit the proofs of results usually proven using class field theory and reduction theory (we refer the reader to [31, §II] or [20] for a more complete account). Ergo, §6 can be skipped without interrupting the flow of ideas, especially if one is familiar with complex multiplication and elementary calculations involving elliptic curves.

2. A characterization of Ramanujan's theta operator

As indicated above, in this section we will prove a useful characterization of the derivative of a modular form. First we require some preparation. Let

$$\mathfrak{F} := \left\{ z : -\frac{1}{2} \le \mathrm{Re}(z) \le 0 \text{ and } |z| \ge 1 \right\} \cup \left\{ z : 0 < \mathrm{Re}(z) < \frac{1}{2} \text{ and } |z| > 1 \right\}$$

be the standard fundamental domain for the action of $\mathrm{SL}_2(\mathbb{Z})$ on the upper half plane $\mathbb{H}$, and let

$$e_\tau = \begin{cases} \frac{1}{2} & \text{if } \tau = i, \\ \frac{1}{3} & \text{if } \tau = e^{2\pi i/3}, \\ 1 & \text{otherwise.} \end{cases} \tag{2.1}$$

The purpose of this section is to prove the characterization of the logarithmic derivative of a modular form given by Theorem 2. The proof of the theorem requires two steps. The first is an identity due to Asai, Kaneko, and Ninomiya [2]. To introduce this result, define $j_0(z) := 1$, and, for $m > 1$, define $j_m(z)$ to be the unique weight zero meromorphic modular form with q-expansion

$$j_m(z) := J_m(q) := q^{-m} + \sum_{n=1}^{\infty} a_m(n) q^n \in q^{-m}\mathbb{Z}[[q]] \tag{2.2}$$

We note that $j_m(z)$ is a polynomial in $j(z)$ for all m. In fact, it is a polynomial in j with integral coefficients, for $J_m(q)$ can be formed by subtracting suitable integer multiples of the q-series $J(q)^k \in q^{-k}\mathbb{Z}[[q]]$ from $J(q)^m$ (where $0 \le k < m$). The first few $j_m(z)$ follow:

$$\begin{aligned}
j_0(z) = J_0(q) &= 1, \\
j_1(z) = J_1(q) &= j(z) - 744 = q^{-1} + 196884q + \cdots, \\
j_2(z) = J_2(q) &= j(z)^2 - 1488j(z) + 159768 = q^{-2} + 42987520q + \cdots, \\
j_3(z) = J_3(q) &= j(z)^3 - 2232j(z)^2 + 1069956j(z) - 36866976 = q^{-3} + 2592899910q + \cdots.
\end{aligned}$$

We may equivalently define $J_0(q) := j_0(z) := 1$, $J_1(q) := j_1(z) := j(z) - 744$, and

$$J_m(q) := j_m(z) := m j_1(z) | T_{0,m} \tag{2.7}$$

for $m > 1$. The equivalence of this definition to the q-series definition (2.2) follows from (1.9) and the fact that a weakly modular form, being a polynomial in j, is uniquely determined by the coefficients of non-positive exponent in its q-series expansion. Indeed, from this fact we see that the $J_m(q)$ form a basis for $\mathcal{M}_0^\infty$.

We have the following:

Theorem 6 (Asai, Kaneko, Ninomiya)**.** *As an identity of formal power series in ρ, q, we have*

$$\sum_{n=0}^{\infty} J_n(\rho) q^n = \frac{E_4(q)^2 E_6(q)}{\Delta(q)} \cdot \frac{1}{J(q) - J(\rho)}. \tag{2.8}$$

Remark. Asai, Kaneko, and Ninomiya show in [2] how Theorem 6 implies the famous denominator formula for the Monster Lie algebra, namely

$$J(\rho) - J(q) = \rho^{-1} \prod_{m>0 \text{ and } n \in \mathbb{Z}} (1 - \rho^m q^n)^{\beta(mn)},$$

where the coefficients $\beta(n)$ are defined by

$$j_1(z) = \sum_{n=-1}^{\infty} \beta(n) q^n.$$

Proof of Theorem 6. We require a companion set of functions $g_m(\rho)$ indexed by positive integers m, the mth of which can be defined in analogy with (2.2) as the unique weight 2 weakly modular form with ρ-expansion

$$g_m(\rho) := \rho^{-m} + \sum_{n=1}^{\infty} b_m(n)\rho^n \in \mathcal{M}_2^{\infty}. \tag{2.9}$$

Alternately, we may define $g_1(\rho) := \frac{E_4(\rho)^2 E_6(\rho)}{\Delta(\rho)}$ and

$$g_m(\rho) := m^{-1} g_1(\rho)|T_{2,m}.$$

As before, the equivalence of these two definitions follows from the definition of the $T_{2,m}$ and the fact that any weight 2 weakly holomorphic form is uniquely determined by the coefficients in its q-expansion of negative order. We note that this fact follows from the well-known "$k/12$ valence formula" (see, for example, [18, §III.2]), as does the corresponding fact for weight zero weakly holomorphic forms. In fact, as in the weight zero case, this implies that the $g_m(\rho)$ form a basis for the space $\mathcal{M}_2^{\infty}$. Further, from (1.14), if $f \in \mathcal{M}_0^{\infty}$ then $\Theta f \in \mathcal{M}_2^{\infty}$, and by simply looking at the bases $\{J_m\}$,$\{g_m\}$ we have just written down we see that every element of $\mathcal{M}_2^{\infty}$ can be written as Θf for some $f \in \mathcal{M}_0^{\infty}$. In particular, it follows from this observation and the definition of Θ that the constant term of any element of $\mathcal{M}_2^{\infty}$ is identically zero (which justifies the indexing of (2.9)).

Now we note that

$$J_m(q) := mJ_1(q)|T_{0,m} = q^{-m} + ma_1(m)q + \cdots \tag{2.10}$$

and

$$g_m(\rho) := m^{-1} g_1(\rho)|T_{2,m} = \rho^{-m} + b_1(m)q + \cdots \tag{2.11}$$

for $m \geq 1$ simply by (1.9) and the fact that $b_1(0) = 0$. Further, by noting that the constant term of $J_m(q)g_1(q) \in \mathcal{M}_2^{\infty}$ must be zero by the comments in the preceding paragraph and using (2.9) and (2.10), we have that

$$b_1(m) = -ma_1(m) \tag{2.12}$$

for $m \geq 1$. Now $J(\rho)J_m(\rho) \in \mathcal{M}_0$ and $J(q)g_m(q) \in \mathcal{M}_2^{\infty}$ are uniquely determined by their ρ- (resp., q-) expansion coefficients of non-positive exponent, as we've remarked before. Define ρ-expansion coefficients $c(n)$ by

$$J(\rho) = \rho^{-1} + \sum_{n=0}^{\infty} c(n)\rho^n$$

By comparing coefficients using equalities (2.10), (2.11), (2.12) and the observation that $b_1(0) = 0$, we obtain the recurrence relation

$$J(\rho)J_m(\rho) = J_{m+1}(\rho) + \sum_{i=0}^{m} c(m-i)J_i(\rho) - b_1(m) \tag{2.13}$$

for all $m \geq 0$. Thus, multiplying both sides of (2.13) by q^m and summing over $m \geq 0$ we obtain

$$J(\rho)\sum_{m=0}^{\infty} J_m(\rho)q^m = \frac{1}{q}(\sum_{m=0}^{\infty} J_m(\rho)q^m - 1) + (J(q) - \frac{1}{q})\sum_{m=0}^{\infty} J_m(\rho)q^m - g_1(q) + \frac{1}{q}. \tag{2.14}$$

Noting that $g_1(q) = \frac{E_4(q)^2 E_6(q)}{\Delta(q)}$, we see that (2.14) is a rewriting of (2.8). □

Corollary 7. *Fix $\tau \in \mathbb{H}$. Then*

$$\frac{E_4(z)^2 E_6(z)}{\Delta(z)} \frac{1}{j(z) - j(\tau)} = \sum_{n=0}^{\infty} j_m(\tau) q^n$$

as meromorphic functions in z on $\mathfrak{F}$.

Proof. Compare Fourier (q-series) coefficients in a deleted neighborhood of infinity using Theorem 6. □

Remark. The main result of [2] is the statement that the zeros of $j_m(z)$ in $\mathfrak{F}$ are simple and are all contained in the intersection of the unit circle with $\mathfrak{F}$. The technique they use is analogous to that used by Rankin and Swinnerton-Dyer to prove that the "nontrivial" zeros of $E_k(z)$ have the same property, see [26]. For yet another family of modular forms whose zeros have the same property, see [12].

We also require the following proposition, which follows from basic complex analysis:

Proposition 8 ([7])**.** *Let $f = \sum_{n=h}^{\infty} a_f(n)q^n$ be a meromorphic function in a neighborhood of $q = 0$, normalized so that $a_f(h) = 1$. Then there are complex numbers $c(n)$ such that*

$$f = q^h \prod_{n=1}^{\infty} (1 - q^n)^{c(n)},$$

where the product converges in a sufficiently small neighborhood of $q = 0$. Moreover,

$$\frac{\Theta f}{f} = h - \sum_{n=1}^{\infty} \sum_{d|n} c(d) d q^n. \tag{2.15}$$

Remark. We will refer to the $c(n)$ associated to a given meromorphic modular form f by Proposition 8 as the *Borcherds exponents* of f.

Proof. As usual, we understand that complex powers are defined by the principle branch of the complex logarithm. Write $F(q) := f(z)$, and then note that $qF'(q)/F(q)$ is holomorphic at $q = 0$. We may therefore write its Taylor expansion around $q = 0$, valid in $|q| < \epsilon$ for some $\epsilon > 0$, as

$$qF'(q)/F(q) = h - \sum_{n \geq 1} \alpha(n) q^n. \tag{2.16}$$

For $n \geq 1$ define

$$c(n) := \frac{1}{n} \sum_{d|n} \alpha(d) \mu(n/d)$$

where μ is the Möbius function. By Möbius inversion we have

$$\alpha(n) = \sum_{d|n} c(d)d. \tag{2.17}$$

If we fix q_0 with $|q_0| < \epsilon$, then by absolute convergence of (2.16) we have $\alpha(n) = \mathcal{O}(|q_0|^{-n})$ for all n. Thus the double sum

$$\sum_{m,n\geq 1} c(n)nq^{mn} \tag{2.18}$$

converges absolutely in $|q| < |q_0|$ and hence in $|q| < \epsilon$.

Suppose for the remainder of the proof that $|q| < \epsilon$. From (2.16) and (2.17) we have

$$\begin{aligned}
\frac{d}{dq}\log(F(q)q^{-h}) &= \frac{F'(q)}{F(q)} - \frac{h}{q} \\
&= -\sum_{n\geq 1} c(n)\frac{d}{dq}\left(\sum_{m\geq 1}\frac{q^{mn}}{m}\right) \\
&= \frac{d}{dq}\left(\sum_{n\geq 1} c(n)\log(1-q^n)\right).
\end{aligned}$$

The interchange of summation and integration can be justified by using local uniform convergence as we did in proving the absolute convergence of (2.18).

Upon integrating, we obtain

$$\log(F(q)q^{-h}) = \sum_{n\geq 1} c(n)\log(1-q^n).$$

Here we use the normalization $a_f(h) = 1$. Now $c(n)\log(1-q^n)$ and $\log(1-q^n)^{c(n)}$ differ by integer multiples of $2\pi i$. Since $c(n)\log(1-q^n) \to 0$ as $n \to \infty$, we have $\log(1-q^n)^{c(n)} \to 0$ as well. Thus, as $n \to \infty$, these two quantities differ in value only finitely many times; it follows that there exists an integer N such that

$$\log(F(q)q^{-h}) = \sum_{n\geq 1} \log(1-q^n)^{c(n)} + 2\pi i N.$$

Taking the exponential on both sides finishes the proof of the proposition. □

We now prove Theorem 2.

Proof of Theorem 2. Choose $C > 0$ large enough so that all poles of f in $\mathfrak{F}$ (excluding any at the cusp at infinity) have imaginary part less than C. Let $L := \{t + iC : -\frac{1}{2} \leq t \leq \frac{1}{2}\}$ and consider the contour in $\mathbb{H}$ formed from the part of $\partial\mathfrak{F}$ of imaginary part less than C and L. Modify this contour as in the proof of the classical $k/12$ valence formula (see, for example, [18, §III.2, p. 115]), specifically, if there are poles of f at i or $\omega := e^{2\pi i/3}$ (which, by modularity, implies the existence of a pole at $e^{\pi i/3}$), form half and "sixth" circles of radius $r > 0$ around them, and if there are poles of f on the boundary, form two half circles of radius $r > 0$ around them, one enclosing the pole on one side of the fundamental domain, one not enclosing the pole which must exist on the other side (given that f is modular). Call the left vertical side of this contour $\gamma_1(r)$, the right vertical side $\gamma_2(r)$, and the bottom $\gamma_3(r)$. Take the modified contour $\gamma_1(r) \cup L \cup \gamma_2(r) \cup \gamma_3(r)$ to have positive (counterclockwise) orientation.

If we integrate

$$\frac{1}{2\pi i}\frac{f'(z)}{f(z)}j_n(z) \tag{2.19}$$

along this full contour and let $r \to 0$, by holomorphicity of j_n on $\mathbb{H}$ the integral will be equal to

$$\sum_{\tau \in \mathfrak{F} - \{\omega, i\}} \operatorname{ord}_\tau(f) j_n(\tau). \tag{2.20}$$

We can also integrate (2.19) in pieces, from which we see that (2.20) is equal to

$$\begin{aligned} -\frac{1}{3}\operatorname{ord}_\omega(f)j_n(\omega) - \frac{1}{2}\operatorname{ord}_i(f)j_n(i) + \int_L \frac{f'(z)}{f(z)}j_n(z)dz + \int_{\gamma_3(r)} \frac{f'(z)}{f(z)}j_n(z)dz \\ = -\frac{1}{3}\operatorname{ord}_\omega(f)j_n(\omega) - \frac{1}{2}\operatorname{ord}_i(f)j_n(i) + \frac{1}{2\pi i}\int_{L'} \frac{F'(q)}{F(q)}J_n(q)dq + \int_{\gamma_3(r)} \frac{f'(z)}{f(z)}j_n(z)dz. \end{aligned} \tag{2.21}$$

Here L' is a simple loop around $q = 0$. By Proposition 8 we have

$$\frac{qF'(q)}{F(q)} = \frac{\Theta(f)}{f} = h - \sum_{n=1}^{\infty}\sum_{d|n} c(d)dq^n$$

and thus, applying the residue theorem, we have

$$\frac{1}{2\pi i}\int_{L'} \frac{F'(q)}{F(q)}J_n(q)dq = \sum_{d|n} c(d)d.$$

We now deal with the last term in (2.21). By Proposition 1, if the weight of f is k, there exists a weight $k+2$ modular form g such that

$$\begin{aligned} \int_{\gamma_3(r)} \frac{f'(z)}{f(z)}j_n(z) &= 2\pi i \int_{\gamma_3(r)} \frac{\Theta(f)}{f}j_n(z)dz \\ &= 2\pi i \int_{\gamma_3(r)} \frac{g(z)}{f(z)}j_n(z)dz + 2\pi i \int_{\gamma_3(r)} \frac{k}{12}j_n(z)E_2(z)dz. \end{aligned} \tag{2.22}$$

Now let β denote the path along the unit circle from i to ω, taken with positive orientation, and S the fractional linear transformation defined by $S(z) = -1/z$. Then $\gamma_3 = -\beta + S\beta$, and thus the right hand side of equation (2.22) is equal to

$$\begin{aligned} &\left(\int_{-\beta} \frac{g(z)}{f(z)}j_n(z)dz + \int_{S\beta} \frac{g(z)}{f(z)}j_n(z)dz\right) + \frac{k}{12}\left(\int_{-\beta} j_n(z)E_2(z)dz + \int_{S\beta} j_n(z)E_2(z)dz\right) \\ = &\frac{k}{12}\left(\int_{-\beta} j_n(z)E_2(z)dz + \int_{S\beta} j_n(z)E_2(z)dz\right) \\ = &\frac{k}{12}\left(\int_{-\beta} j_n(z)E_2(z)dz + \int_{\beta} j_n(z)E_2(z)dz + \int_{\beta} \frac{12}{2\pi i}\frac{j_n(z)}{z}dz\right) \\ = &\frac{k}{2\pi i}\int_{\beta} \frac{j_n(z)}{z}dz. \end{aligned}$$

To obtain the first equality we used the functional equation for elements of $\mathcal{M}_2^\infty$ along with a standard change of variables (which introduces a factor of $1/z^2$). To move from the second

line to the third we used the functional equation for elements of $\mathcal{M}_2^\infty$, a change of variables, and the functional equation (1.5) for $E_2(z)$.

