2-ADIC PROPERTIES OF HECKE TRACES OF SINGULAR MODULI.

Matthew Boylan

Abstract. In [Z], Zagier initiated a study of the function $t_1(d)$, the function which gives the trace of a singular modulus of discriminant $-d < 0$. Ahlgren and Ono [A-O, Theorem 1 (1)] proved that if p is an odd prime which splits in $\mathbb{Q}(\sqrt{-d})$, then $t_1(p^2 d) \equiv 0 \pmod{p}$. A question of Ono [O, Problem 7.30] asks for generalizations modulo arbitrary prime powers. We provide the answer for $p = 2$. In particular, we show, for all positive integers n and d, that

$$t_1(4^n \cdot (8d+7)) \equiv 0 \pmod{2 \cdot 16^n}.$$

1. Introduction and Statement of Results.

An important function in number theory is the elliptic modular invariant,

$$j(z) := q^{-1} + 744 + 196884q + 21493760q^2 + \cdots \in \frac{1}{q}\mathbb{Z}[[q]],$$

where throughout, $z \in \mathfrak{h}$, the complex upper half-plane, and $q := e^{2\pi i z}$. Of particular interest are *singular moduli*, values of j at quadratic irrationalities in $\mathfrak{h}$. These values are algebraic integers which generate ring class field extensions of imaginary quadratic number fields.

We begin by fixing notation. If $d \equiv 0, 3 \pmod 4$ is a positive integer (so that $-d$ is the discriminant of an order in an imaginary quadratic field), we define $\mathcal{Q}_d$ to be the set of positive definite integral binary quadratic forms $Q(x,y) = ax^2 + bxy + cy^2$ with discriminant $-d = b^2 - 4ac$. The modular group $\Gamma := \mathrm{PSL}_2(\mathbb{Z})$ acts on $\mathcal{Q}_d$ in the usual way. For each $Q \in \mathcal{Q}_d$, we define α_Q to be the unique solution in $\mathfrak{h}$ to the equation $Q(x,1) = 0$. The value of the singular modulus $j(\alpha_Q)$ depends only on the Γ-equivalence class of Q.

When $-d < 0$ is a fundamental discriminant, $\mathcal{Q}_d$ consists of primitive forms. In this case, the number of equivalence classes of forms of discriminant $-d$ is equal to $h(-d)$, the class number of $\mathbb{Q}(\sqrt{-d})$. As Q runs through a complete set of representatives of $\mathcal{Q}_d/\Gamma$, the corresponding singular moduli $j(\alpha_Q)$ run through a complete set of algebraic conjugates. Therefore $j(\alpha_Q)$ has degree $h(-d)$ over $\mathbb{Q}$, and the sum

$$\sum_{Q \in \mathcal{Q}_d/\Gamma} j(\alpha_Q) \tag{1.1}$$

is its absolute algebraic trace.

2000 *Mathematics Subject Classification.* Primary: 11F33. Secondary: 11F37.

The author thanks the National Science Foundation for its support through a VIGRE postdoctoral fellowship.

Following Zagier [Z], we study a modified form of (1.1). We define

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

If m and d are positive integers with $d \equiv 0,3 \pmod 4$ (we do not require that $-d$ be fundamental), and if $T_0(m)$ is the normalized weight zero Hecke operator of index m, then the mth Hecke trace of the singular modulus of discriminant $-d$ is

$$t_m(d) := \sum_{Q \in \mathcal{Q}_d/\Gamma} \frac{((j(z)-744) \mid T_0(m))(\alpha_Q)}{\omega_Q}.$$

Using the Shimura Correspondence and ℓ-adic Galois representations, Ahlgren and Ono recently proved striking congruences of several types for the functions $t_m(d)$. One of these [A-O, Theorem 1 (1)] states that if $p \nmid m$ is an odd prime which splits in $\mathbb{Q}(\sqrt{-d})$, then $t_m(p^2 d) \equiv 0 \pmod p$. Problem 7.30 of Ono's CBMS monograph [O] asks for natural generalizations modulo arbitrary prime powers. As a special case of a more general theorem, we provide the answer for the case of $p = 2$.

Theorem 1. *Suppose that d, n, and m are positive integers with m odd. If $d \equiv 7 \pmod 8$, then we have*

$$t_m(4^n d) \equiv 0 \pmod{2 \cdot 16^n}.$$

Remarks.

(1) If we keep the hypotheses in Theorem 1 and denote by $h(-d)$ the class number of the order of discriminant $-d$, then by Gauss' genus theory, we have

$$h(-4^n d) \equiv 0 \pmod{2^{n-1}}.$$

It is interesting to note the similarity between these congruences and the congruences in Theorem 1.

(2) The congruences in Theorem 1 are reminiscent of the famous Ramanujan congruences for the ordinary partition function $p(n)$ modulo powers of 5, 7, and 11 (see, for example [A] and [Kn, §7, 8]). However, the proofs of these congruences and the proof of Theorem 1 differ in several fundamental ways.

