ORDERS AT INFINITY OF MODULAR FORMS WITH HEEGNER DIVISORS

CARL ERICKSON, ALISON MILLER, AND AARON PIXTON

Abstract. Borcherds described the exponents $a(n)$ in product expansions $f = q^h \prod_{n=1}^{\infty}(1-q^n)^{a(n)}$ of meromorphic modular forms with a Heegner divisor. His description does not directly give any information about h, the order of vanishing at infinity of f. We give p-adic formulas for h in terms of generalized traces given by sums over the zeroes and poles of f. Specializing to the case of the Hilbert class polynomial $f = \mathcal{H}_d(j(z))$ yields p-adic formulas for class numbers that generalize past results of Bruinier, Kohnen and Ono. We also give new proofs of known results about the irreducible decomposition of the supersingular polynomial $S_p(X)$.

1. Introduction and Statement of Results

At the International Congress of Mathematicians in 1994, Borcherds [1] announced a fascinating theorem describing the product expansions of those modular forms with a *Heegner divisor*, that is, forms whose zeros and poles are all at Heegner points and cusps.[1] Borcherds defined an isomorphism Ψ between the Kohnen plus-space $M^!_{1/2}(\Gamma_0(4))$ of certain weakly holomorphic modular forms and the set of integer weight meromorphic modular forms with a Heegner divisor, integer coefficients, and leading coefficient 1. His result is as follows. Let $H(d)$ be the Hurwitz-Kronecker class numbers, defined as

$$H(d) = \sum_{Q \in \mathcal{Q}_d/\Gamma} \frac{1}{|\Gamma_Q|},$$

where $\mathcal{Q}_d$ is the set of positive definite binary quadratic forms of discriminant $-d$ and Γ_Q is the stabilizer of Q under the action of $\Gamma = \mathrm{PSL}_2(\mathbb{Z})$. Let $\widetilde{H}(z) = -1/12 + \sum_{n\geq 1} H(n)q^n$, where $q = e^{2\pi i z}$. A modular form $f \in M^!_{1/2}(\Gamma_0(4))$ with Fourier expansion $f(z) = \sum_{n \geq n_0} A(n)q^n$ maps under Borcherds' isomorphism to

$$\Psi(f) = q^{-h} \prod_{n=1}^{\infty} (1-q^n)^{A(n^2)},$$

where h is the constant coefficient of $\widetilde{H}(z)f(z)$. Moreover, the multiplicity of the zero of $\Psi(f)$ at a Heegner point of discriminant $-d$ is $\sum_{n>0} c(n^2 D)$ (see Theorem 1.1 of [1]).

Example. The Eisenstein series of weight 4 has the formal product expansion

$$E_4(z) = 1 + 240 \sum_{n=1}^{\infty} \sigma_3(n) q^n = (1-q)^{-240}(1-q^2)^{26760} \cdots = \prod_{n=1}^{\infty} (1-q^n)^{c(n)}.$$

By Borcherds' theorem, there is a unique form in $M^!_{1/2}(\Gamma_0(4))$ with Fourier expansion $\sum_{n \geq n_0} b(n)q^n$ such that $b(1) = -240$, $b(4) = 26760$, and generally $b(n^2) = c(n)$ for positive integer n.

[1] We use the term "Heegner point" in its original meaning as a CM point, not as an element of the Mordell-Weil group of an elliptic curve.

The most basic modular forms with Heegner divisors and rational coefficients are the Hilbert class polynomials[2] in the usual elliptic modular invariant j, defined by

$$\mathcal{H}_d(j(z)) = \prod_{Q \in \mathcal{Q}_d/\Gamma} (j(z) - j(\alpha_Q))^{1/|\Gamma_Q|}, \tag{1}$$

where α_Q is the Heegner point determined by $Q(\alpha_Q, 1) = 0$. This modular function $\mathcal{H}_d(j)$ has zeroes at the Heegner points of discriminant $-d$ and a pole (of order $H(d)$) at infinity. We can obtain the Borcherds exponents of $\mathcal{H}_d(j)$ by observing that the logarithmic derivative of $\mathcal{H}_d(j)$ is

$$\frac{1}{2\pi i}\frac{d}{dz}(\log \mathcal{H}_d(j)) = -H(d) - \sum_{m=1}^{\infty} \mathrm{Tr}_m(d) q^m. \tag{2}$$

This generalized trace $\mathrm{Tr}_m(d)$, due to Zagier [10], is defined by

$$\mathrm{Tr}_m(d) = \sum_{Q \in \mathcal{Q}_d/\Gamma} \frac{1}{|\Gamma_Q|} j_m(\alpha_Q),$$

where $j_m(z)$ is the unique weakly holomorphic modular function on $\mathrm{SL}_2(\mathbb{Z})$ having a Fourier expansion of the form $q^{-m} + O(q)$.

Zagier [10] reproved Borcherds' theorem in the setting described above by using recurrences involving the traces $\mathrm{Tr}_m(d)$. In Theorem 3 of [10], Zagier characterized the forms $f_d = \Psi^{-1}(\mathcal{H}_d(j))$ as the unique elements of $M^!_{1/2}(\Gamma_0(4))$ with Fourier expansions of the form $q^{-d} + \sum_{D>0} A(D, d) q^D$. In other words, we have the Borcherds product

$$\mathcal{H}_d(j) = q^{-H(d)} \prod_{n=1}^{\infty} (1 - q^n)^{A(n^2, d)}. \tag{3}$$

Logarithmically differentiating and comparing with equation (2), we see that the traces $\mathrm{Tr}_m(d)$ can be expressed in terms of the coefficients $A(n^2, d)$ for $m > 0$. However, this method does not give any direct information about the class number $H(d) = \mathrm{Tr}_0(d)$.