Now, instead of trying to evaluate $\frac{k}{2\pi i}\int_\beta \frac{j_n(z)}{z}dz$ directly, we plug $f=\Delta$ into (2.21), notice that $\sum_{\tau\in\mathfrak{F}} \operatorname{ord}_\tau(f)j_n(\tau)=0$, and thereby obtain

$$\begin{aligned}\frac{1}{2\pi i}\int_\beta \frac{j_n(z)}{z}dz &= -\frac{1}{12}\int_\beta \frac{\Delta'(q)}{\Delta(q)}J_n(q)dq\\ &= -\frac{1}{12}\sum_{d|n} c(d)d\\ &= -2\sigma_1(n)\end{aligned}$$

where $c(d)\equiv 24$ are (just for the purposes of the preceding equation) the product expansion exponents of $\Delta(z)=q\prod_{n=1}^\infty(1-q^n)^{24}$.

Thus, collecting all of this, equation (2.21) implies that

$$\sum_{\tau\in\mathfrak{F}} e_\tau \operatorname{ord}_\tau(f)j_n(\tau)=\sum_{d|n} c(d)d-2k\sigma_1(n)$$

Now we recall that by Theorem 6, it is sufficient to show that

$$\frac{\Theta(f)}{f}=\frac{kE_2}{12}-\sum_{n=1}^\infty\left(\sum_{\tau\in\mathfrak{F}} e_\tau \operatorname{ord}_\tau(f)j_n(\tau)\right)q^n.$$

To prove this identity, we apply Proposition 8, note

$$\frac{k}{12}E_2(z)=\frac{k}{12}-2k\sum_{n=1}^\infty\sigma_1(n)q^n,$$

and argue coefficient by coefficient. The only coefficient that might be unclear is the constant $n=0$ term. In this case, on the left we have h, which is the order of f at infinity, and on the right we have $\frac{k}{12}-\sum_{\tau\in\mathfrak{F}} e_\tau \operatorname{ord}_\tau(f)$, which is precisely $\operatorname{ord}_\infty(f)=h$ by the $k/12$ valence formula (for example, see [18, §III.II, p. 115]).

□

We remark here that the derivative formula of Theorem 2 explicitly relates, via Proposition 2.15, the coefficients $c(n)$ of the product expansion of a modular form to a specific weight 2 meromorphic modular form. This relationship is in the spirit of the work of Borcherds on the product expansion exponents of Jacobi forms with Heegner divisors. See [6] for the details of this theory.

As we mentioned in the introduction, Ahlgren, in [1], has proven a generalization of Theorem 4 to certain genus zero congruence subgroups. We will state his theorem after fixing some notation. Define Dedekind's eta-function

$$\eta(z):=q^{\frac{1}{24}}\prod_{n=1}^\infty(1-q^n)$$

as usual. For $p=2,3,5,7$ or 13, let

$$j^{(p)}(z):=\left(\frac{\eta(z)}{\eta(pz)}\right)^{\frac{24}{p-1}}\in\mathcal{M}_0^\infty(\Gamma_0(p)).$$

This $j^{(p)}(z)$ is a modular form with a simple pole at ∞ and a simple zero (with respect to local coordinates) at 0. Additionally, its restriction to a fundamental domain for the action of $\Gamma_0(p)$ on $\mathbb{H}$ forms a bijection from that fundamental domain to $\mathbb{C}$. In analogy with (2.2), we now define a sequence of modular functions $\{j_m^{(p)}(z)\}_{m=0}^{\infty}$. Let $j_0^{(p)}(z) := 1$ and for $m > 0$ let $j_m^{(p)}(z) \in \mathcal{M}_0^{\infty}(\Gamma_0(p))$ be the unique modular function which is holomorphic on $\mathbb{H}$, vanishes at the cusp 0 and whose Fourier expansion at infinity has the form

$$j_m^{(p)}(z) = q^{-m} + c(0) + c(1)q + c(2)q^2 + \cdots . \tag{2.23}$$

Because $\Gamma_0(p)$ is genus zero, each of these functions can be written as monic polynomials in $j_1^{(p)}(z) = j^{(p)}(z)$ with constant term equal to zero. For example, we have

$$\begin{aligned}
j_0^{(5)}(z) &= 1, \\
j_1^{(5)}(z) &= j^{(5)}(z) = q^{-1} - 6 + 9q + 10q^2 - 30q^3 + \cdots \\
j_2^{(5)}(z) &= j^{(5)}(z)^2 + 12j^{(5)}(z) = q^{-2} - 18 + 20q + 21q^2 + 192q^3 + \cdots \\
j_3^{(5)}(z) &= j^{(5)}(z)^3 + 18j^{(5)}(z)^2 + 81j^{(5)}(z) = q^{-3} - 24 - 90q + 288q^2 + 144q^3 + \cdots
\end{aligned}$$

In analogy with our definition of $\mathfrak{F}$, we define $\mathfrak{F}_p$ to be a fundamental domain for the action of $\Gamma_0(p)$ on $\mathbb{H}$, taking the convention that $\mathfrak{F}_p$ does not include the two cusps ∞ and 0. If $\tau \in \mathbb{H}$, then (in analogy with (2.1)) we define $e_\tau^{(p)} \in \left\{1, \frac{1}{2}, \frac{1}{3}\right\}$ by

$$e_\tau^{(p)} := (\text{the order of the isotropy subgroup of } \tau \text{ in } \Gamma_0(p)/\{\pm I\})^{-1}.$$

We can now state the following theorem:

Theorem 9 ([1])**.** *Suppose that $p \in \{2, 3, 5, 7, 13\}$ and that $f(z) = \sum_{n=h}^{\infty} a(n)q^n \in \mathcal{M}_k^{mero}(\Gamma_0(p))$, normalized so that $a(h) = 1$. Then*

$$\frac{\theta f}{f} = -\sum_{\tau \in \mathfrak{F}_p} \left(e_\tau^{(p)} \sum_{n=1}^{\infty} j_n^{(p)}(\tau) q^n \right) + \frac{h - k/12}{p-1} \cdot pE_2|V(p) + \frac{pk/12 - h}{p-1} \cdot E_2.$$

We will not provide a proof of this theorem; it is entirely analogous to the proof of Theorem 2 except for some difficulties which naturally arise when dealing with congruence subgroups. We note that a formula analogous to Corollary 7 holds in the $\Gamma_0(p)$ case for $p \in \{2, 3, 5, 7, 13\}$ as well (see [1]).

3. Serre's p-adic modular forms

We begin with the notion of congruent q-series. Two q-series $f(z) = \sum_{n=n_0}^{\infty} a(n)q^n \in q^{n_0}\mathbb{Z}[[q]]$ and $g(z) = \sum_{m=m_0}^{\infty} b(m)q^m \in q^{m_0}\mathbb{Z}[[q]]$ are said to be *congruent modulo N* if

$$a(k) \equiv b(k) \pmod{N}$$

for all k. For primes p, we say that a q-series $f(z)$ with integral coefficients is a *weakly modular form modulo p^n* if it is congruent modulo p^n to a modular form $g(z) \in \mathcal{M}^{\infty} \cap q^{-m_0}\mathbb{Z}[[q]]$. This is written as

$$f(z) \equiv g(z) \pmod{p^n}$$

We note here that the theory of modular forms modulo prime powers is quite well developed; for a basic introduction, see [19, §IV.X], and for a variety of interesting number-theoretic applications, see [24].

We begin by establishing some well-known congruences involving the Eisenstein series $E_k(z)$. First we recall two classical Bernoulli number congruences (see [15, p. 233-238]). Let D_n be the denominator of the nth Bernoulli number, written in lowest terms. The von Staudt-Clausen congruences state

$$D_n = 6 \prod_{(p_i-1)|n} p_i \tag{3.1}$$

where the p_i's are prime. Let $p \geq 5$ be prime. Now suppose $m \geq 2$ is even and $m' \equiv m \pmod{\phi(p^r)}$ where ϕ is the Euler ϕ-function. Then the Kummer congruences state

$$\frac{(1-p^{m'-1})B_{m'}}{m'} \equiv \frac{(1-p^{m-1})B_m}{m} \pmod{p^r}. \tag{3.2}$$

Using these congruences, we prove the following lemma:

Lemma 10. *For $r \geq 1$ and $p \geq 5$,*

$$(E_{p-1}(z))^{p^{r-1}} \equiv 1 \pmod{p^r}. \tag{3.3}$$

Proof. We have

$$(E_{p-1}(z))^{p^{r-1}} = \left(1 - \frac{2(p-1)}{B_{p-1}} \sum_{n=1}^{\infty} \sigma_{p-1}(n) q^n\right)^{p^{r-1}} = \left(1 - \frac{2(p-1)D_{p-1}}{U_{p-1}} \sum_{n=1}^{\infty} \sigma_{p-1}(n) q^n\right)^{p^{r-1}}$$

where U_{p-1} is an integer coprime to D_{p-1}. From (3.1) we have $p|D_{p-1}$ which implies (3.3) after an application of the binomial theorem. □

We also record here the following congruences, which will be useful in §7:

Lemma 11. *Suppose $k \geq 4$ is even. Then*

$$E_k(z) \equiv 1 \pmod{24},$$

and, if $p \geq 5$ is a prime such that $(p-1) \mid k$,

$$E_k(z) \equiv 1 \pmod{p}.$$

Proof. These both follow immediately from the von Staudt-Clausen equation (3.1). □

Before we can proceed any farther, we must generalize the notion of congruent modular forms introduced above. Let K be a number field with ring of integers $\mathcal{O}_K$, and $\mathfrak{m} \subset \mathcal{O}_K$ an ideal. We define the *order of f modulo $\mathfrak{m}$* by

$$\mathrm{Ord}_{\mathfrak{m}}(f) := \min\{n : a(n) \notin \mathfrak{m}\}$$

with the convention that $\mathrm{Ord}_{\mathfrak{m}}(f) := +\infty$ if $a(n) \in \mathfrak{m}$ for all n. Though this is certainly not obvious a priori, given a modular form with coefficients in $\mathcal{O}_K$, one need only check finitely many q-series coefficients to calculate $\mathrm{ord}_{\mathfrak{m}}(f)$. The following theorem of Sturm (see [24, §2.9] or [32]) makes this precise:

Theorem 12. *Suppose $k \geq 0$ is an integer and K is a number field with ring of integers O_K. Moreover let $f = \sum_{n=0}^{\infty} a(n)q^n \in M_k(\Gamma_0(N)) \cap \mathcal{O}_K[[q]]$. If $\mathfrak{m} \subset \mathcal{O}_K$ is an ideal for which*

$$\mathrm{Ord}_{\mathfrak{m}}(f) > \frac{k}{12}[\Gamma_0(1) : \Gamma_0(N)]$$

then $Ord_{\mathfrak{m}}(f) = +\infty$.

Remark. We will not prove this theorem in this thesis. We will only require it for the proofs of theorems 3 and 4, and there we only invoke it briefly to prove that we can normalize certain forms so that they have coefficients in a ring of integers. To see how this works, consider some form $f \in M_k(\Gamma_0(N))$ with p-integral algebraic coefficients. Then we can pick an integer $M \equiv 1 \pmod{p}$ such that the first $\frac{k}{12}[\Gamma_0(1) : \Gamma_0(N)]$ coefficients of Mf are contained in the ring of integers of some number field $\mathcal{O}_K$. Applying Theorem 12, it follows that all of the coefficients of Mf are in $\mathcal{O}_K$, in other words, we have produced a form $Mf \equiv f \pmod{p}$ with algebraic integer coefficients.

Elements of $M_k(\Gamma')$ have the extremely useful property that they determined by their first few q-series coefficients. Though, as noted above, we will not need Theorem 12 until §5, we included it at this point to call the reader's attention to the fact that a similar statement is true when working with modular forms congruent modulo ideals in a number field.

We are now in a position to justify the title of this section. Let K be a number field and let $\mathcal{O}_v$ be the completion of its ring of integers at a finite place v with residue characteristic p. Moreover, let λ be a uniformizer for $\mathcal{O}_v$. Finally, for $a_n \in K_v$, let

$$\operatorname{ord}_\lambda\left(\sum_{n=n_0}^{\infty} a_n q^n\right) := \inf\{\operatorname{ord}_\lambda(a_n)\}.$$

We make the following:

Definition. *A formal power series*

$$f := \sum_{n=0}^{\infty} a(n) q^n \in \mathcal{O}_v[[q]]$$

is a p***-adic modular form of weight*** $k \in \mathcal{O}_v$ *if there is a sequence* $f_i \in \mathcal{O}_v[[q]]$ *of holomorphic modular forms on* Γ *with weights* k_i *for which* $\operatorname{ord}_\lambda(f_i - f) \to +\infty$ *and* $\operatorname{ord}_\lambda(k - k_i) \to +\infty$.

Remark (1). This is Serre's original definition of a p-adic modular form [29]. The notion of a p-adic modular form has been substantially generalized by Katz; for an introduction and an explanation of how the two definitions relate, see [13, §I].

Remark (2). Note that the $\operatorname{ord}_\lambda$ here is different from the Ord introduced above.

Thus we observe, with the help of Lemma 10 and Lemma 11, that 1 is a p-adic modular form for all primes p, or, more precisely, is a p-adic modular forms when identified with its q-expansion considered as an element of $\mathcal{O}_v[[q]]$ (the q-expansion of 1 is just $1+0q+0q^2+\cdots$). Further, any element of $M_k \cap \mathcal{O}_v[[q]]$ is trivially a p-adic modular form. As another example, we have the following:

Proposition 13. *The* q*-series* $E_2(z)$ *is a* p*-adic modular form for all* p.

Proof. We have

$$\frac{B_{\phi(p^r)+2}}{\phi(p^r)+2} E_{\phi(p^r)}(z) \equiv \frac{B_2}{2} E_2(z) - p\frac{B_2}{2} E_2(z)|V(p) \mod p^{r+1}$$

for all $r \geq 1$ by examining q-series using the Kummer congruences (3.2) and Euler's theorem. The proposition then follows by inverting the formal operator $(1 - pV(p))^{-1}$, which preserves the space of p-adic modular forms. For details, see [29, §2.1]. □

The only nontrivial result we will require from the theory of p-adic modular forms is a theorem, due to Serre, which allows us to compute the constant term of a p-adic modular form in terms of a p-adic limit of its other coefficients for small primes p. Let $\zeta_p^*(s)$ be the Kubota-Leopoldt p-adic zeta function. We have

Theorem 14 (Theorem 7, [29])**.** *If $p \leq 7$ is prime and*

$$f = \sum_{n=0}^{\infty} a(n)q^n$$

is a p-adic modular form of weight $k \neq 0$, then

$$a(0) = \frac{\zeta_p^*(1-k)}{2} \cdot \lim_{n \to +\infty} a(p^n).$$

This theorem is proven by decomposing the vector space M of p-adic modular forms into $M = E \oplus N$, where N is a space on which the U operator (defined exactly as in (1.11)) acts nilpotently and E is a space on which U acts bijectively. It turns out that for $2 \leq p \leq 7$ prime, E is spanned by the reductions of Eisenstein series, and N is spanned by the reductions of cusp forms. By analyzing each subspace, the theorem follows. For a complete proof, see [29, §2.3]. Incidentally, [29] is a beautiful paper, and provides an interesting counterpoint to Katz's geometric approach to p-adic modular forms.

