Compositio Math. 141 (2005) 293–312
DOI: 10.1112/S0010437X04001198

Arithmetic of singular moduli and class polynomials

Scott Ahlgren and Ken Ono

Abstract

We investigate divisibility properties of the traces and Hecke traces of singular moduli. In particular we prove that, if p is prime, these traces satisfy many congruences modulo powers of p which are described in terms of the factorization of p in imaginary quadratic fields. We also study generalizations of Lehner's classical congruences $j(z)|U_p \equiv 744 \pmod{p}$ (where $p \leqslant 11$ and $j(z)$ is the usual modular invariant), and we investigate connections between class polynomials and supersingular polynomials in characteristic p.

1. Introduction and statement of results

Let

$$j(z) = q^{-1} + 744 + 196\,884q + 21\,493\,760q^2 + \cdots \in \frac{1}{q}\mathbb{Z}[[q]]$$

denote the usual elliptic modular function on $\mathrm{SL}_2(\mathbb{Z})$ ($q := e^{2\pi iz}$ throughout). The values of $j(z)$ at imaginary quadratic arguments in the upper half of the complex plane are known as *singular moduli;* two important examples are the evaluations

$$j(i) = 1728 \quad \text{and} \quad j\left(\frac{1+\sqrt{-3}}{2}\right) = 0. \tag{1.1}$$

Singular moduli are algebraic integers which play many important roles in classical and modern number theory. For example, they generate ring class field extensions of imaginary quadratic fields. Also, the work of Deuring [Deu58, Deu46] highlights their deep connections with the theory of elliptic curves with complex multiplication. In recent work, Borcherds [Bor95a, Bor95b] used them to define an important class of automorphic forms possessing certain striking infinite product expansions.

There is a vast amount of literature on the computation of singular moduli which dates back to the works of Kronecker; this includes the classical calculations of Berwick [Ber28] and Weber [Web61]. In more recent work, Gross and Zagier [GZ85] computed exactly the prime factorization of the absolute norm of suitable differences of singular moduli (further work in this direction has been carried out by Dorman [Dor89, Dor88]).

In this paper we investigate the divisibility properties of the traces and Hecke traces of singular moduli in terms of the factorization of primes in imaginary quadratic fields. We begin by fixing notation. Throughout, d denotes a positive integer congruent to 0 or 3 modulo 4 (so that $-d$ is the discriminant of an order in an imaginary quadratic field). Denote by $\mathcal{Q}_d$ the set of positive definite integral binary quadratic forms

$$Q(x, y) = ax^2 + bxy + cy^2$$

Received 29 April 2003, accepted in final form 14 May 2004, published online 10 February 2005.
2000 Mathematics Subject Classification 11F33, 11F37 (primary).
Keywords: singular moduli, class polynomials, modular forms.
The first author thanks the National Science Foundation for its support through grant DMS 01-34577. The second author is supported by the National Science Foundation, a Guggenheim Fellowship, a Packard Research Fellowship, and an H. I. Romnes Fellowship.

with discriminant $-d = b^2 - 4ac$. For each Q let α_Q be the unique complex number in the upper half-plane which is a root of $Q(x, 1)$; the singular modulus $j(\alpha_Q)$ depends only on the equivalence class of Q under the action of $\Gamma := \mathrm{PSL}_2(\mathbb{Z})$.

We define the *class polynomial of discriminant* $-d$ as

$$\mathcal{H}_d(x) := \prod_{Q \in \mathcal{Q}_d/\Gamma} (x - j(\alpha_Q)) \in \mathbb{Z}[x].$$

This is a mild departure from the customary definition since the product above is taken over all Q with discriminant $-d$, not just the primitive ones (note also the mild departure from the definition in [Zag02]). Nevertheless, if $-d$ is a fundamental discriminant, then $\mathcal{H}_d(x)$ is the minimal polynomial of each $j(\alpha_Q)$ over $\mathbb{Q}$.

Define $\omega_Q \in \{1, 2, 3\}$ by

$$\omega_Q := \begin{cases} 2 & \text{if } Q \sim_\Gamma [a, 0, a], \\ 3 & \text{if } Q \sim_\Gamma [a, a, a], \\ 1 & \text{otherwise.} \end{cases}$$

Let $J(z)$ be the Hauptmodul

$$J(z) := j(z) - 744 = q^{-1} + 196\,884q + 21\,493\,760q^2 + \cdots .$$

Then, following Zagier [Zag02], define the trace of the singular moduli of discriminant $-d$ by

$$t(d) := \sum_{Q \in \mathcal{Q}_d/\Gamma} \frac{J(\alpha_Q)}{\omega_Q} = \sum_{Q \in \mathcal{Q}_d/\Gamma} \frac{j(\alpha_Q) - 744}{\omega_Q}.$$

We also consider more general Hecke traces; these are defined in terms of a natural sequence of modular functions. Let $J_0(z) := 1$, and for positive integers m define $J_m(z)$ by

$$J_m(z) = J(z)|T_0(m), \tag{1.2}$$

where $T_0(m)$ is the normalized weight zero Hecke operator of index m. Each $J_m(z)$ is a monic polynomial in $j(z)$ of degree m with integer coefficients; the first few are

$$\begin{aligned} J_0(z) &= 1, \\ J_1(z) &= j(z) - 744 = J(z), \\ J_2(z) &= j(z)^2 - 1488j(z) + 159\,768 = q^{-2} + 42\,987\,520q + \cdots . \end{aligned}$$

Then, for each positive integer m, we define the mth Hecke trace of the singular moduli of discriminant $-d$ as the integer

$$t_m(d) := \sum_{Q \in \mathcal{Q}_d/\Gamma} \frac{J_m(\alpha_Q)}{\omega_Q}.$$

Zagier [Zag02] showed that these traces $t_m(d)$ are determined as the coefficients of a certain sequence of meromorphic modular forms on $\Gamma_0(4)$ (see § 3 for details). Note that $t_1(d) = t(d)$; for convenience, we define $t_m(n) := 0$ for every positive integer $n \equiv 1, 2 \pmod 4$.

Remark. For fundamental discriminants $-d$, let $h(-d)$ denote the class number of primitive positive definite binary quadratic forms of discriminant $-d$. Then the values $t_m(d)$ for $0 \leqslant m \leqslant h(-d)$ determine the respective power sums in the $j(\alpha_Q)$. Therefore, these Hecke traces completely determine the polynomial $\mathcal{H}_d(x)$.

Our first result shows that these traces satisfy many striking congruences based on the factorization of primes in certain imaginary quadratic fields.

THEOREM 1.1. *Suppose that p is an odd prime and that s and m are positive integers with $p \nmid m$. Then the following are true.*

(1) *If n is a positive integer for which p splits in $\mathbb{Q}(\sqrt{-n})$, then*
$$t_m(p^2 n) \equiv 0 \pmod{p}.$$
(2) *A positive proportion of the primes ℓ have the property that*
$$t_m(\ell^3 n) \equiv 0 \pmod{p^s}$$
for every positive integer n coprime to ℓ such that p is inert or ramified in $\mathbb{Q}(\sqrt{-n\ell})$.
(3) *A positive proportion of the primes ℓ have the property that*
$$t_m(\ell^2 n) \equiv t_m(n)\left(2 - \left(\frac{-n}{\ell}\right)\right) \pmod{p^s}$$
for every positive integer n with $\ell^2 \nmid n$ such that p is inert or ramified in $\mathbb{Q}(\sqrt{-n})$.

Remarks.

(1) It would be interesting to find a natural description of the primes ℓ which arise in the second and third parts of Theorem 1.1.
(2) If $-d$ is a fundamental discriminant and ℓ is a prime, then the class numbers $h(-d)$ and $h(-\ell^2 d)$ are related by the formula
$$h(-\ell^2 d) = h(-d) \cdot \left(\ell - \left(\frac{-d}{\ell}\right)\right).$$
Note the resemblance between this formula and the congruences in the third part of Theorem 1.1.
(3) The proof of the second (respectively, third) part of Theorem 1.1 shows that the primes ℓ can be chosen from the arithmetic progression $-1 \pmod{4p^s}$ (respectively, $1 \pmod{4p^s}$).

Here we give some examples of the phenomena described in Theorem 1.1.

Example 1.2. For each $p \leqslant 11$, the maximal congruence modulus in the first part of Theorem 1.1 exceeds p; these moduli are 729, 125, 49, and 121. If $p = 7$, for example, then for every non-negative integer n we have
$$t_1(343n + 147) \equiv t_1(343n + 245) \equiv t_1(343n + 294) \equiv 0 \pmod{49}.$$

Example 1.3. As an example of the phenomenon described in the second part of Theorem 1.1, we have
$$t_1(13^3 n) \equiv 0 \pmod{7}$$
for every positive integer n coprime to 13 with $\left(\frac{-13n}{7}\right) \neq 1$.

Example 1.4. As an example of the third part of Theorem 1.1, we have, for each positive integer n such that $\left(\frac{-n}{7}\right) \neq 1$ and $29^2 \nmid n$, the congruence
$$t_1(29^2 n) \equiv t_1(n)\left(2 - \left(\frac{-n}{29}\right)\right) \pmod{7}.$$

In the second part of the paper we turn to a study of the arithmetic properties of the class polynomial $\mathcal{H}_d(x)$. If p is prime, then let $\mathbb{F}_p[x]$ denote the polynomial ring over the finite field with p elements. For fundamental discriminants $-d$, it is natural to study the factorizations of $\mathcal{H}_d(x)$ over $\mathbb{F}_p[x]$. This question is of particular interest for those primes p which are inert or ramified in $\mathbb{Q}(\sqrt{-d})$; for such p a theorem of Deuring (see, for example, Theorem 12 of [Lan87, § 13.4]) implies

that each root of $\mathcal{H}_d(x)$ over $\overline{\mathbb{F}}_p[x]$ is the j-invariant of a supersingular elliptic curve in characteristic p (this fact is an essential ingredient in Elkies' proof [Elk87] that every elliptic curve over $\mathbb{Q}$ has infinitely many supersingular primes).