Bruinier and Ono [3] found p-adic formulas for the class number $H(d)$ in terms of the Fourier coefficients $A(n^2, d)$ by applying Serre's theory of p-adic modular forms [8] to the logarithmic derivative given in equation (2). For fixed d, the series (2) is a p-adic modular form for certain primes p. Serre's theory implies that if $p \leq 7$, then the constant coefficient of a p-adic modular form is proportional to the p-adic limit of its p^{th}-power coefficients (see Theorem 7 of [8]). More explicitly, the result for fundamental discriminants $-d < -4$ in appropriate congruence classes modulo a fixed prime $p \leq 7$ is that

$$H(d) = \frac{p-1}{24} \lim_{n \to +\infty} \mathrm{Tr}_{p^n}(d).$$

Here we generalize these results to a large class of modular forms with Heegner divisors, and we obtain results that hold for all primes p.

Definition. Given a prime $p \geq 5$ and discriminant $-d$, the pair (p, d) is called *tractable* if $\left(\frac{-d}{p}\right) = -1$, or if both $p \mid d$ and $\mathbb{Q}(\sqrt{-d}) \neq \mathbb{Q}(i), \mathbb{Q}(\sqrt{-3})$. Also, if $p \geq 5$ is prime and f is a meromorphic modular form on $\mathrm{SL}_2(\mathbb{Z})$ with a Heegner divisor, the pair (p, f) is called *tractable* if f only has poles and zeroes at Heegner points of discriminants $-d$ such that (p, d) is tractable.

By a theorem of Ono (see Theorem 4.15 of [7]), if a modular form f with a Heegner divisor has zeros and poles at Heegner points of discriminants $\{-d_i\}$ such that (p, d_i) is tractable for every d_i, then the logarithmic derivative $\Theta f / f$ is a p-adic modular form.

[2]Note that these are not strictly polynomials if d is a square or three times a square.

We define generalized traces that bear the same relationship to arbitrary meromorphic modular forms that traces of singular moduli do to $\mathcal{H}_d(j)$. If f is a meromorphic modular form on $\mathrm{SL}_2(\mathbb{Z})$ whose zeroes and poles in the fundamental domain $\mathcal{F}$ are $z_1, z_2, \ldots, z_r$ with multiplicities $e_1, e_2, \ldots, e_r$, then we define

$$\mathrm{Tr}_m(f) = \sum_{i=1}^{r} \frac{e_i}{|\Gamma_{z_i}|} j_m(z_i). \tag{4}$$

Also, let $\mathrm{ord}_\infty(f)$ denote the order of vanishing of f at infinity. Note that $\mathrm{Tr}_m(\mathcal{H}_d(j)) = \mathrm{Tr}_m(d)$ and $\mathrm{ord}_\infty(\mathcal{H}_d(j)) = -H(d)$.

We recall the definition of the operator $U = U_p$, which acts on formal power series by

$$\sum_{n\in\mathbb{Z}} a(n)q^n \mid U_p = \sum_{n\in\mathbb{Z}} a(pn)q^n. \tag{5}$$

If Ω is a vector space of formal power series stable under U, we let Ω^U denote the 1-eigenspace of the action of U on Ω.

For a subfield $\mathbb{F} \leq \mathbb{C}$ and a congruence subgroup $A \leq \mathrm{SL}_2(\mathbb{Z})$, let $M_k(A, \mathbb{F})$ be the space of holomorphic modular forms of weight k on A whose Fourier coefficients are elements of $\mathbb{F}$. We set $M_k := M_k(\mathrm{SL}_2(\mathbb{Z}), \mathbb{Q})$ for brevity.

We begin with our result in its greatest generality. Note that the following limits are taken in the p-adic topology.

Theorem 1.1. *Let $p \geq 5$ be a prime. For some $n \leq \dim M_2(\Gamma_0(p), \mathbb{Q}) = \dim M_{p+1}$, there exist n positive integers $m_1 < m_2 < \cdots < m_n \leq \frac{p+1}{6}$ and p-integral rational constants $c_1, \ldots, c_n$ such that*

$$\mathrm{ord}_\infty(f) = \frac{k}{12} - \sum_{i=1}^{n} c_i \lim_{t\to\infty} \mathrm{Tr}_{m_i p^{2t}}(f)$$

for every meromorphic modular form f on $\mathrm{SL}_2(\mathbb{Z})$ with a Heegner divisor such that (p, f) is tractable. Here k denotes the weight of f.

We can obtain a slightly stronger result if we restrict ourselves to forms with rational Fourier coefficients. The primary difference is that we do not need to restrict ourselves to even powers of p because the trace limit $\lim_{t\to\infty} \mathrm{Tr}_{m_i p^t}(f)$ now converges.

Theorem 1.2. *Let $p \geq 5$ be a prime. For some $n \leq \dim M_2(\Gamma_0(p), \mathbb{Q})^U$, there exist n positive integers $m_1 < m_2 < \cdots < m_n \leq \frac{p+1}{6}$ and p-integral rational constants $c_1, \ldots, c_n$ such that*

$$\mathrm{ord}_\infty(f) = \frac{k}{12} - \sum_{i=1}^{n} c_i \lim_{t\to\infty} \mathrm{Tr}_{m_i p^{t}}(f)$$

for every meromorphic modular form f on $\mathrm{SL}_2(\mathbb{Z})$ with rational Fourier coefficients and a Heegner divisor such that (p, f) is tractable.