Also mentioned in [29, §1.6] is the fact that $\zeta_p^*(1-k) = (1-p^{k-1})\zeta(1-k)$ for even integers $k \geq 2$, where $\zeta(s)$ is the usual characteristic zero Riemann zeta function. In the sequel we will only be interested in the special case $k = 2$, in which we have:

$$\zeta_p^*(1-2) = (1-p)\zeta(-1) = \frac{p-1}{12}.$$

Thus we immediately have the following corollary of Theorem 14:

Corollary 15. *If $p \leq 7$ is prime and*

$$f = \sum_{n=0}^{\infty} a(n)q^n$$

is a p-adic modular form of weight $k \neq 0$, then

$$a(0) = \frac{p-1}{24} \cdot \lim_{n \to +\infty} a(p^n).$$

4. Varying the level

Given a modular form $f \in M_k(\Gamma_0(M))$ (resp., $f \in S_k(\Gamma_0(M))$) and recalling (1.10) and (1.13), it is not hard to verify using the functional equation (1.2) that $f|V(d) \in M_k(\Gamma_0(dM))$ (resp., $f|V(d) \in S_k(\Gamma_0(dM))$). These forms are holdovers from lower levels; they're nothing new, which justifies the notation

$$S_k(\Gamma_0(N)) \supset S_k^{\text{old}}(\Gamma_0(N)) := \bigoplus_{dM|N} S_k(\Gamma_0(M))|V(d).$$

We define *the space of newforms* $S_k^{new}(\Gamma_0(N))$ to be the orthogonal complement to $S_k^{\text{old}}(\Gamma_0(N)$ with respect to a certain inner product, called the *Petersson inner product* (see [19, §III.4] or [18, §III.3]). As a first example, for $p \geq 3$ prime, we have

$$M_2(\Gamma_0(p)) = \langle E_2(z) - pE_2(pz) \rangle \oplus S_2^{\text{new}}(\Gamma_0(p)) \tag{4.1}$$

because $M_2(\Gamma) = 0$. One can check that $E_2(z) - pE_2(pz)$ satisfies the requisite functional equation using (1.5). For arbitrary weights, the space of newforms has the useful property that it is preserved under the action of the Hecke operators. It is also invariant under another operator, the Atkin-Lehner involution, which we now define.

Definition. *For a prime divisor p of N with $\mathrm{ord}_p(N) = \ell$, let $Q_p := p^\ell$. We define the **Atkin-Lehner operator** $|_k W(Q_p)$ on $M_k(\Gamma_0(N))$ by any matrix*

$$W(Q_p) := \left(\begin{smallmatrix} Q_p a & b \\ Nc & Q_p d \end{smallmatrix}\right) \in M_{2\times 2}(\mathbb{Z})$$

*with determinant Q_p, where $a, b, c, d \in \mathbb{Z}$. Further, define the **Fricke involution** $|_k W(N)$ on $M_k(\Gamma_0(N))$ by the matrix*

$$W(N) := \begin{pmatrix} 0 & -1 \\ N & 0 \end{pmatrix}.$$

Well-definition of $|_k W(Q_p)$ follows from the functional equation of $f \in M_k(\Gamma_0(N))$ and the fact that $W(Q_p)$ is unique up to left multiplication by elements of $\Gamma_0(N)$. We note here that for $f \in M_k(\Gamma_0(p))$ we have $f|_k W(Q_p) = f|_k W(p)$. By abuse of language, we will call $W(p)$ an Atkin-Lehner operator in this setting.

We now are in a position to make the following:

Definition. *A **newform** in $S_k^{new}(\Gamma_0(N))$ is a normalized cusp form that is an eigenform for all the Hecke operators, all of the Atkin-Lehner involutions $|_k W(Q_p)$ for $p|N$, and the Fricke involution $|_k W(N)$.*

Newforms enjoy remarkable properties. We recall a few such properties on the more utilitarian side of things:

Theorem 16. *Suppose that k is a positive even integer. Then*

1. *The space $S_k^{new}(\Gamma_0(N))$ has a basis of newforms.*
2. *If $f(z) = \sum_{n=1}^{\infty} a(n)q^n \in S_k^{new}(\Gamma_0(N))$ is a newform, then there is a number field K with the property that for every integer n we have $a(n) \in \mathcal{O}_K$, the ring of algebraic integers of K.*
3. *If $f \in S_k^{new}(\Gamma_0(N))$ is a newform then there is an integer $\lambda_f \in \{\pm 1\}$ for which*

$$f|_k W(Q_p) = \lambda_p f.$$

For the statements of a collection of results, including the above, on newforms, see [24, §2.4,§2.5]. For proofs, see [3], and for generalizations, see [21] and [23].

We began this section by discussing how one can raise the level of an element of $M_k(\Gamma_0(N))$ to obtain an element of $M_k(\Gamma_0(MN))$. We now discuss the *trace operator* Tr_N^{MN}, which lowers the level. For coprime M, N, define

$$\mathrm{Tr}_N^{MN} : M_k(\Gamma_0(MN)) \to M_k(\Gamma_0(N))$$

by

$$\mathrm{Tr}_N^{MN}(f) = \sum_{i=1}^{r} f|_k \gamma_i$$

where $\{\gamma_1, ..., \gamma_r\}$ is a complete set of coset representatives for $\Gamma_0(NM)\backslash\Gamma_0(N)$. The fact that $\mathrm{Tr}_N^{MN}(f) \in M_k(\Gamma_0(N))$ is immediate; acting on $\mathrm{Tr}_N^{MN}(f)$ by an element of $\Gamma_0(N)$ simply permutes the γ_i by the invariance of f under the action of $\Gamma_0(NM)$. We have the following explicit formula for Tr_p^{Np}:

Lemma 17 ([22]). *Suppose that p is an odd prime and that $p \nmid N$. If $f \in M_k(\Gamma_0(Np))$ then*

$$Tr_N^{Np}(f) = f + p^{1-k/2} f|_k W(p) U(p)$$

Proof. A complete set of coset representatives for $\Gamma_0(Np)$ in $\Gamma_0(N)$ is given by

$$\left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right\} \cup \left\{ \begin{pmatrix} 1 & 0 \\ N & 1 \end{pmatrix} \begin{pmatrix} 1 & j \\ 0 & 1 \end{pmatrix} \right\}_{j=0}^{p-1}.$$

We also have

$$\begin{pmatrix} 1 & 0 \\ N & 1 \end{pmatrix} \begin{pmatrix} 1 & j \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1/p & 0 \\ 0 & 1/p \end{pmatrix} \begin{pmatrix} p & a \\ Np & pb \end{pmatrix} \begin{pmatrix} 1 & j-a \\ 0 & p \end{pmatrix}$$

where

$$\begin{pmatrix} p & a \\ Np & pb \end{pmatrix}$$

is a matrix for $W(p)$. Since scalar matrices act trivially on $M_k(\Gamma_0(Np))$,

$$\mathrm{Tr}_N^{MN}(f) = f + \sum_{j=1}^{p-1} f|_k W(p) \begin{pmatrix} 1 & j \\ 0 & p \end{pmatrix}.$$

By considering q-expansions, we have

$$\sum_{j=0}^{p-1} g\left(\frac{z+j}{p}\right) = p(g|U(p))(z),$$

which completes the proof of the lemma. □

It is well-known that if p is prime with $p \nmid N$, then $\mathrm{Tr}_N^{Np}(f) = 0$ for $f \in S_k^{\mathrm{new}}(\Gamma_0(Np))$ (see [21]). Combining this observation with Lemma 17 yields the following:

Proposition 18 ([3]). *If $f \in S_k^{new}(\Gamma_0(p))$, then*

$$f|_k W(p) = -p^{1-k/2} f|U(p).$$

Proof. First suppose that f is a newform. From Lemma 17, we have

$$0 = \mathrm{Tr}_1^p(f) = f + p^{1-k/2} f|_k W(p) U(p).$$

Thus

$$f = -p^{1-k/2} f|_k W(p) U(p). \tag{4.2}$$

Note that $U(p) = T_{k,p}$ because the level is p (see (1.12)). Now note that f, being a newform, is an eigenform both for the Hecke operators and $W(p)$ (by Theorem 16). Thus the actions of $W(p)$ and $U(p)$ on f commute. With all this in mind, applying $W(p)$ to both sides of (4.2), we have

$$\begin{aligned} f|_k W(p) &= -p^{1-k/2} f|_k W(p) U(p) W(p) \\ &= -p^{1-k/2} f|_k W(p)^2 U(p) \\ &= -p^{1-k/2} f|_k U(p). \end{aligned}$$

To derive the last equality, we used the fact that the action of $W(p)^2$ is trivial, which can be seen from directly from a matrix representation of $W(p)$: $\left(\begin{smallmatrix} 0 & -1 \\ p & 0 \end{smallmatrix}\right)\left(\begin{smallmatrix} 0 & -1 \\ p & 0 \end{smallmatrix}\right) = \left(\begin{smallmatrix} -p & 0 \\ 0 & -p \end{smallmatrix}\right)$. Since $U(p)$ and $W(p)$ are both linear operators, the proposition now follows for all $f \in S_k^{\mathrm{new}}(\Gamma_0(p))$. □

5. p-adic properties of Borcherds exponents

We begin with the following:

Definition. *Let f be a meromorphic modular form of weight k over Γ or $\Gamma_0(p)$ whose poles and zeros, away from $z = \infty$, are at the points $z_1, ..., z_s \in \mathbb{H}$. We say that $f(z)$ is* **good at** *p if there is a holomorphic modular form $\mathcal{E}_f(z) \in M_b(\Gamma)$ with p-integral algebraic coefficients for which the following are true:*

1. *As q-series, $\mathcal{E}_f(z) \equiv 1 \pmod{p}$.*
2. *For each $1 \leq i \leq s$ we have $\mathcal{E}_f(z_i) = 0$.*

Remark (1). It follows immediately that if f and g are good, then fg is good.

Remark (2). As mentioned in the introduction, we will provide several families of good forms in §7; other families are provided in [8].

Remark (3). Using Theorem 30 below and the fact that the canonical reduction map

$$\bigoplus_{2m \geq 0} M_{2m}(\Gamma) \cap \overline{\mathbb{Q}}[[q]] \longrightarrow \mathbb{F}_p[[q]].$$

given by reducing q-series coefficients modulo a prime $p \geq 5$ has kernel generated by $(E_{p-1}(z) - 1)$ (see [21, §IV.X], for example), one can show that a form is good at p if and only if its poles and zeros are supported at points τ_i such that $j(\tau_i)$ reduces to a supersingular j-invariant in characteristic p. In particular, it is possible to use this fact to give examples of forms that are *not* good at a given prime p. Though this characterization is perhaps theoretically more interesting and should be kept in mind, we will emphasize the definition given previously because it is lends itself more readily to our explicit methods of proof.

In view of the observations we made in sections 1 and 2, it is now straightforward to prove Theorem 3:

Proof of Theorem 3. By examining the proof of Proposition 1.14, we see that if f is a meromorphic modular form of weight k over Γ, then

$$\widetilde{f} := 12\Theta f(z) - kE_2(z)f(z) \tag{5.1}$$

is a meromorphic modular form of weight $k+2$ over Γ. Further, from (5.1) we see that the poles of $\widetilde{f}(z)$ are supported at the poles of $f(z)$.

Now consider

$$\frac{\theta f}{f} = \frac{1}{12}\left(\frac{\widetilde{f}(z)}{f(z)} + kE_2(z)\right).$$

By 10, E_2 is a p-adic modular form of weight 2 with integer coefficients. Thus it suffices to show that $\widetilde{f}/f$ is as well. If b is the weight of $\mathcal{E}_f(z)$, then note $\mathcal{E}_f(z)^{p^j}\widetilde{f}/f \in M_{p^j b+2}$. If $\mathcal{E}_f(z)^{p^j}\widetilde{f}/f$ does not have algebraic integer coefficients, then multiply it by a suitable integer $t_{j+1} \equiv 1 \pmod{p^{j+1}}$ so that the resulting series does. Thus we have

$$t_{j+1}\mathcal{E}_f(z)^{p^j}\frac{\widetilde{f}}{f} \equiv \frac{\widetilde{f}}{f} \pmod{p^{j+1}}.$$

If we define $F_{j+1}(z) := t_{j+1}\mathcal{E}(z)^{p^j}\widetilde{f}(z)/f(z)$, then we have that $\{F_{j+1}\}$ is a sequence of holomorphic modular forms whose coefficients p-adically converge to $\widetilde{F}(z)/F(z)$ and whose weights p-adically converge to 2. □

We will devote the rest this section to proving Theorem 4, a generalization of Bruinier and Ono's result to forms of prime level $p \geq 5$. We require two lemmas before we start on the main body of the proof. The first is most naturally proven using the notion of the divisor polynomial of a modular form, which we now recall. If $k \geq 4$ is even, then define $\widetilde{E}_k(z)$ by

$$\widetilde{E}_k(z) := \begin{cases} 1 & \text{if } k \equiv 0 \pmod{12}, \\ E_4(z)^2E_6(z) & \text{if } k \equiv 2 \pmod{12}, \\ E_4(z) & \text{if } k \equiv 4 \pmod{12}, \\ E_6(z) & \text{if } k \equiv 6 \pmod{12}, \\ E_4(z)^2 & \text{if } k \equiv 8 \pmod{12}, \\ E_4(z)E_6(z) & \text{if } k \equiv 10 \pmod{12}, \end{cases} \tag{5.2}$$

and polynomials h_k by

$$h_k(x) := \begin{cases} 1 & \text{if } k \equiv 0 \pmod{12}, \\ x^2(x-1728) & \text{if } k \equiv 2 \pmod{12}, \\ x & \text{if } k \equiv 4 \pmod{12}, \\ x-1728 & \text{if } k \equiv 6 \pmod{12}, \\ x^2 & \text{if } k \equiv 8 \pmod{12}, \\ x(x-1728) & \text{if } k \equiv 10 \pmod{12}. \end{cases} \tag{5.3}$$

Further, define $m(k)$ by

$$m(k) := \begin{cases} \lfloor k/12 \rfloor & \text{if } k \not\equiv 2 \pmod{12}, \\ \lfloor k/12 \rfloor - 1 & \text{if } k \equiv 2 \pmod{12}. \end{cases}$$

With this notation, if $f(z) \in M_k$ and $\widetilde{F}(f,x)$ is the unique rational function in x for which

$$f(z) = \Delta(z)^{m(k)}\widetilde{E}_k(z)\widetilde{F}(f, j(z)), \tag{5.4}$$

then $\widetilde{F}(f,x)$ is a polynomial; this follows from the familiar fact that any element of $\mathcal{M}_0^\infty$ is a polynomial in j. We will refer to

$$F(f,x) := h_k(x)\widetilde{F}(f,x) \tag{5.5}$$

as the *divisor polynomial* for f. From (5.2), (5.4) and the classical $k/12$ valence formula (again, see [18, §III.2]) the polynomial $F(f,x)$ will have a zero of order n_k precisely at $j(z_k)$ for all zeros z_k of f, where $n_k := \mathrm{ord}_{z_k}(f)$. For a discussion of divisor polynomials, see [24, §2.6].

Lemma 19. *Suppose $f = q^h\prod_{n=1}^\infty(1-q^n)^{c(n)} \in \mathcal{M}_k^{mero}(\Gamma_0(p)) \cap q^h\mathcal{O}_K[[q]]$ for some number field K and some prime $p \geq 5$, and further that f is good at p. Then*

$$\left(\frac{\Theta(f) - k(12)^{-1}E_2}{f}\right)|_2W(p) \in \mathcal{M}_2^{mero}(\Gamma_0(p))$$

is p-integral.