(3) There are many other divisibility results for singular moduli in the literature. The most famous 2-divisibility result is the congruence of Gross and Zagier [G-Z, Cor. 2.5] which states that if α is an imaginary quadratic argument of discriminant $-d \equiv 5 \pmod 8$, then $j(\alpha) \equiv 0 \pmod{2^{15}}$.

(4) Since the writing of this paper, corresponding congruences modulo arbitrary powers of odd primes have been proved independently by Edixhoven [E], Jenkins [J], and Guerzhoy [G]. Moreover, Bruinier, Jenkins, and Ono [B-J-O] have proved explicit formulas for traces using weak Maass Poincaré series.

Theorem 1 is a consequence of the following general theorem. The cube of the ordinary theta function is $\theta(z)^3 = \left(\sum_{n\in\mathbb{Z}} q^{n^2}\right)^3$, a holomorphic modular form of weight $\frac{3}{2}$ on the congruence subgroup $\Gamma_0(4)$ of $\mathrm{SL}_2(\mathbb{Z})$. We denote by $T_{\frac{3}{2}}(m^2)$ the usual weight $\frac{3}{2}$ Hecke operator of index m^2. Since $\theta(z)^3$ lies in a one-dimensional space and since the Hecke operators preserve spaces of modular forms, we find that for every integer $m \geq 1$, there is an integer α_m for which

$$\theta(z)^3 \mid T_{\frac{3}{2}}(m^2) = \alpha_m \theta(z)^3.$$

For example, when m is an odd prime, $\alpha_m = m + 1$. Our general theorem is

Theorem 2. *Suppose that n and m are positive integers with m odd. Then we have*

$$\sum_{d=0}^{\infty} t_m(4^n d) q^d \equiv 2\alpha_m \theta(z)^3 \pmod{2 \cdot 16^n}.$$

If $d \equiv 0, 3 \pmod 4$ is a positive integer, we recall that the Hurwitz-Kronecker class number of discriminant $-d$ is

$$H(-d) := \sum_{Q \in \mathcal{Q}_d/\Gamma} \frac{1}{\omega_Q}.$$

As a consequence of Theorem 2 and Gauss' formula for the coefficients of $\theta(z)^3$ in terms of Hurwitz-Kronecker class numbers, we obtain

Theorem 3. *Suppose that d, n, and m are positive integers with $4 \nmid d$ and m odd. Then we have*

$$t_m(4^n d) \equiv \begin{cases} 24\alpha_m H(-4d) \pmod{2 \cdot 16^n} & \text{if } d \equiv 1, 2 \pmod 4, \\ 48\alpha_m H(-d) \pmod{2 \cdot 16^n} & \text{if } d \equiv 3 \pmod 8, \\ 0 \pmod{2 \cdot 16^n} & \text{if } d \equiv 7 \pmod 8. \end{cases}$$

Since Theorems 1 and 3 are immediate corollaries of Theorem 2, Sections 2-5 of this paper are devoted to the proof of Theorem 2. The proof involves a detailed study of the action of the U_{4^n} operator, where n is a positive integer, on a certain weakly holomorphic modular form whose coefficients interpolate Hecke traces. In particular, we carefully study the 2-divisibility of the coefficients of the form resulting from this action.

The proof is organized as follows. In Section 2, we briefly record some facts about modular forms. In Section 3, we state Theorem 3.1 and show that it implies Theorem 2. In Sections 4 and 5, we prove Theorem 3.1.

2. Preliminaries on modular forms.

In this section we record some facts about modular forms. For more details, see for example [K] or [O]. If $N > 0$ is an integer, $k > 0$ is an integer or half-integer, and χ is a Dirichlet character modulo N, then we define $\mathcal{M}_k(\Gamma_0(N), \chi)$ to be the complex vector space of weakly holomorphic modular forms of weight k on the congruence subgroup $\Gamma_0(N)$ with character χ. These forms are holomorphic on $\mathfrak{h}$ and meromorphic at the cusps of $\Gamma_0(N)$. We let $M_k(\Gamma_0(N), \chi)$ denote the finite-dimensional subspace of forms which are holomorphic at the cusps.

The Dedekind eta-function,

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

is an important building block for modular forms. We also define

$$E_4(z) := 1 + 240\sum_{n=1}^{\infty}\sum_{d|n} d^3q^n = \frac{\eta^{16}(z)}{\eta^8(2z)} + 2^8 \cdot \frac{\eta^{16}(2z)}{\eta^8(z)} = 1 + 240q + 2160q^2 + \cdots \in M_4(\Gamma_0(1)), \tag{2.1}$$

$$\Delta(z) := \eta^{24}(z) = q - 24q^2 + 252q^3 + \cdots \in M_{12}(\Gamma_0(1)),$$

$$F(z) := \frac{\eta^8(4z)}{\eta^4(2z)} = q + 4q^3 + 6q^5 + \cdots \in M_2(\Gamma_0(4)), \tag{2.2}$$

and

$$\theta(z) := 1 + 2\sum_{n=1}^{\infty} q^{n^2} = \frac{\eta^5(z)}{\eta^2(z)\eta^2(4z)} \in M_{\frac{1}{2}}(\Gamma_0(4)). \tag{2.3}$$

If $m \geq 1$ is an integer, we recall that the usual U_m operator acts on formal power series by

$$\left(\sum_{n=n_0}^{\infty} a(n)q^n\right) \mid U_m = \sum_{mn=n_0} a(mn)q^n.$$

For more details concerning how this operator acts on spaces of holomorphic modular forms, see for example, [A-L] or [S-S].