The following p-adic formula for $H(d)$ is simply the specialization of Theorem 1.2 to the case $f = \mathcal{H}_d(j)$.

Corollary 1.3. *Let $p \geq 5$ be a prime. For some $n \leq \dim M_2(\Gamma_0(p), \mathbb{Q})^U$, there exist n positive integers $m_1 < m_2 < \ldots < m_n \leq \frac{p+1}{6}$ and p-integral rational constants $c_1, \ldots, c_n$ such that*

$$H(d) = \sum_{i=1}^{n} c_i \lim_{t\to\infty} \mathrm{Tr}_{m_i p^{t}}(d)$$

for all $d > 0$ such that (p, d) is tractable.

For certain values of p, it is possible to choose $n = 1$ in the above results and obtain a simpler formula.

Corollary 1.4. *Let $p \geq 5$ be a prime. If m is a positive integer such that $p \nmid m$ and the m^{th} Fourier coefficient of every cusp form in $M_2(\Gamma_0(p), \mathbb{Q})^U$ is zero, then*

$$H(d) = \frac{p-1}{24\sigma_1(m)} \lim_{t\to\infty} \mathrm{Tr}_{mp^t}(d)$$

for all $d > 0$ such that (p, d) is tractable.

Remark. Similar results hold for $p = 2$ or 3, but we omit them for simplicity.

In Section 2, we review the relevant results from Serre's theory of p-adic modular forms. We then use these results to prove our theorems in Section 3. Section 4 contains a brief discussion of the effectiveness of our results, followed by two examples in which we use the results to determine class numbers. We conclude by explaining the connections to the theory of supersingular elliptic curves and give new proofs of known results about the irreducible decomposition of the supersingular polynomial.

Acknowledgments

We thank the NSF and the Guggenheim Foundation for their generous support. We also thank Ken Ono, Jeremy Rouse, and the referee for their helpful comments.

2. Preliminaries

In order to prove our results, we will need to work with the classical theory of p-adic modular forms, as first developed by Serre. We first recall definitions and basic results, which can be found in Serre's seminal paper [8]. Throughout, we suppose that $p \geq 5$ is prime.

Definition. A *p-adic modular form* is a formal series $f = \sum_{n=0}^{\infty} a_n q^n$ with coefficients $a_n \in \mathbb{Q}_p$ for which there exists a sequence $\{f_i\}$ of modular forms on $\mathrm{SL}_2(\mathbb{Z})$ with rational q-series coefficients which converge p-adically uniformly to those of f.

A nonzero p-adic modular form has a well-defined weight, which is an element of the group $X = \mathbb{Z}_p \times (\mathbb{Z}/(p-1)\mathbb{Z})$. We will use the canonical injection $\mathbb{Z} \hookrightarrow X$ to identify $\mathbb{Z}$ with a dense subgroup of X.

Definition. The *weight* of a nonzero p-adic modular form f is defined as the limit in X of the weights of the f_i.

Remark. This limit exists and is independent of the choice of the sequence f_i (see Theorem 2 of [8]).

We will use the notation $\mathcal{M}_k$ for the space of all p-adic modular forms of weight k. We recall the definition of the closely related space $\widetilde{M}_k$ of modular forms mod p, which is the space of formal power series in $\mathbb{F}_p[[q]]$ that are the reductions mod p of modular forms of weight k on $\mathrm{SL}_2(\mathbb{Z})$ with p-integral rational coefficients. The operator U defined in (5) acts naturally on both $\mathcal{M}_k$ and $\widetilde{M}_k$. Another operator which is important in the theory of p-adic modular forms is the Ramanujan theta operator $\Theta = q\frac{d}{dq}$.

We will need the following results of Serre relating p-adic modular forms on $\mathrm{SL}_2(\mathbb{Z})$ to modular forms on $\Gamma_0(p)$ (see Theorem 10 and Theorem 11(c) of [8]).

Proposition 2.1. *(a) Let $f = \sum a_n q^n$ be a modular form of weight k on $\Gamma_0(p)$. If the coefficients a_n are rational, then f is a p-adic modular form of weight k.*

(b) Any element of $\widetilde{M}_{p+1}$ is the mod p reduction of a weight 2 modular form on $\Gamma_0(p)$ with p-integral rational coefficients.

In order to use these results on p-adic modular forms, we need the following theorem of Ono (see Theorems 4.15 and 4.16 of [7]), which tells us that under certain conditions, the logarithmic derivative of a modular form is a p-adic modular form (of weight 2).

Proposition 2.2. *Let p be prime, and let f be a meromorphic modular form on $\mathrm{SL}_2(\mathbb{Z})$ with a Heegner divisor. If (p, f) is tractable, then the logarithmic derivative $\frac{\Theta f}{f}$ is a weight two p-adic modular form.*

3. Proofs of Our Results

Throughout we assume that $p \geq 5$ is prime. We first prove three lemmas.

