THE ARITHMETIC OF BORCHERDS' EXPONENTS

Jan H. Bruinier and Ken Ono

1. Introduction and Statement of Results.

Recently, Borcherds [B] provided a striking description for the exponents in the naive infinite product expansion of many modular forms. For example, if $E_k(z)$ denotes the usual normalized weight k Eisenstein series, let $c(n)$ denote the integer exponents one obtains by expressing $E_4(z)$ as an infinite product:

$$E_4(z) = 1 + 240\sum_{n=1}^{\infty}\sum_{d|n} d^3 q^n = (1-q)^{-240}(1-q^2)^{26760}\cdots = \prod_{n=1}^{\infty}(1-q^n)^{c(n)} \tag{1.1}$$

($q := e^{2\pi i z}$ throughout). Although one might not suspect that there is a precise description or formula for the exponents $c(n)$, Borcherds provided one. He proved that there is a weight 1/2 meromorphic modular form

$$G(z) = \sum_{n\geq -3} b(n)q^n = q^{-3} + 4 - 240q + 26760q^4 + \cdots - 4096240q^9 + \dots$$

with the property that $c(n) = b(n^2)$ for every positive integer n.

It is natural to examine other methods for studying such exponents. Here we point out a p-adic method which is based on the fact that the logarithmic derivative of a meromorphic modular form is often a weight two p-adic modular form. To illustrate our result, use (1.1) to define the series $C(q)$

$$C(q) = 6\sum_{n=1}^{\infty}\sum_{d|n} c(d)dq^n = -1440q + 319680q^2 - 73733760q^3 + \cdots \tag{1.2}$$

Both authors thank the Number Theory Foundation and the National Science Foundation for their generous support. The first author acknowledges the support of a Heisenberg Fellowship. The second author acknowledges the support of an Alfred P. Sloan Foundation Fellowship, a David and Lucile Packard Foundation Fellowship, and an H. I. Romnes Fellowship.

Typeset by $\mathcal{A}\mathcal{M}\mathcal{S}$-TEX

If $\eta(z) = q^{1/24}\prod_{n=1}^{\infty}(1-q^n)$ denotes Dedekind's eta-function, then it turns out that

$$C(q) \equiv q + 9q^2 + 10q^3 + 2q^4 + q^5 + \cdots \equiv \eta^2(z)\eta^2(11z) \pmod{11}.$$

Therefore, if $p \neq 11$ is prime, then $a_E(p) \equiv 1 + 6c(p)p \pmod{11}$, where $a_E(p)$ is the trace of the pth Frobenius endomorphism on $X_0(11)$. This example illustrates our general result.

Let K be a number field and let O_v be the completion of its ring of integers at a finite place v with residue characteristic p. Moreover, let λ be a uniformizer for O_v. Following Serre [S2], we say that a formal power series

$$f = \sum_{n=0}^{\infty} a(n)q^n \in O_v[[q]]$$

is a p-adic modular form of weight k if there is a sequence $f_i \in O_v[[q]]$ of holomorphic modular forms on $SL_2(\mathbb{Z})$, with weights k_i, for which $\mathrm{ord}_\lambda(f_i - f) \to +\infty$ and $\mathrm{ord}_\lambda(k - k_i) \to +\infty$.

Theorem 1. *Let $F(z) = q^h\left(1 + \sum_{n=1}^{\infty} a(n)q^n\right) \in O_K[[q]]$ be a meromorphic modular form on $SL_2(\mathbb{Z})$, where O_K is the ring of integers in a number field K. Moreover, let $c(n)$ denote the numbers defined by the formal infinite product*

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

If p is prime and $F(z)$ is good at p (see §3 for the definition), then the formal power series

$$B = h - \sum_{n=1}^{\infty}\sum_{d|n} c(d)dq^n$$

is a weight two p-adic modular form.