Next, we define the function v_2 on $\mathbb{Q}$ by

$$v_2\left(\frac{m}{n}\right) := \text{ord}_2(m) - \text{ord}_2(n).$$

We also set $v_2(0) := \infty$. If $f = \sum_{n=n_0}^{\infty} a(n)q^n \in \mathbb{Z}[[q]]$, then we define

$$v_2(f) := \inf_{n \geq n_0}\{v_2(a(n))\}.$$

3. A reduction.

In this section, we prove that Theorem 2 follows from

Theorem 3.1. *Suppose that $n \geq 1$ is an integer. For every integer $m = 1, 2, \ldots, 4^{n-1}$, there are integers $c_n(m)$ such that*

$$\frac{\frac{F(z)}{\theta(z)} \mid U_{4^n}}{\theta(z)^3} = \sum_{m=1}^{4^{n-1}} c_n(m)\left(\frac{\eta^8(4z)}{\eta^8(z)}\right)^m$$

and such that

$$v_2(c_n(m)) \geq 4n + 4m - 4.$$

We begin by relating Hecke traces to modular forms. We define

$$g_1(z) := \frac{\eta^2(z)}{\eta(2z)} \cdot \frac{E_4(4z)}{\eta^6(4z)} \in \mathcal{M}_{\frac{3}{2}}(\Gamma_0(4)).$$

In [Z, Theorem 1], Zagier showed that

$$g_1(z) = q^{-1} - 2 - \sum_{\substack{d \equiv 0,3 \pmod 4 \\ d>0}} t_1(d) q^d.$$

If $m \geq 1$ is an odd integer, we define a weakly holomorphic modular form $g_m(z)$ with coefficients $b_m(d)$ by

$$g_m(z) := g_1(z) \mid T_{\frac{3}{2}}(m^2) = \sum_{d \equiv 0,3 \pmod 4} b_m(d) q^d \in \mathcal{M}_{\frac{3}{2}}(\Gamma_0(4)).$$

By [Z, Theorem 5], for every positive integer $d \equiv 0, 3 \pmod 4$, we find that $t_m(d) = -b_m(d)$. Now we suppose that $n \geq 1$ is an integer. Since

$$g_m(z) \mid U_{4^n} = (g_1(z) \mid T_{\frac{3}{2}}(m^2)) \mid U_{4^n} = (g_1(z) \mid \ U_{4^n}) \mid \ T_{\frac{3}{2}}(m^2),$$

to prove Theorem 2 it suffices to prove that

$$g_1(z) \mid U_{4^n} \equiv -2\theta(z)^3 \pmod{2 \cdot 16^n}. \tag{3.1}$$

In particular, we will show that Theorem 3.1 implies (3.1).

If Theorem 3.1 holds, then for every integer $n \geq 1$, we have that

$$v_2\left(\frac{\frac{F(z)}{\theta(z)} \mid U_{4^n}}{\theta(z)^3}\right) = v_2\left(\frac{F(z)}{\theta(z)} \mid U_{4^n}\right) \geq 4n.$$

Hence, Theorem 3.1 implies that

$$\frac{F(z)}{\theta(z)} \mid U_{4^n} \equiv 0 \pmod{16^n}.$$

Therefore, (3.1) will follow from

Lemma 3.2. *Suppose that $n \geq 1$ is an integer. If we have*

$$\frac{F(z)}{\theta(z)} \mid U_{4^{n-1}} \equiv 0 \pmod{16^{n-1}},$$

then

$$g_1(z) \mid U_{4^n} \equiv -2\theta(z)^3 \pmod{2 \cdot 16^n}.$$

To prove Lemma 3.2, we require an auxiliary proposition. For convenience, we define

$$g(z) := \frac{\eta^8(4z)}{\eta^8(z)} = q + 8q^2 + 44q^3 + \cdots \in \mathcal{M}_0(\Gamma_0(4)). \tag{3.2}$$

We remark that $g(z)$ is a generator of the modular function field of $\Gamma_0(4)$.