In view of this, it is natural to seek a general description, for arbitrary primes p, of the set of $-d$ for which the distinct roots of $\mathcal{H}_d(x)$ in $\overline{\mathbb{F}}_p$ form the complete set of supersingular j-invariants in characteristic p. Using a result of Koike (which is related to work of Dwork and Deligne on the p-adic rigidity of $j(z)$) we show in Theorem 1.5 below that this question is closely related to the problem of classifying certain congruences for the Fourier coefficients of nearly holomorphic modular functions.

We recall that a modular form on a congruence subgroup Γ' is called *nearly holomorphic* if its poles (if there are any) are supported at the cusps of Γ'. Every non-zero nearly holomorphic modular function $f(z)$ on $\mathrm{SL}_2(\mathbb{Z})$ is a polynomial in $j(z)$ and has a Fourier expansion of the form

$$f(z) = \sum_{n \geqslant n_0} a(n) q^n,$$

where $n_0 \leqslant 0$ and $a(n_0) \neq 0$. We define the operator U_p by

$$f(z)|U_p := \sum_{n=-\infty}^{\infty} a(pn) q^n.$$

For nearly holomorphic modular forms with integral coefficients, we consider congruences of the form

$$f(z)|U_p \equiv a(0) \pmod{p}. \tag{1.3}$$

Perhaps the most famous congruences of the form (1.3) are due to Lehner [Leh49], who proved that if $p \leqslant 11$ is prime, then

$$j(z)|U_p \equiv 744 \pmod{p}. \tag{1.4}$$

To state our first result in this context, it is convenient to make the following definition. If $p \leqslant 11$ is prime, then let $S_p(x) := 1$, and for $p > 11$ define $S_p(x) \in \mathbb{F}_p[x]$ by

$$S_p(x) := \prod_{\substack{E/\overline{\mathbb{F}}_p \text{ supersingular} \\ j(E) \notin \{0,1728\}}} (x - j(E)), \tag{1.5}$$

where the product is taken over $\overline{\mathbb{F}}_p$-isomorphism classes of supersingular elliptic curves E. It is well known that the degree of $S_p(x)$ is $\lfloor p/12 \rfloor$. With this notation we have the following general result.

Theorem 1.5. *Let $F(x) \in \mathbb{Z}[x]$ be a polynomial of degree m, and let $p > m$ be a prime for which $F(x) \not\equiv 0 \pmod{p}$. If $S_p(x)^2$ divides $F(x)$ in $\mathbb{F}_p[x]$, then*

$$F(j(z))|U_p \equiv a(0) \pmod{p},$$

where $a(0)$ is the constant term in the Fourier expansion of $F(j(z))$.

Remarks.

(1) The converse is false in view of the fact that if the conclusion of the theorem holds for $F(x)$, then it holds for $F(x) + \alpha$ for every $\alpha \in \mathbb{F}_p$.

(2) Since $S_p(x) = 1$ for $p \leqslant 11$, Lehner's congruences (1.4) follow from Theorem 1.5.

For fundamental discriminants $-d$, define integers $c_d(n)$ by

$$\mathcal{H}_d(j(z)) = \sum_{n=-h(-d)}^{\infty} c_d(n) q^n.$$

After Theorem 1.5, it would be desirable to find a characterization of those primes p for which

$$\mathcal{H}_d(j(z))|U_p \equiv c_d(0) \pmod{p}. \tag{1.6}$$

Computations reveal many uniform sets of examples. For example, we have the following corollary.

COROLLARY 1.6. *If $-239 < -d < 0$ is a fundamental discriminant and $h(-d) < p < 6h(-d) - 1$ is a prime which is inert or ramified in $\mathbb{Q}(\sqrt{-d})$, then $S_p(x)^2$ divides $\mathcal{H}_d(x)$ in $\mathbb{F}_p[x]$ and*

$$\mathcal{H}_d(j(z))|U_p \equiv c_d(0) \pmod{p}.$$

The uniformity of the range of primes in Corollary 1.6 suggests that this phenomenon might hold in generality. However, this is not true; when $-d = -239$, we have

$$\mathcal{H}_{239}(j(z))|U_{79} \equiv 44 + 2q + 62q^2 + \cdots \pmod{79},$$

although 79 is inert in $\mathbb{Q}(\sqrt{-239})$ and $h(-239) = 15$. In this case $S_{79}(x)$ divides $\mathcal{H}_{239}(x)$ in $\mathbb{F}_{79}[x]$, but the supersingular j-invariant $j = -15$ is a root of multiplicity only 1.

Another natural question to ask is whether or not, for those primes $p > h(-d)$ which are inert in $\mathbb{Q}(\sqrt{-d})$, the condition that $S_p(x)^2$ divides $\mathcal{H}_d(x)$ in $\mathbb{F}_p[x]$ is implied by a congruence of the form (1.6) (recall the first remark following Theorem 1.5). Computations reveal that the answer is affirmative for all fundamental discriminants $-d$ with $-700 < -d < 0$. However, further calculation reveals sporadic counterexamples (there are only three counterexamples with $d < 1000$; these are the cases when $(-d, p) = (-707, 47)$, $(-731, 79)$, and $(-767, 101)$). Nevertheless, this condition appears to be necessary for the vast majority of $-d$; for these $-d$ it is clear by comparing the degrees of $S_p(x)$ and $\mathcal{H}_d(x)$ that $\mathcal{H}_d(j(z))$ can satisfy the congruence (1.6) only for those inert primes p with

$$p \leqslant 6h(-d) + r_p, \quad \text{where } r_p \in \{1, 5, 7, 11\} \text{ has } r_p \equiv p \pmod{12}. \tag{1.7}$$

In view of (1.7), it is natural to seek an unconditional upper bound for those primes p which admit a congruence of the form (1.6). Here, as a special case of a result for nearly holomorphic modular forms on $\mathrm{SL}_2(\mathbb{Z})$, we show, for all $-d$, that (1.6) can only hold for those primes

$$p \leqslant 12h(-d) + 1.$$

To state our general result, some notation is required. If $k \geqslant 4$ is an even integer, then let M_k denote the space of weight k holomorphic modular forms on $\mathrm{SL}_2(\mathbb{Z})$. Furthermore, if p is prime, then let $M_{k,p}$ denote the set of reductions modulo p of those forms $f(z) \in M_k$ with integral coefficients. The *filtration* of a power series $f(z)$ whose reduction belongs to $M_{k',p}$ for some k' is defined by

$$\omega_p(f) := \inf\{k : f(z) \pmod{p} \in M_{k,p}\}.$$

Let $\Delta(z) := q\prod_{n=1}^{\infty}(1-q^n)^{24}$ be the unique normalized cusp form of weight 12 on $\mathrm{SL}_2(\mathbb{Z})$. We define the usual theta-operator on power series by

$$\Theta\Big(\sum_{n\geqslant n_0} a(n)q^n\Big) = \sum_{n\geqslant n_0} na(n)q^n. \tag{1.8}$$

Then we have the following theorem.

THEOREM 1.7. *Suppose that $f(z) = \sum_{n=m}^{\infty} a(n)q^n$ is a nearly holomorphic modular form of integral weight k on $\mathrm{SL}_2(\mathbb{Z})$ with integral coefficients. Furthermore, suppose that $p \geqslant \max(5, k - 12m)$ is a prime for which $p \nmid a(m)$ and $p \nmid m$. If there is a non-negative integer s for which $p^s + m > 0$ and*

$$\omega_p(\Theta f_{p,s}) \equiv 1, 2 \pmod{p},$$

where

$$f_{p,s}(z) := f(z) \cdot \Delta(z)^{p^s},$$

then $f(z)|U_p \not\equiv 0 \pmod{p}$.

As a corollary, we obtain the following.

Corollary 1.8. *Suppose that $F(x) \in \mathbb{Z}[x]$ is a polynomial of degree $D \geqslant 1$. If $p > 12D + 1$ is a prime which does not divide the leading coefficient of $F(x)$, then*

$$F(j(z))|U_p \not\equiv 0 \pmod{p}.$$

In particular, if $-d$ is a fundamental discriminant and p is a prime for which

$$\mathcal{H}_d(j(z))|U_p \equiv c_d(0) \pmod{p},$$

then $p \leqslant 12h(-d) + 1$.

We remark that, since $j(z)|U_{13} \not\equiv 744 \pmod{13}$, Corollary 1.8 implies that Lehner's list of congruences of the form (1.4) is complete. This recovers an observation of Serre (see (6.16) of [Ser76]).

In § 2 we record some preliminaries on modular forms. In § 3 we recall recent work of Zagier, and in § 4 we use the theory of integral and half-integral weight modular forms to prove Theorem 1.1. In § 5 we prove Theorem 1.5 and Corollary 1.6, and in § 6 we prove Theorem 1.7 and Corollary 1.8.