Lemma 3.1. *The inclusion $M_2(\Gamma_0(p), \mathbb{Q}) \hookrightarrow \mathcal{M}_2$ induces an isomorphism*

$$M_2(\Gamma_0(p), \mathbb{Q})^U \otimes_{\mathbb{Q}} \mathbb{Q}_p \xrightarrow{\sim} \mathcal{M}_2^U.$$

Proof. It is clear that the induced map is injective, so it suffices to prove surjectivity. Let $N \leq \mathcal{M}_2^U$ be the $\mathbb{Z}_p$-submodule of those forms with q-series coefficients in $\mathbb{Z}_p$. Then any element of $\mathcal{M}_2^U$ is a $\mathbb{Q}_p$-multiple of some element of N, so it suffices to prove that the image of $M_2(\Gamma_0(p), \mathbb{Q})^U \otimes_{\mathbb{Q}} \mathbb{Q}_p \to \mathcal{M}_2^U$ contains N, which is implied if the image intersects every coset of N mod p. Suppose f is an element of N. By the Corollary to Theorem 6 of [8], the reduction of f mod p lies in $\widetilde{M}_{p+1}$. Proposition 2.1(b) gives that we can find a modular form g of weight 2 over $\Gamma_0(p)$ such that $g \equiv f \pmod{p}$, and g is an eigenform of U with eigenvalue ± 1 (see the Corollary to Theorem 11 of [8]). Because g is congruent to f mod p, the eigenvalue must be 1, so $g \in M_2(\Gamma_0(p), \mathbb{Q})^U$ lies in the same coset mod p of N as f, as desired. □

The following lemma is a more effective version of Lemma 6 of [8] in a special case.

Lemma 3.2. *Let Y be a subspace of $\mathcal{M}_2$ of finite dimension n such that the mod p reduction of any element of Y belongs to $\widetilde{M}_{p+1}$. There exist n positive integers $m_1 < m_2 < \cdots < m_n \leq \frac{p+1}{6}$ and p-adic integers $c_1, c_2, \ldots, c_n$ such that*

$$a_0(f) = \sum_{i=1}^{n} c_i a_{m_i}(f)$$

for all $f \in Y$, where $a_m(f)$ denotes the m^{th} q-series coefficient of f.

Proof. Let $s = \lfloor \frac{p+1}{6} \rfloor$. Let $Y_0 \leq Y$ be the $\mathbb{Z}_p$-submodule of forms with p-integral coefficients, so Y_0 is a free $\mathbb{Z}_p$-module of rank n. We view the coefficient functions a_i as elements of the dual space $Y_0^* = \mathrm{Hom}_{\mathbb{Z}_p}(Y_0, \mathbb{Z}_p)$.

We first claim that the homomorphism $\psi : Y_0/pY_0 \to \mathbb{Z}_p^s/p\mathbb{Z}_p^s$ given by $f \mapsto (a_i(f))_{i=1}^s$ is injective. Suppose otherwise for a contradiction. Then there exists $f \in Y_0$ such that $f \notin pY_0$ but $a_i(f) \equiv 0$ mod p for all $1 \leq i \leq s$. Let $\tilde{f} \in \widetilde{M}_{p+1}$ be the reduction of f modulo p, so $\tilde{f} \neq 0$. Then $\Theta\tilde{f} \in \widetilde{M}_{2p+2}$ (see Lemma 5(ii) of [9]). Since $a_n(\Theta\tilde{f}) = 0$ for each $n \leq \frac{2p+2}{12} = \frac{p+1}{6}$, Lemma 6 of [9] gives that $\Theta\tilde{f} = 0$. However, this implies that the filtration of $\tilde{f}$ is a multiple of p (see Lemma 5(ii) of [9]), so $\tilde{f} = 0$, which is a contradiction.

Thus ψ is injective, so the dual map $\psi^* : (\mathbb{Z}_p^s)^*/p(\mathbb{Z}_p^s)^* \to Y_0^*/pY_0^*$ given by $(c_i)_{i=1}^s \mapsto \sum_{i=1}^s c_i a_i$ is surjective. This implies that the lifted map $\varphi : (\mathbb{Z}_p^s)^* \to Y_0^*$ is surjective, because its image is a $\mathbb{Z}_p$-submodule which intersects every coset mod p. Thus $a_0 = \sum_{i=1}^s c_i a_i$ for some $c_1, c_2, \ldots, c_s \in \mathbb{Z}_p$.

Because Y_0^* has rank n, these c_i can be chosen such that no more than n of them are nonzero, and we have the desired result. □

Lemma 3.3. *Let $\mathcal{O}$ be the ring of integers of a number field K, and let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}$ lying over p. If $f \in \mathcal{O}[[q]]$ is a formal power series such that $f \equiv 1 \pmod{\mathfrak{p}}$, then*

$$a_{mp^t}\left(\frac{\Theta f}{f}\right) \equiv 0 \pmod{p^{t-\alpha}}$$

for all positive integers m and t, where α is a constant that depends only on the ramification index $e_{\mathfrak{p}}$ of $\mathfrak{p}$ in the extension $K/\mathbb{Q}$. In particular, if $\mathfrak{p}$ is unramified in $\mathcal{O}$, we can set $\alpha = -1$.

Proof. Write $f = 1 - g$, where $g \in \mathfrak{p}\mathcal{O}[[q]]$. Then the formal series $\log f = -\sum_{i=1}^{\infty} \frac{g^i}{i}$ converges in the completion $K_{\mathfrak{p}}$ of K at the ideal $\mathfrak{p}$, which is a finite extension of $\mathbb{Q}_p$, and it can be differentiated term-by-term to give

$$\frac{\Theta f}{f} = \Theta(\log f) = -\Theta \sum_{i=1}^{\infty} \frac{g^i}{i}.$$

We extend the p-adic valuation v_p on $\mathbb{Q}_p$ to a valuation on $K_{\mathfrak{p}}$: because $g \in \mathfrak{p}\mathcal{O}[[q]]$, all coefficients of g have valuation at least $\frac{1}{e_{\mathfrak{p}}}$, so all coefficients of $\frac{g^i}{i}$ have valuation at least $\frac{i}{e_{\mathfrak{p}}} - v_p(i)$. However, it is easy to see that $\frac{i}{e_{\mathfrak{p}}} - v_p(i)$ is bounded below independently of i. We conclude that we can find an integer α depending only on $e_{\mathfrak{p}}$ such that the coefficients of $-\sum_{i=1}^{\infty} \frac{g^i}{i}$ all have p-adic valuation at least $-\alpha$. (In particular, when $e_{\mathfrak{p}} = 1$, we can take $\alpha = -1$ because of the bound $i \geq v_p(i) + 1$.)