Proposition 3.3. *The following are true.*

(1)
$$g_1(z) \mid U_4 = -2 \cdot \frac{\theta(z)^3 F(z) E_4(z)}{\eta^{12}(2z)}.$$

(2)
$$\frac{F(z)}{\theta(z)} \mid U_4 = -2^4 \theta(z)^3 g(z).$$

(3)
$$\frac{\eta^{16}(z)}{\eta^8(2z)} = \frac{\eta^{16}(2z)}{\eta^8(4z)} - 2^4 \cdot \frac{\eta^8(4z)\eta^8(z)}{\eta^8(2z)}.$$

Proof. To prove (1), we see by a standard calculation using facts about modular forms that

$$\theta(4z)\eta^{12}(8z)g_1(z) \in M_8(\Gamma_0(16)).$$

Hence, we have

$$(\theta(4z)\eta^{12}(8z)g_1(z)) \mid U_4 = \theta(z)\eta^{12}(2z) \cdot (g_1(z) \mid U_4) \in M_8(\Gamma_0(4)).$$

Using a suitable basis for this space, we verify that

$$\theta(z)\eta^{12}(2z) \cdot (g_1(z) \mid U_4) = -2\theta(z)^4 F(z) E_4(z),$$

from which (1) follows. Part (2) follows in a similar way, by verifying that

$$\left(\theta(4z)\eta^{12}(8z) \cdot \frac{F(z)}{\theta(z)}\right) \mid U_4 = -2^4 \theta(z)^8 F(z)^2 \in M_8(\Gamma_0(4)).$$

One easily verifies (3) since both forms lie in $M_4(\Gamma_0(4))$, a space of dimension 3. $\square$

We now use Proposition 3.3 to prove Lemma 3.2. An application of Proposition 3.3.1 and (2.1) gives

$$g_1(z) \mid U_4 = -2 \cdot \frac{\theta(z)^3 F(z)}{\eta^{12}(2z)} \cdot \left(\frac{\eta^{16}(z)}{\eta^8(2z)} + 2^8 \cdot \frac{\eta^{16}(2z)}{\eta^8(z)}\right).$$

Then using Proposition 3.3.3, (2.2), (2.3), (3.2), and Proposition 3.3.2, we deduce that

$$g_1(z) \mid U_4 = -2\theta(z)^3 + 2^5 \cdot \frac{F(z)}{\theta(z)} + 2^5 \cdot \left(\frac{F(z)}{\theta(z)} \mid U_4\right).$$

If for a fixed integer $n \geq 1$, we assume that $\frac{F(z)}{\theta(z)} \mid U_{4^{n-1}} \equiv 0 \pmod{16^{n-1}}$, then the above calculation together with the fact that $\theta(z)^3 \mid U_4 = \theta(z)^3$ gives

$$g_1(z) \mid U_{4^n} = -2\theta(z)^3 \mid U_{4^{n-1}} + 2 \cdot 16 \cdot \left(\frac{F(z)}{\theta(z)} \mid U_{4^{n-1}} + \frac{F(z)}{\theta(z)} \mid U_{4^n}\right) \equiv -2\theta(z)^3 \pmod{2 \cdot 16^n}.$$

This proves Lemma 3.2, and with it, Theorem 2. $\square$

4. Proof of Theorem 3.1.

The proof of Theorem 3.1 proceeds by induction on n. By Proposition 3.3, part 2, we find that

$$\frac{\frac{F(z)}{\theta(z)} \mid U_4}{\theta(z)^3} = -2^4 g(z), \tag{4.1}$$

which proves the base case of the induction. For integers $n \geq 1$, we define

$$L_n(z) := \frac{\frac{F(z)}{\theta(z)} \mid U_{4^n}}{\theta(z)^3}.$$

Before proceeding with the induction step, we make the vital observation that

$$\left(\frac{\theta(z)^3}{\theta(4z)^3} \cdot L_n(z)\right) \mid U_4 = \left(\frac{\theta(z)^3}{\theta(4z)^3} \cdot \frac{\frac{F(z)}{\theta(z)} \mid U_{4^n}}{\theta(z)^3}\right) \mid U_4 = \frac{\frac{F(z)}{\theta(z)} \mid U_{4^{n+1}}}{\theta(z)^3} = L_{n+1}(z). \tag{4.2}$$

We first show that the case of $n = 1$ implies the case of $n = 2$. By (4.1) and (4.2), we calculate

$$L_2(z) = \left(\frac{\theta(z)^3}{\theta(4z)^3} \cdot L_1(z)\right) \mid U_4 = -2^4 \cdot \left(\frac{\theta(z)^3}{\theta(4z)^3} \cdot g(z)\right) \mid U_4. \tag{4.3}$$

Using standard facts about modular forms, we verify that

$$\begin{aligned}&\left(\Delta(4z)^2 \cdot \frac{\theta(z)^3}{\theta(4z)^3} \cdot g(z)\right) \mid U_4 = \Delta(z)^2 \cdot \left(\frac{\theta(z)^3}{\theta(4z)^3} \cdot g(z)\right) \mid U_4 \\ &= \Delta(z)^2 \cdot (2^4 \cdot 35 g(z) + 2^{12} \cdot 23 g(z)^2 + 2^{18} \cdot 13 g(z)^3 + 2^{25} g(z)^4) \in M_{24}(\Gamma_0(4)),\end{aligned}$$

which implies that

$$\left(\frac{\theta(z)^3}{\theta(4z)^3} \cdot g(z)\right) \mid U_4 = 2^4 \cdot 35 g(z) + 2^{12} \cdot 23 g(z)^2 + 2^{18} \cdot 13 g(z)^3 + 2^{25} g(z)^4. \tag{4.4}$$

Combining (4.3) and (4.4), we find that

$$L_2(z) = -2^8 \cdot 35 g(z) - 2^{16} \cdot 23 g(z)^2 - 2^{22} \cdot 13 g(z)^3 - 2^{29} g(z)^4,$$

which verifies the case of $n = 2$.

