Compositio Math. 140 (2004) 552–566
DOI: 10.1112/S0010437X03000721

The arithmetic of the values of modular functions and the divisors of modular forms

Jan H. Bruinier, Winfried Kohnen and Ken Ono

Abstract

We investigate the arithmetic and combinatorial significance of the values of the polynomials $j_n(x)$ defined by the q-expansion

$$\sum_{n=0}^{\infty} j_n(x)q^n := \frac{E_4(z)^2E_6(z)}{\Delta(z)} \cdot \frac{1}{j(z)-x}.$$

They allow us to provide an explicit description of the action of the Ramanujan Theta-operator on modular forms. There are a substantial number of consequences for this result. We obtain recursive formulas for coefficients of modular forms, formulas for the infinite product exponents of modular forms, and new p-adic class number formulas.

1. Introduction and statement of results

Let $j(z) = q^{-1} + 744 + 196\,884q + \cdots$ denote the usual elliptic modular function on $\mathrm{SL}_2(\mathbb{Z})$ ($q := e^{2\pi iz}$ throughout). We shall refer to a complex number τ of the form $\tau = (-b + \sqrt{b^2-4ac})/2a$ with $a, b, c \in \mathbb{Z}$, $\gcd(a,b,c) = 1$ and $b^2 - 4ac < 0$ as a *Heegner point*, and we denote its discriminant by the integer $d_\tau := b^2 - 4ac$. The values of j at such points are known as *singular moduli*, and they play a substantial role in classical and modern number theory. For example, the theory of complex multiplication implies that if τ is a Heegner point with discriminant d_τ, then $j(\tau)$ is an algebraic integer which generates a ring class field of $\mathbb{Q}(\sqrt{d_\tau})$.

Singular moduli also play an important role in Borcherds' [Bor95a, Bor95b] recent work on the infinite product expansions of certain modular forms. A meromorphic modular form f on $\mathrm{SL}_2(\mathbb{Z})$, by definition, has a *Heegner divisor* if its zeros and poles are supported at the cusp at infinity and Heegner points. In particular, Borcherds obtains an elegant description of the infinite product expansion of those meromorphic modular forms on $\mathrm{SL}_2(\mathbb{Z})$ with a Heegner divisor.

Here we consider the values of a specific sequence of elliptic modular functions j_n, where $j_1 = j - 744$. In an important recent paper [Zag02], Zagier expressed the traces of the values of j_n at Heegner points in terms of Fourier coefficients of half integral weight modular forms. Here we consider the more general case of the sums of the values of j_n over divisors of meromorphic modular forms. We show that the 'traces' of these values (see Theorem 1) dictate the properties of modular forms on $\mathrm{SL}_2(\mathbb{Z})$. This result is obtained using a j_n-weighted version of the proof of the classical valence formula for modular forms on $\mathrm{SL}_2(\mathbb{Z})$.

Theorem 1 provides a very useful link relating the values of j to the arithmetic of the Fourier coefficients of modular forms. Naturally, one then expects a wide variety of consequences. Here we

Received 25 February 2002, accepted in final form 14 May 2002.
2000 Mathematics Subject Classification 11F03, 11F11, 11F33.
Keywords: Borcherds products, singular moduli, modular forms and functions.
The first and third authors thank the Number Theory Foundation for its generous support, and the third author is grateful for the support of an Alfred P. Sloan Fellowship, a David and Lucile Packard Fellowship, an H. I. Romnes Fellowship, a John Guggenheim Fellowship and a grant from the National Science Foundation.

begin by considering such consequences in connection with the algebraicity of j-values, congruence properties and bounds for class numbers of imaginary quadratic fields, infinite product expansions of modular forms, and recurrence relations for Fourier coefficients. For example, we show that there are universal recursion formulas for the Fourier coefficients of every modular form on $\mathrm{SL}_2(\mathbb{Z})$ (see Theorem 3). We also obtain formulas for the exponents in the infinite product expansion of every modular form on $\mathrm{SL}_2(\mathbb{Z})$ (see Theorem 5), and we obtain new p-adic formulas for class numbers as traces of j-values (see Theorem 9).

Our investigation begins with a careful analysis of Ramanujan's Theta-operator, the differential operator defined by

$$\Theta\Big(\sum_{n=h}^{\infty} a(n)q^n\Big) := \sum_{n=h}^{\infty} na(n)q^n. \tag{1.1}$$

We refer to Θ as Ramanujan's operator since he first observed [Ram16] that

$$\Theta(E_4) = (E_4E_2 - E_6)/3 \quad \text{and} \quad \Theta(E_6) = (E_6E_2 - E_8)/2, \tag{1.2}$$

where E_k, for every even integer $k \geqslant 2$, is the standard Eisenstein series

$$E_k(z) := 1 - \frac{2k}{B_k}\sum_{n=1}^{\infty}\sigma_{k-1}(n)q^n. \tag{1.3}$$

Here B_k denotes the usual kth Bernoulli number and $\sigma_{k-1}(n) := \sum_{d|n} d^{k-1}$. If $k > 2$, then E_k is a weight k modular form on $\mathrm{SL}_2(\mathbb{Z})$. As usual, let $\Delta := (E_4^3 - E_6^2)/1728$, the unique normalized weight 12 cusp form on $\mathrm{SL}_2(\mathbb{Z})$.

Although the Eisenstein series

$$E_2(z) = 1 - 24\sum_{n=1}^{\infty}\sigma_1(n)q^n \tag{1.4}$$

is not a modular form, it plays an important role. If $f(z) = \sum_{n=h}^{\infty} a(n)q^n$ is a weight k meromorphic modular form on $\mathrm{SL}_2(\mathbb{Z})$, then

$$\Theta(f) = (\tilde{f} + kfE_2)/12, \tag{1.5}$$

where $\tilde{f}$ is a meromorphic modular form of weight $k+2$ on $\mathrm{SL}_2(\mathbb{Z})$. (Note that the formulas in (1.2) imply (1.5).) Because of this fact, the Θ-operator is fundamental in the theory of p-adic modular forms and modular forms modulo p. For instance, if f is a p-adic modular form of weight k, then since E_2 is a p-adic modular form of weight 2, $\Theta(f)$ is a p-adic modular form of weight $k+2$ [Ser73, Theorem 5].