2. Preliminaries on modular forms

We begin by collecting some facts which we require on half-integral weight modular forms. For details on many of these facts one may consult, for example, [Kob84] or [Koh82]. If $f(z)$ is a function of the upper half-plane, $\lambda \in \frac{1}{2}\mathbb{Z}$, and $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2^+(\mathbb{R})$, then we define the usual slash operator by

$$f(z)|_\lambda \begin{pmatrix} a & b \\ c & d \end{pmatrix} := (ad - bc)^{\lambda/2}(cz + d)^{-\lambda} f\left(\frac{az + b}{cz + d}\right) \tag{2.1}$$

(we always take the branch of the square root having non-negative real part). If $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_0(4)$, then define

$$j(\gamma, z) := \left(\frac{c}{d}\right) \epsilon_d^{-1} \sqrt{cz + d}, \tag{2.2}$$

where

$$\epsilon_d := \begin{cases} 1 & \text{if } d \equiv 1 \pmod 4, \\ i & \text{if } d \equiv -1 \pmod 4. \end{cases} \tag{2.3}$$

If k is an integer and N is an odd positive integer, then we denote by $\mathcal{M}_{k+1/2}(\Gamma_0(4N))$ the infinite-dimensional vector space of nearly holomorphic modular forms of weight $k + 1/2$ on $\Gamma_0(4N)$; these are functions $f(z)$ which are holomorphic on the upper half-plane, meromorphic at the cusps, and which satisfy

$$f(\gamma z) = j(\gamma, z)^{2k+1} f(z) \quad \text{for all } \gamma \in \Gamma_0(4N). \tag{2.4}$$

As usual, we denote by $M_{k+1/2}(\Gamma_0(4N))$ (respectively, $S_{k+1/2}(\Gamma_0(4N))$) the finite-dimensional subspace of $\mathcal{M}_{k+1/2}(\Gamma_0(4N))$ consisting of those forms which are holomorphic (respectively, vanish) at the cusps. Finally, denote by $M^+_{k+1/2}(\Gamma_0(4N))$ and $\mathcal{M}^+_{k+1/2}(\Gamma_0(4N))$ the 'Kohnen plus-spaces' of holomorphic and nearly holomorphic forms which transform according to (2.4) and which, in addition, have a Fourier expansion of the form

$$\sum_{(-1)^k n \equiv 0,1 \pmod 4} a(n) q^n. \tag{2.5}$$

We next recall some facts on the expansions of modular forms at the cusps of a congruence subgroup; many of these can be found, for example, in [Mar96]. The cusps are represented by rational numbers a/c together with the point at infinity. We say that the cusps s_1 and s_2 are

equivalent under the congruence subgroup Γ' if there exists $\gamma' \in \Gamma'$ such that $s_1 = \gamma' s_2$; by a cusp of Γ' we typically mean an equivalence class of cusps under this relation.

If N is a positive integer, then a complete set of representatives for the cusps of $\Gamma_0(N)$ is

$$\left\{ \frac{a_c}{c} \in \mathbb{Q} \ : c \mid N, 1 \leqslant a_c \leqslant N, \gcd(a_c, N) = 1, \ a_c \text{ distinct } (\mathrm{mod}\, \gcd(c, N/c)) \right\}. \tag{2.6}$$

If $\gamma_1 \infty$ is a cusp of $\Gamma_0(4N)$ and $g \in \mathcal{M}_{k+1/2}(\Gamma_0(4N))$ is not identically zero, then at the cusp $\gamma_1\infty$ we have an expansion of the form

$$g|_{k+1/2}\gamma_1 = c \cdot q^{\alpha} + \cdots \quad \text{for some } \alpha \in \mathbb{Q} \text{ and } c \neq 0. \tag{2.7}$$

Moreover, if $\gamma_1\infty$ and $\gamma_2\infty$ are equivalent under $\Gamma_0(4N)$, then the first term in the expansion of $g|_{k+1/2}\gamma_2$ differs from (2.7) only by multiplication by some root of unity.

We now consider the cuspidal behavior of products and quotients of Dedekind's eta-function

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

(although only the integral weight case is discussed in [Mar96], similar facts hold in the half-integral weight case). Suppose that $f(z)$ is the eta-quotient $f(z) := \prod_{\delta|N} \eta^{r_\delta}(\delta z)$, and set $\lambda := \frac{1}{2}\sum_{\delta|N} r_\delta \in \frac{1}{2}\mathbb{Z}$. Then for $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$, we have an expansion of the form

$$f(z)|_\lambda \gamma = \xi \cdot q^{\tau(c)} \left(1 + \sum_{n=1}^{\infty} \alpha(n) q^{n/\beta} \right), \tag{2.8}$$

where $\xi \neq 0$ is an algebraic number, the coefficients $\alpha(n)$ are algebraic, $\beta \in \mathbb{N}$, and

$$\tau(c) := \frac{1}{24} \sum_{\delta|N} \frac{(\delta, c)^2}{\delta} r_\delta. \tag{2.9}$$

Finally, we remark that to explicitly compute the expansion (2.8), we can use the fact that, for each $\gamma \in \mathrm{SL}_2(\mathbb{Z})$, we have the transformation formula

$$\eta(z)|_{1/2}\gamma = \epsilon_\gamma \cdot \eta(z), \tag{2.10}$$

where ϵ_γ is a root of unity. Also, for any $\delta \in \mathbb{N}$ and $\gamma \in \mathrm{SL}_2(\mathbb{Z})$, there exist a matrix $\gamma' \in \mathrm{SL}_2(\mathbb{Z})$ and a matrix $\left(\begin{smallmatrix} A & B \\ 0 & D \end{smallmatrix}\right)$, where B is an integer and A and D are positive integers, such that $\left(\begin{smallmatrix} \delta & 0 \\ 0 & 1 \end{smallmatrix}\right)\gamma = \gamma'\left(\begin{smallmatrix} A & B \\ 0 & D \end{smallmatrix}\right)$. By using this fact together with (2.10), one can compute, up to a root of unity, the value of ξ appearing in (2.8).

We briefly recall some properties of the Hecke operators on the spaces $\mathcal{M}^+_{k+1/2}(\Gamma_0(4N))$ (these definitions are given in [Koh82] for holomorphic forms, but the situation is the same if we allow poles at the cusps). Suppose that ℓ is a prime with $\ell \nmid N$ (note that this does not necessarily exclude $\ell = 2$). Then the action of the Hecke operator $T_{k+1/2,4N}(\ell^2)$ on a modular form

$$f(z) := \sum_{(-1)^k n \equiv 0,1 \pmod 4} a(n) q^n \in \mathcal{M}^+_{k+1/2}(\Gamma_0(4N)) \tag{2.11}$$

is given by

$$f(z)|T_{k+1/2,4N}(\ell^2) := \sum_{(-1)^k n \equiv 0,1 \pmod 4} \left(a(\ell^2 n) + \left(\frac{(-1)^k n}{\ell} \right) \ell^{k-1} a(n) + \ell^{2k-1} a\left(\frac{n}{\ell^2} \right) \right) q^n. \tag{2.12}$$

Then, for each positive m coprime to N, the operator $T_{k+1/2,4N}(m^2)$ on $\mathcal{M}^+_{k+1/2}(\Gamma_0(4N))$ can be expressed as a polynomial in the operator $T_{k+1/2,4N}(\ell^2)$ via the usual multiplicative relations.

If $f(z)$ is as in (2.11) and χ is a quadratic Dirichlet character with conductor α, then we have the quadratic twist

$$f \otimes \chi := \sum_{(-1)^k n \equiv 0,1 \pmod 4} \chi(n) a(n) q^n \in \mathcal{M}^+_{k+1/2}(\Gamma_0(4N\alpha^2)). \tag{2.13}$$

Suppose now that $f(z)$ is as in (2.11) and that χ is a quadratic character with conductor α, where m is coprime to $N\alpha$. Then, combining (2.12) with (2.13) and the fact that the operators $T_{k+1/2,4N\alpha^2}(\ell^2)$ with $\ell \nmid N\alpha$ generate the Hecke algebra on $\mathcal{M}^+_{k+1/2}(\Gamma_0(4N\alpha^2))$, we see that

$$(f \otimes \chi)|T_{k+1/2,4N\alpha^2}(m^2) = (f|T_{k+1/2,4N}(m^2)) \otimes \chi. \tag{2.14}$$

3. Zagier's formulas

To prove Theorem 1.1, we make use of recent work of Zagier [Zag02] on the traces of singular moduli. We begin by recalling Zagier's results on two particular sequences of nearly holomorphic modular forms. Let $\theta_1(z)$ and $E_4(z)$ be defined by

$$E_4(z) := 1 + 240 \sum_{n=1}^{\infty} \frac{n^3 q^n}{1-q^n},$$

$$\theta_1(z) := \frac{\eta^2(z)}{\eta(2z)} = \sum_{n=-\infty}^{\infty} (-1)^n q^{n^2} = 1 - 2q + 2q^4 - 2q^9 + \cdots .$$

Then let $g_1(z) \in \mathcal{M}^+_{3/2}(\Gamma_0(4))$ be the nearly holomorphic modular form defined by

$$g_1(z) := \frac{\theta_1(z) E_4(4z)}{\eta^6(4z)} = q^{-1} - 2 + \sum_{0<d\equiv 0,3 \pmod 4} B(1,d) q^d = q^{-1} - 2 + 248q^3 - 492q^4 + \cdots . \tag{3.1}$$

More generally, if $D \equiv 0, 1 \pmod 4$ is a positive integer, then let $g_D(z)$ denote the unique element of $\mathcal{M}^+_{3/2}(\Gamma_0(4))$ whose Fourier expansion has the form

$$g_D(z) = q^{-D} + B(D,0) + \sum_{0<d\equiv 0,3 \pmod 4} B(D,d) q^d.$$

(The existence and uniqueness of these forms is discussed in § 4 of [Zag02]).

Similarly, for a non-negative integer $d \equiv 0, 3 \pmod 4$, let $f_d(z)$ be the unique form in $\mathcal{M}^+_{1/2}(\Gamma_0(4))$ whose expansion has the form

$$f_d(z) = q^{-d} + \sum_{0<D\equiv 0,1 \pmod 4} A(D,d) q^D.$$

Existence and uniqueness follow from Lemma 14.2 of [Bor95a]; see also § 4 of [Zag02]. All of the coefficients of each $f_d(z)$ and $g_D(z)$ are integers.