We now suppose, for some integer $n \geq 2$, that

$$L_n(z) = \sum_{m=1}^{4^{n-1}} c_n(m) g(z)^m, \tag{4.5}$$

where

$$v_2(c_n(m)) \geq 4n + 4m - 4. \tag{4.6}$$

To finish the induction, we must establish (4.5) and (4.6) with n replaced by $n+1$. Using (4.2) and (4.5), we calculate

$$L_{n+1}(z) = \left(\frac{\theta(z)^3}{\theta(4z)^3} \cdot L_n(z)\right) \mid U_4 = \sum_{m=1}^{4^{n-1}} c_n(m) \cdot \left(\frac{\theta(z)^3}{\theta(4z)^3} \cdot g(z)^m\right) \mid U_4. \tag{4.7}$$

Given (4.7), we will show that Theorem 3.1 follows from

Theorem 4.1. *Suppose that $m \geq 1$ is an integer. Then for every integer $s = \left\lfloor \frac{m+3}{4} \right\rfloor, \dots, 4m$, there are integers $b_m(s)$ such that*

$$\left(\frac{\theta(z)^3}{\theta(4z)^3} \cdot g(z)^m \right) \mid U_4 = \sum_{s=\left\lfloor \frac{m+3}{4} \right\rfloor}^{4m} b_m(s) g(z)^s,$$

and such that

$$v_2(b_m(s)) \geq \max(0, 5s - 2m).$$

If we suppose that Theorem 4.1 holds (we defer the proof to Section 5), then combining it with (4.7) gives

$$L_{n+1}(z) = \sum_{m=1}^{4^{n-1}} c_n(m) \cdot \left(\sum_{s=\left\lfloor \frac{m+3}{4} \right\rfloor}^{4m} b_m(s) g(z)^s \right). \tag{4.8}$$

If $n \geq 2$, we express (4.8) as

$$L_{n+1}(z) = \sum_{s=1}^{4^{n-2}} \left(\sum_{m=\left\lfloor \frac{s+3}{4} \right\rfloor}^{4s} c_n(m) b_m(s) \right) g(z)^s + \sum_{s=4^{n-2}+1}^{4^n} \left(\sum_{m=\left\lfloor \frac{s+3}{4} \right\rfloor}^{4^{n-1}} c_n(m) b_m(s) \right) g(z)^s.$$

Hence, for $n \geq 2$, we find that

$$c_{n+1}(s) = \begin{cases} \sum_{m=\left\lfloor \frac{s+3}{4} \right\rfloor}^{4s} c_n(m) b_m(s) & \text{if } 1 \leq s \leq 4^{n-2}, \\ \sum_{m=\left\lfloor \frac{s+3}{4} \right\rfloor}^{4^{n-1}} c_n(m) b_m(s) & \text{if } 4^{n-2}+1 \leq s \leq 4^n. \end{cases} \tag{4.9}$$

To finish the proof of Theorem 3.1, we must show for all integers $s \geq 1$, that

$$v_2(c_{n+1}(s)) \geq 4(n+1) + 4s - 4 = 4n + 4s. \tag{4.10}$$

First, we settle the case of $s = 1$. Since $n \geq 2$, (4.9) gives

$$c_{n+1}(1) = \sum_{m=1}^{4} c_n(m) b_m(1). \tag{4.11}$$

By (4.4), we know that

$$v_2(b_1(1)) = 4, \tag{4.12}$$

while by Theorem 4.1, we know that

$$v_2(b_2(1)),\ v_2(b_3(1)),\ v_2(b_4(1)) \geq 0. \tag{4.13}$$

Using (4.11), (4.6), (4.12), and (4.13), it follows that

$$v_2(c_{n+1}(1)) \geq \min(v_2(c_n(m)) + v_2(b_m(1))) \geq \min(4n + 4m - 4 + v_2(b_m(1))) \geq 4n + 4$$

which establishes (4.10) when $s = 1$.