Here we present cases where $F(z)$ is good at p. As usual, let $j(z)$ be the modular function

$$j(z) = q^{-1} + 744 + 196884q + 21493760q^2 + \cdots.$$

Let $\mathbb{H}$ be the upper half of the complex plane. We shall refer to any complex number $\tau \in \mathbb{H}$ of the form $\tau = \frac{-b+\sqrt{b^2-4ac}}{2a}$ with $a, b, c \in \mathbb{Z}$, $\gcd(a, b, c) = 1$ and $b^2 - 4ac < 0$ as a *Heegner point*. Moreover, we let $d_\tau := b^2 - 4ac$ be its discriminant. The values of j at such points are known as *singular moduli*, and it is well known that these values are algebraic integers. A meromorphic modular form $F(z)$ on $SL_2(\mathbb{Z})$ has a *Heegner divisor* if its zeros and poles are supported at the cusp at infinity and Heegner points.

Although we shall emphasize those forms $F(z)$ which have Heegner divisors, we stress that Theorem 1 holds for many forms which do not have a Borcherds product. For example, $E_{p-1}(z)$ is good at p for every prime $p \geq 5$. The next result describes some forms with Heegner divisors which are good at a prime p.

Theorem 2. *Let* $F(z) = q^h\left(1 + \sum_{n=1}^{\infty} a(n)q^n\right) \in \mathbb{Z}[[q]]$ *be a meromorphic modular form on* $SL_2(\mathbb{Z})$ *with a Heegner divisor whose Heegner points* $\tau_1, \tau_2, \cdots, \tau_s \in \mathbb{H}/SL_2(\mathbb{Z})$ *have fixed discriminant* d. *The following are true.*

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

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

then $F(z)$ *is good at* p.

(2) *If* $s = 1$ *and* $\tau_1 = (-1 + \sqrt{-3})/2$ *(resp.* $\tau_1 = i$*), then* $F(z)$ *is good at every prime* $p \equiv 2, 3, 5, 11 \pmod{12}$ *(resp.* $p \equiv 2, 3, 7, 11 \pmod{12}$*).*

(3) *If* $p = 2$ *(resp.* $p = 3$*) and* $|d| \equiv 3 \pmod 8$ *(resp.* $|d| \equiv 1 \pmod 3$*), then* $F(z)$ *is good at* p.

(4) *Suppose that* $5 \leq p \equiv 2 \pmod 3$ *is a prime for which* $\left(\frac{d}{p}\right) \in \{0, -1\}$ *and*

$$\prod_{i=1}^{s} j(\tau_i) \equiv 0 \pmod{p}.$$

If $\mathbb{Q}(\sqrt{d}) \neq \mathbb{Q}(\sqrt{-3})$ *or* $\left(\frac{d}{p}\right) = -1$, *then* $F(z)$ *is good at* p.

(5) *Suppose that* $5 \leq p \equiv 3 \pmod 4$ *is a prime for which* $\left(\frac{d}{p}\right) \in \{0, -1\}$ *and*

$$\prod_{i=1}^{s} (j(\tau_i) - 1728) \equiv 0 \pmod{p}.$$

If $\mathbb{Q}(\sqrt{d}) \neq \mathbb{Q}(i)$ *or* $\left(\frac{d}{p}\right) = -1$, *then* $F(z)$ *is good at* p.

Remarks.

(1) Since $j(i) = 1728$ (resp. $j((-1 + \sqrt{-3})/2) = 0$), Theorem 2 (2) applies to the modular form $j(z) - 1728$ (resp. $j(z)$), as well as the Eisenstein series $E_6(z)$ (resp. $E_4(z)$).

(2) By the theory of complex multiplication, the singular moduli $j(\tau_1), \ldots, j(\tau_s)$, associated to the points in Theorem 2, form a complete set of Galois conjugates over $\mathbb{Q}$, and the multiplicities of each τ_i is fixed in the divisor of $F(z)$.

(3) For fundamental discriminants d, the work of Gross and Zagier [G-Z] provides a simple description of those primes p which do not satisfy the condition in Theorem 2 (1).

(4) Theorem 2 admits a generalization to those forms with algebraic integer coefficients and Heegner divisors. In particular, it can be modified to cover such forms where the multiplicities of the τ_i in the divisor of $F(z)$ are not all equal.