Proof. Note that $F(\mathcal{E}_f, j)$ has p-integral algebraic coefficients as a q-series and as a polynomial because $\mathcal{E}_f$ has p-integral algebraic coefficients. Thus, if $z_1, ..., z_n$ are the zeros and poles of f as before (written without multiplicity),

$$G(j(z)) := (j(z) - j(z_1)) \cdots (j(z) - j(z_n))$$

has p-integral algebraic q-series coefficients. Because no prime above p divides the q-expansion coefficient of lowest exponent in $G(j(z))$, we also have that $(G(j))^{-1}$ is p-integral (again as a q-series). Thus we may write

$$\frac{\Theta(f) - k(12)^{-1}E_2}{f} = \frac{g}{G(j)}$$

where $g \in M_2(\Gamma_0(p)) \cap \overline{\mathbb{Q}}[[q]]$ has p-integral algebraic coefficients. We have

$$\left(\frac{\Theta(f) - k(12)^{-1}E_2}{f}\right)|_2 W(p) = \left(\frac{1}{G(j)}\right)|_0 W(p) g|_2 W(p).$$

We will prove that each of the factors on the right hand side is p-integral. First,

$$\begin{aligned}\left(\frac{1}{G(j(z))}\right)|_0 W(p) &= \left(\frac{1}{G(j(z))}\right)|_0 \begin{pmatrix} 0 & -1 \\ p & 0 \end{pmatrix} = \left(\frac{1}{G(j(z))}\right)|_0 \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix} \\ &= \left(\frac{1}{G(j(z))}\right)|_0 \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix} = \frac{1}{G(j(pz))},\end{aligned}$$

which is evidently p-integral. Now note that we can write $g = c_1(E_2(z) - pE_2(pz)) + h(z)$, where $h(z) \in S_2^{\text{new}}(\Gamma_0(p))$ has p-integral algebraic coefficients and c_1 is a p-integral algebraic number. From Proposition 18 we have $h(z)|_2 W(p) = -h(z)|U(p)$, which is p-integral by the q-series definition (1.11) of the $U(p)$ operator. Using (1.5), we also have

$$\begin{aligned}(E_2(z) - pE_2(pz))|_2 W(p) &= E_2(z)|_2 \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix} - p^2(pz)^{-2}E_2(-1/z) \\ &= \left(\frac{12}{2\pi i z} + E_2(z)\right)|_2 \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix} - \frac{12}{2\pi i z} - E_2(z) \\ &= pE_2(pz) - E_2(z).\end{aligned}$$

which is also p-integral. Since we have dealt with both factors, the lemma follows. □

Remark. If restrict to the case $k = 0$, this lemma is also true for $p = 3$; the proof is the same.

Define

$$\widetilde{E}_3(z) := E_2(z) - 3E_2(3z) \in M_2(\Gamma_0(3)) \tag{5.6}$$

(see 4.1) and

$$\widetilde{E}_p := E_{p-1}(z) - p^{(p-1)/2}(E_{p-1}(z)|_{p-1} W(p)) \in M_{p-1}(\Gamma_0(p)) \tag{5.7}$$

for primes $p \geq 5$. We have following:

Lemma 20. *If p is an odd prime, then*

$$\widetilde{E}_p(z) \equiv 1 \pmod{p} \tag{5.8}$$

$$(\widetilde{E}_p(z)|_{p-1} W(p)) \equiv 0 \pmod{p^{(p-1)/2+1}} \tag{5.9}$$

Proof. For $p = 3$, the first claim is obvious, and the second follows from the end of the proof of Lemma 19. For $p \geq 5$ we compute

$$\begin{aligned} E_{p-1}|_{p-1}W(p) &= E_{p-1}|_{p-1}\begin{pmatrix} 0 & -1 \\ p & 0 \end{pmatrix} \\ &= E_{p-1}|_{p-1}\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix} \\ &= p^{(p-1)/2}E_{p-1}|V(p) \end{aligned}$$

From Lemma 10, we know that E_{p-1} is p-integral. Thus we have the congruence $\widetilde{E}_p \equiv E_{p-1} \pmod{p}$, which yields $\widetilde{E}_p \equiv 1 \pmod{p}$ for all odd primes p after an application of Lemma 10.

For the second claim, we have

$$\begin{aligned} \widetilde{E}_p|_{p-1}W(p) &= E_{p-1}|_{p-1}W(p) - p^{(p-1)/2}E_{p-1}|_{p-1}W(p)W(p) \\ &= E_{p-1}|_{p-1}W(p) - p^{(p-1)/2}E_{p-1} \\ &= p^{(p-1)/2}E_{p-1}|V(p) - p^{(p-1)/2}E_{p-1}. \end{aligned}$$

We note the p-integrality of E_{p-1} and $E_{p-1}|V(p)$ and again apply Lemma 10 to finish the proof of the lemma. □

We now prove Theorem 4. The two main inputs into this proof are the ideas behind the proof of Theorem 3 and Serre's proof that a newform in $S_k^{\text{new}}(\Gamma_0(p))$ is a p-adic modular form (see [22] and [29]).

Proof of Theorem 4. By (1.14), there exists a meromorphic modular form g on $\Gamma_0(p)$ so that

$$\frac{\Theta f}{f} = \frac{g}{f} + \frac{k}{12}E_2.$$

Because E_2 is a p-adic modular form of weight two, it suffices to show that the same is true of $\frac{\Theta f - k(12)^{-1}E_2 f}{f} = \frac{g}{f}$.

Fix a positive integer r. Then (using the fact that f is good at p), we have

$$(\mathcal{E}_f)^{p^{r-1}}\frac{\Theta f - k(12)^{-1}E_2 f}{f} \in M_{2+p^{r-1}b}(\Gamma_0(p))$$

where b is the weight of $\mathcal{E}_f$. Further, this form is congruent modulo p^r to g/f. Now consider

$$f_r(z) := (\widetilde{E}_p)^{p^{r-1}}(\mathcal{E}_f)^{p^{r-1}}\frac{\Theta f - k(12)^{-1}E_2 f}{f} \equiv \frac{g}{f} \pmod{p^r}.$$

We clearly have $f_r \in M_{2+p^{r-1}b+p^r-p^{r-1}}(\Gamma_0(p))$. We now take the trace of these f_r to lower their level. We certainly have $\mathrm{Tr}_1^p(f_r) \in M_{2+p^{r-1}b+p^r-p^{r-1}}$, and we will prove shortly that $\mathrm{Tr}_1^p(f_r) \equiv f_r \equiv \frac{g}{f} \pmod{p^r}$. Now, as in the proof of Theorem 3, choose a suitable integer $t_r \equiv 1 \pmod{p^r}$ such that $t_r\mathrm{Tr}_1^p(f_r)$ has coefficients in the ring of integers $\mathcal{O}_{K_r}$ of some number field $\mathcal{O}_{K_r}$ (this normalization may or may not be necessary depending on $\mathcal{E}_f$). Then $\{t_r\mathrm{Tr}_1^p(f_r)\}$ forms a sequence of holomorphic modular forms over Γ whose coefficients converge p-adically to g/f and whose weights converge to 2, thus g/f is a p-adic modular form of weight 2.

We now prove that $\mathrm{Tr}_1^p(f_r) \equiv f_r \pmod{p^r}$. By Lemma 17, we have

$$\begin{aligned}\mathrm{Tr}_1^p(f_r) &= f_r + p^{1-(2+p^{r-1}b+p^r-p^{r-1})/2} f_r|_{(2+p^{r-1}b+p^r-p^{r-1})/2} W(p)U(p) \\ &= f_r + p^{1-(2+p^{r-1}b+p^r-p^{r-1})/2} \\ &\quad \times \left(\left(\frac{\Theta f - k(12)^{-1} E_2 f}{f} \right) |_2 W(p) (\widetilde{E}_p)^{p^{r-1}} |_{p^r-p^{r-1}} W(p) (\mathcal{E}_f)^{p^{r-1}} |_{p^{r-1}b} W(p) \right) U(p)\end{aligned}$$

Because f is good, applying Lemma 19 implies that $\left(\frac{\Theta(f) - k(12)^{-1}E_2}{f} \right) |_2 W(p)$ is p-integral, which, together with the definition of $U(p)$, implies that

$$\left(\frac{\Theta f - k(12)^{-1} E_2 f}{f} \right) |_2 W(p) U(p) \tag{5.10}$$

is p-integral. Using (5.9), we also compute

$$\begin{aligned}&\widetilde{E}^{p^{r-1}}|_{p^r-p^{r-1}} W(p)U(p) \\ &= (\widetilde{E}_p|_{p-1} W(p))^{p^{r-1}} | U(p) \equiv 0 \pmod{p^{(p-1)p^{r-1}/2+p^{r-1}}},\end{aligned} \tag{5.11}$$

and, just from the definitions,

$$\begin{aligned}&(\mathcal{E}_f)^{p^{r-1}}|_{p^{r-1}} W(p)U(p) \\ &= p^{p^{r-1}b/2} (\mathcal{E}_f)^{p^{r-1}}|_{p^{r-1}b} \left(\begin{smallmatrix} p & 0 \\ 0 & 1 \end{smallmatrix}\right) U(p) \equiv 0 \pmod{p^{p^{r-1}b/2}}.\end{aligned} \tag{5.12}$$

The inequalities (5.10), (5.11) and (5.12) together imply (as claimed) that $\mathrm{Tr}_1^p(f_r) \equiv f_r \pmod{p^r}$. □

Remark. As with Lemma 19, Theorem 4 is true in the case $k = 0$ for $p = 3$ as well. We will use this fact without further comment in the proof of Theorem 33.

6. CM elliptic curves and supersingularity

As indicated in the introduction, the construction of explicit families of good forms will require a discussion of complex multiplication and supersingularity, which we now begin. Recall that for an elliptic curve $E/\mathbb{C}$, there exists a lattice $L \subset \mathbb{C}$ such that

$$\begin{aligned}\mathbb{C}/L &\xrightarrow{\sim} E \\ z \notin L &\mapsto (\wp(z,L), \wp'(z,L), 1) \\ z \in L &\mapsto (0:1:0)\end{aligned} \tag{6.1}$$

is an analytic isomorphism. Here $\wp$ is the classical Weierstrass $\wp$-function. Conversely, given any lattice $L \subset \mathbb{C}$, one can show that there exists an elliptic curve E for which an analytic isomorphism of the form (6.1) holds. Under this correspondence between lattices and elliptic curves, isomorphism classes of elliptic curves over $\mathbb{C}$ correspond to equivalence classes of lattices, where the equivalence is given by $L \sim L'$ if $L = cL'$ for some $c \in \mathbb{C}^*$. By way of terminology, the map $L' \to L$ given by multiplication by $c \in \mathbb{C}^*$ is called a *homothety*, and two lattices related in such a way are called *homothetic*. Note that we may choose a lattice L_τ with basis $\{\tau, 1\}$ with $\tau \in \mathbb{H}$ in each homothety class. Different bases of L_τ are given by applying elements of Γ to the basis $\{\tau, 1\}$; it follows that we may take $\tau \in \mathfrak{F}$. With this stipulation, the basis $\{\tau, 1\}$ is uniquely determined. We will denote by E_τ the corresponding elliptic curve under the map

$$\mathbb{C}/L_\tau \to E_\tau.$$

We call this map (which is induced by (6.1)) an *analytic representation* of E_τ.

We now wish to make this analytic representation more explicit; additionally, because it will be useful later, we work in a slightly more general context. Let E/K be an elliptic curve over a field K of characteristic not equal to 2 or 3. Up to isomorphism, we can assume that E is given in affine coordinates by

$$E : y^2 = 4x^3 - g_4 x - g_6 \tag{6.2}$$

(see, for example, [17, §III.2]). If we restrict to the case $K = \mathbb{C}$, with the normalizations given above, the map (6.1) just formalizes the parametrization

$$E : (\wp'(z, L))^2 = 4(\wp(z, L))^3 - g_4\wp(z, L) - g_6.$$

that exists for some lattice $L \subset \mathbb{C}$.

We now wish define the j-invariant of E_τ, and show how it relates to $j(\tau)$. First, the *discriminant* $\Delta(E)$ of the elliptic curve E/k is defined as

$$\Delta(E) = (2\pi)^{-12}(g_4^3 - 27g_6^2). \tag{6.3}$$

Remark. It is important to observe that the discriminant function $\Delta(E)$ is *not* equal to the discriminant of the cubic polynomial defining the curve. Since the discriminant of the polynomial defining an elliptic curve E is *not* an isomorphism invariant of E, there are a variety of essentially equivalent ways to define the discriminant; the reason for our particular definition will soon be apparent.

We define the *j-invariant of E* to be the quantity

$$j(E) := \frac{1728g_4^3}{(2\pi)^{12}\Delta(E)}. \tag{6.4}$$

One can show by elementary means over any field K of characteristic not equal to 2 or 3 that $j(E)$ is indeed an invariant of the isomorphism class of E, and, further, given any $j(E) \in K$, there exists a curve of j-invariant $j(E)$ (see [17, §III.2]).

Note the similarity of (6.4) and (1.7). This is no accident. Let $\mathbb{C}/L_\tau \to E_\tau$ be an analytic representation. It turns out that, with the normalizations given above, we have $g_2 = \frac{4}{3}\pi^4 E_4(\tau)$, $g_3 = \frac{8}{27}\pi^6 E_6(\tau)$. Hence, we have

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

and

$$j(E_\tau) = j(\tau). \tag{6.5}$$

Thus the coincidence of the "j" in j-function and j-invariant is really no coincidence. Indeed, noting the fact that as the j-invariant varies over K it parameterizes isomorphism classes of elliptic curves over K (at least if we continue to assume that the characteristic of K is not 2 or 3), and recalling that the j-function is a bijection between $\mathfrak{F}$ and $\mathbb{C}$, we have a bijective map

$$\mathfrak{F} \longleftrightarrow \{\text{isomorphism classes of } E/\mathbb{C}\}.$$

For proofs of the statements we just made on the equality of the various definitions of j and Δ, see [18, §I and p. 112]. For a basic introduction to the theory of elliptic curves, see [17].

Later we will be giving examples of elliptic curves in the form $E : y^2 = x^3 + ax + b$ for some $a, b \in k$. It is easy to see that given any elliptic curve over k with defining affine equation

$y^2 = 4x^3 + cx + d$, if the characteristic of k is not 2, then this curve is isomorphic to a curve with defining affine equation $y^2 = x^3 + \widetilde{c}x + \widetilde{d}$ for some $\widetilde{c}, \widetilde{d} \in K$. We shall call an elliptic curve written in this form an elliptic curve in *Weierstrass form*. We now write formally as a proposition some elementary properties of curves written in Weierstrass form; for a proof, see [17, §III.2]

Proposition 21. *Suppose $a, b \in K$, where K is a field with characteristic not equal to 2 or 3. Then the discriminant of $x^3 + ax + b$ is $-4a^3 - 27b^2$. If the discriminant is nonzero, then $E : y^2 = x^3 + ax + b$ is nonsingular. Further, the j-invariant of $E : y^2 = x^3 + ax + b$ is $1728\frac{4a^3}{4a^3+27b^2}$.*

Now that we have (6.1) and the isomorphism invariant $j(E)$ in hand, we completely understand isomorphism classes of elliptic curves over $\mathbb{C}$ considered as analytic objects; they are explicitly parameterized by $\wp(z, L_\tau)$ (considered as a function of $\tau \in \mathfrak{F}$). For example, define $E[N]$, *the N-division points of E*, to be the points of E of order dividing N. Viewing $E/\mathbb{C}$ as $\mathbb{C}/L_\tau$, it is evident that $E[N]$ is simply the group $\frac{1}{N}L_\tau/L_\tau$, that is,

$$E[N] \approx \mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}.$$

The ring of endomorphisms of E, or $\mathrm{End}(E)$, can also be understood in a relatively straightforward manner using analytic representations. To begin, we have the following:

Lemma 22. *Let L, M be two lattices in $\mathbb{C}$, and let*

$$\lambda : \mathbb{C}/L \to \mathbb{C}/M$$

be a complex analytic homomorphism. Then there exists a complex number α so that the following diagram commutes:

$$\begin{array}{rccc} \alpha: & \mathbb{C} & \to & \mathbb{C} \\ & \downarrow & & \downarrow \\ \lambda: & \mathbb{C}/L & \to & \mathbb{C}/M. \end{array}$$

Here the top map is multiplication by α and the bottom is the homomorphism λ.