We now suppose that $s \geq 2$. By (4.9), (4.6), and Theorem 4.1, we find that

$$\begin{aligned} v_2(c_{n+1}(s)) &\geq \min(v_2(c_n(m)) + v_2(b_m(s))) \geq 4n + 5s - 4 + \min(2m) \\ &\geq 4n + 5s - 4 + 2 \cdot \left\lfloor \frac{s+3}{4} \right\rfloor, \end{aligned} \tag{4.14}$$

where the minimum in (4.14) is taken over m in the intervals specified in (4.9). Moreover, we find that

$$4n + 5s - 4 + 2 \cdot \left\lfloor \frac{s+3}{4} \right\rfloor \geq 4n + 4s$$

if and only if $s \geq 2$. This establishes (4.10) for $s \geq 2$, and with it, Theorem 3.1. $\square$

5. Proof of Theorem 4.1.

We first note that (4.4) verifies the $m = 1$ case of Theorem 4.1. A similar computation shows that

$$\begin{aligned} \left(\frac{\theta(z)^3}{\theta(4z)^3} \cdot g(z)^2 \right) \mid U_4 &= 2^2 \cdot 65g(z) + 2^8 \cdot 17303g(z)^2 + 2^{14} \cdot 7085g(z)^3 + 2^{21} \cdot 5305g(z)^4 \\ &\quad + 2^{28} \cdot 1855g(z)^5 + 2^{36} \cdot 165g(z)^6 + 2^{42} \cdot 29g(z)^7 + 2^{49}g(z)^8, \end{aligned}$$

verifying the $m = 2$ case.

The first step toward verifying the cases where $m \geq 3$ is to show that the modular function $\frac{\theta(z)^3}{\theta(4z)^3} \cdot g(z)^m$ on $\Gamma_0(16)$ is expressible as a polynomial with integer coefficients in a suitably chosen generator of the modular function field of $\Gamma_0(16)$. We then obtain lower bounds on the 2-divisibility of the coefficients of this polynomial. For our purpose, we choose the generator

$$h(z) := \frac{\eta^2(16z)\eta(2z)}{\eta(8z)\eta^2(z)} = q + 2q^2 + 4q^3 + \cdots. \tag{5.1}$$

Theorem 4.1 follows by applying the next two lemmas together.

Lemma 5.1. *Suppose that $m \geq 3$ is an integer. Then for $t = m, \ldots, 4m$, there are integers $d_m(t)$ such that*

$$\frac{\theta(z)^3}{\theta(4z)^3} \cdot g(z)^m = \sum_{t=m}^{4m} d_m(t) h(z)^t,$$

and such that

$$v_2(d_m(t)) \geq t - m.$$

Lemma 5.2. *Suppose that $t \geq 1$ is an integer. Then for $s = \left\lfloor \frac{t+3}{4} \right\rfloor, \ldots, t$, there are integers $a_t(s)$ such that*

$$h(z)^t \mid U_4 = \sum_{s=\left\lfloor \frac{t+3}{4} \right\rfloor}^{t} a_t(s) g(z)^s,$$

and such that

$$v_2(a_t(s)) \geq 5s - t - \left\lfloor \frac{t+3}{4} \right\rfloor.$$

Proof that Lemma 5.1 and Lemma 5.2 $\implies$ Theorem 4.1.

Calculating directly using Lemmas 5.1 and 5.2, we obtain

$$\left(\frac{\theta(z)^3}{\theta(4z)^3} \cdot g(z)^m\right) \mid U_4 = \sum_{t=m}^{4m} d_m(t) \cdot \left(h(z)^t \mid U_4\right) = \sum_{t=m}^{4m} d_m(t) \cdot \left(\sum_{s=\left\lfloor \frac{t+3}{4} \right\rfloor}^{t} a_t(s) g(z)^s\right).$$

We rewrite this sum as

$$\left(\frac{\theta(z)^3}{\theta(4z)^3} \cdot g(z)^m\right) \mid U_4 = \sum_{s=\left\lfloor \frac{m+3}{4} \right\rfloor}^{m} \left(\sum_{t=m}^{4s} d_m(t) a_t(s)\right) g(z)^s + \sum_{s=m+1}^{4m} \left(\sum_{t=s}^{4m} d_m(t) a_t(s)\right) g(z)^s.$$

Therefore, we find that

$$b_m(s) = \begin{cases} \sum_{t=m}^{4s} d_m(t) a_t(s) & \text{if } \left\lfloor \frac{m+3}{4} \right\rfloor \leq s \leq m, \\ \sum_{t=s}^{4m} d_m(t) a_t(s) & \text{if } m+1 \leq s \leq 4m. \end{cases} \tag{5.2}$$

By Lemmas 5.1 and 5.2, it follows that

$$\begin{aligned} v_2(b_m(s)) &\geq \min(v_2(d_m(t)) + v_2(a_t(s))) \geq 5s - m + \min\left(-\left\lfloor \frac{t+3}{4} \right\rfloor\right) \\ &\geq \begin{cases} 5s - m - \left\lfloor \frac{4s+3}{4} \right\rfloor = 4s - m & \text{if } \left\lfloor \frac{m+3}{4} \right\rfloor \leq s \leq m, \\ 5s - m - \left\lfloor \frac{4m+3}{4} \right\rfloor \geq 5s - 2m & \text{if } m+1 \leq s \leq 4m, \end{cases} \end{aligned} \tag{5.3}$$

where the minimum in (5.3) is taken over t in the intervals specified by (5.2). Since all the $b_m(s)$ are integral and since $4s - m \geq 5s - 2m$ when $\left\lfloor \frac{m+3}{4} \right\rfloor \leq s \leq m$, the theorem follows. $\square$

Proof of Lemma 5.1.