We now use the fact that the action of Θ multiplies the coefficient of q^{mp^t} by mp^t, so

$$a_{mp^t}\left(\frac{\Theta f}{f}\right) = -mp^t a_{mp^t}\left(\sum_{i=1}^{\infty} \frac{g^i}{i}\right) \equiv 0 \pmod{p^{t-\alpha}},$$

as desired. □

Proof of Theorems 1.1 and 1.2. The proofs of these two theorems will be analogous; we focus on the case covered by Theorem 1.2, in which the Fourier coefficients are rational, but we also describe the necessary alterations for Theorem 1.1.

Recall that $M_2(\Gamma_0(p), \mathbb{Q})^U \otimes_{\mathbb{Q}} \mathbb{Q}_p$ can be naturally viewed as a subspace of $\mathcal{M}_2$ of finite dimension equal to $\dim M_2(\Gamma_0(p), \mathbb{Q})^U$. Then by Lemma 3.2, for some $n \leq \dim M_2(\Gamma_0(p), \mathbb{Q})^U$ there exist positive integers $m_1 < \ldots < m_n \leq \frac{p+1}{6}$ and constants $c_1, \ldots, c_n \in \mathbb{Z}_p$ such that

$$a_0(f) = \sum_{i=1}^{n} c_i a_{m_i}(f) \tag{6}$$

for every $f \in M_2(\Gamma_0(p), \mathbb{Q})^U \otimes_{\mathbb{Q}} \mathbb{Q}_p$. Since $M_2(\Gamma_0(p), \mathbb{Q})^U \otimes_{\mathbb{Q}} \mathbb{Q}_p$ contains a basis of forms with rational Fourier coefficients, these constants c_i must belong to $\mathbb{Q} \cap \mathbb{Z}_p$.

For Theorem 1.1, we choose the m_i and c_i analogously by applying Lemma 3.2 to $M_2(\Gamma_0(p), \mathbb{Q}) \otimes_{\mathbb{Q}} \mathbb{Q}_p$.

We now show that the theorems hold with the integers m_i and constants c_i chosen above. Suppose that f satisfies the conditions in Theorem 1.1. Dividing by the appropriate power of Δ to reduce the weight to zero and writing the resulting modular function as a rational function of j yields

$$f(z) = A\Delta^{k/12} \prod_{i=1}^{r} (j(z) - j(z_i))^{e_i/|\Gamma_{z_i}|}, \tag{7}$$

where $A \in \mathbb{C}^\times$ and f has zeroes and poles z_i with multiplicities $e_i \in \mathbb{Z}$. Since the z_i are Heegner points, the singular moduli $j(z_i)$ are algebraic integers, and we can find some finite Galois extension

$K/\mathbb{Q}$ with ring of integers $\mathcal{O}$ such that $A^{-1}f$ has coefficients in $\mathcal{O}$. Note that if f has rational coefficients, then we can take $K = \mathbb{Q}$. Also, we can still ensure in the general case that the characteristic p residue field of K has order at most p^2. (See [4] for one proof. We will give an independent proof in Section 5.)

By Proposition 2.2, the logarithmic derivative of f is a p-adic modular form of weight 2 with coefficients in the completion $\mathcal{O}_{\mathfrak{p}}$ of $\mathcal{O}$ at some prime ideal $\mathfrak{p}$ over p. Logarithmically differentiating (7), and using the standard identity $\frac{\Theta j(z)}{j(\tau)-j(z)} = \sum_{m=0}^{\infty} j_m(\tau)q^m$ (see page 10 of [10]), we obtain the q-series expansion

$$\begin{aligned}\frac{\Theta f(z)}{f(z)} &= \frac{k}{12}\frac{\Theta\Delta}{\Delta} + \sum_{i=1}^{r}\frac{e_i}{|\Gamma_{z_i}|}\frac{\Theta j(z)}{j(z)-j(z_i)} = \frac{k}{12}E_2(z) - \sum_{i=1}^{r}\frac{e_i}{|\Gamma_{z_i}|}\sum_{m=0}^{\infty} j_m(z_i)q^m \\ &= \frac{k}{12}E_2(z) - \sum_{m=0}^{\infty}\mathrm{Tr}_m(f)q^m.\end{aligned}$$

If $K = \mathbb{Q}$, then we claim that $\frac{\Theta f(z)}{f(z)}|U^t$ converges p-adically as $t \to \infty$. Moreover, we can give a lower bound for the rate of convergence; we have

$$\begin{aligned}a_m\left(\frac{\Theta f(z)}{f(z)}|U^t - \frac{\Theta f(z)}{f(z)}|U^{t-1}\right) &= a_{p^t m}\left(\frac{\Theta f(z)}{f(z)} - \frac{(\Theta f)(pz)}{f(pz)}\right) \\ &= \frac{1}{p}a_{p^t m}\left(\frac{\Theta(f(z)^p)}{f(z)^p} - \frac{\Theta(f(pz))}{f(pz)}\right) \\ &= \frac{1}{p}a_{p^t m}\left(\frac{\Theta(f(z)^p/f(pz))}{f(z)^p/f(pz)}\right),\end{aligned}$$

which is a multiple of p^t by Lemma 3.3, since $f(z)^p/f(pz) \equiv 1 \bmod p$.