Theorem 2 has interesting consequences regarding class numbers of imaginary quadratic fields. If $0 < D \equiv 0, 3 \pmod 4$, then let $H(-D)$ be the Hurwitz class number for the discriminant $-D$. For each such D there is a unique meromorphic modular form of weight $1/2$ on $\Gamma_0(4)$, which is holomorphic on the upper half complex plane, whose Fourier expansion has the form [Lemma 14.2, B]

$$f(D;z) = q^{-D} + \sum_{1 \leq n \equiv 0,1 \pmod 4} c_D(n) q^n \in \mathbb{Z}[[q]]. \tag{1.3}$$

Borcherds' theory implies that

$$F(D;z) = q^{-H(-D)} \prod_{n=1}^{\infty} (1-q^n)^{c_D(n^2)} \tag{1.4}$$

is a weight zero modular function on $SL_2(\mathbb{Z})$ whose divisor is a Heegner divisor consisting of a pole of order $H(-D)$ at $z = \infty$ and a simple zero at each Heegner point with discriminant $-D$. At face value, to compute this correspondence one needs the coefficients of $f(D;z)$ and the class number $H(-D)$. Here we obtain, in many cases, a p-adic class number formula for $H(-D)$ in terms of the coefficients of $f(D;z)$. Therefore, in these cases the correspondence is uniquely determined by the coefficients of $f(D;z)$.

Corollary 3. *If $0 < D \equiv 0, 3 \pmod 4$ and $-D$ is fundamental, then the following are true.*

(1) *If $D \equiv 3 \pmod 8$, then as 2-adic numbers we have*

$$H(-D) = \frac{1}{24} \sum_{n=0}^{\infty} c_D(4^n) 2^n.$$

(2) *If $D \equiv 1 \pmod 3$, then as 3-adic numbers we have*

$$H(-D) = \frac{1}{12} \sum_{n=0}^{\infty} c_D(9^n) 3^n.$$

(3) *If $D \equiv 0, 2, 3 \pmod 5$, then as 5-adic numbers we have*

$$H(-D) = \frac{1}{6} \sum_{n=0}^{\infty} c_D(25^n) 5^n.$$

(4) *If $D \equiv 0, 1, 2, 4 \pmod 7$, then as 7-adic numbers we have*

$$H(-D) = \frac{1}{4} \sum_{n=0}^{\infty} c_D(49^n) 7^n.$$

Acknowledgements

The authors thank Scott Ahlgren, Winfried Kohnen, Barry Mazur and Tonghai Yang for their helpful comments and suggestions.

2. Preliminaries

We recall essential facts regarding meromorphic modular forms on $SL_2(\mathbb{Z})$ and the arithmetic of infinite products. If $F(q) = \sum_{n \geq n_0} a(n)q^n$, then let Θ be the standard differential operator on formal q-series defined by

$$\Theta(F(q)) = \sum_{n \geq n_0} na(n)q^n. \tag{2.1}$$

Throughout, let $F(q)$ be a formal power series of the form

$$F(q) = q^h \left(1 + \sum_{n=1}^{\infty} a(n)q^n\right), \tag{2.2}$$

and let the $c(n)$ be the numbers for which

$$F(q) = q^h \prod_{n=1}^{\infty} (1 - q^n)^{c(n)}. \tag{2.3}$$

Proposition 2.1. *If $F(q)$ and the numbers $c(n)$ are as in (2.2) and (2.3), then*

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

Proof. For convenience, let $H(q)$ be the series defined by

$$H(q) = -\sum_{n=1}^{\infty} c(n)q^n. \tag{2.4}$$

As formal power series, we have

$$\begin{aligned}\log(F(q)) = \log(q^h) + \sum_{n=1}^{\infty} c(n)\log(1 - q^n) &= \log(q^h) - \sum_{n=1}^{\infty} c(n) \sum_{m=1}^{\infty} \frac{q^{mn}}{m} \\ &= \log(q^h) - \sum_{m=1}^{\infty} \frac{H(q^m)}{m}.\end{aligned}$$

By logarithmic differentiation, with respect to q, we obtain

$$\frac{qF'(q)}{F(q)} = \frac{\Theta(F(q))}{F(q)} = h - \sum_{m=1}^{\infty} H'(q^m)q^m = h - \sum_{m=1}^{\infty}\sum_{n=1}^{\infty} c(n)nq^{mn}.$$