For each $m \geqslant 1$ and each pair of integers $D \equiv 0, 1 \pmod 4$ and $0 \leqslant d \equiv 0, 3 \pmod 4$, define integers $A_m(D,d)$ and $B_m(D,d)$ in the following manner:

$$A_m(D,d) := \text{ the coefficient of } q^D \text{ in } f_d(z)|T_{1/2,4}(m^2),$$
$$B_m(D,d) := \text{ the coefficient of } q^d \text{ in } g_D(z)|T_{3/2,4}(m^2).$$

For $D = 1$ and $m \geqslant 1$ (see (19) of [Zag02]) we have

$$A_m(1,d) = \sum_{n|m} n A(n^2, d). \tag{3.2}$$

Using this notation, Zagier [Zag02, Theorem 5] proved the following result.

THEOREM 3.1. *The following are true.*

(1) *If $m \geqslant 1$ and $0 < d \equiv 0, 3 \pmod 4$, then*

$$t_m(d) = -B_m(1, d).$$

(2) *If $m \geqslant 1$, $0 < D \equiv 0, 1 \pmod 4$, and $0 \leqslant d \equiv 0, 3 \pmod 4$, then*

$$A_m(D, d) = -B_m(D, d).$$

Example. As an illustration of the first part of Theorem 3.1, we compare the coefficients on q^3 and q^4 in (3.1) with the following values (which are computed using (1.1)):

$$t_1(3) = \frac{j((1+\sqrt{-3})/2) - 744}{3} = -248,$$
$$t_1(4) = \frac{j(i) - 744}{2} = 492.$$

4. Proof of Theorem 1.1

We now turn to the proof of Theorem 1.1. The proof of the first part follows easily from Zagier's work.

Proof of Theorem 1.1(1). Since $p \nmid m$, a calculation using the definition (2.12) and the first part of Theorem 3.1 shows that it suffices to prove Theorem 1.1(1) in the case where $m = 1$. Suppose that n is a positive integer for which $(\frac{-n}{p}) = 1$. By (2.12) and Theorem 3.1, we have

$$\begin{aligned} t_1(p^2 n) &= -B_1(1, p^2 n) \\ &= -B_p(1, n) + \left(\frac{-n}{p}\right) B_1(1, n) + pB_1\left(1, \frac{n^2}{p}\right) \\ &\equiv -B_p(1, n) + B_1(1, n) \pmod p. \end{aligned}$$

Then, using the second part of Theorem 3.1 and (3.2), we obtain

$$\begin{aligned} t_1(p^2 n) &\equiv A_p(1, n) + B_1(1, n) \\ &\equiv A_1(1, n) + pA_1(p^2, n) + B_1(1, n) \\ &\equiv A_1(1, n) + B_1(1, n) \\ &\equiv -B_1(1, n) + B_1(1, n) \equiv 0 \pmod p. \end{aligned}$$

This establishes the first claim in Theorem 1.1. □

The proofs of the second and third parts of Theorem 1.1 are more involved. To begin, for each odd prime p we define

$$h_{1,p} := g_1 - \left(\frac{-1}{p}\right) g_1 \otimes \left(\frac{\bullet}{p}\right) \in \mathcal{M}^+_{3/2}(\Gamma_0(4p^2)). \tag{4.1}$$

Using (3.1) and Theorem 3.1, we find that

$$h_{1,p}(z) = -2 - \sum_{\substack{0 < d \equiv 0,3 \pmod 4 \\ p \mid d}} t_1(d) q^d - 2 \sum_{\substack{0 < d \equiv 0,3 \pmod 4 \\ (\frac{-d}{p}) = -1}} t_1(d) q^d. \tag{4.2}$$

We next define, for each positive integer m with $p \nmid m$, the modular form

$$h_{m,p}(z) := h_{1,p} | T_{3/2, 4p^2}(m^2) \in \mathcal{M}^+_{3/2}(\Gamma_0(4p^2)). \tag{4.3}$$

Using (2.14), (4.2), (4.3) and Theorem 3.1, we see that for some integer $c_{m,p}$ we have

$$\begin{aligned} h_{m,p}(z) &= g_1|T_{3/2,4}(m^2) - \left(\frac{-1}{p}\right)\cdot (g_1|T_{3/2,4}(m^2)) \otimes \left(\frac{\bullet}{p}\right) \\ &= c_{m,p} - \sum_{\substack{0<d\equiv 0,3 \pmod 4 \\ p|d}} t_m(d)q^d - 2\sum_{\substack{0<d\equiv 0,3 \pmod 4 \\ (\frac{-d}{p})=-1}} t_m(d)q^d. \end{aligned} \tag{4.4}$$

We require the following crucial result.

Theorem 4.1. *Suppose that $p \geqslant 3$ is prime, and that s and m are positive integers with $p \nmid m$. Then there exists an integer $\beta \geqslant s-1$ and a holomorphic modular form $f_{m,p,s}(z) \in M^+_{3/2+(p^\beta(p^2-1))/2}(\Gamma_0(4p^2))$ with the property that*

$$f_{m,p,s}(z) \equiv h_{m,p}(z) \pmod{p^s}.$$

To prove Theorem 4.1, we employ the following lemma.

Lemma 4.2. *The form $h_{1,p}(z)$ defined in (4.1) is a nearly holomorphic modular form on $\Gamma_0(4p^2)$ which is holomorphic on the upper half-plane and at the cusps $1/p^2$ and $1/4p^2$, and which vanishes at the cusp $1/2p^2$.*

Proof. Using (4.1) and (2.13), we see that $h_{1,p}(z)$ is a modular form on $\Gamma_0(4p^2)$. From (3.1) and (4.2) it is clear that $h_{1,p}$ is holomorphic on the upper half-plane and at $1/4p^2$ (which is equivalent to ∞ under $\Gamma_0(4p^2)$).

Therefore, we only have to prove that $h_{1,p}(z)$ is holomorphic at $1/p^2$ and vanishes at $1/2p^2$; to this end we consider the series

$$h_{1,p}(z)|_{3/2}\begin{pmatrix} 1 & 0 \\ p^2 & 1 \end{pmatrix} \quad \text{and} \quad h_{1,p}(z)|_{3/2}\begin{pmatrix} 1 & 0 \\ 2p^2 & 1 \end{pmatrix}.$$

We begin by noting that

$$g_1(z) = \frac{\eta^2(z)}{\eta(2z)\eta^6(4z)}\cdot E_4(4z).$$

Using this description together with (2.8), (2.9) (and the discussion thereafter) and the fact that $E_4(z)$ is a modular form on $\mathrm{SL}_2(\mathbb{Z})$, we conclude (after a lengthy computation) that there exist roots of unity ζ_1 and ζ_2 such that

$$g_1(z)|_{3/2}\begin{pmatrix} 1 & 0 \\ p^2 & 1 \end{pmatrix} = \frac{\zeta_1}{2^{3/2}} + O(q^{1/4}), \tag{4.5}$$

$$g_1(z)|_{3/2}\begin{pmatrix} 1 & 0 \\ 2p^2 & 1 \end{pmatrix} = \frac{\zeta_2}{2}\cdot q^{-1/4} + O(q^{3/4}). \tag{4.6}$$

Let $g := \sum_{v=1}^{p-1}(\frac{v}{p})e^{2\pi i v/p}$ be the usual Gauss sum. Then we have

$$g_1 \otimes \left(\frac{\bullet}{p}\right)(z) = \frac{g}{p}\sum_{v=1}^{p-1}\left(\frac{v}{p}\right) g_1(z)|_{3/2}\begin{pmatrix} 1 & -v/p \\ 0 & 1 \end{pmatrix}. \tag{4.7}$$

The expansion of $g_1 \otimes (\frac{\bullet}{p})$ at $1/2p^2$ is given by

$$\left(g_1 \otimes \left(\frac{\bullet}{p}\right)\right)\Big|_{3/2}\begin{pmatrix} 1 & 0 \\ 2p^2 & 1 \end{pmatrix}. \tag{4.8}$$

We now make the crucial observation that if, for each v appearing in (4.7), we choose an integer k_v satisfying

$$4k_v \equiv 3v \pmod{p}, \tag{4.9}$$

then we have

$$\begin{pmatrix} 1 & -v/p \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 2p^2 & 1 \end{pmatrix} = \gamma_v \begin{pmatrix} 1 & 0 \\ 2p^2 & 1 \end{pmatrix} \begin{pmatrix} 1 & -4v/p + 4k_v/p \\ 0 & 1 \end{pmatrix},$$

where

$$\gamma_v = \begin{pmatrix} -8pv + 8pk_v - 16p^2vk_v + 16p^2v^2 + 1 & 1/p(3v - 4k_v - 8pv^2 + 8pvk_v) \\ -16p^3v + 16p^3k_v & 8pv - 8pk_v + 1 \end{pmatrix} \in \Gamma_0(4).$$

Using (2.1)–(2.4), we see that

$$(g_1|_{3/2}\gamma_v)(z) = \left(\frac{-16p^3v + 16p^3k_v}{8pv - 8pk_v + 1}\right) g_1(z) = \left(\frac{-pv + pk_v}{8(pv - pk_v) + 1}\right) g_1(z) = g_1(z).$$

Using these facts, together with (4.6), (4.7) and (4.8), we see that the only term in (4.8) with a non-positive exponent on q is the term

$$\frac{g}{p}\frac{\zeta_2}{2} q^{-1/4} \sum_{v=1}^{p-1} \left(\frac{v}{p}\right) e^{2\pi i(v-k_v)/p}. \tag{4.10}$$