Although Θ is simple to define, its arithmetic nature is much deeper and is dictated by the $\tilde{f}$ appearing in (1.5). We derive an explicit formula for $\Theta(f)$ in terms of a natural sequence of modular functions $j_m(z)$. Let $j_0(z) := 1$, and for every positive integer m let $j_m(z)$ be the unique modular function which is holomorphic on $\mathcal{H}$, the upper half of the complex plane, whose Fourier expansion is of the form

$$j_m(z) = q^{-m} + \sum_{n=1}^{\infty} c_m(n)q^n. \tag{1.6}$$

Note that if m is a positive integer, then $j_m(z) = j_1(z) \mid T_0(m)$, where $T_0(m)$ is the usual normalized mth weight zero Hecke operator. The first few j_m are

$$j_0(z) = 1,$$
$$j_1(z) = j(z) - 744 = q^{-1} + 196\,884q + \cdots,$$

$$j_2(z) = j(z)^2 - 1488j(z) + 159\,768 = q^{-2} + 42\,987\,520q + \cdots,$$
$$j_3(z) = j(z)^3 - 2232j(z)^2 + 1069\,956j(z) - 36\,866\,976 = q^{-3} + 2\,592\,899\,910q + \cdots.$$

Each j_m is a monic degree m polynomial in j with integer coefficients.

Let $\mathfrak{F}$ denote the usual fundamental domain of the action of $\mathrm{SL}_2(\mathbb{Z})$ on $\mathcal{H}$. By assumption, $\mathfrak{F}$ does not include the cusp at ∞. Throughout, let $i = \sqrt{-1}$ and let $\omega := (1+\sqrt{-3})/2$. If $\tau \in \mathfrak{F}$, then define e_τ by

$$e_\tau := \begin{cases} 1/2 & \text{if } \tau = i, \\ 1/3 & \text{if } \tau = \omega, \\ 1 & \text{otherwise.} \end{cases} \tag{1.7}$$

For every point $\tau \in \mathcal{H}$, Asai, Kaneko, and Ninomiya [AKN97, Theorem 3] proved that

$$H_\tau(z) := \sum_{n=0}^{\infty} j_n(\tau) q^n = \frac{E_4^2(z)E_6(z)}{\Delta(z)} \cdot \frac{1}{j(z) - j(\tau)}. \tag{1.8}$$

For $\tau = i$ and ω, we have the following beautiful formulas:

$$H_\omega = \frac{E_6}{E_4} = \sum_{n=0}^{\infty} j_n(\omega) q^n, \tag{1.9}$$

$$H_i = \frac{E_8}{E_6} = \sum_{n=0}^{\infty} j_n(i) q^n. \tag{1.10}$$

In particular, for every τ it turns out that H_τ is a weight 2 meromorphic modular form. The utility of (1.8) was already known; for example, it can be used to prove that

$$j(\tau) - j(z) = p^{-1} \exp\left(- \sum_{n=1}^{\infty} j_n(z) \cdot \frac{p^n}{n} \right),$$

where $p = e^{2\pi i \tau}$. This identity is equivalent to the famous denominator formula for the monster Lie algebra

$$j(\tau) - j(z) = p^{-1} \prod_{m>0 \text{ and } n \in \mathbb{Z}} (1 - p^m q^n)^{c(mn)},$$

where the exponents $c(n)$ are defined as the coefficients of $j_1 = \sum_{n=-1}^{\infty} c(n) q^n$.

Here we obtain a new proof of (1.8) and consider many of its number theoretic consequences.

Theorem 1. *If $f = \sum_{n=h}^{\infty} a_f(n) q^n$ is a non-zero weight k meromorphic modular form on $\mathrm{SL}_2(\mathbb{Z})$ for which $a_f(h) = 1$, then*

$$\Theta(f) = \frac{kE_2 f}{12} - f f_\Theta,$$

where f_Θ is defined by

$$f_\Theta := \sum_{\tau \in \mathfrak{F}} e_\tau \operatorname{ord}_\tau(f) H_\tau(z).$$

Theorem 1 easily reveals some algebraic information about the j_n evaluated at the finite points of the divisor of any meromorphic modular form. A celebrated result of Schneider asserts that, if τ is an algebraic number of degree >2, then $j(\tau)$ is transcendental. Under certain conditions, we observe that the values of j at the points in the divisor of an algebraic modular form are algebraic. Although there are more direct ways of establishing this result, it follows rather nicely from Theorem 1.

Corollary 2. *Let $f = \sum_{n=h}^{\infty} a_f(n)q^n$ be a meromorphic modular form on $\mathrm{SL}_2(\mathbb{Z})$ for which $a_f(h) = 1$. If $\tau_0 \in \mathfrak{F}$ is a point for which $\mathrm{ord}_{\tau_0}(f) \neq 0$ and the coefficients of f are in a number field K, then $j(\tau_0)$ is algebraic.*

Using Borcherds' work on infinite product expansions of modular forms, this corollary generalizes the classical fact that $j(\tau)$ is algebraic whenever τ is a Heegner point.

We consider the arithmetic of the Fourier coefficients of meromorphic modular forms. If $k \geqslant 4$ is an even integer and p is prime, then let $T_k(p)$ be the usual Hecke operator. In particular, if $f = \sum_{n=0}^{\infty} a_f(n)q^n \in M_k(1)$, the space of holomorphic modular forms of weight k on $\mathrm{SL}_2(\mathbb{Z})$, then

$$f \mid T_k(p) := \sum_{n=0}^{\infty} (a_f(np) + p^{k-1}a_f(n/p))q^n. \tag{1.11}$$

If $f \in S_k(1)$, the space of weight k cusp forms on $\mathrm{SL}_2(\mathbb{Z})$, then $f \mid T_k(p) \in S_k(1)$. If $\mathfrak{T}_k(p, x)$ denotes the characteristic polynomial of $T_k(p)$ on S_k, then it is well known that $\mathfrak{T}_k(p, x) \in \mathbb{Z}[x]$. There is wide speculation that $\mathfrak{T}_k(p, x)$ is irreducible for every prime p, and has the additional property that the Galois group of its splitting field is the symmetric group S_{d_k}, where d_k denotes the dimension of $S_k(1)$. Here we express these polynomials in terms of the values of j_n at the zeros of the eigenforms in $S_k(1)$ (see (1.12)). We begin with the following universal recursion relation for certain modular forms.

Theorem 3. *For every $n \geqslant 2$ define $F_n(x_1, \dots, x_{n-1}) \in \mathbb{Q}[x_1, \dots, x_{n-1}]$ by*

$$F_n(x_1, \dots, x_{n-1}) := -\frac{2x_1\sigma_1(n-1)}{n-1} + \sum_{\substack{m_1,\dots,m_{n-2}\geqslant 0,\\ m_1+2m_2+\cdots+(n-2)m_{n-2}=n-1}} (-1)^{m_1+\cdots+m_{n-2}} \cdot \frac{(m_1+\cdots+m_{n-2}-1)!}{m_1!\cdots m_{n-2}!} \cdot x_2^{m_1}\cdots x_{n-1}^{m_{n-2}}.$$

If $f = q + \sum_{n=2}^{\infty} a_f(n)q^n$ is a weight k meromorphic modular form on $\mathrm{SL}_2(\mathbb{Z})$, then for every integer $n \geqslant 2$ we have

$$a_f(n) = F_n(k, a_f(2), \dots, a_f(n-1)) - \frac{1}{n-1}\sum_{\tau\in\mathfrak{F}} e_\tau \,\mathrm{ord}_\tau(f)\cdot j_{n-1}(\tau).$$

It is simple to modify Theorem 3 for any modular form with leading coefficient 1.