□

Following Ramanujan, let $P(z)$ denote the nearly modular Eisenstein series

$$P(z) = 1 - 24\sum_{n=1}^{\infty}\sum_{d|n} dq^n. \tag{2.5}$$

Lemma 2.2. *Let $F(z) = F(q)$ be a weight k meromorphic modular form on $SL_2(\mathbb{Z})$ satisfying (2.2). If the numbers $c(n)$ are as in (2.3), then there is a weight $k+2$ meromorphic modular form $\tilde{F}(z)$ on $SL_2(\mathbb{Z})$ for which*

$$\frac{1}{12}\left(\frac{\tilde{F}(z)}{F(z)} + kP(z)\right) = h - \sum_{n=1}^{\infty}\sum_{d|n} c(d)dq^n.$$

If $F(z)$ is a holomorphic modular (resp. cusp) form, then $\tilde{F}(z)$ is a holomorphic modular (resp. cusp) form. Moreover, the poles of $\tilde{F}(z)$ are supported at the poles of $F(z)$.

Proof. It is well known [p. 17, O] that the function $\tilde{F}(z)$ defined by

$$\tilde{F}(z) := 12\Theta(F(z)) - kP(z)F(z)$$

is a meromorphic modular form of weight $k+2$ on $SL_2(\mathbb{Z})$. Moreover, if $F(z)$ is a holomorphic modular (resp. cusp) form, then $\tilde{F}(z)$ is a holomorphic modular (resp. cusp) form. The result now follows immediately from Proposition 2.1.

□

The remaining results in this section are useful for computing explicit examples of Theorem 1, and for proving Theorems 2 and 3. As usual, if $k \geq 4$ is an even integer, then let $E_k(z)$ denote the Eisenstein series

$$E_k(z) := 1 - \frac{2k}{B_k}\sum_{n=1}^{\infty} \sigma_{k-1}(n)q^n. \tag{2.6}$$

Throughout, let ω be the cube root of unity

$$\omega := \frac{-1+\sqrt{-3}}{2}. \tag{2.7}$$

Lemma 2.3. *Suppose that $k \geq 4$ is even.*

(1) *We have $E_k(z) \equiv 1 \pmod{24}$.*
(2) *If $p \geq 5$ is prime and $(p-1) \mid k$, then $E_k(z) \equiv 1 \pmod{p}$.*
(3) *If $k \not\equiv 0 \pmod{3}$, then $E_k(\omega) = 0$.*
(4) *If $k \equiv 2 \pmod{4}$, then $E_k(i) = 0$.*

Proof. Since $z = i$ (resp. $z = \omega$) is fixed by the modular transformation $Sz = -1/z$ (resp. $Az = -(z+1)/z$), the definition of a modular form implies that $E_k(i) = 0$ whenever $k \equiv 2 \pmod{4}$, and $E_k(\omega) = 0$ whenever $k \not\equiv 0 \pmod{3}$. The claimed congruences follows immediately from (2.6) and the von Staudt-Clausen theorem on the divisibility of denominators of Bernoulli numbers [p. 233, I-R].

□

3. Proofs of the main results

We begin by defining what it means for a modular form to be "good at p".

Definition 3.1. *Let $F(z) = q^h \left(1 + \sum_{n=1}^{\infty} a(n)q^n\right) \in O_K[[q]]$ be a meromorphic modular form on $SL_2(\mathbb{Z})$ whose zeros and poles, away from $z = \infty$, are at the points $z_1, z_2, \cdots z_s$. We say that $F(z)$ is good at p if there is a holomorphic modular form $\mathcal{E}(z)$ with p-integral algebraic coefficients for which the following are true:*

(1) *We have the congruence $\mathcal{E}(z) \equiv 1 \pmod{p}$.*
(2) *For each $1 \leq i \leq s$ we have $\mathcal{E}(z_i) = 0$.*