A computation shows that if N is defined by $4N \equiv 1 \pmod{p}$, then the expression in (4.10) is equal to

$$\frac{g}{p}\frac{\zeta_2}{2} q^{-1/4} \sum_{v=1}^{p-1} \left(\frac{v}{p}\right) e^{(2\pi i/p)Nv} = \frac{g^2}{p}\frac{\zeta_2}{2} q^{-1/4} = \left(\frac{-1}{p}\right)\frac{\zeta_2}{2} q^{-1/4}. \tag{4.11}$$

Using (4.11) together with (4.1) and (4.6) we conclude that

$$h_{1,p}(z)|_{3/2} \begin{pmatrix} 1 & 0 \\ 2p^2 & 1 \end{pmatrix} = O(q^{3/4}).$$

The situation is similar at the cusp $1/p^2$; here we use the fact that if k_v is defined by (4.9), then we have

$$\begin{pmatrix} 1 & -v/p \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ p^2 & 1 \end{pmatrix} = \gamma'_v \begin{pmatrix} 1 & 0 \\ p^2 & 1 \end{pmatrix} \begin{pmatrix} 1 & -4v/p + 4k_v/p \\ 0 & 1 \end{pmatrix},$$

where, as in the previous case, $\gamma'_v \in \Gamma_0(4)$ has $(g_1|_{3/2}\gamma'_v)(z) = g(z)$. It follows from this together with (4.5) that the first term in the expansion of

$$g_1 \otimes \left(\frac{\bullet}{p}\right)(z)|_{3/2} \begin{pmatrix} 1 & 0 \\ p^2 & 1 \end{pmatrix}$$

is

$$\frac{\zeta_1}{2^{3/2}} \cdot \frac{g}{p} \sum_{v=1}^{p-1} \left(\frac{v}{p}\right) = 0.$$

We conclude from this together with (4.1) that $h_{1,p}(z)$ is indeed holomorphic at $1/p^2$. This finishes the proof of Lemma 4.2. □

Proof of Theorem 4.1. Suppose first that the result has been proved in the case when $m = 1$, and let $f_{1,p,s}$ be the form given by the theorem in this case. Using (2.12) together with the facts that $\phi(p^s) \mid p^\beta(p^2 - 1)/2$ and that the operators of prime index generate the Hecke algebra, we conclude, for each m coprime to p, that

$$f_{1,p,s}|T_{3/2+p^\beta(p^2-1)/2,4p^2}(m^2) \equiv h_{1,p}|T_{3/2,4p^2}(m^2) \pmod{p^s}.$$

Since the form on the left is again an element of $M^+_{3/2+(p^\beta(p^2-1))/2}(\Gamma_0(4p^2))$, we conclude that it suffices to prove the theorem in the case when $m = 1$.

To accomplish this task, we first consider the modular form

$$F_p(z) := \begin{cases} \dfrac{\eta^{p^2}(4z)}{\eta(4p^2z)} = 1 - p^2q^4 + O(q^8) & \text{if } p \geqslant 5, \\ \dfrac{\eta^{27}(4z)}{\eta^3(36z)} = 1 - 27q^4 + \cdots & \text{if } p = 3. \end{cases} \tag{4.12}$$

By a well-known criterion (see, for example, [GH93]) together with (2.8) and (2.9), it follows, for each prime $p \geqslant 3$, that $F_p(z)$ is a holomorphic form of integral weight on $\Gamma_0(4p^2)$ which vanishes at each cusp $a/c \in \mathbb{Q}$ for which $p^2 \nmid c$ (when $p \geqslant 5$ the weight is $(p^2-1)/2$, and when $p = 3$ the weight is 12). Moreover, it is clear from the definition of the eta-function that $F_p(z) \equiv 1 \pmod{p}$ for each p.

Suppose that we are in the case when $p \geqslant 5$. By the preceding discussion, we see that if $\beta \geqslant s-1$ is sufficiently large, then the modular form

$$f_{1,p,s} := h_{1,p} \cdot F_p^{p^\beta} \equiv h_{1,p} \pmod{p^s}$$

is a form of weight $3/2 + (p^\beta(p^2-1))/2$ on $\Gamma_0(4p^2)$ which vanishes at all cusps a/c for which $p^2 \nmid c$. Using (2.6), we see that the equivalence classes of cusps of $\Gamma_0(4p^2)$ for which $p^2 \mid c$ are represented by $1/p^2$, $1/2p^2$, and $1/4p^2$, and after Lemma 4.2 we know that $h_{1,p}$ is holomorphic on the upper half-plane and at these cusps. This gives Theorem 4.1.

In the case when $p = 3$, the situation is essentially the same; the only difference is that the form $f_{1,p,s}$ defined above has weight $3/2 + (p^{\beta+1}(p^2-1))/2$. Therefore, Theorem 4.1 follows exactly as before. □

We proceed with the proof of Theorem 1.1. Fix p, s, and m with $p \nmid m$, and let

$$\begin{aligned} f_{m,p,s}(z) &:= \sum_{n=0}^{\infty} a_{m,p,s}(n)q^n \\ &\equiv c_{m,p} - \sum_{\substack{0<d\equiv 0,3 \pmod 4 \\ p\mid d}} t_m(d)q^d - 2 \sum_{\substack{0<d\equiv 0,3 \pmod 4 \\ \left(\frac{-d}{p}\right)=-1}} t_m(d)q^d \pmod{p^s} \end{aligned} \tag{4.13}$$

be the form given by Theorem 4.1. Theorem 1.1 is an easy consequence of the following result.

Lemma 4.3. *Let $f_{m,p,s}(z) \in M^+_{3/2+(p^\beta(p^2-1))/2}(\Gamma_0(4p^2))$ be the form given in (4.13). Then we have the following.*

(a) *A positive proportion of the primes $\ell \equiv -1 \pmod{4p^s}$ have the property that*

$$f_{m,p,s}(z)|T_{3/2+(p^\beta(p^2-1))/2,4p^2}(\ell^2) \equiv 0 \pmod{p^s}.$$

(b) *A positive proportion of the primes $\ell \equiv 1 \pmod{4p^s}$ have the property that*

$$f_{m,p,s}(z)|T_{3/2+(p^\beta(p^2-1))/2,4p^2}(\ell^2) \equiv 2f_{m,p,s}(z) \pmod{p^s}.$$

Deduction of Theorem 1.1(2) and (3) from Lemma 4.3. Suppose for the moment that the lemma has been proved, and let ℓ be a prime as in the first part of the lemma. Then, using (2.12), we obtain

$$\begin{aligned} f_{m,p,s}|T_{3/2+(p^\beta(p^2-1))/2,4p^2}(\ell^2) &\equiv \sum_{n=0}^{\infty} \left(a_{m,p,s}(\ell^2 n) + \left(\frac{-n}{\ell}\right) a_{m,p,s}(n) + \ell a_{m,p,s}\left(\frac{n}{\ell^2}\right) \right) q^n \\ &\equiv 0 \pmod{p^s}. \end{aligned}$$

Replacing n by $n\ell$ in the last equation, we conclude that

$$a_{m,p,s}(\ell^3 n) \equiv 0 \pmod{p^s} \quad \text{for all } n \text{ with } \ell \nmid n.$$

By (4.13) it follows that $t_m(\ell^3 n) \equiv 0 \pmod{p^s}$ for all n coprime to ℓ such that p is inert or ramified in $\mathbb{Q}(\sqrt{-n\ell})$. This establishes the second assertion in Theorem 1.1.

We turn to the third assertion. If ℓ is a prime as in the second part of Lemma 4.3, then for all n we have

$$a_{m,p,s}(\ell^2 n) + \left(\left(\frac{-n}{\ell}\right) - 2\right) a_{m,p,s}(n) + \ell a_{m,p,s}\left(\frac{n}{\ell^2}\right) \equiv 0 \pmod{p^s}.$$

Therefore, if $\ell^2 \nmid n$ and p is inert or ramified in $\mathbb{Q}(\sqrt{-n})$, we conclude from (4.13) that

$$t_m(\ell^2 n) \equiv \left(2 - \left(\frac{-n}{\ell}\right)\right) t_m(n) \pmod{p^s}.$$

This gives the statement in the third part of Theorem 1.1. □

Lemma 4.3 is a consequence of the next result, which was proved by Serre [Ser76, § 6.4] using the Chebotarev Density Theorem and modular Galois representations.

LEMMA 4.4. *Suppose that λ and N are positive integers. Suppose that K is an algebraic number field with ring of integers $\mathcal{O}_K$, and that M is a positive integer. Then let $M_\lambda(\Gamma_0(N))_M$ denote the set of reductions modulo M of those forms in $M_\lambda(\Gamma_0(N))$ with coefficients in $\mathcal{O}_K$. If ℓ is prime then let $\mathcal{T}_{\lambda,N}(\ell)$ be the usual integral weight Hecke operator of index ℓ on $M_\lambda(\Gamma_0(N))$. Then we have the following.*

(1) *A positive proportion of the primes $\ell \equiv -1 \pmod{NM}$ have the property that for all $f \in M_\lambda(\Gamma_0(N))_M$ we have*

$$f|\mathcal{T}_{\lambda,N}(\ell) \equiv 0 \pmod{M}.$$

(2) *A positive proportion of the primes $\ell \equiv 1 \pmod{NM}$ have the property that for all $f \in M_\lambda(\Gamma_0(N))_M$ we have*

$$f|\mathcal{T}_{\lambda,N}(\ell) \equiv 2f \pmod{M}.$$

Proof of Lemma 4.3. To begin, recall that for all m coprime to p we may take

$$f_{m,p,s} = f_{1,p,s}|T_{3/2+(p^\beta(p^2-1))/2}(m^2).$$

By the commutativity of the Hecke operators, we see that it suffices to prove the lemma in the case when $m = 1$.