Proof (compare [21]*).* In a neighborhood of zero, λ can be expressed by a power series

$$\lambda(z) = a_0 + a_1 z + a_2 z^2 + \cdots,$$

On the other hand, λ is a homomorphism, so $a_0 = 0$ and additionally we have

$$\lambda(z + z') \equiv \lambda(z) + \lambda(z') \pmod{M}.$$

If we choose a small enough neighborhood U of zero, we must have that this congruence is an equality in U; thus

$$\lambda(z) = a_1 z$$

for $z \in U$. But for any $z \in \mathbb{C}$, z/n is in U for sufficiently large integers n, and from this we conclude that, identifying z with its reduction modulo L,

$$\lambda(z) = \lambda\left(n\left(\frac{z}{n}\right)\right) = n\lambda\left(\frac{z}{n}\right) = na_1\left(\frac{z}{n}\right) = a_1 z.$$

□

Remark. Abusing notation, we will often denote the complex number α and the homomorphism λ by the same symbol λ. We will also only be considering the special case $L = M$ of Lemma 22.

It is clear that any $\lambda \in \mathbb{Z}$ will induce an endomorphism of $\mathbb{C}/L_\tau$, which we can then identify with an element of $\mathrm{End}(E_\tau)$. We will call these endomorphisms the *trivial endomorphisms of* E_τ. We have the following:

Definition. *If $E/\mathbb{C}$ is an elliptic curve with nontrivial elements in its endomorphism ring $\mathrm{End}(E/\mathbb{C})$, then we say E* ***is a curve with complex multiplication****, or, briefly, E* ***has CM****.*

The complex numbers λ inducing a nontrivial endomorphism of a lattice L turn out to be algebraic numbers; more specifically, they are quadratic over $\mathbb{Q}$. Before we formalize and prove this as a proposition, we offer another definition, which will also be useful in §7:

Definition. *Suppose $\tau \in \mathbb{H}$ is the root of a quadratic equation with integer coefficients; that is, $\tau = \frac{-b+\sqrt{b^2-4ac}}{2a}$ with $a, b, c \in \mathbb{Z}$ and $\gcd(a, b, c) = 1$. We say that τ is a* ***Heegner point*** *and that $d_\tau = b^2 - 4ac$ is the* ***discriminant*** *of τ.*

Proposition 23. *Suppose $E/\mathbb{C}$ is an elliptic curve. Then*

1. *Every nontrivial endomorphism of $E/\mathbb{C}$ is induced (in the sense of Theorem 22) either by a Heegner point $\lambda \in \mathbb{H}$ or by $-\lambda$ for a Heegner point $\lambda \in \mathbb{H}$.*
2. *The curve $E/\mathbb{C}$ has CM if and only if $j(E) = j(\tau)$ for some Heegner point $\tau \in \mathfrak{F}$.*
3. *The curve $E/\mathbb{C}$ has CM if and only if $\mathrm{End}(E) \cong \mathcal{O}$, where $\mathcal{O}$ is an order in an imaginary quadratic number field K.*

Proof. The endomorphism ring of E is unchanged if we replace it with another elliptic curve isomorphic to it, so we assume without loss of generality that $E = E_\tau$, $\tau \in \mathfrak{F}$. Thus we have an analytic representation

$$\mathbb{C}/L_\tau \to E_\tau.$$

As we proved in Lemma 22, a nontrivial automorphism of E_τ can now be realized as a $\lambda \in \mathbb{C}^* - \mathbb{Z}$ such that

$$\lambda L_\tau \subset L_\tau$$

or, equivalently, for some $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{Q}) \cap M_{2\times 2}(\mathbb{Z})$,

$$\begin{aligned} \lambda\tau &= a\tau + b \\ \lambda &= c\tau + d. \end{aligned}$$

This implies that λ is a root of the quadratic equation

$$\begin{vmatrix} x-a & -b \\ -c & x-d \end{vmatrix} = 0.$$

Thus λ is a quadratic irrational algebraic integer. Now note that τ cannot be real; otherwise L_τ would not be a lattice, and $c \neq 0$, for then λ would be an integer. Thus $\mathbb{Q}(\tau) = \mathbb{Q}(\lambda)$, and, further, both λ and τ are imaginary quadratic numbers. This proves (1).

We've also proven the "only if" implication of (2), just by recalling that j is an isomorphism invariant. The other direction follows similarly: note that if $j(E) = j(\tau)$ with τ a Heegner point, then $E_\tau \approx E$, and E_τ is evidently CM.

Finally, for (3), note that if E is CM, as proven above, there is an isomorphic curve E_τ where τ is a Heegner point. Thus $\mathrm{End}(E) \approx \mathrm{End}(L_\tau)$, and, again as proven above, any complex number inducing a nontrivial endomorphism of L_τ is an element of $\mathcal{O}_{\mathbb{Q}(\tau)}$, the ring of integers of $\mathbb{Q}(\tau)$, but not an element of $\mathbb{Z}$. With this observation in mind it is easy to see that the evident map $\mathrm{End}(L_\tau) \to \mathcal{O}_{\mathbb{Q}(\tau)}$ is a homomorphism of rings with identity, and, further,

the image of this homomorphism is not contained in $\mathbb{Z} \subset \mathcal{O}_{\mathbb{Q}(\tau)}$. Thus $\mathrm{End}(L_\tau) \approx \mathrm{End}(E_\tau)$ is isomorphic to an order in $\mathcal{O}_{\mathbb{Q}(\tau)}$. Conversely, note that if $\mathrm{End}(E) \approx \mathcal{O}$, with $\mathcal{O}$ an order in a quadratic imaginary field, then $\mathrm{End}(E)$ is not isomorphic to $\mathbb{Z}$, so E must be CM. $\square$

By way of terminology, if $\tau \in \mathbb{H}$ is a Heegner point, then $j(\tau) \in \mathbb{C}$ is called a *singular modulus*. In view of parts (3) and (4) of the last proposition, one might guess that these singular moduli would be of interest in the study of the arithmetic of imaginary quadratic number fields. This is indeed the case, but before we can explain anything in any more detail we must briefly explore the connection between the CM elliptic curves and quadratic imaginary fields. The content of our discussion is derived mostly from [31, §II].

We've seen in Proposition 23 that every CM elliptic curve has endomorphism ring isomorphic to an order in a quadratic number field. We now work in an opposite direction. Fix an imaginary quadratic number field K, and let $\mathcal{O}_K$ be its ring of integers. We wish to study the following sets:

$$\begin{aligned} \mathcal{ELL}(\mathcal{O}_K) : &= \frac{\{\text{elliptic curves } E/\mathbb{C} \text{ with } \mathrm{End}(E) \cong \mathcal{O}_K\}}{\text{isomorphism over } \mathbb{C}} \\ &\cong \frac{\{\text{lattices } L \text{ with } \mathrm{End}(L) \cong \mathcal{O}_K\}}{\text{homothety}}. \end{aligned} \tag{6.6}$$

We now show that these sets are nonempty for any imaginary quadratic number field K. Fix an embedding $K \hookrightarrow \mathbb{C}$. Given any nonzero fractional ideal $\mathfrak{a} \subset K$, we know from elementary algebraic number theory that the image of $\mathfrak{a}$ under our chosen embedding (which we will also denote by $\mathfrak{a}$) is a lattice in $\mathbb{C}$. Denote by $E_\mathfrak{a}$ the elliptic curve associated to this lattice. We have

$$\begin{aligned} \mathrm{End}(E_\mathfrak{a}) &\cong \{\alpha \in \mathbb{C} : \alpha\mathfrak{a} \subset \mathfrak{a}\} \\ &= \{\alpha \in K : \alpha\mathfrak{a} \subset \mathfrak{a}\} \text{ since } \mathfrak{a} \subset K, \\ &= \mathcal{O}_K \text{ since } \mathfrak{a} \text{ is a fractional ideal.} \end{aligned}$$

Thus given $\mathcal{O}_K$, we can find an elliptic curve E with $\mathrm{End}(E) \approx \mathcal{O}_K$. Further, since homothetic lattices give rise to isomorphic elliptic curves, if $c \in K$, then $E_{(c)\mathfrak{a}} \approx E_\mathfrak{a}$. In other words, multiplying a fractional ideal by a principal ideal in $\mathcal{O}_K$ does not change the elliptic curve that arises from that ideal. In particular, if we denote by $\mathcal{CL}(K)$ the ideal class group of K, that is,

$$\mathcal{CL}(K) := \frac{\{\text{nonzero fractional ideals of } K\}}{\{\text{nonzero principal ideals of } K\}}.$$

then we have a map

$$\begin{aligned} \mathcal{CL}(K) &\longrightarrow \mathcal{ELL}(\mathcal{O}_K) \\ \overline{\mathfrak{a}} &\longmapsto E_\mathfrak{a} \end{aligned}$$

where $\overline{\mathfrak{a}}$ is the ideal class of $\mathfrak{a} \in \mathcal{CL}(k)$. More generally, if L is any lattice and $\mathfrak{a}$ any nonzero fractional ideal of K, then define the product

$$\mathfrak{a}L := \{\alpha_1\lambda_1 + \cdots + \alpha_r\lambda_r : \alpha_i \in \mathfrak{a}, \lambda_i \in L\}.$$

Now fix a lattice L with $E_L \in \mathcal{ELL}(\mathcal{O}_K)$ its associated elliptic curve. One can show in an elementary manner that the map

$$\begin{aligned} \mathcal{CL}(k) &\longrightarrow \mathcal{ELL}(\mathcal{O}_K) \\ \overline{\mathfrak{a}} &\longmapsto E_{\mathfrak{a}^{-1}L} \end{aligned} \tag{6.7}$$

defines a simply transitive action of $\mathcal{CL}(K)$ on $\mathcal{ELL}(\mathcal{O}_K)$ (see Proposition 1.2, [31, §II.2]). In particular, because $\mathcal{CL}(K)$ is finite, $\mathcal{ELL}(\mathcal{O}_K)$ is as well. This observation is the main input into Proposition 24 below. Fix the notation

$$h_K = |\mathcal{CL}(K)|.$$

For $\sigma \in \mathrm{Aut}(\mathbb{C})$, let c^σ denote $\sigma(c)$ for all $c \in \mathbb{C}$, and let E^σ denote the elliptic curve formed by letting σ act on the coefficients of the defining affine equation of E. Further, if $\phi : E \to E$ is an endomorphism of E, then denote by $\phi^\sigma : E^\sigma \to E^\sigma$ the induced endomorphism (i.e. isogeny from E^σ to itself) of E^σ.

Remark. We are implicitly identifying the ring of analytic endomorphisms of E, thought of as a lattice, with the ring of algebraic endomorphisms of E, thought of as group. It is a fact that these two rings are indeed isomorphic; see [30, §VI.4, Theorem 4.1].

Then we have the following:

Proposition 24. *Let $E/\mathbb{C}$ be an representative of a class of elliptic curves in $\mathcal{ELL}(\mathcal{O}_K)$ for $\mathcal{O}_K$ the ring of integers of an imaginary quadratic field K. We have*

1. *$j(E) \in \overline{\mathbb{Q}}$.*
2. *Let $E_1, ..., E_{h_K}$ be a complete set of representatives for $\mathcal{ELL}(\mathcal{O}_K)$. Then $j(E_1), ..., j(E_{h_K})$ are the $Gal(\overline{K}/K)$ conjugates for $j(E)$.*

Proof. Let $\sigma : \mathbb{C} \to \mathbb{C}$ be a field automorphism of $\mathbb{C}$. First note that $\mathrm{End}(E^\sigma) \simeq \mathrm{End}(E)$, simply because if $\phi : E \to E$ is any endomorphism of E, then $\phi^\sigma : E^\sigma \to E^\sigma$ is an endomorphism of E^σ. Thus $\mathrm{End}(E^\sigma) \approx \mathrm{End}(E)$. In particular, as σ varies, E^σ varies over only finitely many $\mathbb{C}$-automorphism classes of elliptic curves with endomorphism ring isomorphic to $\mathcal{O}_K$ because the action (6.7) is simply transitive and the class group is finite.

Now E^σ is obtained from E by letting σ act on the coefficients of the affine equation defining E. The invariant $j(E)$ is just a rational combination of those coefficients, so we have

$$j(E^\sigma) = j(E)^\sigma.$$

Since the isomorphism class of an elliptic curve is determined by its j-invariant, and, as we've noted above, there are only finitely many $\mathbb{C}$-isomorphism classes in $\{E^\sigma\}_{\sigma \in \mathrm{Aut}(\mathbb{C})}$, it follows that $j(E)^\sigma$ takes on only finitely many values as σ ranges over $\mathrm{Aut}(\mathbb{C})$. Therefore $[\mathbb{Q}(j(E)) : \mathbb{Q}]$ is finite, so $j(E)$ is an algebraic number. This completes the proof of (1).

To prove (2), first note that the action of $\mathcal{CL}(K)$ on $\mathcal{ELL}(\mathcal{O}_K)$ induces a simply transitive action $\Psi : \mathcal{CL}(K) \to \{j(E_1), ..., j(E_{h_K})\}$ if we identify an isomorphism class of elliptic curves with its j-invariant. One then defines a surjective homomorphism $\Phi : \mathrm{Gal}(\overline{K}/K) \to \mathcal{CL}(K)$ such that the canonical action of $\mathrm{Gal}(\overline{K}/K)$ on the set $\{j(E_1), ..., j(E_{h_K})\}$ is just $\Psi \circ \Phi$. See [31, §II.2] for the construction of this homomorphism; the proof of Theorem 4.3, [31, §II.4] shows that it has the desired property. The fact that (6.7) is simply transitive then immediately yields the desired result. □

Actually, the $j(E)$ for E as in the previous proposition are integral, which can be proven by constructing certain polynomials related to n-isogenies of elliptic curves. This proof requires no more machinery than that which we have already developed (and in fact many of the ideas behind it will be used in the proof of Theorem 33), but it is rather long, and the reader would do just as well to read it in [31, §II.6]. We state this fact as a theorem:

Theorem 25. *Let $E/\mathbb{C}$ be an elliptic curve with complex multiplication. Then $j(E)$ is an algebraic integer.*

We now wish to restate Proposition 24 using the language of Heegner points. Recall that an integer $d \neq 1$ is a *fundamental discriminant* if it is not divisible by the square of any odd prime and satisfies either $d \equiv 1 \pmod 4$ or $d \equiv 8, 12 \pmod{16}$. We prove the following lemma:

Lemma 26. *Let $d < 0$ be a fundamental discriminant, and $K = \mathbb{Q}(\sqrt{d})$. Then there are precisely h_K Heegner points of discriminant d in $\mathfrak{F}$.*

Proof. Notice that if $\tau = \frac{-b+\sqrt{b^2-4ac}}{2a} \in \mathfrak{F}$ with $a, b, c \in \mathbb{Z}$, $\gcd(a, b, c) = 1$, and $b^2 - 4ac = d$, then $ax^2 + bxy + cy^2$ is a primitive positive definite quadratic form of discriminant d. Since d is fundamental, the number of such forms is precisely $|\mathcal{CL}(K)| = h_K$. □

We now have the following corollary of Proposition 24:

Corollary 27. *Let $d < 0$ be a fundamental discriminant and $\tau_1, ..., \tau_{h_K}$ be the Heegner points of discriminant d in $\mathfrak{F}$. Then $j(\tau_i) \in \overline{\mathbb{Z}}$ for all i, and $j(\tau_1), ..., j(\tau_{h_K})$ is a complete set of Galois conjugates under the action of Gal$(\overline{K}/K)$.*

Proof. First note that the map

$$\begin{array}{ccc} \mathfrak{F} & \longleftrightarrow & \dfrac{\{\text{lattices } L \subset \mathbb{C}\}}{\text{homothety}} \\ z & \longmapsto & [L_z] \end{array} \tag{6.8}$$

is a bijection. Suppose $\tau \in \mathfrak{F}$ is a Heegner point of discriminant d. Using (6.5), we have that $j(E_\tau) = j(\tau)$, which implies by part (2) of Proposition 23 that E_τ has endomorphism ring isomorphic to an order in an imaginary quadratic number field. This implies that the same is true of L_τ. By the proof of Proposition 23, we may take this imaginary quadratic number field to be K. In fact, $\mathrm{End}(L_\tau) \cong \mathcal{O}_K$, the full ring of integers. To see this, we observe that $\mathcal{O}_K = \mathbb{Z}[\frac{1+\sqrt{d}}{2}]$ if d is odd (resp., $\mathcal{O}_K = \mathbb{Z}[\frac{\sqrt{d}}{2}]$ if d is even), hence one need only check that $\frac{1+\sqrt{d}}{2} \cdot \tau \in L_\tau$ (resp., $\frac{\sqrt{d}}{2} \cdot \tau \in L_\tau$). We omit this calculation.