Proof of Theorem 1. By Lemma 2.2, there is a weight $k+2$ meromorphic modular form $\tilde{F}(z)$ on $SL_2(\mathbb{Z})$, whose poles are supported at the poles of $F(z)$, for which

$$\frac{1}{12}\left(\frac{\tilde{F}(z)}{F(z)} + kP(z)\right) = h - \sum_{n=1}^{\infty} \sum_{d \mid n} c(d) d q^n.$$

Since Serre [S2] proved that $P(z)$ is a weight two p-adic modular form, it suffices to prove that $\tilde{F}(z)/F(z)$ is a weight 2 p-adic modular form. For every $j \geq 0$, we have

$$\mathcal{E}(z)^{p^j} \equiv 1 \pmod{p^{j+1}}. \tag{3.1}$$

Since $\tilde{F}(z)/F(z)$ has weight two, it follows that $\mathcal{E}(z)^{p^j}\tilde{F}(z)/F(z)$, for sufficiently large j, is a holomorphic modular form of weight $p^j b + 2$, where b is the weight of $\mathcal{E}(z)$. If $\mathcal{E}(z)^{p^j}\tilde{F}(z)/F(z)$ does not have algebraic integer coefficients, then multiply it by a suitable integer $t_{j+1} \equiv 1 \pmod{p^{j+1}}$ so that the resulting series does. Therefore by (3.1), the sequence $\mathfrak{F}_{j+1}(z) := t_{j+1}\mathcal{E}(z)^{p^j}\tilde{F}(z)/F(z)$ defines a sequence of holomorphic modular forms which p-adically converges to $\tilde{F}(z)/F(z)$ with weights which converge p-adically to 2. In other words, $\tilde{F}(z)/F(z)$ is a p-adic modular form of weight 2.

□

Proof of Theorem 2. In view of Definition 3.1, it suffices to produce a holomorphic modular form $\mathcal{E}(z)$ on $SL_2(\mathbb{Z})$ with algebraic p-integral coefficients for which $\mathcal{E}(\tau_i) = 0$, for each $1 \leq i \leq s$, which satisfies the congruence

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

First we prove (1). For each $1 \leq i \leq s$, let A_i be the elliptic curve

$$A_i: \quad y^2 = x^3 - 108j(\tau_i)(j(\tau_i) - 1728)x - 432j(\tau_i)(j(\tau_i) - 1728)^2. \tag{3.2}$$

Each A_i is defined over the number field $\mathbb{Q}(j(\tau_i))$ with j-invariant $j(\tau_i)$. A simple calculation reveals that if $\mathfrak{p}$ is a prime ideal above a prime $p \geq 5$ in the integer ring of $\mathbb{Q}(j(\tau_i))$ for which

$$j(\tau_i)(j(\tau_i) - 1728) \not\equiv 0 \pmod{\mathfrak{p}}, \tag{3.3}$$

then A_i has good reduction at $\mathfrak{p}$. Suppose that $p \geq 5$ is a prime which is inert or ramified in $\mathbb{Q}(\sqrt{d})$ satisfying (3.3) for every prime ideal $\mathfrak{p}$ above p. By the theory of complex multiplication [p. 182, L], it follows that $j(\tau_i)$ is a supersingular j-invariant in $\overline{\mathbb{F}}_p$.

A famous observation of Deligne (see, for example [S1], [Th. 1, K-Z]) implies that every supersingular j-invariant in characteristic p is the reduction of $j(Q)$ modulo p for some point Q which is a zero of $E_{p-1}(z)$. Therefore, there are points $Q_1, Q_2, \dots, Q_s$ in the fundamental domain of the action of $SL_2(\mathbb{Z})$ (not necessarily distinct) for which $E_{p-1}(Q_i) = 0$, for all $1 \leq i \leq s$, with the additional property that

$$\prod_{i=1}^{s}(X - j(Q_i)) \equiv \prod_{i=1}^{s}(X - j(\tau_i)) \pmod{p} \tag{3.4}$$

in $\mathbb{F}_p[X]$. Now define $\mathcal{E}(z)$ by

$$\mathcal{E}(z) := \prod_{i=1}^{s}\left(E_{p-1}(z) \cdot \frac{j(z) - j(\tau_i)}{j(z) - j(Q_i)}\right). \tag{3.5}$$

By Lemma 2.3 (2), (3.4) and (3.5), it follows that $\mathcal{E}(\tau_i) = 0$ for each $1 \leq i \leq s$, and also satisfies the congruence $\mathcal{E}(z) \equiv 1 \pmod{p}$. Moreover, $\mathcal{E}(z)$ is clearly a holomorphic modular form, and so $F(z)$ is good at p. This proves (1).