In general, we claim that $\frac{\Theta f(z)}{f(z)}|U^{2t}$ converges similarly. As above, we have

$$a_m\left(\frac{\Theta f(z)}{f(z)}|U^t - \frac{\Theta f(z)}{f(z)}|U^{t-2}\right) = \frac{1}{p^2}a_{p^t m}\left(\frac{\Theta(f(z)^{p^2}/f(p^2z))}{f(z)^{p^2}/f(p^2z)}\right), \tag{8}$$

which has p-adic valuation at least $t-\alpha$ (for some constant α only depending on p) by Lemma 3.3, since $f(z)^{p^2}/f(p^2z) \equiv 1 \bmod \mathfrak{p}$ for some prime ideal $\mathfrak{p}$ above p.

We then have (in the case when $K = \mathbb{Q}$) that

$$\lim_{t\to\infty}\frac{\Theta f(z)}{f(z)} \mid U^t = \frac{k}{12}E_2^* - \mathrm{Tr}_0(f) - \sum_{m=1}^{\infty}\lim_{t\to\infty}\mathrm{Tr}_{mp^t}(f)q^m$$

is a p-adic modular form of weight 2, and subtracting a multiple of the p-adic Eisenstein series E_2^* then gives that

$$\mathrm{ord}_\infty(f) - \frac{k}{12} - \sum_{m=1}^{\infty}\lim_{t\to\infty}\mathrm{Tr}_{mp^t}(f)q^m \tag{9}$$

is also a p-adic modular form of weight 2. Since this form is invariant under U, it is in the subspace $M_2(\Gamma_0(p),\mathbb{Q})^U \otimes_{\mathbb{Q}} \mathbb{Q}_p$ by Lemma 3.1. Applying equation (6) then yields the desired formula for $\mathrm{ord}_\infty(f)$ in Theorem 1.2. Theorem 1.1 is obtained similarly by replacing U with U^2 and $M_2(\Gamma_0(p),\mathbb{Q})^U \otimes_{\mathbb{Q}} \mathbb{Q}_p$ with $M_2(\Gamma_0(p),\mathbb{Q}) \otimes_{\mathbb{Q}} K_{\mathfrak{p}}$. □

Proof of Corollary 1.4. Because the form given by (9), which we here denote g, is in $M_2(\Gamma_0(p),\mathbb{Q})^U$, it can be written as a linear combination of cusp forms in $M_2(\Gamma_0(p),\mathbb{Q})^U$ and the p-adic Eisenstein series E_2^* (see Example 1.6 of [8]). The ratio of $a_0(g)$ to $a_m(g)$ is therefore equal to the same

ratio for E_2^*. This ratio is $(p-1)/(24\sigma_1(m))$ when $p \nmid m$, so the corollary follows when we set $g = \mathcal{H}_d(j)$. □

4. Discussion and Examples

We first consider for which primes p we can apply Corollary 1.4. For primes $p \in \{5, 7, 13\}$, the vector space $M_2(\Gamma_0(p), \mathbb{Q})^U$ is one-dimensional, so the corollary holds for any m. Taking $m = 1$ gives the result of Bruinier, Kohnen, and Ono (see Theorem 9 of [2]). When $p \in \{11, 17, 19\}$, the modular curves $X_0(p)$ are elliptic and the corresponding single cusp form generates $S_2(\Gamma_0(p))^U$. By a theorem of Elkies [5], in these cases the m^{th} Fourier coefficient of the cusp form is zero for infinitely many relatively prime m. For primes p greater than 19, the situation is less clear; the only such primes under 100 for which an appropriate $m \leq 1000$ exists are $23, 37, 43$, and 73. Using the above ten primes p, as well as $p = 2, 3$, for which similar results hold (see [2]), we can write the class numbers for all fundamental discriminants $0 > -d > -25016$ as single trace limits.

For a given discriminant $-d$, we may not be able to find a prime p and an integer m so that we can apply Corollary 1.4. However, we can still find explicit p-adic formulas for $H(d)$, because our bound $m_1, m_2, \ldots, m_n \leq \frac{p+1}{6}$ in Corollary 1.3 allows us to work in a finite-dimensional space of linear functionals. Also, we can explicitly calculate coefficients of forms in $M_2(\Gamma_0(p), \mathbb{Q})^U$ by using a basis of newforms.

We can give a lower bound for the rate of convergence of general trace limits. When f has rational coefficients, it easily follows from our proof of Theorem 1.2 that $\operatorname{ord}_\infty(f)$ is congruent to its t^{th} convergent $-\frac{k}{12} + \sum_{i=1}^{n} c_i \operatorname{Tr}_{m_i p^t}(f)$ modulo p^{t+1}. Specializing to the case in Corollary 1.3, we obtain congruences for $H(d)$ modulo any power of p. For sufficiently high powers of p, such a congruence determines the class number explicitly because $H(d)$ is well known to be bounded above by $\frac{1}{\pi}\sqrt{d}\log d$ for $d > 4$.