The first few polynomials F_n are

$$\begin{aligned} F_2(x_1) &:= -2x_1, \\ F_3(x_1, x_2) &:= -3x_1 + \frac{x_2^2}{2}, \\ F_4(x_1, x_2, x_3) &:= -\frac{8x_1}{3} - \frac{x_2^3}{3} + x_2x_3, \\ F_5(x_1, x_2, x_3, x_4) &:= -\frac{7x_1}{2} - x_2^2x_3 + x_2x_4 + \frac{x_2^4}{4} + \frac{x_3^2}{2}. \end{aligned}$$

By arguing inductively with Theorem 3, it turns out that every Fourier coefficient $a_f(n)$ is a $\mathbb{Q}$-rational expression in the weight k and the values of j at the points in the divisor of f.

Remark. Theorem 3 includes a simple recursion for the coefficients of $\Delta = \sum_{n=1}^{\infty} \tau(n)q^n$. Since Δ has no zeros in $\mathfrak{F}$, for every $n \geqslant 2$ we find that

$$\tau(n) = F_n(12, \tau(2), \dots, \tau(n-1)).$$

As a special case of Theorem 3, we obtain the following strange formula.

Corollary 4. *If $f = q + \sum_{n=2}^{\infty} a_f(n)q^n$ is a meromorphic modular form of weight k on $\mathrm{SL}_2(\mathbb{Z})$, then*

$$a_f(2) = 60k - 744 - \sum_{\tau \in \mathfrak{F}} e_\tau \operatorname{ord}_\tau(f) \cdot j(\tau).$$

As an immediate consequence of Theorem 3, we obtain an expression for $\mathfrak{T}_k(p, x)$. If d_k is the dimension of $S_k(1)$, then for $1 \leqslant s \leqslant d_k$ let

$$f_s = q + \sum_{n=2}^{\infty} a_{f_s}(n)q^n$$

be the normalized Hecke eigenforms in $S_k(1)$. For every prime p, we have

$$\mathfrak{T}_k(p, x) = \prod_{s=1}^{d_k} \left(x - F_p(k, a_{f_s}(2), \ldots, a_{f_s}(p-1)) + \frac{1}{p-1} \sum_{\tau \in \mathfrak{F}} e_\tau \operatorname{ord}_\tau(f_s) \cdot j_{p-1}(\tau) \right). \tag{1.12}$$

These results are closely related to Borcherds' recent work on the infinite product expansions of modular forms. Borcherds [Bor95a, Bor95b] provided a striking description for the exponents in the infinite product expansion for those modular forms with a Heegner divisor. For example, if the integers $c(n)$ are defined by

$$E_4(z) = 1 + 240 \sum_{n=1}^{\infty} \sigma_3(n)q^n = (1-q)^{-240}(1-q^2)^{26\,760} \cdots = \prod_{n=1}^{\infty} (1-q^n)^{c(n)},$$

then Borcherds' theorem implies that there is a weight $1/2$ meromorphic modular form

$$G(z) = \sum_{n \geqslant -3} b(n)q^n = q^{-3} + 4 - 240q + 26\,760q^4 + \cdots - 4\,096\,240q^9 + \cdots$$

on $\Gamma_0(4)$ with the property that $c(n) = b(n^2)$ for every positive integer n. We obtain an arithmetic formula for the exponents of the infinite product expansion of every meromorphic modular form on $\mathrm{SL}_2(\mathbb{Z})$.

Theorem 5. *Suppose that $f = \sum_{n=h}^{\infty} a_f(n)q^n$ is a weight k meromorphic modular form on $\mathrm{SL}_2(\mathbb{Z})$ for which $a_f(h) = 1$, and let $c(n)$ denote the complex numbers for which*

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

If n is a positive integer, then

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

In an important paper [GZ85], Gross and Zagier described the divisibility properties of differences of singular moduli. More recently [Zag02], Zagier described the arithmetic of the traces of singular moduli in terms of the Fourier coefficients of modular forms of half integral weight. Since the modular functions j_n play an important role, we consider their divisibility and congruence properties. We consider the arithmetic of the values of j_n as we vary n. First we obtain the following theorem for the special values at $\tau = \omega$ and $\tau = i$.

Theorem 6. *If $\tau = \omega$, then let M be a positive integer which is not divisible by a prime $p \equiv 1 \pmod 3$. If $\tau = i$, then suppose that M is a positive integer which is not divisible by a prime $p \equiv 1 \pmod 4$. Then there is a positive real number $\alpha(M)$ for which*

$$\#\{1 \leqslant n \leqslant X : j_n(\tau) \equiv 0 \pmod M\} = \mathcal{O}\left(\frac{X}{(\log X)^{\alpha(M)}} \right).$$

In particular, for almost all n we have $j_n(\tau) \equiv 0 \pmod M$.

In addition to results of this type, there are examples of explicit congruences. For example, congruences with modulus $2k$ relating such values to Borcherds exponents follow immediately from Theorem 5. We highlight two further types of congruence properties.

Theorem 7. *If $k \geqslant 4$ is even, then for every positive integer n we have*

$$\sum_{\tau\in\mathfrak{F}} e_\tau \operatorname{ord}_\tau(E_k)\cdot j_n(\tau) \equiv -2k\sigma_1(n) \pmod{4\prod_{\substack{p-1\mid k\\ 5\leqslant p \text{ prime}}} p}.$$

Theorem 8. *Let $f=\sum_{n=h}^{\infty} a_f(n)q^n$ be a weight k meromorphic modular form on $\mathrm{SL}_2(\mathbb{Z})$ whose coefficients are in O_K, the ring of algebraic integers in a number field K. Suppose that $a_f(h)=1$ and that f has a Heegner divisor whose Heegner points in $\mathfrak{F}$ are $\tau_1,\tau_2,\dots,\tau_t$. Furthermore, suppose that $p\in\{2,3,5,7\}$ has the property that for all $1\leqslant s\leqslant t$ we have*

$$|d_{\tau_s}| \equiv \begin{cases} 3 \pmod 8 & \text{if } p=2,\\ 1 \pmod 3 & \text{if } p=3,\\ 2,3 \pmod 5 & \text{if } p=5,\\ 1,2,4 \pmod 7 & \text{if } p=7. \end{cases}$$

If ν is a positive integer, then there is a positive real number $\alpha(p,\nu)$ for which

$$\#\left\{1\leqslant n\leqslant X : \sum_{c=1}^{t} e_{\tau_c}\operatorname{ord}_{\tau_c}(f)\cdot j_n(\tau_c)\equiv 0 \pmod{p^\nu}\right\} = \mathcal{O}\left(\frac{X}{(\log X)^{\alpha(p,\nu)}}\right).$$

In particular, for almost all n we have $\sum_{c=1}^{t} e_{\tau_c}\operatorname{ord}_{\tau_c}\cdot j_n(\tau_c)\equiv 0 \pmod{p^\nu}$.