Since $j(i) = 1728$ (resp. $j(\omega) = 0$), Lemma 2.3 shows that $F(z)$ is good at every prime $p \equiv 2, 3, 7, 11 \pmod{12}$ (resp. $p \equiv 2, 3, 5, 11 \pmod{12}$). This proves (2).

To prove (3), one argues as in the proof of (1) and (2) using Lemma 2.3 (1, 3, 4), and the Gross and Zagier congruences [Cor. 2.5, G-Z]

$$|d| \equiv 3 \pmod 8 \implies j(\tau_i) \equiv 0 \pmod{2^{15}},$$
$$|d| \equiv 1 \pmod 3 \implies j(\tau_i) \equiv 1728 \pmod{3^6}.$$

In view of (2), to prove (4) and (5) we may assume that

$$\prod_{i=1}^{s} j(\tau_i)(j(\tau_i) - 1728) \neq 0.$$

We use a classical theorem of Deuring on the reduction of differences of singular moduli modulo prime ideals $\mathfrak{p}$. In particular, if $\mathbb{Q}(\sqrt{d}) \notin \{\mathbb{Q}(i), \mathbb{Q}(\sqrt{-3})\}$, then since $\{j(\tau_1), \ldots, j(\tau_s)\}$ forms a complete set of Galois conjugates over $\mathbb{Q}$, Deuring's result implies that (see [Th. 13.21, C], [D])

$$\prod_{i=1}^{s} j(\tau_i) \equiv 0 \pmod p \implies p \equiv 2 \pmod 3, \tag{3.6}$$

$$\prod_{i=1}^{s} (j(\tau_i) - 1728) \equiv 0 \pmod p \implies p \equiv 3 \pmod 4. \tag{3.7}$$

The same conclusion in (3.6) (resp. (3.7)) holds if $\mathbb{Q}(\sqrt{d}) = \mathbb{Q}(\sqrt{-3})$ (resp. $\mathbb{Q}(\sqrt{d}) = \mathbb{Q}(i)$) provided that $p \nmid d$. A straightforward modification of the proof of (1), using Lemma 2.3 (2, 3, 4), now proves that $F(z)$ is good at p.

□

Proof of Corollary 3. Since $-D$ is fundamental, Theorem 2 shows that $F(D;z)$ is good at the primes p as dicated by the statement of Corollary 3. Define integers $A_D(n)$ by

$$\sum_{n=1}^{\infty} A_D(n) q^n := \sum_{n=1}^{\infty} \sum_{d|n} c_D(d^2) d q^n. \tag{3.8}$$

Therefore, by the conclusion of Theorem 1 it follows that

$$-H(-D) - \sum_{n=1}^{\infty} A_D(n) q^n \tag{3.9}$$

is a weight two p-adic modular form for the relevant primes $p \leq 7$.

Serre proved [Th. 7, S2], 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 p^{th} powers. In these cases we obtain

$$H(-D) = \begin{cases} \frac{1}{24}\lim_{n\to+\infty} A_D(2^n) & \text{if } D \equiv 3 \pmod 8, \\ \frac{1}{12}\lim_{n\to+\infty} A_D(3^n) & \text{if } D \equiv 1 \pmod 3, \\ \frac{1}{6}\lim_{n\to+\infty} A_D(5^n) & \text{if } D \equiv 0,2,3 \pmod 5, \\ \frac{1}{4}\lim_{n\to+\infty} A_D(7^n) & \text{if } D \equiv 0,1,2,4 \pmod 7. \end{cases}$$