With this claim in hand, (6.8) yields an injection

$$\begin{array}{ccc} \{\text{Heegner points in } \mathfrak{F} \text{ of discriminant } d\} & \hookrightarrow & \dfrac{\{\text{lattices } L \subset \mathbb{C} \text{ with } \mathrm{End}(L) \cong \mathcal{O}_K\}}{\text{homothety}} \\ \tau & \longmapsto & [L_\tau]. \end{array} \tag{6.9}$$

The set on the left hand side of (6.9) has cardinality h_K by Lemma 26 as does the set on the right hand side by (6.6) and the fact that the action (6.7) is simply transitive. Thus (6.9) is a bijection.

We now identify the set on the right of (6.9) with (6.6). Applying Proposition 24 then yields the corollary. □

We close our discussion of the connection between the j-invariants of CM elliptic curves over $\mathbb{C}$ by noting that the propositions and lemmas we have proven above are really the elementary preliminaries to a discussion of the class field theory of imaginary quadratic fields. This is one of two cases in which the class field theory of an extension of $\mathbb{Q}$ has been explicitly worked out (the other is the class field theory of $\mathbb{Q}$ itself). It would take us too far afield to prove the following theorem, but it seems important to state for the reader the main result in the class field theory of imaginary quadratic extensions of $\mathbb{Q}$, namely a characterization of the Hilbert class field of such an extension. The connection with the CM theory of elliptic curves will be evident.

Theorem 28. *Let E be an elliptic curve representing an isomorphism class in $\mathcal{ELL}(\mathcal{O}_K)$. Then $K(j(E))$ is the maximal unramified abelian extension of K, that is, $K(j(E))$ is the Hilbert class field of K.*

For a proof of this result, see either [31, §II.4] or [20, §10.1].

It should come as no surprise that in order to apply our discussion of CM to the construction of p-adic modular forms, we will have to understand at some level what happens when we move from elliptic curves defined over $\overline{\mathbb{Q}}$ to those defined over a field of prime characteristic greater than or equal to 5. We begin with the notion of good reduction:

Definition. *Let K be a number field, and let $\mathfrak{P} \subset \mathcal{O}_K$ be a prime ideal. An elliptic curve $E/\overline{\mathbb{Q}} : y^2 = x^3 + ax + b$ with $\mathfrak{P}$-integral coefficients a, b is said to have **good reduction at $\mathfrak{P}$** if the reduced elliptic curve $\widetilde{E} : y^2 = x^3 + \widetilde{a}x + \widetilde{b}$ is nonsingular. Here $\widetilde{a}$ denotes the reduction of a in $\mathcal{O}_K/\mathfrak{P}$.*

Remark (1). For ease of exposition, we have restricted our definition of good reduction so as only to include elliptic curves written in Weierstrass form. With this definition, whether or not an elliptic curve E has good reduction at a particular prime is not an invariant of the isomorphism class of the curve. For a more general (and natural) discussion of good reduction, see [30, §VII.5].

Remark (2). Suppose $\mathfrak{P}$ is a prime ideal above a prime integer $p \notin \{2, 3\}$. From Proposition 21, we have an easy way to determine whether or not the elliptic curve $E/\overline{\mathbb{Q}} : y^2 = x^3+ax+b$ has good reduction at $\mathfrak{P}$; this is the case if and only if $\mathrm{ord}_{\mathfrak{P}}(-4a^3 - 27b^2) = 0$.

We discussed two algebraic objects attached to an elliptic curve defined in characteristic zero, namely, its group of N-division points and its endomorphism ring. The corresponding objects for elliptic curves defined over fields of positive characteristic are a good deal more subtle; a proper treatment of them would be a thesis in itself. In the remainder of this section we indicate some of what is true about them as motivation for the concept of supersingularity.

First, suppose E is the reduction of an elliptic curve or an elliptic curve defined over a field K of prime characteristic $p \geq 5$. It is natural to ask for a description of the groups $E[N]$. For N coprime to p, we have the same answer as before, namely

$$E[N] \approx \mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$$

(see, for example, Corollary 6.4 of [30, §III.6]). The behavior is quite different at p; we have

$$E[p^e] \approx \{0\} \text{ for all } e \in \mathbb{N}$$

or

$$E[p^e] \approx \mathbb{Z}/p^e\mathbb{Z} \text{ for all } e \in \mathbb{N}.$$

Again, see [30, §III.6]. In the first case, we say that E is *supersingular*.

The endomorphism rings, which we completely described for elliptic curves over $\mathbb{C}$ using analytic parameterizations, also behave in a much less straightforward manner upon reduction of the curve. In particular, let K be a number field, and let $E/\overline{\mathbb{Q}}$ have good reduction at $\mathfrak{P} \subset \mathcal{O}_K$. Then one can show that the natural reduction map

$$\mathrm{End}(E) \to \mathrm{End}(\widetilde{E})$$

is injective (see [30, §VII.3] and Proposition 4.4, [31, §II.4]). If E has CM, and this map is *not* surjective, then it turns out that $\mathrm{End}(\widetilde{E})$, instead of being an order in a quadratic imaginary field, is an order in a quaternion algebra (see Corollary 9.4, [30, §III.9]). Whether or not E has CM, the condition that $\mathrm{End}(\widetilde{E})$ is an order in a quaternion algebra is in fact equivalent to supersingularity of the curve as defined above; sometimes it is said that a supersingular elliptic curve has "extra" endomorphisms. We write the two definitions of supersingularity we have encountered as a displayed definition so they are not lost in the text:

Definition. *Let K be a number field, $\mathfrak{P} \subset \mathcal{O}_K$ an prime ideal above $p \geq 3$. An elliptic curve $E/\overline{\mathbb{Q}}$ with good reduction at $\mathfrak{P}$ is said to be* ***supersingular at*** $\mathfrak{P}$ *if one of the following equivalent conditions holds:*

1. $E[p^e] = 0$ *for all* $e > 0$.
2. $\mathrm{End}(E)$ *is an order in a quaternion algebra.*

Remark. In fact, if $E[p^k] = 0$ for some $k > 0$, then $E[p^e] = 0$ for all $e > 0$.

For a discussion of the equivalence of these two definitions, see [30, §V.3]. Essentially everything proven therein is derived from the classical results of Deuring in [11].

Recalling that $j(E)$ is an isomorphism invariant of E, and given the central role that the study of j-invariants plays in CM theory, it should come as no surprise that it enters the discussion here as well. We note first that if $E/\overline{\mathbb{Q}}$ has good reduction at a prime ideal $\mathfrak{P} \subset \mathcal{O}_K$ above $p \geq 5$, then $j(E)$ is p-integral. This follows trivially for any curve written in Weierstrass form by Proposition 21 (and we are restricting our discussion of good reduction to curves in Weierstrass form). Thus we can make the following:

Definition. *Let K be a number field, and suppose $E/\overline{\mathbb{Q}}$ is supersingular at a prime ideal $\mathfrak{P} \subset \mathcal{O}_K$ above a prime $p \geq 5$. Then the reduction of $j(E)$ in $\overline{\mathbb{F}}_p$ is said to be a* ***supersingular j-invariant*** *over $\overline{\mathbb{F}}_p$.*

Using the dictionary between Heegner points and CM elliptic curves we have developed, we can state the following theorem, which yields a particularly nice method of deciding whether or not a CM curve is supersingular at a particular prime:

Theorem 29. *Let τ be a Heegner point of discriminant d_τ, and E_τ be an elliptic curve with j-invariant $j(\tau)$. Fix a prime $p \geq 5$, and suppose that p is inert or ramified in $Q(\sqrt{d_\tau})$. If E_τ has good reduction at $\mathfrak{p}$ for all primes $\mathfrak{p}$ above p in $\mathbb{Q}(j(\tau))$, then $j(\tau)$ reduces to a supersingular j-invariant in $\overline{\mathbb{F}}_p$.*

See [20, §13.4, p. 182] for a proof of this result.

We are now almost ready to state the theorem which will be the main tool used in the construction of a family of good forms. We fix the notation

$$\Omega_p := \left\{ j_E : j_E \text{ is a supersingular } j\text{-invariant over } \overline{\mathbb{F}}_p \right\} \tag{6.10}$$

and

$$g_p := |\Omega_p|. \tag{6.11}$$

Further, define the supersingular locus $\mathfrak{S}_p(x)$ as

$$\mathfrak{S}_p(x) = \prod_{j_E \in \Omega_p} (x - j_E) \in \mathbb{F}_p[x]. \tag{6.12}$$

We have swept under the rug the assertion that $|\Omega_p|$ is finite and $\mathfrak{S}_p(x) \in \mathbb{F}_p[x]$. For proofs of these assertions, see either [16] or [30, §V.4]. We have the following result of Deligne:

Theorem 30 (Deligne)**.** *If $p \geq 5$ is prime, then*

$$\mathfrak{S}_p(x) \equiv F(E_{p-1}, x) \pmod{p}.$$

Note that the "F" in Theorem 30 is a divisor polynomial (see §5). An elementary proof of Theorem 30 using only basic properties of Hasse invariants and complex analysis can be found in [16].

In this section we have asked the reader to accept many results without proof. An explicit example could be enlightening:

Example. Consider the elliptic curve $E : y^2 = x^3 + x$. Using Proposition 21, we calculate that the discriminant of this curve is -4 and conclude that it has good reduction at any prime $p \geq 3$. We then use Proposition 21 to calculate that the j-invariant is 1728. It is a standard fact from the theory of modular functions that j maps the arc from $e^{2\pi i/3} = -\frac{1}{2} + \frac{\sqrt{-3}}{2}$ to i along the unit disc $\{z : |z| = 1\}$ bijectively onto the interval $[0, 1728]$; in particular, $j(i) = 1728$. It follows that from Proposition 23 that E has CM with endomorphism ring an order in $K = \mathbb{Q}(i)$.

It is a fact from elementary number theory that a prime $p \geq 5$ splits in K if and only if $p \equiv 1 \pmod 4$. Therefore, by Theorem 29, we should expect that $E : y^2 = x^3 + x$ is supersingular when considered as a curve in $\mathbb{F}_p$ for primes $p \geq 5$ with $p \equiv 3 \pmod 4$. We prove this in an elementary manner by demonstrating that $|E/\mathbb{F}_p| = p + 1$. This implies $E/\mathbb{F}_p$ has no p-torsion, which is one of our definitions of supersingularity.

Let $\left(\frac{\cdot}{\cdot}\right)$ denote the typical Legendre symbol. We have

$$\left(\frac{x^3 + x}{p}\right) = \left(\frac{x}{p}\right)\left(\frac{x^2 + 1}{p}\right).$$

Because $p \equiv 3 \pmod 4$, $\left(\frac{-1}{p}\right) = -1$, so

$$\left(\frac{(-x)^3 + (-x)}{p}\right) = \left(\frac{-x}{p}\right)\left(\frac{(-x)^2 + 1}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{x}{p}\right)\left(\frac{x^2 + 1}{p}\right) = -\left(\frac{x}{p}\right)\left(\frac{x^2 + 1}{p}\right).$$

By pairing x and $-x$ for $x \in \mathbb{F}_p^*$, we can conclude that exactly half the $p - 1$ elements $x \in \mathbb{F}_p^*$ have the property that $x^3 + x$ is a quadratic residue. Each such x yields two solutions to the equation $y^2 = x^3 + x$ over $\mathbb{F}_p^*$, corresponding to $\pm y$. Adding in the point $(x, y) = (0, 0)$ and the point at infinity, we have $|E/\mathbb{F}_p| = p + 1$.

7. Good forms

As promised, in this section we now provide several families of good forms. Before we begin, however, we recall the following congruences involving singular moduli:

Proposition 31 (Gross and Zagier)**.** *Let $p < 12$ be a prime and τ be a Heegner point of discriminant $d < -4$. If $\left(\frac{d}{p}\right) = -1$ we have*

$$\begin{aligned} j(\tau) &\equiv 0 \pmod{2^{15}} && \text{if } p = 2 \\ j(\tau) &\equiv 12^3 \pmod{3^6} && \text{if } p = 3 \\ j(\tau) &\equiv 0 \pmod{5^3} && \text{if } p = 5 \\ j(\tau) &\equiv 12^3 \pmod{7^2} && \text{if } p = 7. \end{aligned}$$

Proof. If $p \neq 2$, then this proposition follows from elementary manipulations of elliptic curves and Theorem 29. The case $p = 2$ is more complicated. For a proof, see [14, Corollary 2.5]. □

We can now state and prove the following:

Theorem 32. *Let K be a number field and $\mathcal{O}_K$ be its ring of integers. Suppose that $f(z) = q^h \prod_{n=1}^{\infty}(1-q^n)^{c(n)} \in \mathcal{M}_k^{mero}(\Gamma_0(p)) \cap q^h\mathcal{O}_K[[q]]$ has poles and zeros at the Heegner points $\tau_1, ..., \tau_s \in \mathfrak{F}$, all of fixed discriminant $d < -4$. Then the following are true:*

(1) *If $p \geq 5$ is a prime for which $\left(\frac{d}{p}\right) \in \{0, -1\}$ and*

$$\prod_{i=1}^{s} j(\tau_i)(j(\tau_i) - 1728) \not\equiv 0 \pmod{p}$$

then f is good at p.

(2) *If $p \in \{2, 3, 5, 7\}$ and $\left(\frac{d}{p}\right) = -1$ then f is good at p.*

Remark (1). The work of Gross and Zagier on differences of singular moduli [14] provides a simple description of those primes p which do not satisfy the congruence condition given in part (1) of Theorem 32.

Remark (2). In [8], Bruinier and Ono provide several additional families of good modular forms. The proof that these forms are good requires the classical work of Deuring on singular moduli (see [11]) as well as further results from [14], but the method of proof is essentially the same.

Remark (3). The proof of (2) was given by Ono and Papanikolas in [25].