The p-adic properties of the values of the j_n are closely related to the arithmetic of class numbers of imaginary quadratic fields. Let $H(-D)$ be the Hurwitz class number for the discriminant $-D$.

Theorem 9. *Suppose that $-D<-4$ is a fundamental discriminant of an imaginary quadratic field, and let τ be any Heegner point of discriminant $-D$. If $K=\mathbb{Q}(j(\tau))$, then the following are true:*

1) *If $D\equiv 3 \pmod 8$, then as 2-adic numbers we have*
$$H(-D)=\tfrac{1}{24}\lim_{n\to+\infty}\operatorname{Tr}_{K/\mathbb{Q}}(j_{2^n}(\tau)).$$
2) *If $D\equiv 1 \pmod 3$, then as 3-adic numbers we have*
$$H(-D)=\tfrac{1}{12}\lim_{n\to+\infty}\operatorname{Tr}_{K/\mathbb{Q}}(j_{3^n}(\tau)).$$
3) *If $D\equiv 2,3 \pmod 5$, then as 5-adic numbers we have*
$$H(-D)=\tfrac{1}{6}\lim_{n\to+\infty}\operatorname{Tr}_{K/\mathbb{Q}}(j_{5^n}(\tau)).$$
4) *If $D\equiv 1,2,4 \pmod 7$, then as 7-adic numbers we have*
$$H(-D)=\tfrac{1}{4}\lim_{n\to+\infty}\operatorname{Tr}_{K/\mathbb{Q}}(j_{7^n}(\tau)).$$

Remark. Analogs of Theorem 9 hold for $-D=-3$ (respectively $-D=-4$). Subject to the same congruence conditions on D, these results simply require replacing $j_{p^n}(\tau)$ by $j_{p^n}(\omega)/3$ (respectively $j_{p^n}(i)/2$). Moreover, simple analogs hold for every $-D$, not just those which are fundamental. More generally, there are analogs of Theorems 8 and 9 for primes $p\geqslant 11$, but these results are more complicated to state.

If $D\equiv 3 \pmod 8$, it turns out that the 2-adic behavior of these traces, for all j_n, are also controlled by the class number $H(-D)$. Using the fact that the Hecke algebra for holomorphic

modular forms is locally nilpotent at 2, we obtain the following 2-divisibility results. Let $\omega(n)$ denote the number of distinct prime factors of n.

Theorem 10. *Suppose that $-3 \neq -D \equiv 5 \pmod 8$ is a fundamental discriminant of an imaginary quadratic field, and suppose that τ is a Heegner point of discriminant $-D$. If $K = \mathbb{Q}(j(\tau))$ and $s \geqslant 4$, then*

$$\mathrm{Tr}_{K/\mathbb{Q}}(j_n(\tau)) \equiv 0 \pmod{2^s}$$

for every positive square-free integer n for which

$$\omega(n) > 2^{s-4} H(-D).$$

Theorem 10 yields theoretical lower bounds for $H(-D)$. To state these results, for $D \equiv 0, 3 \pmod 4$, let

$$F(D;z) = q^{-H(-D)} \prod_{n=1}^{\infty} (1-q^n)^{c_D(n)} \tag{1.13}$$

be the unique weight zero modular function on $\mathrm{SL}_2(\mathbb{Z})$, with leading coefficient 1, whose divisor consists of a pole of order $H(-D)$ at $z = \infty$ and a simple zero at each Heegner point with discriminant $-D$. These functions have integer coefficients. Consider the formal power series

$$\frac{\Theta(F(D;z))}{F(D;z)} := -H(-D) - \sum_{n=0}^{\infty} A(D;n) q^n = -H(-D) - \sum_{n=1}^{\infty} \sum_{d|n} c_D(d)\, dq^n. \tag{1.14}$$

Corollary 11. *Suppose that $-3 \neq -D \equiv 5 \pmod 8$ is a fundamental discriminant of an imaginary quadratic field. If $s \geqslant 4$ and there is an odd square-free integer n for which $\mathrm{ord}_2(A(D;n)) < s$, then*

$$H(-D) > \frac{\omega(n)}{2^{s-4} s} - \frac{1}{3 \cdot 2^{s-3}}.$$

It will be extremely interesting to see whether a detailed study of the Hecke algebra modulo powers of 2, perhaps combined with further 2-adic arguments, can be used to transform Corollary 11 into a lower bound like the celebrated bound due to Goldfeld, Gross and Zagier.

In § 2 we prove Theorems 1, 3, and 5, and Corollaries 2 and 4. In § 3 we prove Theorems 6, 7, 8, and 9. There we consider the p-adic behavior of the Θ-operator under certain conditions. In § 4 we prove Theorem 10 and Corollary 11 using an analysis of the behavior of the Hecke algebra on modular forms modulo 2.

2. Proof of Theorems 1, 3, and 5 and Corollaries 2 and 4

For convenience, we begin by proving Theorem 5 on the infinite product expansion of generic modular forms. Before we prove Theorem 5, we call attention to earlier work of Eholzer and Skoruppa [ES96] which also considers product expansions of modular forms.

Proposition 2.1. *Let $f = \sum_{n=h}^{\infty} a_f(n) q^n$ be a meromorphic function in a neighborhood of $q = 0$, and suppose that $a_f(h) = 1$. Then there are uniquely determined complex numbers $c(n)$ such that*

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

where the product converges in a small neighborhood of $q = 0$. Moreover, the following identity is true:

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

Proof. As usual, we understand that complex powers are defined by the principal branch of the complex logarithm. If $F(q) := f(z)$, then the function $qF'(q)/F(q)$ is holomorphic at $q = 0$. Write its Taylor expansion as

$$qF'(q)/F(q) = h - \sum_{n\geqslant 1} \alpha(n) q^n \quad (|q| < \epsilon), \tag{2.1}$$

and for $n \geqslant 1$ let

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

where μ denotes the Möbius function. This implies that

$$\alpha(n) = \sum_{d|n} c(d)d. \tag{2.2}$$

Obviously, the numbers $c(n)$ are uniquely determined by f.