□

4. Some examples

Example 4.1. Let $f(7;z) = \sum_{n=-7}^{\infty} c_7(n)q^n$ be the weight 1/2 modular form on $\Gamma_0(4)$ defined in (1.3). Its q-expansion begins with the terms

$$f(z) = q^{-7} - 4119q + 8288256q^4 - 52756480q^5 + \cdots .$$

By the Borcherds isomorphism [Th. 14.1, B], there is a modular form of weight 0 on $SL_2(\mathbb{Z})$ with a simple pole at ∞ and a simple zero at $z = (1+\sqrt{-7})/2$ with the Fourier expansion

$$F(7;z) = q^{-1}\prod_{n=1}^{\infty}(1-q^n)^{c_7(n^2)} = \frac{1}{q} + 4119 + 196884q + 21493760q^2 + 864299970q^3 + \cdots$$

Since $j((1+\sqrt{-7})/2) = -15^3 \equiv 0 \pmod 5$, by the proof of Theorem 2 (4), there is a weight 6 holomorphic modular form on $SL_2(\mathbb{Z})$ which is congruent to

$$-1 - \sum_{n=1}^{\infty}\sum_{d|n} c_7(d^2)dq^n \equiv 4 + 4q + 2q^2 + q^3 + \cdots \pmod 5.$$

This is $4E_6(z) \pmod 5$, and so $c_7(n^2) \equiv 1 \pmod 5$ if $n \not\equiv 0 \pmod 5$.

Example 4.2. Here we illustrate the class number formulas stated in Corollary 3. If $D = 59$, then we have that

$$f(59;z) = q^{-59} + \sum_{n=1}^{\infty} c_{59}(n)q^n = q^{-59} - 30197680312q + 4559500440054043557 12q^4 + \cdots .$$

By Corollary 3 (1), we have

$$H(-59) = 3 = \frac{1}{24}\sum_{n=0}^{\infty} c_D(4^n)2^n.$$

One easily checks that the first two terms satisfy

$$H(-59) = 3 \equiv \frac{1}{24}(-30197680312 + 455950044005404355712\cdot 2) \pmod{2^9}.$$

References

[B] R. E. Borcherds, *Automorphic forms on* $O_{s+2,2}(\mathbb{R})$ *and infinite products*, Inventiones Mathematicae **120** (1995), 161-213.

[C] D. Cox, *Primes of the form* x^2+ny^2*, Fermat, Class Field Theory, and Complex Multiplication*, Wiley Publ., New York, 1989.

[D] M. Deuring, *Teilbarkeitseigenschaften der singulären moduln der elliptischen funktionen und die diskriminante der klassengleichung*, Comm. Math. Helv. **19** (1946), 74-82.

[G-Z] B. Gross and D. Zagier, *On singular moduli*, J. reine angew. math. **355** (1985), 191-220.

[I-R] K. Ireland and M. Rosen, *A classical introduction to modern number theory*, Springer-Verlag, New York, 1990.

[K-Z] M. Kaneko and D. Zagier, *Supersingular* j*-invariants, hypergeometric series and Atkin's orthogonal polynomials*, Comp. perspectives on Number Theory (Chicago, Illinois 1995), AMS/IP Stud. Adv. Math., Amer. Math. Soc. **7** (1998), 97-126.

[L] S. Lang, *Elliptic functions, 2nd edition*, Springer-Verlag, 1987.

[O] A. Ogg, *Survey of modular functions of one variable*, Springer Lect. Notes in Math. **320** (1973), 1-36.

[S1] J.-P. Serre, *Congruences et formes modulaires (d'après H. P. F. Swinnerton-Dyer)*, Sem. Bourbaki **416** (1971-1972), 74-88.

[S2] J.-P. Serre, *Formes modulaires et fonctions zêta* p*-adiques*, Springer Lect. Notes in Math. **350** (1973), 191-268.

[Sh] G. Shimura, *Introduction to the arithmetic of automorphic forms*, Iwanawi Shoten and Princeton Univ. Press, 1971.

Department of Mathematics, University of Wisconsin, Madison, Wisconsin 53706
E-mail address: `bruinier@math.wisc.edu`

Department of Mathematics, University of Wisconsin, Madison, Wisconsin 53706
E-mail address: `ono@math.wisc.edu`