We begin by recalling some facts about the Shimura correspondence [Shi73]. In particular, if $g(z) := \sum_{n=1}^{\infty} b(n)q^n \in S_{k+1/2}(\Gamma_0(4N))$ with $k \geqslant 1$, then for every positive squarefree integer t, we have the Shimura lift $S_t(g)(z) := \sum_{n=1}^{\infty} B_t(n)q^n$, where the coefficients $B_t(n)$ are given by

$$\sum_{n=1}^{\infty} B_t(n)n^{-s} = L(s-k+1, \chi_t\chi_{-1}^k) \cdot \sum_{n=1}^{\infty} b(tn^2)n^{-s} \tag{4.14}$$

(here χ_{-1} and χ_t denote the Kronecker characters for the fields $\mathbb{Q}(i)$ and $\mathbb{Q}(\sqrt{t})$, respectively). For each such t we have

$$S_t(g)(z) \in M_{2k}(\Gamma_0(4N)).$$

Moreover, if $k \geqslant 2$, then $S_t(g)(z) \in S_{2k}(\Gamma_0(4N))$. This correspondence commutes with the action of the Hecke operators $T(\ell^2)$ and $\mathcal{T}(\ell)$ on the relevant half-integral and integral weight spaces.

For simplicity, we define

$$f(z) := f_{1,p,s}(z) = h_{1,p}(z) \cdot F_p^{p^\beta}(z) \in M^+_{3/2+(p^\beta(p^2-1))/2}(\Gamma_0(4p^2)) \tag{4.15}$$

with some sufficiently large $\beta \geqslant s-1$.

Unfortunately, we cannot apply the Shimura correspondence directly to $f(z)$, since $f(z)$ is not a cusp form. Overcoming this obstacle requires some additional work. To begin, note that, using Lemma 4.2 and the properties of the form $F_p(z)$, we may assume that $f(z)$ vanishes at each cusp a/c which is equivalent neither to $1/p^2$ nor to $1/4p^2$ under $\Gamma_0(4p^2)$.

We now recall some important properties of half-integral weight Eisenstein series on $\Gamma_0(4)$ as developed, for example, in § 4.2 of [Kob84]. For each integer $k \geqslant 2$ there are Eisenstein series $E_{k+1/2}(z)$ and $F_{k+1/2}(z) \in M_{k+1/2}(\Gamma_0(4))$ (these Eisenstein series are not in the plus space) with the following properties.

(i) $E_{k+1/2}(z)$ has constant term equal to 1 and vanishes at the cusps 1 and $\frac{1}{2}$ of $\Gamma_0(4)$. $F_{k+1/2}(z)$ has value $\zeta_3(\sqrt{2})^{-2k-1}$ at the cusp 1 (where ζ_3 is some root of unity) and vanishes at ∞ and $\frac{1}{2}$ (recall that the value of a modular form at an equivalence class of cusps is defined only up to multiplication by roots of unity).

(ii) For each prime $\ell \neq 2$, the forms $E_{k+1/2}(z)$ and $F_{k+1/2}(z)$ are eigenforms of the operator $T_{k+1/2,4}(\ell^2)$ defined in (2.12) (where the domain of definition is extended to all of $M_{k+1/2}(\Gamma_0(4))$). Moreover, the eigenvalue of each of these forms under $T_{k+1/2,4}(\ell^2)$ is $1+\ell^{2k-1}$ (this fact follows from the Euler factors given in (2.30) and (2.32) in § 4.2 of [Kob84]).

Using (4.15), (4.12), (4.2), and item (i) above, we see that, for any constant c, the modular form

$$f' := f + 2E_{3/2+(p^\beta(p^2-1))/2} + cF_{3/2+(p^\beta(p^2-1))/2} \tag{4.16}$$

vanishes at the cusp ∞. Using the discussion following (2.9), we compute that the first non-vanishing term in the expansion of $F_p^{p^\beta}$ at the cusp $1/p^2$ is (up to a root of unity) an integral power of 2. It follows from this together with item (i) above, (4.15), and (4.5) that, if we set $c = \zeta_4 2^{\lambda/2}$ with some appropriate root of unity ζ_4 and integer λ, then the modular form f' defined in (4.16) vanishes at the cusps $1/p^2$, $1/2p^2$, and ∞.

Of course, it will now be the case that f' does not vanish at the other cusps of $\Gamma_0(4p^2)$ which are equivalent to $1/p^2$ and ∞ under $\Gamma_0(4)$. However, this situation is easily remedied using the form $F_p(z)$ defined in (4.12). In particular, since $F_p(z)^{p^{s-1}} \equiv 1 \pmod{p^s}$ vanishes at each cusp a/c for which $p^2 \nmid c$, we see that the modular form

$$f'' := (f + 2E_{3/2+(p^\beta(p^2-1))/2} + cF_{3/2+(p^\beta(p^2-1))/2}) \cdot F_p^{p^{s-1}}$$

is in fact a cusp form of weight $3/2 + ((p^\beta + p^{s-1})(p^2-1))/2$ on $\Gamma_0(4p^2)$.

Before we proceed we need the following fact.

Lemma 4.5. *Suppose that $p \geqslant 3$ and that β is a non-negative integer (with $\beta \geqslant 1$ if $p = 3$). Then the Eisenstein series $E_{3/2+(p^\beta(p^2-1))/2}$ and $F_{3/2+(p^\beta(p^2-1))/2}$ have p-integral Fourier expansions at ∞.*

Proof. Write $E_{3/2+(p^\beta(p^2-1))/2} = \sum_{n=0}^{\infty} a(n)q^n$, $F_{3/2+(p^\beta(p^2-1))/2} = \sum_{n=0}^{\infty} b(n)q^n$. Using the Euler factors (2.30) and (2.32) in § 4.2 of [Kob84], we see that it suffices to prove that if n is square-free, then $a(n)$ and $b(n)$ are p-integral. Moreover, formula (2.18) of the same section shows that it is enough to prove that $b(n)$ is integral for each square-free n. Set $\lambda := 1 + (p^\beta(p^2-1))/2$.

Then from (2.16) in that section we obtain, for each such n,

$$b(n) = \frac{L(\chi_{-n}, 1-\lambda)}{(1-i)\zeta(1-2\lambda)} \cdot \begin{cases} \dfrac{2^{2\lambda-1/2}}{2^\lambda + \chi_{-n}(2)} & \text{if } -n \equiv 1 \pmod 4, \\ \dfrac{2^{1/2+\lambda}}{2^{2\lambda}-1} & \text{if } -n \equiv 2, 3 \pmod 4. \end{cases}$$

The desired result now follows after a lengthy case by case computation (in particular, one must separate the case when $p = 3$; recall that in this case we have $\beta \geqslant 1$). In each case, the L- and ζ-values in this formula can be written in terms of Bernoulli numbers and generalized Bernoulli numbers. The desired conclusion follows after applying standard results on the divisibility properties of these numbers (see, in particular, Theorems 1 and 3 of [Car59], and Proposition 15.2.1 and Theorem 5 of [IR90, § 15.2]). We do not include the details here. □

Together with item (ii) above and (2.12), this result implies that for each prime $\ell \equiv -1 \pmod{p^s}$ we have

$$f''|T_{3/2+((p^\beta+p^{s-1})(p^2-1))/2,4p^2}(\ell^2) \equiv 0 \pmod{p^s} \iff f|T_{3/2+(p^\beta(p^2-1))/2,4p^2}(\ell^2) \equiv 0 \pmod{p^s}, \tag{4.17}$$

and that for each prime $\ell \equiv 1 \pmod{p^s}$ we have

$$f''|T_{3/2+((p^\beta+p^{s-1})(p^2-1))/2,4p^2}(\ell^2) \equiv 2f'' \pmod{p^s} \iff f|T_{3/2+(p^\beta(p^2-1))/2,4p^2}(\ell^2) \equiv 2f \pmod{p^s}. \tag{4.18}$$

After this discussion, Lemma 4.3 follows from Lemma 4.4. Here we prove only the first case. Lemma 4.4 shows that a positive proportion of the primes $\ell \equiv -1 \pmod{4p^s}$ have the property that

$$(S_t f'')|\mathcal{T}_{2+(p^\beta+p^{s-1})(p^2-1),4p^2}(\ell) \equiv 0 \pmod{p^s} \quad \text{for all squarefree } t.$$

Since the Shimura correspondence commutes with the Hecke operators, we conclude that for such a prime ℓ we have

$$S_t(f''|T_{3/2+((p^\beta+p^{s-1})(p^2-1))/2,4p^2}(\ell^2)) \equiv 0 \pmod{p^s} \quad \text{for all squarefree } t. \tag{4.19}$$

A computation using (4.14) shows that (4.19) implies that

$$f''|T_{3/2+((p^\beta+p^{s-1})(p^2-1))/2,4p^2}(\ell^2) \equiv 0 \pmod{p^s},$$

which, together with (4.17) and (4.15), gives the first assertion in Lemma 4.3. Using (4.18), the proof in the second case proceeds in a similar manner, and we do not include it here. This proves Lemma 4.3, and so finishes the proof of Theorem 1.1. □

Remark. There are other congruences, similar to those appearing in the second part of Theorem 1.1, which correspond to instances where $g_m(z)$ (or some related modular form) is an eigenform modulo p^s of the relevant Hecke operator $T(\ell^2)$, and the eigenvalue has some special property. As examples of such congruences, we have

$$t_1(81n+9) \equiv t_1(81n+36) \equiv t_1(81n+63) \equiv 0 \pmod 3,$$
$$t_1(135n+63) \equiv t_1(135n+90) \equiv t_1(135n+117) \equiv 0 \pmod 5.$$