Example 1. Suppose $d = 20$ and $p = 19$: because $\left(\frac{-20}{19}\right) = -1$, $(19, 20)$ is tractable. We can verify that Corollary 1.4 applies with $m = 2$. The zeroth convergent then is

$$\frac{1}{4}\operatorname{Tr}_2(20) = 399294607884 \equiv 2 \pmod{19}.$$

and the first convergent is

$$\begin{aligned}\frac{1}{4}\operatorname{Tr}_{38}(20) =& 18266226519446348115204660277104564227269462784064395511752463092982158966327448120502564423526806634683797423097552321975639256938427043721099687796440314343491118109605350411415091889138488256864091462653047289851799019029737576 80\\ \equiv& 2 \pmod{19^2}.\end{aligned}$$

Example 2. Suppose $d = 163$ and $p = 23$. We could apply Corollary 1.4 with $m = 43$, but we instead observe that Corollary 1.3 applies with $n = 3$, $m_i = i$ for $i = 1, 2, 3$, and $c_1 = c_3 = \frac{1}{12}$, $c_2 = \frac{1}{6}$. The zeroth convergent then is

$$\begin{aligned}&\frac{1}{12}(\operatorname{Tr}_1(163) + 2\operatorname{Tr}_2(163) + \operatorname{Tr}_3(163))\\ &= -150796880180454255531363078825374126558301656982968 2 \equiv 1 \pmod{23},\end{aligned}$$

so $H(163) \equiv 1 \pmod{23}$. The upper bound on the size of $H(d)$ gives that $H(163) \leq 20$, and so we have $H(163) = 1$.

5. The Supersingular Connection

Recall that an elliptic curve E over a field K of characteristic $p > 0$ is called *supersingular* if $E(\overline{K})$ has no p-torsion. The supersingular polynomial for a prime p is then the polynomial in $\mathbb{F}_p[X]$ defined by

$$S_p(X) := \prod_{E/\overline{\mathbb{F}}_p \text{ supersingular}} (X - j(E)).$$

The work of Deuring on supersingular j-invariants (see Theorem 7.25 of [7]) implies that for fundamental discriminants $-d$,

$$\mathcal{H}_d(X) \mid S_p(X)^{H(d)} \text{ in } \mathbb{F}_p[X] \tag{10}$$

when p is inert or ramified in $\mathbb{Q}(\sqrt{-d})$. We define a homomorphism $\mathfrak{L} : \mathbb{Z}_p((q))^\times \to \mathbb{Z}_p[[q]]^+$ by

$$\mathfrak{L}(f) = \lim_{n\to\infty} \left(\frac{\Theta f}{f}\right)|U^n.$$

It follows easily from Lemma 3.3 that $\mathfrak{L}(f)$ depends only on the reduction of f mod p. By (10), the reduction mod p of $\mathcal{H}_d(j)$ lies in a finitely generated subgroup of $\mathbb{F}_p((q))$ spanned by $\mathfrak{L}(P_i(j))$, where P_i runs over the irreducible factors of $S_p(X)$, so $\mathfrak{L}(\mathcal{H}_d(j))$ lies in the corresponding finite-dimensional subspace of $\mathbb{Q}_p[[q]]$.

From this fact, one immediately obtains an ineffective version of Corollary 1.3 without invoking the theory of p-adic modular forms. This approach gives only a nonconstructive proof that a_0 is a linear combination of the a_m. It does not give any explicit information about the nature of the coefficients of such a linear combination. Similar nonconstructive arguments apply to the case of a general modular form with a Heegner divisor.

We can also use the methods from Section 3 to study the supersingular polynomial and its factorization in $\mathbb{F}_p[X]$. We first state a more general proposition that we will apply to factors of the supersingular polynomial.

Proposition 5.1. *Let $\mathcal{O}_p$ be the ring of integers of a finite extension K_p of $\mathbb{Q}_p$. If $f \in \mathcal{O}_p((q))^\times$ with leading coefficient 1 is such that $\frac{\Theta f}{f}$ is a p-adic modular form of weight 2, then the extension of $\mathbb{Q}_p$ generated by the coefficients of f has residue field $\mathbb{F}_p$ or $\mathbb{F}_{p^2}$.*

Proof. By the usual argument, reminiscent of that of Serre in [8], Lemma 3, $\lim_{t\to\infty} \frac{\Theta f}{f}|U^{2t}$ exists and lies in $M_2(\Gamma_0(p), \mathbb{Q}) \otimes K_p$, and the same is true if we replace $2t$ by $2t+1$ (although the limit might be different). By the identity (8),

$$\lim_{t\to\infty} a_{p^t m}\left(\frac{\Theta(f(z)^{p^2}/f(p^2z))}{f(z)^{p^2}/f(p^2z)}\right) = p^2 \lim_{t\to\infty} a_m\left(\frac{\Theta f(z)}{f(z)}|U^t - \frac{\Theta f(z)}{f(z)}|U^{t-2}\right) = 0$$

for all positive integers m. Let $g = \frac{f(z)^{p^2}}{f(p^2z)}$. We claim that $g \equiv 1 \pmod{\mathfrak{p}}$, where $\mathfrak{p}$ is the maximal ideal of $\mathcal{O}_p$. Assuming this claim for the moment, we observe that this implies $a_m(f)^{p^2} \equiv a_m(f) \bmod \mathfrak{p}$ for each m, which is equivalent to the desired result.