For fixed q_0 with $|q_0| < \epsilon$ we have $\alpha(n) = \mathcal{O}(|q_0|^{-n})$ for all n, and this easily implies that the double series

$$\sum_{m,n\geqslant 1} c(n) n q^{mn}$$

is absolutely convergent in $|q| < |q_0|$, hence in $|q| < \epsilon$.

In the following, suppose that $|q| < \epsilon$. From the above we see that

$$\begin{aligned}
\frac{d}{dq} \log(F(q)q^{-h}) &= \frac{F'(q)}{F(q)} - \frac{h}{q} \\
&= -\sum_{n\geqslant 1} c(n) \frac{d}{dq} \Bigg(\sum_{m\geqslant 1} \frac{q^{mn}}{m} \Bigg) \\
&= \frac{d}{dq} \Bigg(\sum_{n\geqslant 1} c(n) \log(1 - q^n) \Bigg),
\end{aligned}$$

the interchange of differentiation and summation being justified because of local uniform convergence as can easily be seen in a similar way as above.

We thus obtain

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

The values $c(n) \log(1 - q^n)$ and $\log(1 - q^n)^{c(n)}$ differ by integer multiples of $2\pi i$. Since $c(n)$ $\log(1 - q^n) \to 0$ $(n \to \infty)$ the same is true for $\log(1 - q^n)^{c(n)}$. Hence we see that there is an integer N such that

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

Taking the exponential on both sides proves our claim. □

Proof of Theorem 5. Let

$$\mathcal{F} := \{z \in \mathcal{H} : |z| \geqslant 1, |\mathrm{Re}(z)| \leqslant \tfrac{1}{2}\}$$

be the standard fundamental domain for the action of $\mathrm{SL}_2(\mathbb{Z})$ on $\mathcal{H}$. We cut off $\mathcal{F}$ by a horizontal line $\mathcal{L} := \{iC - t : -\frac{1}{2} \leqslant t \leqslant \frac{1}{2}\}$ where $C > 0$ is chosen so large that all poles and zeros of f, apart from those at the cusp at infinity, are contained in $\{z \in \mathcal{H} : \mathrm{Im}(z) < C\}$.

For simplicity, suppose that f has no zero or pole on the boundary $\partial\mathcal{F}$ except possibly i or ω (if not, one has to modify the arguments in the same way as in the classical proof of the '$k/12$-identity').

We let γ be the closed path with positive orientation consisting of $\mathcal{L}$ and γ_1 where γ_1 is the part of $\partial\mathcal{F}$ below $\mathcal{L}$ modified in the usual way: in a small neighborhood U of ω (respectively i; respectively $-\overline{\rho}$) we replace $U\cap\partial\mathcal{F}$ by $\mathcal{F}\cap\mathcal{C}_\omega$ (respectively $\mathcal{F}\cap\mathcal{C}_i$; respectively $\mathcal{F}\cap\mathcal{C}_{-\overline{\omega}}$) where $\mathcal{C}_\omega$ (respectively $\mathcal{C}_i$; respectively $\mathcal{C}_{-\overline{\omega}}$) are small circles with radius r around ω (respectively i; respectively $-\overline{\omega}$).

We integrate

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

along γ. By the residue theorem, taking into account that $j_n(z)$ is holomorphic on $\mathcal{H}$, this integral is equal to

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

On the other hand, the integral can be evaluated separately along the different pieces of γ, in a well-known way. If we let r tend to zero, we then find that

$$\begin{aligned}\sum_{\tau\in\mathfrak{F}-\{\omega,i\}}\operatorname{ord}_\tau(f)j_n(\tau) &= -\frac{1}{3}\operatorname{ord}_\omega(f)j_n(\omega)-\frac{1}{2}\operatorname{ord}_i(f)j_n(i)\\ &\quad+\frac{1}{2\pi i}\int_\rho\frac{F'(q)}{F(q)}J_n(q)\,dq-\frac{k}{2\pi i}\int_\sigma\frac{j_n(z)}{z}\,dz.\end{aligned}\tag{2.3}$$

Here $F(q)=f(z)$ as before and $J_n(q):=j_n(z)$. Furthermore, ρ is a small circle around $q=0$ with negative orientation and not containing any pole or zero of $F(q)$ except possibly 0, and σ is the part of the unit circle in the upper half-plane that connects ω and i, with positive orientation.

By Proposition 2.1, for $|q|<\epsilon$ we see that

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

where h is the order of F at $q=0$. Hence recalling that $J_n(q)=q^{-n}+\mathcal{O}(q)$ we find that

$$\frac{1}{2\pi i}\int_\rho\frac{F'(q)}{F(q)}J_n(q)\,dq=\sum_{d|n}c(d)d.\tag{2.4}$$

We cannot directly evaluate the last integral on the right-hand side of (2.3). Instead we proceed as follows. Formula (2.3) in particular is valid for the function $f=\Delta$ of weight 12. In this case we have

$$\sum_{d|m}c(d)d=24\sigma_1(m)\quad(m\geqslant 1),$$

by definition. Since Δ has no zeros on $\mathcal{H}$, we obtain from (2.3) that

$$\frac{1}{2\pi i}\int_\sigma\frac{j_n(z)}{z}dz=2\sigma_1(n).\tag{2.5}$$

Inserting (2.4) and (2.5) into (2.3), we deduce the theorem. □

Proof of Theorem 1. We begin by proving that if

$$\frac{\Theta(f)}{f}=\frac{kE_2}{12}-f_\Theta,\tag{2.6}$$

then f_Θ has the claimed form. If n is a positive integer, then Proposition 2.1 and Theorem 5 imply

that the coefficient of q^n in $\Theta(f)/f$ is $-2k\sigma_1(n) - \sum_{\tau\in\mathfrak{F}} e_\tau \operatorname{ord}_\tau(f)\cdot j_n(\tau)$. Since the E_2 is given by

$$E_2 = 1 - 24\sum_{n=1}^{\infty}\sigma_1(n)q^n,$$

(2.6) verifies the truth of Theorem 1 for every coefficient with the exception of the constant term. The constant term in $\Theta(f)/f$ is $h = \operatorname{ord}_\infty(f)$. However, the constant term of $kE_2/12 - f_\Theta$ is $(k/12) - \sum_{\tau\in\mathfrak{F}} e_\tau \operatorname{ord}_\tau(f)$, which equals h by the classical '$k/12$' valence formula. □