5. U_p-congruences and the proof of Theorem 1.5

We begin by recalling a result of Koike [Koi73] which is closely related to work of Dwork and Deligne [Dwo69] on the p-adic rigidity of the map $j(z) \to j(pz)$. If $p \geqslant 5$ is prime, then let $\mathfrak{S}_p$ denote the set of those supersingular j-invariants in characteristic p which are in $\mathbb{F}_p \setminus \{0, 1728\}$, and let $\mathfrak{M}_p$

denote the set of monic irreducible quadratic polynomials in $\mathbb{F}_p[x]$ whose roots are supersingular j-invariants. If $\epsilon_\rho(p)$ and $\epsilon_i(p)$ are defined by

$$\epsilon_\rho(p) := \begin{cases} 0 & \text{if } p \equiv 1 \pmod 3, \\ 1 & \text{if } p \equiv 2 \pmod 3, \end{cases}$$

$$\epsilon_i(p) := \begin{cases} 0 & \text{if } p \equiv 1 \pmod 4, \\ 1 & \text{if } p \equiv 3 \pmod 4, \end{cases}$$

then it is well known (see, for example, [Sil86]) that, with $S_p(x)$ as defined in (1.5), we have

$$\prod_{\substack{E/\overline{\mathbb{F}}_p \\ \text{supersingular}}} (x - j(E)) = x^{\epsilon_\rho(p)}(x-1728)^{\epsilon_i(p)} \cdot \prod_{\alpha \in \mathfrak{S}_p} (x-\alpha) \cdot \prod_{g \in \mathfrak{M}_p} g(x)$$

$$= x^{\epsilon_\rho(p)}(x-1728)^{\epsilon_i(p)} \cdot S_p(x). \tag{5.1}$$

Koike's result describes the Fourier expansion of $j(pz) \pmod{p^2}$ in terms of $j(z)$ and the collection of supersingular j-invariants in characteristic p. To be precise, Proposition 1 of [Koi73] implies, for primes $p \geqslant 5$, that there exist integers $A(\alpha)$, $B(g)$, and $C(g)$, as well as a polynomial $D_p(x) \in \mathbb{Z}[x]$, such that

$$j(pz) \equiv j(z)^p + pD_p(j(z)) + p \sum_{\alpha \in \mathfrak{S}_p} \frac{A(\alpha)}{j(z)-\alpha} + p \sum_{g(x) \in \mathfrak{M}_p} \frac{B(g)j(z) + C(g)}{g(j(z))} \pmod{p^2}. \tag{5.2}$$

Moreover, the integers $A(\alpha)$, $B(g)$, $C(g)$ have the property that

$$p \nmid A(\alpha) \quad \text{and} \quad p \nmid \gcd(B(g), C(g)).$$

The work of Deligne and Dwork (see [Dwo69, § 7]) considers the full p-adic expansion of $j(pz)$.

Example. As an example of (5.2), when $p = 37$ we have $\mathfrak{M}_p = \{x^2 + 31x + 31\}$, $\mathfrak{S}_{37} = \{-29\}$, and

$$j(37z) \equiv j(z)^{37} + 37(33j(z)^{36} + 22j(z)^{35} + 30j(z)^{34} + \cdots + 5j(z) + 6) + \frac{370}{j(z)+29} + \frac{37(9j(z)+10)}{j(z)^2 + 31j(z) + 31} \pmod{37^2}.$$

Remark. In [KZ98], Kaneko and Zagier give many descriptions of the supersingular polynomials $S_p(x)$. In § 10 of the same paper, they provide an explicit description of the interplay between supersingular polynomials and certain modular polynomials.

Proof of Theorem 1.5. We begin by considering the cases where $p \leqslant 11$. For these primes p, a calculation shows that for each non-negative $r < p$, we have

$$j(z)^r | U_p \equiv a_r(0) \pmod p,$$

where $a_r(0)$ is the constant in the Fourier expansion of $j(z)^r$. Since U_p is a linear operator, it follows that every $F(x) \in \mathbb{Z}[x]$ with degree $m < p$ has the property that $F(j(z))\big|U(p) \equiv 0 \pmod p$. The theorem holds since $S_p(x) = 1$ for these primes.

In the case when $p \geqslant 13$, denote the Fourier expansion of $F(j(z))$ by

$$F(j(z)) = \sum_{n \geqslant -m} a(n) q^n.$$

The action of the normalized weight zero Hecke operator $T_0(p)$ on $F(j(z))$ is given by

$$F(j(z))|T_0(p) = pF(j(z))|U_p + F(j(pz)).$$

Since $p > m$, it follows that

$$pF(j(z))|U_p = F(j(z))|T_0(p) - F(j(pz)) = p\sum_{n=0}^{\infty} a(pn)q^n. \tag{5.3}$$

Using the modular functions $J_m(z)$ defined in (1.2), we see that $F(j(z))|T_0(p)$ is a polynomial in $j(z)$ with integral coefficients (this also follows from the fact that $F(j(z))|T_0(p)$ is a nearly holomorphic modular function on $\mathrm{SL}_2(\mathbb{Z})$). Suppose now that $F(j(pz)) \pmod{p^2}$ is congruent to an integral polynomial in $j(z)$. Then (5.3) implies that there is a polynomial $\widetilde{F}(x) \in \mathbb{Z}[x]$ for which

$$F(j(z))|U_p \equiv \widetilde{F}(j(z)) \equiv \sum_{n=0}^{\infty} a(pn)q^n \pmod{p}.$$

However, the constants in $\mathbb{F}_p[j(z)]$ are the only polynomials whose Fourier expansions modulo p have no terms with negative exponents; it follows that $F(j(z))|U_p \equiv a(0) \pmod{p}$. Therefore, to prove Theorem 1.5 it suffices to prove that if $S_p(x)^2$ divides $F(x)$ in $\mathbb{F}_p[x]$, then $F(j(pz))$ is congruent modulo p^2 to a polynomial in $j(z)$.

To this end, suppose that $S_p(x)^2$ divides $F(x)$ in $\mathbb{F}_p[x]$, and write $F(x) = \prod_{s=1}^{m}(x - r_s)$. Then (5.2) implies that

$$\begin{aligned}
F(j(pz)) &= \prod_{s=1}^{m}(j(pz) - r_s) \\
&\equiv \prod_{s=1}^{m}\left(j(z)^p - r_s + pD_p(j(z)) + p\sum_{\alpha\in\mathfrak{S}_p}\frac{A(\alpha)}{j(z)-\alpha} + p\sum_{g(x)\in\mathfrak{M}_p}\frac{B(g)j(z)+C(g)}{g(j(z))}\right) \\
&\equiv \prod_{s=1}^{m}(j(z)^p - r_s) + pD_p(j(z))\cdot\sum_{s=1}^{m}\prod_{1\leqslant t\neq s\leqslant m}(j(z)^p - r_t) \\
&\quad + p\left(\sum_{\alpha\in\mathfrak{S}_p}\frac{A(\alpha)}{j(z)-\alpha} + \sum_{g(x)\in\mathfrak{M}_p}\frac{B(g)j(z)+C(g)}{g(j(z))}\right)\cdot\sum_{s=1}^{m}\prod_{1\leqslant t\neq s\leqslant m}(j(z)^p - r_t) \pmod{p^2}.
\end{aligned} \tag{5.4}$$

Since $\sum_{s=1}^{m}\prod_{1\leqslant t\neq s\leqslant m}(j(z)^p - r_t)$ is a polynomial in $j(z)$ with integer coefficients (note that this polynomial is symmetric in the r_t), the first two summands in the last expression above are integral polynomials in $j(z)$. Moreover, it follows that for the last summand we have

$$\begin{aligned}
&\left(\sum_{\alpha\in\mathfrak{S}_p}\frac{A(\alpha)}{j(z)-\alpha} + \sum_{g(x)\in\mathfrak{M}_p}\frac{B(g)j(z)+C(g)}{g(j(z))}\right)\cdot\sum_{s=1}^{m}\prod_{1\leqslant t\neq s\leqslant m}(j(z)^p - r_t) \\
&\quad\equiv \left(\sum_{\alpha\in\mathfrak{S}_p}\frac{A(\alpha)}{j(z)-\alpha} + \sum_{g(x)\in\mathfrak{M}_p}\frac{B(g)j(z)+C(g)}{g(j(z))}\right)\cdot\sum_{s=1}^{m}\prod_{1\leqslant t\neq s\leqslant m}(j(z) - r_t)^p \pmod{p},
\end{aligned}$$

which is a polynomial in $j(z)$ over $\mathbb{F}_p$ (in view of (5.1) and the fact that $S_p(x)^2$ divides $F(x)$ in $\mathbb{F}_p[x]$). Consequently, (5.4) shows that $F(j(pz)) \pmod{p^2}$ is an integral polynomial in $j(z)$, and this completes the proof. □

Proof of Corollary 1.6. Corollary 1.6 is obtained by verifying that $S_p(x)^2$ divides $\mathcal{H}_d(x)$ in $\mathbb{F}_p[x]$ for those primes p and fundamental discriminants $-d$ satisfying the given hypotheses. The factorizations of $\mathcal{H}_d(x)$ were computed using MAGMA. □

6. Filtrations and the Proof of Theorem 1.7 and Corollary 1.8

Here we prove Theorem 1.7 and Corollary 1.8 using the theory of modular forms modulo p as developed by Serre and Swinnerton-Dyer (see, for example, [Swi73]). Recall the definition (1.8) of the theta-operator. Then we have the following facts.