The key ingredients in the proof of Lemma 5.1 are the next two propositions.

Proposition 5.3. *If $m \geq 1$ is an integer, then*

$$\frac{\theta(z)^3}{\theta(4z)^3} \cdot g(z)^m = h(z)^m \cdot (1 + 4h(z))^3 \cdot (1 + 2h(z))^{m-3} \cdot (1 + 4h(z) + 8h(z)^2)^m.$$

Proof. First, we find that

$$\Delta(z)g(z) = \Delta(z)h(z) \cdot (1 + 2h(z)) \cdot (1 + 4h(z) + 8h(z)^2) \in M_{12}(\Gamma_0(16)),$$

which implies that

$$g(z)^m = h(z)^m \cdot (1 + 2h(z))^m \cdot (1 + 4h(z) + 8h(z)^2)^m. \tag{5.4}$$

A similar calculation shows that

$$\theta(z)^4\eta^{12}(8z)\cdot(1+2h(z)) = \theta(z)^3\eta^{12}(8z)\theta(4z)\cdot(1+4h(z)) \in M_8(\Gamma_0(16)),$$

from which it follows that

$$\frac{\theta(z)^3}{\theta(4z)^3} = \left(\frac{1+4h(z)}{1+2h(z)}\right)^3. \tag{5.5}$$

The proposition follows from (5.4) and (5.5). □

For $m \geq 3$, we define polynomials $P_m(x)$ and $Q_m(x)$ with coefficients w_m and u_m, respectively, by

$$P_m(x) := \sum_{j=0}^{m} w_m(j)x^j = (1+4x)^3\cdot(1+2x)^{m-3},$$

$$Q_m(x) := \sum_{k=0}^{2m} u_m(k)x^k = (1+4x+8x^2)^m.$$

Proposition 5.4. *If $m \geq 3$ is an integer, then for every integer $j \geq 0$, we have*

$$v_2(w_m(j)) \geq j, \tag{5.6}$$

and for every integer $k \geq 0$, we have

$$v_2(u_m(k)) \geq 2k - \left\lfloor \frac{k}{2} \right\rfloor. \tag{5.7}$$

Proof. Expanding $P_m(x)$ gives

$$\begin{aligned} P_m(x) &= ((1+2x)+2x))^3\cdot(1+2x)^{m-3} \\ &= (1+2x)^m + 3\cdot 2x\cdot(1+2x)^{m-1} + 3\cdot 4x^2\cdot(1+2x)^{m-2} + 8x^3\cdot(1+2x)^{m-3} \\ &= \sum_{j=0}^{m}\binom{m}{j}2^jx^j + 3\sum_{j=1}^{m}\binom{m-1}{j-1}2^jx^j + 3\sum_{j=2}^{m}\binom{m-2}{j-2}2^jx^j + \sum_{j=3}^{m}\binom{m-3}{j-3}2^jx^j, \end{aligned}$$

which implies (5.6).

Expanding $Q_m(x)$ gives

$$Q_m(x) = \sum_{\substack{a+b+c=m \\ a,b,c\geq 0}} \frac{m!}{a!b!c!}(4x)^a(8x^2)^b.$$

If we set $r = a+b$, then we obtain

$$\begin{aligned} Q_m(x) &= \sum_{r=0}^{m}\sum_{\substack{a+b=r \\ a,b\geq 0}} \frac{m!}{(m-r)!a!b!}\cdot(4x)^a(8x^2)^b = \sum_{r=0}^{m}\sum_{b=0}^{r}\frac{m!}{(m-r)!(r-b)!b!}\cdot 2^{2r+b}x^{r+b} \\ &= \sum_{r=0}^{m}\sum_{b=0}^{r}\binom{m}{r}\binom{r}{b}\cdot 2^{2r+b}x^{r+b}. \end{aligned}$$

Next, setting $k = r + b$ gives

$$Q_m(x) = \sum_{k=0}^{m} \left(\sum_{b=0}^{\lfloor \frac{k}{2} \rfloor} \binom{m}{k-b} \binom{k-b}{b} 2^{2k-b} \right) x^k + \sum_{k=m+1}^{2m} \left(\sum_{b=k-m}^{\lfloor \frac{k}{2} \rfloor} \binom{m}{k-b} \binom{k-b}{b} 2^{2k-b} \right) x^k, \tag{5.8}$$

from which (5.7) follows by calculating

$$v_2(u_m(k)) \geq \min(2k - b) \geq 2k - \left\lfloor \frac{k}{2} \right\rfloor,$$

where the minimum is taken over b in the intervals specified by (5.8). □

We now turn to the proof of Lemma 5.1. For every integer $m \geq 3$, we define a polynomial $R_m(x)$ with coefficients y_m by

$$R_m(x) := P_m(x)Q_m(x) = \sum_{\ell=0}^{3m} y_m(\ell) x^\ell.$$

By Proposition 5.3, for every integer $m \geq 3$ we have that

$$h(z)^m \cdot R_m(h(z)) = \frac{\theta(z)^3}{\theta(4z)^3} \cdot g(z)^m.$$

Hence, for $t = m, \ldots, 4m$, we see that $y_m(t - m) = d_m(t)$. Therefore, to prove Lemma 5.1, it suffices to show, for all integers $\ell \geq 0$, that $v_2(y_m(\ell)) \geq \ell$.