Proof of Corollary 2. We begin by fixing notation. Let $\tau_1, \tau_2, \ldots, \tau_t \in \mathfrak{F}$ be the numbers for which $\operatorname{ord}_\tau(f) \neq 0$. If n is a positive integer, then the coefficient of q^n in $kE_2/12$ is the integer $-2k\sigma_1(n)$. Therefore by Theorem 1, if the Fourier coefficients of f are in a field K, then the coefficients of f_Θ and $1/f$ belong to K. Hence if n is a positive integer, then

$$\sum_{s=1}^{t} j_n(\tau_s) = \sum_{s=1}^{t} G_n(j(\tau_s)) \in K, \tag{2.7}$$

where $G_n \in \mathbb{Z}[x]$ is a monic polynomial of degree n. Since $j_1 = j - 744$, for every positive integer n we have

$$\sum_{s=1}^{t} j(\tau_s)^n \in K.$$

Therefore, by solving for the elementary symmetric functions in $j(\tau_1), \ldots, j(\tau_t)$, we find that

$$\prod_{s=1}^{t}(x - j(\tau_s)) \in K[x].$$

This proves the corollary. □

Proof of Theorem 3. By Theorem 1, we have that

$$\sum_{\tau\in\mathfrak{F}} e_\tau \operatorname{ord}_\tau(f)\sum_{n=0}^{\infty} j_n(\tau)q^n = -\frac{\Theta(f)}{f} + \frac{kE_2}{12}.$$

If $n \geqslant 2$, then Theorem 5 gives

$$\sum_{\tau\in\mathfrak{F}} e_\tau \operatorname{ord}_\tau(f) j_{n-1}(\tau) = \sum_{d|n-1} c(d)d - 2k\sigma_1(n-1),$$

where

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

Therefore, to prove the theorem it suffices to obtain a closed formula for $b(n) := \sum_{d|n} c(d)d$ in terms of $a_f(n)$. In particular, it suffices to show that, if $n \geqslant 1$, then

$$b(n) = n \sum_{\substack{m_1,\ldots,m_n\geqslant 0,\\ m_1+2m_2+\cdots+nm_n=n}} (-1)^{m_1+\cdots+m_n}\frac{(m_1+\cdots+m_n-1)!}{m_1!\cdots m_n!}a_f(2)^{m_1}\cdots a_f(n+1)^{m_n}. \tag{2.8}$$

To prove (2.8), one observes that

$$0 = b(n) + b(n-1)a_f(2) + b(n-2)a_f(3) + \cdots + b(1)a_f(n) + na_f(n+1),$$

and uses the well-known fact that

$$0 = s_n - s_{n-1}\sigma_1 + s_{n-2}\sigma_2 - \cdots + (-1)^{n-1}s_1\sigma_{n-1} + (-1)^n n\sigma_n.$$

Here the σ_i are the elementary symmetric functions in $X_1, \dots, X_n$ and the s_i are the power functions in these variables (i.e. $s_i := X_1^i + \cdots + X_n^i$). One now obtains (2.8) by evaluating these identities at $(X_1, \dots, X_n) = (\lambda(1,n), \dots, \lambda(n,n))$ where the $\lambda(j,n)$ are the roots of the polynomial

$$X^n + a_f(2)X^{n-1} + a_f(3)X^{n-2} + \cdots + a_f(n+1).$$

One requires the fact that

$$s_i = i \sum_{\substack{m_1,\dots,m_n \geqslant 0,\\ m_1+2m_2+\cdots+nm_n=i}} (-1)^{m_2+m_4+\cdots} \frac{(m_1+m_2+\cdots+m_n-1)!}{m_1!m_2!\cdots m_n!} \sigma_1^{m_1}\cdots\sigma_n^{m_n}. \qquad \square$$

Proof of Corollary 4. Since $j_1(z) = j(z) - 744$ and $\sum_{\tau\in\mathfrak{F}} e_\tau \operatorname{ord}_\tau(f) = (k/12) - 1$, this result is the $n = 2$ case of Theorem 3. $\square$

3. Proofs of Theorems 6, 7, 8, and 9

In this section we prove Theorems 6, 7, 8, and 9 using theorems of Serre on p-adic modular forms and the divisibility of the Fourier coefficients of modular forms modulo M (see [Ser73, Ser76]).

Proof of Theorem 6. By (1.9) and (1.10), it suffices to prove that the coefficients of the Fourier series

$$H_\omega = \frac{E_6}{E_4} = \sum_{n=0}^{\infty} j_n(\omega) q^n = 1 - 744q + 159\,768q^2 - 36\,866\,976q^3 + \cdots, \tag{3.1}$$

$$H_i = \frac{E_8}{E_6} = \sum_{n=0}^{\infty} j_n(i) q^n = 1 + 984q + 574\,488q^2 + 307\,081\,056q^3 + \cdots \tag{3.2}$$

satisfy the claim.

Since $z = i$ (respectively $z = \omega$) is fixed by the modular transformation $Sz = -1/z$ (respectively $Az = -(z+1)/z$), the definition of a modular form implies that, if $k \geqslant 4$ is even, then

$$k \equiv 2 \pmod 4 \Longrightarrow E_k(i) = 0,$$
$$k \equiv 2, 4 \pmod 6 \Longrightarrow E_k(\omega) = 0.$$

If $p \geqslant 5$ is prime, then these observations together with the von Staudt–Clausen Theorem [IR90, p. 233] and (1.3) imply that, if $p \not\equiv 1 \pmod 4$, then there is an Eisenstein series $\mathcal{E}_{i,p}$ for which

$$\mathcal{E}_{i,p}(i) = 0 \quad \text{and} \quad \mathcal{E}_{i,p} \equiv 1 \pmod{24p}, \tag{3.3}$$

and if $p \not\equiv 1 \pmod 3$, then there is an Eisenstein series $\mathcal{E}_{\omega,p}$ for which

$$\mathcal{E}_{\omega,p}(\omega) = 0 \quad \text{and} \quad \mathcal{E}_{\omega,p} \equiv 1 \pmod{24p}. \tag{3.4}$$

Now observe that if $H \equiv 1 \pmod \ell$, where ℓ is prime, then $H^{\ell^s} \equiv 1 \pmod{\ell^{s+1}}$. If $p_1 \not\equiv 1 \pmod 4$ is prime, then for every positive integer s we have that

$$\frac{E_8}{E_6} \equiv \frac{E_8}{E_6} \cdot \mathcal{E}_{i,p_1}^{p_1^s} \pmod{p_1^{s+1}}. \tag{3.5}$$