Proposition 6.1. *Suppose that $f(z) \in M_k$ and $g(z) \in M_{k'}$ have integral coefficients. If $p \geqslant 5$ is prime and*

$$0 \not\equiv f(z) \equiv g(z) \pmod{p},$$

then $k \equiv k' \pmod{p-1}$.

Proposition 6.2 [Swi73, Lemma 5]. *If $p \geqslant 5$ is prime and $f(z) \in M_k \cap \mathbb{Z}[[q]]$ has $f(z) \not\equiv 0 \pmod{p}$, then*

$$\omega_p(\Theta f) \equiv \omega_p(f) + 2 \pmod{p-1}.$$

Moreover, we have $\omega_p(\Theta f) \leqslant \omega_p(f) + p + 1$, with equality if and only if $p \nmid \omega_p(f)$.

If $f(z) \in M_k$, then the valence formula implies that $\mathrm{ord}_\infty(f) \leqslant k/12$. This implies the following proposition.

Proposition 6.3. *Suppose that $p \geqslant 5$ is prime, and that $f(z) = \sum_{n=n_0}^{\infty} a(n)q^n \in S_k \cap \mathbb{Z}[[q]]$. Suppose further that $p \nmid a(n_0)$ and that $p \nmid n_0$. Then for every non-negative integer m we have $\omega_p(\Theta^m f) \geqslant 12n_0$.*

We are now in a position to prove Theorem 1.7.

Proof of Theorem 1.7. In the notation of Theorem 1.7, we have

$$f_{p,s}(z) = f(z) \cdot \Delta(z)^{p^s} = a(m)q^{p^s+m} + \cdots \in S_{12p^s+k}. \tag{6.1}$$

Suppose that the conclusion of the theorem is false (in other words, suppose that $f(z)|U_p \equiv 0 \pmod{p}$). Since $\Delta(z)^{p^s} \equiv \Delta(p^s z) \pmod{p}$, we conclude from this that

$$f_{p,s}(z)|U_p \equiv 0 \pmod{p}.$$

Since we have $(f|U_p)^p \equiv f - \Theta^{p-1} f \pmod{p}$ for all f, it follows from this assumption that

$$0 \not\equiv \Theta^{p-1} f_{p,s}(z) \equiv f_{p,s}(z) \pmod{p}. \tag{6.2}$$

Suppose that $p \nmid \omega_p(\Theta^{p-2} f_{p,s})$. Then by Proposition 6.2, we would have

$$\omega_p(\Theta^{p-1} f_{p,s}) = \omega_p(\Theta^{p-2} f_{p,s}) + p + 1. \tag{6.3}$$

However, Proposition 6.3 and (6.1) together give $\omega_p(\Theta^{p-2} f_{p,s}) \geqslant 12(p^s + m)$, while by (6.1) and (6.2) we have $\omega_p(\Theta^{p-1} f_{p,s}) \leqslant 12p^s + k$. Taken together with (6.3), these inequalities contradict the assumption that $p \geqslant k - 12m$. Therefore, we must have $p \mid \omega_p(\Theta^{p-2} f_{p,s})$; it follows that there is a smallest positive integer $j \leqslant p-3$ for which $p \mid \omega_p(\Theta^{j+1} f_{p,s})$. For this j, Proposition 6.2 implies that

$$\omega_p(\Theta^{j+1} f_{p,s}) = \omega_p(\Theta f_{p,s}) + j(p+1) \equiv \omega_p(\Theta f_{p,s}) + j \equiv 0 \pmod{p}.$$

Since $1 \leqslant j \leqslant p-3$, this contradicts the assumption that $\omega_p(\Theta f_{p,s}) \equiv 1, 2 \pmod{p}$. This completes the proof of Theorem 1.7. □

Proof of Corollary 1.8. Let the notation be as in the statement of Corollary 1.8. Since $p > 12D+1$ is prime, we have $p > 12D + 3 > 5$. Set $f(z) := F(j(z))$, and consider the modular form

$$f_{p,1}(z) := f(z) \cdot \Delta(z)^p = a(-D)q^{p-D} + \cdots \in S_{12p}. \tag{6.4}$$

By Proposition 6.3 and (6.4), we obtain

$$12(p-D) \leqslant \omega_p(f_{p,1}) \leqslant 12p.$$

Therefore, since $p > 12D+3$ and $\omega_p(f_{p,1}) \equiv 12p \pmod{p-1}$, we must have $\omega_p(f_{p,1}) = 12p$. It follows by Propositions 6.2 and 6.3 that

$$12(p-D) \leqslant \omega_p(\Theta f_{p,1}) \leqslant 12p+2. \tag{6.5}$$

The facts that $\omega_p(\Theta f_{p,1}) \equiv 12p+2 \pmod{p-1}$ and that $p > 12D+3$, together with (6.5), show that

$$\omega_p(\Theta f_{p,1}) = 12p+2.$$

Corollary 1.8 now follows from Theorem 1.7. □

Acknowledgements

The authors thank Masanobu Kaneko, Jean-Pierre Serre, and Don Zagier for their comments on a preliminary version of this manuscript.

References

Ber28 W. E. H. Berwick, *Modular invariants*, Proc. London Math. Soc. (2) **28** (1928), 53–69.

Bor95a R. E. Borcherds, *Automorphic forms on $O_{s+2,2}(\mathbb{R})$ and infinite products*, Invent. Math. **120** (1995), 161–213.

Bor95b R. E. Borcherds, *Automorphic forms on $O_{s+2,2}(\mathbb{R})^+$ and generalized Kac-Moody algebras*, in *Proc. International Congress of Mathematicians* (Zürich, 1994) (Birkhäuser, Basel, 1995), 744–752.

Car59 L. Carlitz, *Arithmetic properties of generalized Bernoulli numbers*, J. reine angew. Math. **202** (1959), 174–182.

Deu46 M. Deuring, *Teilbarkeitseigenschaften der singulären Moduln der elliptischen Funktionen und die Diskriminante der Klassengleichung*, Comment. Math. Helv. **19** (1946), 74–82.

Deu58 M. Deuring, *Die Klassenkörper der komplexen Multiplikation*, in *Enzyklopädie der Mathematischen Wissenschaften*, Band I 2, Heft 10, Teil II (Teubner, Stuttgart, 1958).

Dor88 D. Dorman, *Special values of the elliptic modular function and factorization formulae*, J. reine angew. Math. **383** (1988), 207–220.

Dor89 D. Dorman, *Singular moduli, modular polynomials, and the index of the closure of $\mathbb{Z}[j(\tau)]$*, Math. Ann. **283** (1989), 177–191.

Dwo69 B. Dwork, *p-adic cycles*, Publ. Math. Inst. Hautes Études Sci. **37** (1969), 27–115.

Elk87 N. Elkies, *The existence of infinitely many supersingular primes for every elliptic curve over $\mathbb{Q}$*, Invent. Math. **89** (1987), 561–567.

GH93 B. Gordon and K. Hughes, *Multiplicative properties of η-products*, Comment. Math. **143** (1993), 415–430.

GZ85 B. Gross and D. Zagier, *On singular moduli*, J. reine angew. Math. **355** (1985), 191–220.

IR90 K. Ireland and M. Rosen, *A classical introduction to modern number theory* (Springer, New York, 1990).

Kob84 N. Koblitz, *Introduction to elliptic curves and modular forms*, Graduate Texts in Mathematics, vol. 97 (Springer, New York, 1984).

Koh82 W. Kohnen, *Newforms of half-integral weight*, J. reine angew. Math. **333** (1982), 32–72.

Koi73 M. Koike, *Congruences between modular forms and functions and applications to the conjecture of Atkin*, J. Fac. Sci. Univ. Tokyo Sect. IA Math. **20** (1973), 129–169.

KZ98 M. Kaneko and D. Zagier, *Supersingular j-invariants, hypergeometric series, and Atkin's orthogonal polynomials*, in *Computational perspectives on number theory* (Chicago, IL, 1995), AMS/IP Stud. Adv. Math., vol. 7 (American Mathematical Society, Providence, RI, 1998), 97–126.

Lan87 S. Lang, *Elliptic functions*, second edition (Springer, New York, 1987).

Leh49 J. Lehner, *Divisibility properties of the Fourier coefficients of the modular invariant $j(\tau)$*, Amer. J. Math. **71** (1949), 136–148.

Mar96 Y. Martin, *Multiplicative η-quotients*, Trans. Amer. Math. Soc. **348** (1996), 4825–4856.

Ser76 J.-P. Serre, *Divisibilité de certaines fonctions arithmétiques*, L'Enseign. Math. **22** (1976), 227–260.

Shi73 G. Shimura, *On modular forms of half-integral weight*, Ann. of Math. (2) **97** (1973), 440–481.

Sil86 J. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Mathematics, vol. 106 (Springer, New York, 1986).

Swi73 H. P. F. Swinnerton-Dyer, *On ℓ-adic representations and congruences for coefficients of modular forms*, Lecture Notes in Mathematics, vol. 350 (Springer, Berlin, 1973), 1–55.

Web61 H. Weber, *Lehrbuch der Algebra*, vol. III, third edition (Chelsea, New York, 1961).

Zag02 D. Zagier, *Traces of singular moduli*, in *Motives, polylogarithms and Hodge theory*, part I (F. Bogomolov and L. Katzarkov, eds.), International Press Lecture Series (International Press, Somerville, MA, 2002), 211–244.

Scott Ahlgren ahlgren@math.uiuc.edu
Department of Mathematics, University of Illinois, Urbana, IL 61801, USA

Ken Ono ono@math.wisc.edu
Department of Mathematics, University of Wisconsin, Madison, WI 53706, USA