Proof. By the definition of good, we must produce a holomorphic modular form $\mathcal{E}_f$ on Γ with algebraic p-integral coefficients for which $\mathcal{E}_f(\tau_i) = 0$ for $1 \leq i \leq s$ that additionally satisfies the congruence

$$\mathcal{E}_f(z) \equiv 1 \pmod{p}.$$

We first prove (1). For each $1 \leq i \leq s$ let A_i be the curve

$$A_i : y^2 = x^3 - 108j(\tau_i)(j(\tau_i) - 1728)x - 432j(\tau_i)(j(\tau_i) - 1728)^2. \tag{7.1}$$

This curve is defined over the number field $\mathbb{Q}(j(\tau_i))$. Let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_{\mathbb{Q}(j(\tau_i))}$ lying above a prime $p \geq 5$. By assumption,

$$j(\tau_i)(j(\tau_i) - 1728) \not\equiv 0 \pmod{\mathfrak{p}}.$$

We check that the discriminant of the cubic defining A_i is nonzero modulo $\mathfrak{p}$. Applying Proposition 21 and the definition of good reduction, this will simultaneously show us that A_i is an elliptic curve (i.e. it is nonsingular) and that it has good reduction at $\mathfrak{p}$. The discriminant of the cubic defining A_i is

$$\begin{aligned} &-4(-108j(\tau_i)(j(\tau_i)-1728))^3 - 27(-432j(\tau_i)(j(\tau_i)-1728)^2)^2 \\ &= \quad 2^{14}3^{12}j(\tau_i)^2(j(\tau_i)-1728)^3 \end{aligned} \tag{7.2}$$

By assumption, $j(\tau_i)(j(\tau_i) - 1728) \not\equiv 0 \pmod{p}$, so (7.2) is nonzero modulo $\mathfrak{p}$; in other words, A_i is an elliptic curve that has good reduction at $\mathfrak{p}$.

Using Proposition 21 and (7.2) (the discriminant of the cubic defining A_i), we compute that

$$j(A_i) = 1728\frac{4(-108j(\tau_i)(j(\tau_i)-1728))^3}{-2^{14}3^{12}j(\tau_i)^2(j(\tau_i)-1728)^3} = j(\tau_i).$$

Thus we have a CM curve A_i with good reduction at $\mathfrak{p}$ for all primes $\mathfrak{p} \subset \mathcal{O}_{\mathbb{Q}(j(\tau_i))}$ above an integer prime $p \geq 5$. The condition $\left(\frac{d}{p}\right) \in \{0, -1\}$ implies that p does not split in $\mathbb{Q}(\sqrt{d})$, ergo, applying Theorem 29, we have that $j(\tau_i)$ reduces to a supersingular j-invariant in $\overline{\mathbb{F}}_p$.

Since $j(\tau_i)$ is supersingular, Theorem 30 implies that there exists some $Q_i \in \mathfrak{F}$ such that $E_{p-1}(Q_i) = 0$ and $j(Q_i) \equiv j(\tau_i) \pmod{p}$, which implies

$$(j(z) - j(Q_i)) \equiv (j(z) - j(\tau_i)) \pmod{p}.$$

Recalling from Lemma 10 that $E_{p-1}(z) \equiv 1 \pmod{p}$, we may take

$$\mathcal{E}_f(z) := \prod_{i=1}^{s} \left(E_{p-1}(z)\frac{j(z) - j(\tau_i)}{j(z) - j(Q_i)} \right).$$

For (2), we claim that we may take

$$\mathcal{E}_f(z) = \prod_{i=1}^{s} \Delta(z)(j(z) - j(\tau_i)) \in M_{12s}(\Gamma)$$

Because $j(\tau_i)$ is an algebraic integer, the weight $12s$ holomorphic modular form $\mathcal{E}_f$ has coefficients in the ring of integers of some fixed number field K. It is evident that $\mathcal{E}_f(\tau_i) = 0$ for all $1 \leq i \leq s$. In view of the fact that

$$\Delta(z) = \frac{E_4(z)^3}{j(z)} = \frac{E_6(z)^2}{j(z) - 1728}$$

the congruences in Lemma 11 and Proposition 31 yield the desired result. □

With the machinery we have now developed, it is straightforward to prove Corollary 5:

Proof of Corollary 5. Let $\tau_1(:= \tau), \tau_2, ..., \tau_{h_{\mathbb{Q}(\sqrt{d})}} \in \mathfrak{F}$ be the Heegner points of discriminant d (see Lemma 26). Define

$$f_d(z) := \prod_{s=1}^{h_{\mathbb{Q}(\sqrt{d})}} (j(z) - j(\tau_s)).$$

Our assumptions on d guarantee, via part (2) of Theorem 32, that f_d is good at p for all relevant pairs of p and d. Therefore,

$$\frac{\Theta f_d(z)}{f_d(z)}$$

is a weight two p-adic modular form by Theorem 3. On the other hand, applying Theorem 2, we have

$$\frac{\Theta f_d(z)}{f_d(z)} = -\frac{E_4(z)^2 E_6(z)}{\Delta(z)} \sum_{\tau \in \mathfrak{F}} \frac{e_\tau \operatorname{ord}_\tau(f_d)}{j(z) - j(\tau)}$$

which, by Corollary 7, yields

$$\frac{\Theta f_d(z)}{f_d(z)} = -\sum_{s=1}^{h_{\mathbb{Q}(\sqrt{d})}} \left(\sum_{n=0}^{\infty} j_n(\tau_s) q^n \right) = -h_{\mathbb{Q}(\sqrt{d})} - \sum_{n=1}^{\infty} \left(\sum_{s=1}^{h_{\mathbb{Q}(\sqrt{d})}} j_n(\tau_s) \right) q^n.$$

Recall that from (2.7) that $j_1(z) := j(z) - 744$, and $j_m(z) := m j_1(z) | T_{0,m}$. From (1.8) (the definition of $T_{0,m}$) we have the first of the two following equalities:

$$\begin{aligned} \sum_{s=1}^{h_{\mathbb{Q}(\sqrt{d})}} j_{p^m}(\tau_s) &= \sum_{s=1}^{h_{\mathbb{Q}(\sqrt{d})}} \left(\sum_{a=0}^{m} \sum_{b=0}^{p^a-1} \left(j\left(\frac{p^{m-a}\tau_s + b}{p^a} \right) - 744 \right) \right) \\ &= -\frac{744 h_{\mathbb{Q}(\sqrt{d})}(1 - p^{m+1})}{1-p} + \operatorname{Tr}_{K/\mathbb{Q}} \left(\sum_{a=0}^{m} \sum_{b=0}^{p^a-1} j\left(\frac{p^{m-a}\tau_1 + b}{p^a} \right) \right). \end{aligned} \tag{7.3}$$

The second equality follows from Corollary 24 and the observation that $j_m(\tau)$ is a polynomial in $j(\tau)$ with integer coefficients.

The computation in (7.3), when restricted to $m = p^n$, gives us the p^nth coefficient of the p-adic modular form $\Theta f_d(z)/f_d(z)$. The constant term of this p-adic modular form is precisely $-h_{\mathbb{Q}(\sqrt{d})}$, so, by Corollary 15, we have

$$-h_{\mathbb{Q}(\sqrt{d})} = \frac{p-1}{24} \cdot \lim_{n \to \infty} \left(-\frac{744 h_{\mathbb{Q}(\sqrt{d})}(1 - p^{n+1})}{1-p} + \operatorname{Tr}_{K/\mathbb{Q}} \left(\sum_{a=0}^{n} \sum_{b=0}^{p^a-1} j\left(\frac{p^{n-a}\tau_1 + b}{p^a} \right) \right) \right)$$

as p-adic numbers. Simplifying this expression yields the corollary. □

Recall the weight zero modular forms $j^{(p)}(z) \in \mathcal{M}_0^\infty(\Gamma_0(p))$ introduced in §2. We now provide formulae involving $j^{(p)}(z)$ similar to those in Corollary 5:

Theorem 33. *Suppose that $d < -4$ is a fundamental discriminant of an imaginary quadratic field and that τ is a Heegner point of discriminant d. Then the following are true*

(1) *Let $K = \mathbb{Q}(j^{(3)}(\tau), j(\tau))$. If $d \equiv 2 \pmod 3$, then*

$$\lim_{n \to \infty} \left(\operatorname{Tr}_{K/\mathbb{Q}} \left(\sum_{a=0}^{n} \sum_{b=0}^{3^a-1} j^{(3)}\left(\frac{3^{n-a}\tau + b}{3^a} \right) \right) \right) = 0$$

3-adically.

(2) *Let $K = \mathbb{Q}(j^{5}(\tau), j(\tau))$. If $d \equiv 2, 3 \pmod 5$, then*

$$\lim_{n \to \infty} \left(\operatorname{Tr}_{K/\mathbb{Q}} \left(\sum_{a=0}^{n} \sum_{b=0}^{5^a-1} j^{(5)}\left(\frac{5^{n-a}\tau + b}{5^a} \right) \right) \right) = 0$$

5-*adically.*

(3) *Let* $K = \mathbb{Q}(j^{(7)}(\tau), j(\tau))$. *If* $d \equiv 3, 5, 6 \pmod 7$, *then*

$$\lim_{n\to\infty}\left(\mathrm{Tr}_{K/\mathbb{Q}}\left(\sum_{a=0}^{n}\sum_{b=0}^{7^a-1} j^{(7)}\left(\frac{7^{n-a}\tau+b}{7^a}\right)\right)\right) = 0$$

7-*adically.*

We will see in the course of the proof of Theorem 33 that $j^{(p)}(\tau)$ is an algebraic integer of degree $(p+1)\cdot h_{\mathbb{Q}(\sqrt{d})}$ for p and τ as in the statement of the theorem. Before we begin the main body of the proof, we require the following lemma:

Lemma 34. *Suppose* $p \in \{3, 5, 7, 13\}$ *and* $0 \leq n \leq p$. *Let* $\gamma_1, ..., \gamma_{p+1}$ *be a complete set of coset representatives for* $\Gamma_0(p)$ *in* Γ, *and further let* $s_{n,p}(z)$ *be the* n*th symmetric polynomial in* $\{j^{(p)}(\gamma_i \cdot z)\}_{i=1}^{p+1}$. *Then the* q*-series expansion of* $s_{n,p}(z)$ *has integer coefficients, that is,*

$$s_{n,p}(z) \in q^{-n}\mathbb{Z}[[q]].$$

Proof. As we recalled in Lemma 17, a complete set of coset representatives for $\Gamma_0(p)$ in Γ is given by

$$\left\{\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}\right\} \cup \left\{\begin{pmatrix}1 & 0\\ 1 & 1\end{pmatrix}\begin{pmatrix}1 & j\\ 0 & 1\end{pmatrix}\right\}_{j=0}^{p-1}$$

and we have

$$\begin{pmatrix}1 & 0\\ 1 & 1\end{pmatrix}\begin{pmatrix}1 & j\\ 0 & 1\end{pmatrix} = \begin{pmatrix}1/p & 0\\ 0 & 1/p\end{pmatrix}\begin{pmatrix}p & a\\ p & pb\end{pmatrix}\begin{pmatrix}1 & j-a\\ 0 & p\end{pmatrix}$$

where

$$\begin{pmatrix}p & a\\ p & pb\end{pmatrix}$$

is a matrix for $W(p)$.

Now fix n and p for the remainder of this proof. Let $P(x_1, ..., x_{p+1}) \in \mathbb{Z}[x_1, ..., x_{p+1}]$ be the homogeneous polynomial such that $s_{n,p}(z) = P(j^{(p)}(\gamma_1 \cdot z), ..., j^{(p)}(\gamma_{p+1} \cdot z))$. From the calculation above and the definition of $W(p)$, we have

$$\begin{aligned} s_{n,p}(z) &= P\left(j^{(p)}(z), j^{(p)}(z)|_0 W(p)\left(\begin{smallmatrix}1 & 0\\ 0 & p\end{smallmatrix}\right), ..., j^{(p)}(z)|_0 W(p)\left(\begin{smallmatrix}1 & p-1\\ 0 & p\end{smallmatrix}\right)\right) \\ &= P\left(j^{(p)}(z), j^{(p)}(z)|_0\left(\begin{smallmatrix}0 & -1\\ p & 0\end{smallmatrix}\right)\left(\begin{smallmatrix}1 & 0\\ 0 & p\end{smallmatrix}\right), ..., j^{(p)}(z)|_0\left(\begin{smallmatrix}0 & -1\\ p & 0\end{smallmatrix}\right)\left(\begin{smallmatrix}1 & p-1\\ 0 & p\end{smallmatrix}\right)\right). \end{aligned} \tag{7.4}$$

Recall that $j^{(p)}(z) = \left(\frac{\eta(z)}{\eta(pz)}\right)^{\frac{24}{p-1}}$ by definition, and $\eta(-1/z) = (\sqrt{z/i})\eta(z)$ (see, for example, [18, §III.2, p. 121]). Thus

$$\begin{aligned} j^{(p)}(z)|_0\left(\begin{smallmatrix}0 & -1\\ p & 0\end{smallmatrix}\right) &= \left(\frac{\eta(-1/pz)}{\eta(-1/z)}\right)^{\frac{24}{p-1}} = \left(\frac{(\sqrt{pz/i})\eta(pz)}{(\sqrt{z/i})\eta(z)}\right)^{\frac{24}{p-1}} \\ &= p^{\frac{12}{p-1}}\left(\frac{\eta(pz)}{\eta(z)}\right)^{\frac{24}{p-1}} = p^{\frac{12}{p-1}}\left(\frac{q^{p/24}\prod_{n=1}^{\infty}(1-q^{pn})}{q^{1/24}\prod_{n=1}^{\infty}(1-q^n)}\right)^{\frac{24}{p-1}} \\ &=: \sum_{n=-1}^{\infty} a(n)q^n \in q^{-1}\mathbb{Z}[[q]]. \end{aligned}$$

For ease of notation, following [31, §II.6] we define $\zeta := e^{2\pi i/p}$ and $Q := q^{1/p} = e^{2\pi iz/p}$. Then we have

$$q|_0 \left(\begin{smallmatrix} 1 & j \\ 0 & p \end{smallmatrix}\right) = e^{2\pi i \frac{z+j}{p}} = \zeta^j Q,$$

which implies that

$$\left(\sum_{n=-1}^{\infty} a(n)q^n\right)|_0 \left(\begin{smallmatrix} 1 & j \\ 0 & p \end{smallmatrix}\right) = \sum_{n=-1}^{\infty} a(n)\zeta^{jn}Q^n.$$

Thus each of the arguments of P in (7.4) is a Q-series with coefficients in $\mathbb{Z}[\zeta]$. Let $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$, and write $\zeta^\sigma = \zeta^{r(\sigma)}$ for some $1 \le r(\sigma) \le p-1$. Letting σ act on Q-series coefficients we note that

$$\left(\left(\sum_{n=-1}^{\infty} a(n)q^n\right)|_0 \left(\begin{smallmatrix} 1 & j \\ 0 & p \end{smallmatrix}\right)\right)^\sigma = \sum_{n=-1}^{\infty} a(n)\zeta^{r(\sigma)jn}Q^n.$$

Thus, comparing Q-series coefficients, we have

$$\left(\left(\sum_{n=-1}^{\infty} a(n)q^n\right)|_0 \left(\begin{smallmatrix} 1 & j \\ 0 & p \end{smallmatrix}\right)\right)^\sigma = \left(\sum_{n=-1}^{\infty} a(n)q^n\right)|_0 \left(\begin{smallmatrix} 1 & r(\sigma)j \\ 0 & p \end{smallmatrix}\right).$$