Similarly, if $p_2 \not\equiv 1 \pmod 3$ is prime, then

$$\frac{E_6}{E_4} \equiv \frac{E_6}{E_4} \cdot \mathcal{E}_{\omega,p_2}^{p_2^s} \pmod{p_2^{s+1}}. \tag{3.6}$$

Since $E_4(\omega) = 0$ (respectively $E_6(i) = 0$) and E_4 (respectively E_6) has no other zeros in $\mathfrak{F}$, (3.3) and (3.5) (respectively (3.4) and (3.6)) illustrate that the relevant forms are the reduction modulo p_i^{s+1}

of holomorphic integer weight modular forms on $\mathrm{SL}_2(\mathbb{Z})$. There are obvious analogous constructions for both forms modulo powers of 2 and 3. The theorem now follows from a well-known theorem of Serre which asserts that almost all the coefficients of a modular form with algebraic integer coefficients are multiples of any given integer M [Ser76, Theorem 4.7]. □

Proof of Theorem 7. By (1.3) and the von Staudt–Clausen theorem, if $k \geqslant 4$ is even, then

$$E_k \equiv 1 \pmod{4 \prod_{\substack{p-1|k \\ p \text{ prime}}} p}.$$

This observation and Theorem 1 imply that

$$0 \equiv \frac{\Theta(E_k)}{E_k} = \frac{kE_2}{12} - (E_k)_\Theta \pmod{4 \prod_{\substack{p-1|k \\ p \text{ prime}}} p}.$$

The theorem follows from (1.4). □

Proof of Theorem 8. By [BO03, Corollary 3], $\Theta(f)/f$ is a p-adic modular form of weight 2. Since the Eisenstein series E_2 is also a p-adic modular form of weight 2 [Ser73], we find that

$$f_\Theta = -\frac{\Theta(f)}{f} + \frac{kE_2}{12} = \sum_{\tau \inf \mathfrak{F}} e_\tau \operatorname{ord}_\tau(f) \sum_{n=0}^{\infty} j_n(\tau) q^n$$

is a p-adic modular form of weight 2. Therefore, $f_\Theta \pmod{p^\nu}$ is the reduction modulo p^ν of some holomorphic integer weight modular form on $\mathrm{SL}_2(\mathbb{Z})$. The theorem now follows from [Ser76, Theorem 4.7]. □

Proof of Theorem 9. If $0 < D \equiv 0, 3 \pmod 4$, then there is a unique meromorphic modular form of weight $1/2$ on $\Gamma_0(4)$ that is holomorphic on $\mathcal{H}$ whose Fourier series has the form [Bor95a, Lemma 14.2]

$$f(D; z) = q^{-D} + \sum_{n=1}^{\infty} c(D; n) q^n, \tag{3.7}$$

where $c(D; n) = 0$ for every $n \equiv 2, 3 \pmod 4$. Borcherds' theory [Bor95a, Bor95b] implies that

$$F(D; z) = q^{-H(-D)} \prod_{n=1}^{\infty} (1 - q^n)^{c(D; n^2)} \tag{3.8}$$

is a weight zero modular function on $\mathrm{SL}_2(\mathbb{Z})$ whose divisor consists of a pole of order $H(-D)$ at $z = \infty$ and a simple zero at each Heegner point with discriminant $-D$. For each D we consider the following formal power series (also defined in (1.14)):

$$\mathfrak{F}(D; q) = -H(-D) - \sum_{n=0}^{\infty} A(D; n) q^n := -H(-D) - \sum_{n=1}^{\infty} \sum_{d|n} c(D; d^2)\, dq^n. \tag{3.9}$$

If D and p satisfy the hypotheses of the theorem, then [BO03, Corollary 3] implies that $\mathfrak{F}(D; q)$ is a p-adic modular form of weight 2. Serre proved [Ser73, Theorem 7], for certain p-adic modular forms, that the constant term of the Fourier expansion is essentially the p-adic limit of its Fourier

coefficients at exponents which are pth powers. In these cases we obtain

$$H(-D) = \begin{cases} \frac{1}{24}\lim_{n\to+\infty} A(D;2^n) & \text{if } D \equiv 3 \pmod 8, \\ \frac{1}{12}\lim_{n\to+\infty} A(D;3^n) & \text{if } D \equiv 1 \pmod 3, \\ \frac{1}{6}\lim_{n\to+\infty} A(D;5^n) & \text{if } D \equiv 2,3 \pmod 5, \\ \frac{1}{4}\lim_{n\to+\infty} A(D;7^n) & \text{if } D \equiv 1,2,4 \pmod 7. \end{cases} \tag{3.10}$$

Since $F(D;z)$ has weight zero, for every positive integer n Theorem 5 implies

$$A(D;p^n) = j_{p^n}(\tau_1) + \cdots + j_{p^n}(\tau_{H(-D)}),$$

where $\tau_1, \ldots, \tau_{H(-D)} \in \mathfrak{F}$ are the Heegner points of discriminant $-D$. Since the $j(\tau_i)$ are conjugates over $\mathbb{Q}$, the theorem follows from (3.10) and the fact that each j_n is an integral polynomial in j. □

4. Proofs of Theorem 10 and Corollary 11

We adopt the notation from the proof of Theorem 9. We begin by recalling the following theorem which is proved in [BO03, Corollary 3].

Theorem 4.1. *If $0 < D \equiv 3 \pmod 8$, then $\mathfrak{F}(D;q)$ is a weight two 2-adic modular form.*

Using the local nilpotency of the Hecke algebra on modular forms of $\mathrm{SL}_2(\mathbb{Z})$ modulo 2, we make the following vital observation.

Theorem 4.2. *Suppose that $f = \sum_{n=0}^{\infty} a(n)q^n \in M_k(1)$ has integer coefficients. If s is a positive integer and $t \geqslant ks/12$, then for every set of odd primes $p_1, p_2, \ldots, p_t$ we have*

$$f|T_k(p_1)|T_k(p_2)|\cdots|T_k(p_t) \equiv 0 \pmod{2^s}.$$

Proof. Begin by noticing that the Fourier expansion of every Eisenstein series on $\mathrm{SL}_2(\mathbb{Z})$ is congruent to 1 modulo 2. Serre [Ser76] observed that the Hecke operators act nilpotently on $S_k(1) \pmod 2$, the space of cusp forms modulo 2 on $\mathrm{SL}_2(\mathbb{Z})$. If $\Delta \in S_{12}(1)$ is the unique normalized weight 12 cusp form

$$\Delta(z) = q\prod_{n=1}^{\infty}(1-q^n)^{24} = q - 24q^2 + \cdots,$$

then $S_k(1) \pmod 2$ has $\mathbb{F}_2$-basis

$$\{\Delta^i \pmod 2 : 1 \leqslant i \leqslant \lfloor k/12 \rfloor\}.$$

Serre's observation implies that, if j is a positive integer, then

$$\Delta^j|T_k(p) \equiv \sum_{i=1}^{j-1}\alpha(i)\Delta^i \pmod 2,$$

where $\alpha(i) \in \mathbb{F}_2$, and so we have

$$f|T_k(p_1)|T_k(p_2)|\cdots|T_k(p_t) \equiv 0 \pmod 2 \tag{4.1}$$

whenever $t \geqslant k/12$. One easily obtains the result by successive division by 2 and iteration of (4.1). □

As an immediate corollary, we obtain the following inequality.