We now prove the claim. Suppose for contradiction that $a_m(g) \notin \mathfrak{p}$ for some $m > 0$. Take m to be minimal and replace g by $g' = 1 + \sum_{n=m}^\infty a_n(g)q^n$. By Lemma 3.3 $\lim_{t\to\infty} a_{p^t m}\left(\frac{\Theta g'}{g'}\right) = \lim_{t\to\infty} a_{p^t m}\left(\frac{\Theta g}{g}\right) = 0$. However,

$$a_{p^t m}\left(\frac{\Theta g'}{g'}\right) = -a_{p^t m}\left(\Theta\left(\sum_{i=1}^\infty \frac{(1-g')^i}{i}\right)\right) = -m\left(p^t a_{p^t m}\left(\sum_{i=1}^{p^t-1} \frac{(1-g')^i}{i}\right) + (-a_m(g))^{p^t}\right).$$

Thus $v_p\left(a_{p^t m}\left(\frac{\Theta g'}{g'}\right)\right) = v_p(m)$ for all t, contradicting the fact that $a_{p^t m} \to 0$. □

We use this proposition to give a new proof of known results about the irreducible factors of the supersingular polynomial.

Theorem 5.2. *The supersingular polynomial $S_p(X)$ splits completely over $\mathbb{F}_{p^2}$, and the number of irreducible factors of $S_p(X)$ over $\mathbb{F}_p$ is equal to $\dim M_2(\Gamma_0(p), \mathbb{Q})^U$.*

Proof. Suppose $\alpha \in \overline{\mathbb{F}}_p$ is a root of $S_p(X)$, and let $a \in \mathcal{O}$ be a lifting of α into the ring of integers of some number field. Using well-known facts (for example, see [6]) relating the supersingular polynomial to the mod p reduction of the Eisenstein series E_{p-1}, we can easily determine that the hypotheses in Theorem 4.15 of [7] hold with $f = j - a$. Thus $\frac{\Theta f}{f}$ is a p-adic modular form of weight 2, so by the previous proposition we have $\alpha \in \mathbb{F}_{p^2}$.

Thus the supersingular polynomial splits as a product of l_1 linear and l_2 quadratic factors over $\mathbb{F}_p$. It is well-known that the degree $l_1 + 2l_2$ of S_p is equal to $\dim(M_2(\Gamma_0(p)), \mathbb{Q}) = \dim M_{p+1}$, so it suffices to show that $\dim(M_2(\Gamma_0(p), \mathbb{Q})^U) \geq l_1 + l_2$ and $\dim(M_2(\Gamma_0(p), \mathbb{Q})^{-U}) \geq l_2$. The first of these inequalities follows immediately from the fact that the homomorphism $\mathfrak{L}$ is well-defined and injective on the multiplicative group generated by the irreducible factors of S_p. For the second inequality, suppose that $(X - \alpha)(X - \bar{\alpha})$ is an irreducible factor of S_p over $\mathbb{F}_p$. Then we can iterate the operator $-U$ on $\Theta(\frac{j-\alpha}{j-\bar{\alpha}})/\frac{j-\alpha}{j-\bar{\alpha}}$. By analogous arguments, this iteration will converge to a p-adic modular form fixed by $-U$, and this process produces l_2 linearly independent elements of $M_2(\Gamma_0(p), \mathbb{Q})^{-U}$. □

References

1. R. E. Borcherds, *Automorphic forms on* $\mathrm{O}_{s+2,2}(\mathbf{R})^+$ *and generalized Kac-Moody algebras*, Proceedings of the International Congress of Mathematicians, Vol. 1, 2 (Zürich, 1994) (Basel), Birkhäuser, 1995, pp. 744–752.
2. J. H. Bruinier, W. Kohnen, and K. Ono, *The arithmetic of the values of modular functions and the divisors of modular forms*, Compos. Math. **140** (2004), no. 3, 552–566.
3. J. H. Bruinier and K. Ono, *The arithmetic of Borcherds' exponents*, Math. Ann. **327** (2003), no. 2, 293–303.
4. M. Deuring, *Die Typen der Multiplikatorenringe elliptischer Funktionenkörper*, Abh. Math. Sem. Hansischen Univ. **14** (1941), 197–272.
5. N. D. Elkies, *The existence of infinitely many supersingular primes for every elliptic curve over* **Q**, Invent. Math. **89** (1987), no. 3, 561–567.
6. 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 Stud. Adv. Math., vol. 7, Amer. Math. Soc., Providence, RI, 1998, pp. 97–126.
7. K. Ono, *The web of modularity: arithmetic of the coefficients of modular forms and q-series*, CBMS Regional Conference Series in Mathematics, vol. 102, Published for the Conference Board of the Mathematical Sciences, Washington, DC, 2004.
8. J.-P. Serre, *Formes modulaires et fonctions zêta p-adiques*, Modular functions of one variable, III (Proc. Internat. Summer School, Univ. Antwerp, 1972), Springer, Berlin, 1973, pp. 191–268. Lecture Notes in Math., Vol. 350.
9. H. P. F. Swinnerton-Dyer, *On l-adic representations and congruences for coefficients of modular forms*, Modular functions of one variable, III (Proc. Internat. Summer School, Univ. Antwerp, 1972), Springer, Berlin, 1973, pp. 1–55. Lecture Notes in Math., Vol. 350.
10. D. Zagier, *Traces of singular moduli*, Motives, polylogarithms and Hodge theory, Part I (Irvine, CA, 1998), Int. Press Lect. Ser., vol. 3, Int. Press, Somerville, MA, 2002, pp. 211–244.

PO Box 11934, Stanford, CA 94309
E-mail address: cerickson@stanford.edu

320 Dunster House Mail Center, Cambridge, MA 02138
E-mail address: miller5@fas.harvard.edu

741 Echo Road, Vestal, NY 13850
E-mail address: apixton@princeton.edu