Because the value of $f|_0 \left(\begin{smallmatrix} 1 & j \\ 0 & p \end{smallmatrix}\right)$ depends only on the residue class of j modulo p for $f \in \mathcal{M}_0^\infty(\Gamma_0(p))$, this calculation, along with the fact that $j^{(p)}(z)|_0 \left(\begin{smallmatrix} 0 & -1 \\ p & 0 \end{smallmatrix}\right) \in q^{-1}\mathbb{Z}[[q]]$, implies that

$$\begin{aligned} &P\left(j^{(p)}(z), j^{(p)}(z)|_0 W(p) \left(\begin{smallmatrix} 1 & 0 \\ 0 & p \end{smallmatrix}\right), ..., j^{(p)}(z)|_0 W(p) \left(\begin{smallmatrix} 1 & p-1 \\ 0 & p \end{smallmatrix}\right)\right) \\ &= P\left((j^{(p)}(z))^\sigma, (j^{(p)}(z)|_0 W(p) \left(\begin{smallmatrix} 1 & 0 \\ 0 & p \end{smallmatrix}\right))^\sigma, ..., (j^{(p)}(z)|_0 W(p) \left(\begin{smallmatrix} 1 & p-1 \\ 0 & p \end{smallmatrix}\right))^\sigma\right) \end{aligned}$$

for all $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$. Recalling that P has coefficients in $\mathbb{Z}$, this implies that $s_{n,p}(z)$ has Q-series coefficients in $\mathbb{Z}$. Because the action of Γ just permutes the set $\{j^{(p)}(\gamma_i \cdot z)\}_{i=1}^{p+1}$, it follows that $s_{n,p}(z) \in \mathcal{M}_0^\infty(\Gamma)$. Thus, in particular, if $p \nmid n$, the Q series coefficient of Q^n is zero. This completes the proof of the lemma. □

Proof of Theorem 33. First note that there are precisely

$$[\Gamma_0(1) : \Gamma_0(p)] \cdot h_{\mathbb{Q}(\sqrt{d})} = (p+1) \cdot h_{\mathbb{Q}(\sqrt{d})}$$

Heegner points $\tau_1 (:= \tau), \tau_2, ..., \tau_{h_{\mathbb{Q}(\sqrt{d})}(p+1)}$ of discriminant d in $\mathfrak{F}_p$ because there are $h_{\mathbb{Q}(\sqrt{d})}$ Heegner points of discriminant d in $\mathfrak{F}$. Without loss of generality, we may assume $\tau_1, ..., \tau_{h_{\mathbb{Q}(\sqrt{d})}} \in \mathfrak{F}$. With this in mind we form the product

$$f_d(z) := \prod_{k=1}^{(p+1)\cdot h_{\mathbb{Q}(\sqrt{d})}} (j^{(p)}(z) - j^{(p)}(\tau_k)) \tag{7.5}$$

By our assumptions regarding d, it is evident that $f_d(z)$ satisfies all the hypotheses of Theorem 32, with the possible exception of the hypothesis that

$$f_d(z) \in q^{-(p+1)\cdot h_{\mathbb{Q}(\sqrt{d})}} \mathcal{O}_L[[q]] \tag{7.6}$$

for some number field L. We claim that this hypothesis is also satisfied (in particular, we will see that we can take $L = \mathbb{Q}$).

Let $\gamma_1, ..., \gamma_{p+1}$ be a complete set of coset representatives for $\Gamma_0(p)$ in $\Gamma_0(1)$ as in Lemma 34 (without loss of generality we assume $\gamma_1 = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$). We have

$$f_d(z) := \prod_{k=1}^{h_{\mathbb{Q}(\sqrt{d})}} \prod_{i=1}^{p+1} (j^{(p)}(z) - j^{(p)}(\gamma_i \cdot \tau_k)). \tag{7.7}$$

Consider

$$g_{d,k}(z) := \prod_{i=1}^{p+1} (j^{(p)}(z) - j^{(p)}(\gamma_i \cdot \tau_k)) \in \mathcal{M}_0^\infty(\Gamma_0(1)). \tag{7.8}$$

Let $s_{n,p}(z)$ be as in Lemma 34. As noted in the proof of Lemma 34, $s_{n,p}(z) \in \mathcal{M}_0^\infty(\Gamma_0(1))$. Hence $s_{n,p}(z)$ is a polynomial in $j(z)$, that is, it can be regarded as an element of $\mathbb{C}[j(z)]$. The q-series expansion of $s_{n,p}(z)$ has integral coefficients by Lemma 34, from which it follows that

$$s_{n,p}(z) \in \mathbb{Z}[j(z)]. \tag{7.9}$$

Thus $s_{n,p}(\tau_k) \in \mathbb{Z}[j(\tau_k)]$. Theorem 25 tells us that $j(\tau_k)$ is an algebraic integer. Thus, since

$$g_{d,k}(z) \in q^{-(p+1)} \mathcal{O}_{\mathbb{Q}(j(\tau_k))}[[q]],$$

we have that $f_d(z)$ has a q-expansion with algebraic integer coefficients. If we now apply Corollary 27 we have that $f_d(z)$ has a q-series with integral coefficients, which establishes (7.6) with $L = \mathbb{Q}$ as claimed. In particular, this proves that $f_d(z)$ is a good modular form. We will return to this point in a moment.

Write $g_{d,k}(z) = G_{d,k}(j^{(p)}(z))$ with $G_{d,k}(x) \in \mathcal{O}_{\mathbb{Q}(j(\tau_k))}[x]$. We now show that $G_{d,k}(x)$ is irreducible over $\mathbb{Q}(j(\tau_k))$. The roots of $G_{d,k}(x)$ are $j^{(p)}(\gamma_1 \cdot \tau_k), ..., j^{(p)}(\gamma_{p+1} \cdot \tau_k)$; they are distinct because

$$j^{(p)}(z) : \mathfrak{F}_p \to \mathbb{C}$$

is a bijection. Therefore, it suffices to exhibit a field automorphism of

$$K := \mathbb{Q}(j(\tau_k), j^{(p)}(\gamma_1 \cdot \tau_k), ..., j^{(p)}(\gamma_{p+1} \cdot \tau_k))$$

taking $j^{(p)}(\gamma_1 \cdot \tau_k)$ to $j^{(p)}(\gamma_i \cdot \tau_k)$ for arbitrary i that additionally fixes $\mathbb{Q}(j(\tau_k))$. Choose $\beta \in \Gamma_0(1)$ such that $\beta\gamma_1 = \gamma_i$. Then one can check that the linear map $\phi_i : K \to K$ defined on a basis for K as a vector space over $\mathbb{Q}$ by

$$\begin{aligned} &\phi_i(1) := 1 \\ &\phi_i(j(\tau_k)) := j(\beta \cdot \tau_k) = j(\tau_k) \\ &\phi_i(j^{(p)}(\gamma_s \cdot \tau_k)) := j^{(p)}((\beta\gamma_s) \cdot \tau_k) \qquad 1 \leq s \leq p+1 \end{aligned}$$

induces a well-defined field automorphism with the desired characteristics.

Now we return to $f_d(z)$. From above, $f_d(z)$ is good, so $\frac{\Theta f_d(z)}{f_d(z)}$ is a p-adic modular form. Applying Theorem 9 we have

$$\begin{aligned} \frac{\Theta f_d(z)}{f_d(z)} &= -\sum_{\tau \in \mathfrak{F}_p} \left(e_\tau^{(p)} \sum_{n=1}^{\infty} j_n^{(p)}(\tau) q^n \right) + \frac{(p+1) \cdot h_{\mathbb{Q}(\sqrt{d})}}{p-1} (pE_2(z)|V(p) - E_2(z)) \\ &= -\sum_{n=1}^{\infty} \left(\sum_{k=1}^{h_{\mathbb{Q}(\sqrt{d})}} \sum_{i=1}^{p+1} j_n^{(p)}(\gamma_i \cdot \tau_k) \right) q^n + \frac{(p+1) \cdot h_{\mathbb{Q}(\sqrt{d})}}{p-1} (pE_2(z)|V(p) - E_2(z)). \end{aligned} \tag{7.10}$$

Recall from the discussion before the statement of Theorem 9 that $j_m^{(p)}(z)$ is a polynomial in $j^{(p)}(z)$ with integer coefficients for all positive m. Combining this observation with the fact that $j^{(p)}(\gamma_i \cdot \tau_k)$ is a root of the irreducible polynomial $G_{d,k}(x) \in \mathcal{O}_{\mathbb{Q}(j(\tau_k))}[x]$, we have

$$\sum_{i=1}^{p+1} j_m^{(p)}(\gamma_i \cdot \tau_k) = \mathrm{Tr}_{K/\mathbb{Q}(j(\tau_k))}\, j_m^{(p)}(\gamma_1 \cdot \tau_k) = \mathrm{Tr}_{K/\mathbb{Q}(j(\tau_k))}\, j_m^{(p)}(\tau_k)$$

(recall our convention that $\gamma_1 = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$). Because $\{j(\tau_k)\}_{k=0}^{h_{\mathbb{Q}(\sqrt{d})}}$ is the set of Galois conjugates of $j(\tau)$, we have

$$\sum_{k=1}^{h_{\mathbb{Q}(\sqrt{d})}} \mathrm{Tr}_{K/\mathbb{Q}(j(\tau_k))}\, j_m^{(p)}(\tau_k) = \mathrm{Tr}_{\mathbb{Q}(j(\tau_k))/\mathbb{Q}}\left(\mathrm{Tr}_{K/\mathbb{Q}(j(\tau_k))}\, j_m^{(p)}(\tau_k)\right) = \mathrm{Tr}_{K/\mathbb{Q}}\, j_m^{(p)}(\tau).$$

On the other hand, the p^nth coefficient of $\frac{(p+1)\cdot h_{\mathbb{Q}(\sqrt{d})}}{p-1}(pE_2(z)|V(p) - E_2(z))$ is equal to

$$\frac{(p+1)\cdot h_{\mathbb{Q}(\sqrt{d})}}{p-1}(-24(p\sigma_1(p^{n-1}) - \sigma_1(p^n))) = \frac{24(p+1)\cdot h_{\mathbb{Q}(\sqrt{d})}}{p-1}.$$

Note that the constant term of $\frac{\Theta(f_d(z)}{f_d(z)}$ is $(p+1)\cdot h_{\mathbb{Q}(\sqrt{d})}$. In view of (7.10) and the calculations above, we apply Corollary 15 to conclude that

$$\begin{aligned}(p+1)\cdot h_{\mathbb{Q}(\sqrt{d})} &= \frac{p-1}{24}\cdot \lim_{n\to\infty}\left(\mathrm{Tr}_{K/\mathbb{Q}}\, j_{p^n}^{(p)}(\tau) + \frac{24(p+1)\cdot h_{\mathbb{Q}(\sqrt{d})}}{p-1}\right) \\ &= (p+1)\cdot h_{\mathbb{Q}(\sqrt{d})} + \frac{p-1}{24}\cdot \lim_{n\to\infty}\left(\mathrm{Tr}_{K/\mathbb{Q}}\left(\sum_{a=0}^{n}\sum_{b=0}^{p^a-1} j^{(p)}\left(\frac{p^{n-a}\tau + b}{p^a}\right)\right)\right).\end{aligned}$$

p-adically. Rewriting this expression completes the proof of the theorem. □

Acknowledgements

The author would like to thank his thesis advisor W. Stein for many helpful suggestions and corrections, and K. Ono for suggesting that Theorem 3 could be generalized to congruence subgroups and, more importantly, for introducing him to modular forms in the first place. Finally, E. Smith deserves thanks for help with editing.

References

[1] S. Ahlgren, *The theta-operator and divisors of modular forms on genus zero subgroups*, Math. Res. Letters, accepted for publication.
[2] T. Asai, M. Kaneko, and H. Ninomiya, *Zeros of certain modular functions and an application*, Comment. Math. Univ. St. Pauli, **46** 1 (1997), 93-101.
[3] A.O.L. Atkin and J. Lehner, *Hecke operators on* $\Gamma_0(m)$, Math. Ann. **185** (1970), 134-160.
[4] S. Basha, J. Getz, H. Nover, E. Smith, *Systems of orthogonal polynomials arising from the modular j-function*, Journal of Math. Analysis and Appl., **289** 1 (2004), 336-354.
[5] B.C. Berndt, W. Kohnen, and K. Ono, *The life and work of R.A. Rankin (1915-2001)*, The Ramanujan Journal, **7** (2003), 11-40.
[6] R. Borcherds, *Automorphic forms on* $O_{s+2,2}$ *and infinite products*, Invent. Math., **120** (1995) 161-213.
[7] J. Bruinier, W. Kohnen, and K. Ono, *The arithmetic of the values of modular functions and the divisors of modular forms*, Compositio Math., to appear.
[8] J. Bruinier, K. Ono, *The arithmetic of Borcherds' exponents*, Math. Ann., **327** (2003), 293-303.

[9] D. Choi, *On the values of a modular form on* $\Gamma_0(N)$, preprint.
[10] Y. Choie and W. Kohnen, *Special values of modular functions on Hecke groups*, Abh. Math. Sem. Univ. Hamburg, to appear.
[11] M. Deuring, *Teilbarkeitseigenschaften der singulären modulen der elliptischen funktionen und die diskriminante der klassengleichung*, Comm. Math. Helv. **19** (1945), 74-82.
[12] J. Getz, *A generalization of a theorem of Rankin and Swinnerton-Dyer on zeros of modular forms*, Proc. AMS, to appear.
[13] F.Q. Gouvêa, *Arithmetic of p-adic modular forms*, Springer Lect. Notes in Math., **1304**, 1985.
[14] B. Gross and D. Zagier, *On singular moduli*, J. Reine angew. math. **355** (1985), 191-220.
[15] K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory*, Springer Verlag, New York, 1991.
[16] M. Kaneko and D. Zagier, *Supersingular j-invariants, hypergeometric series, and Atkin's orthogonal polynomials*, Computational Perspectives on Number Theory (Chicago, IL, 1995), AMS/IP **7** (1998), 97–126.
[17] A. Knapp, *Elliptic Curves*, Mathematical Notes, Princeton University Press, **40** Princeton, New Jersey, 1992.
[18] N. Koblitz, *Introduction to Elliptic Curves and Modular Forms*, Springer-Verlag, New York, 1993.
[19] S. Lang, *Introduction to Modular Forms*, Springer-Verlag, New York, 2001.
[20] S. Lang, *Elliptic Functions, 2nd edition*, Springer-Verlag, New York, 1987.
[21] W.-C.W. Li, *Newforms and functional equations*, Math. Ann. **212** (1975), 285-315.
[22] W.J. McGraw and K. Ono, *Modular form congruences and Selmer groups*, J. London Math. Soc. (2) **67** (2003), 302-318.
[23] T. Miyake, Modular forms, Springer-Verlag, Berlin, 1989.
[24] K. Ono, *The Web of Modularity: Arithmetic of the Coefficients of Modular Forms and q-series*, AMS-CBMS Regional Conference Series in Mathematics, **102** (2004) Providence, RI.
[25] K. Ono and M.A. Papanikolas, *p-adic properties of the values of the modular j-function*, Galois Theory and Modular Forms, (eds.) K. Hashimoto, K. Miyake, H. Nakamura, Kluwer Academic Publishers, (2003), 357-366.
[26] F.K.C. Rankin and H.P.F. Swinnerton-Dyer *On the zeros of Eisenstein series*, Bull. London Math. Soc. **2**, (1970), 169-170.
[27] B. Schoenberg, *Elliptic modular functions*, Springer-Verlag, New York, 1970.
[28] J-P. Serre, *A Course in Arithmetic*, Springer-Verlag, New York, 1990.
[29] J-P. Serre, *Formes modulaires et fonctions zêta p-adiques*, Springer Lect. Notes, **350** (1973), 191–268.
[30] J. Silverman, *The Arithmetic of Elliptic Curves*, Springer-Verlag, New York, 1986.
[31] J. Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves*, Springer-Verlag, New York, 1994.
[32] J. Sturm, *On the congruence of modular forms*, Springer Lect. Notes in Math. **1240**, (1984), 275–280.
[33] D. Zagier, *Modular forms and differential operators*, Proc. Indian Acad. Sci. (Math. Sci.), **104** 1 (1994), 57–75.

4404 South Ave. W, Missoula, MT 59804
E-mail address: getz@fas.harvard.edu