Corollary 4.3. *Suppose that $f = \sum_{n=1}^{\infty} a(n)q^n \in M_k(1)$ has integer coefficients. If s is a positive integer, then*

$$\max\{\omega(n) : n \text{ odd and square-free with } \mathrm{ord}_2(a(n)) < s\} < ks/12.$$

Proof. If $t \geqslant ks/12$, then let $p_1, p_2, \ldots, p_t$ be distinct odd primes. Let $f_0 := f$, and for $1 \leqslant i \leqslant t$ let $f_i = \sum_{n=0}^{\infty} a_i(n)q^n$ be the modular forms defined inductively by

$$f_i := f_{i-1} \mid T_k(p_i). \tag{4.2}$$

By Theorem 4.2, we have

$$a_t(M) \equiv 0 \pmod{2^s}$$

for every M. In particular, (4.2) implies that

$$\begin{aligned} 0 &\equiv a_t(1) \\ &= a_{t-1}(p_t) \\ &= a_{t-2}(p_{t-1}p_t) \\ &\;\;\vdots \\ &= a(p_1p_2\cdots p_t) \pmod{2^s}. \end{aligned}$$

This completes the proof. □

Theorem 4.4. *If $s \geqslant 4$ and $0 < D \equiv 3 \pmod 8$, then $\mathfrak{F}(D;q) \pmod{2^s}$ is the reduction modulo 2^s of a modular form with integer coefficients in $M_{k(D,s)}(1)$ where*

$$k(D,s) := 12 \cdot 2^{s-4}H(-D) + 2.$$

Proof. By construction [BO03, Proposition 2.1], we have

$$\mathfrak{F}(D;q) = \frac{\Theta(F(D;z))}{F(D;z)}. \tag{4.3}$$

We see that $\mathfrak{F}(D;q)$ is a weight 2 meromorphic modular form on $\mathrm{SL}_2(\mathbb{Z})$ which is non-vanishing at infinity. Moreover, it has a simple zero at each Heegner point τ with discriminant $-D$ and no other singularities.

It is well known that $j(\omega) = 0$. Let $\tau_1, \ldots, \tau_{H(-D)}$ denote the Heegner points of discriminant $-D$. For each $1 \leqslant i \leqslant H(-D)$ define $E(D,i;z)$ by

$$E(D,i;z) := E_4^3(z) \cdot \left(1 - \frac{j(\tau_i)}{j(z)}\right). \tag{4.4}$$

Observe that the modular function $1 - j(\tau_i)/j(z)$ has a simple pole at $z = \omega$ and a simple zero at $z = \tau_i$. Since $E_4^3(z)$ has a simple zero at $z = \omega$, the modular form $E(D,i;z)$ is a holomorphic modular form in $M_{12}(1)$. Since $E_4(z) \equiv 1 \pmod{16}$ and $j(\tau_i) \equiv 0 \pmod{2^{15}}$ (see [GZ85]), we have that

$$E(D,i;z) \equiv 1 \pmod{16}.$$

Hence, if $s \geqslant 4$, then

$$E(D,i;z)^{2^{s-4}} \equiv 1 \pmod{2^s}.$$

Therefore, if $s \geqslant 4$, then

$$\mathfrak{F}(D;q) \equiv \frac{\Theta(F(D;z))}{F(D;z)} \cdot \prod_{i=1}^{H(-D)} E(D,i;z)^{2^{s-4}} \pmod{2^s}. \tag{4.5}$$

The modular form on the right-hand side of (4.5) is holomorphic and has weight

$$k(D,s) = 12 \cdot 2^{s-4}H(-D) + 2.$$

This completes the proof. □

Proofs of Theorem 10 and Corollary 11. By Corollary 4.3 and Theorem 4.4, we have that if $A(D;n) \not\equiv 0 \pmod{2^s}$, then

$$\begin{aligned}\omega(n) &< \frac{k(D,s)s}{12} \\ &= \frac{(12\cdot 2^{s-4}H(-D)+2)s}{12} \\ &= 2^{s-4}s\cdot H(-D) + s/6.\end{aligned}$$

Therefore, we find that

$$\frac{\omega(n)}{2^{s-4}s} - \frac{1}{3\cdot 2^{s-3}} < H(-D).$$

This completes the proofs. □

References

AKN97 T. Asai, M. Kaneko and H. Ninomiya, *Zeros of certain modular functions and an application*, Comm. Math. Univ. Sancti Pauli **46** (1997), 93–101.

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. Int. Congress of Mathematicians, Zürich, 1994*, vol. 1, 2, ed. S. D. Chatterji (Birkhäuser, Basel, 1995), 744–752.

BO03 J. H. Bruinier and K. Ono, *The arithmetic of Borcherds exponents*, Math. Ann. **327** (2003), 293–303.

ES96 W. Eholzer and N.-P. Skoruppa, *Product expansions of conformal characters*, Phys. Lett. B. **388** (1996), 82–89.

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).

Ram16 S. Ramanujan, *On certain arithmetical functions*, Trans. Camb. Phil. Soc. **22** (1916), 159–184 (Collected Papers, No. 18).

Ser73 J.-P. Serre, *Formes modulaires et fonctions zêta p-adiques*, Lecture Notes in Mathematics, vol. 350 (Springer, Berlin,1973), 191–268.

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

Zag02 D. Zagier, *Traces of singular moduli*, in *Motives, polylogarithms and Hodge theory, part I, Irvine, CA, 1998*, Int. Press Lecture Series, vol. 3, I, eds F. Bogomolov and L. Katzarkov (International Press, Somerville, MA, 2002), 211–244.

Jan H. Bruinier bruinier@math.uni-koeln.de
Department of Mathematics, University of Wisconsin, Madison, Wisconsin 53706, USA
Current address: Mathematisches Institut, Universität Köln, Im Weyertal 86-90, D-50931 Köln, Germany

Winfried Kohnen winfried@mathi.uni-heidelberg.de
Mathematisches Institut, Universität Heidelberg, INF 288, D-69120 Heidelberg, Germany

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