Expanding $R_m(x)$, we find that

$$\begin{aligned} R_m(x) = \left(\sum_{j=0}^{m} w_m(j) x^j \right) \cdot \left(\sum_{k=0}^{2m} u_m(k) x^k \right) &= \sum_{\ell=0}^{m} \left(\sum_{k=0}^{\ell} w_m(\ell - k) u_m(k) \right) x^\ell \\ &+ \sum_{\ell=m+1}^{2m} \left(\sum_{k=\ell-m}^{\ell} w_m(\ell - k) u_m(k) \right) x^\ell + \sum_{\ell=2m+1}^{3m} \left(\sum_{k=\ell-m}^{2m} w_m(\ell - k) u_m(k) \right) x^\ell. \end{aligned} \tag{5.9}$$

Therefore, for a fixed ℓ, we have by Proposition 5.4 that

$$v_2(y_m(\ell)) \geq \min(v_2(w_m(\ell - k)) + v_2(u_m(k))) \geq \min\left(\ell + k - \left\lfloor \frac{k}{2} \right\rfloor \right) \geq \ell,$$

where the minimum is taken over k in the intervals specified in (5.9). □

Proof of Lemma 5.2.

Before proving Lemma 5.2, we state a proposition.

Proposition 5.5. *If $g(z)$ is as in (3.2) and $h(z)$ is as in (5.1), then*

$$h(z)^4 - g(4z) \cdot (2^5 h(z)^3 + 2^3 \cdot 3h(z)^2 + 2^3 h(z) + 1) = 0. \tag{5.10}$$

Proof. We find that

$$\Delta(z) \cdot (h(z)^4 - g(4z) \cdot (2^5 h(z)^3 + 2^3 \cdot 3h(z)^2 + 2^3 h(z) + 1)) \in M_{12}(\Gamma_0(16)).$$

This space has dimension 25. It is therefore easy to verify that this form is identically zero. □

For a fixed integer $t \geq 1$, we want to express $h(z)^t \mid U_4$ as a polynomial in $g(z)$. Equation (5.10) is an identity in the variable z, so for any integer k, replacing z by $\frac{z+k}{4}$ in (5.10) and using the fact that $g\left(4 \cdot \left(\frac{z+k}{4}\right)\right) = g(z+k) = g(z)$, we find that

$$h\left(\frac{z+k}{4}\right)^4 - g(z) \cdot \left(2^5 h\left(\frac{z+k}{4}\right)^3 + 2^3 \cdot 3h\left(\frac{z+k}{4}\right)^2 + 2^3 h\left(\frac{z+k}{4}\right) + 1\right) = 0. \tag{5.11}$$

We now consider the polynomial $T(u)$ in the variable u defined by

$$T(u) := u^4 - g(z) \cdot (2^5 u^3 + 2^3 \cdot 3u^2 + 2^3 u + 1).$$

By (5.11), we see that $h\left(\frac{z}{4}\right)$, $h\left(\frac{z+1}{4}\right)$, $h\left(\frac{z+2}{4}\right)$, and $h\left(\frac{z+3}{4}\right)$ are roots, and by comparing q-expansions, that these four roots are distinct.

For every integer $t \geq 1$, we define $S_t(z)$ to be the sum of the t-th powers of the roots of $T(u)$, and note that

$$S_t(z) := \sum_{k=0}^{3} h\left(\frac{z+k}{4}\right)^t = 4h(z)^t \mid U_4. \tag{5.12}$$

Using Newton's Formula, we obtain

$$\begin{aligned} S_1(z) &= 2^5 g, \\ S_2(z) &= 2^4 \cdot 3g + 2^{10} g^2, \\ S_3(z) &= 2^3 \cdot 3g + 2^8 \cdot 3^2 g^2 + 2^{15} g^3, \\ S_4(z) &= 2^2 g + 2^7 \cdot 17 g^2 + 2^{15} \cdot 3g^3 + 2^{20} g^4, \end{aligned} \tag{5.13}$$

and for all $t \geq 5$,

$$S_t(z) = 2^5 g S_{t-1} + 2^3 \cdot 3g S_{t-2} + 2^3 g S_{t-3} + g S_{t-4}. \tag{5.14}$$

By (5.13) and (5.14), we see for all positive integers t, that there are integers $\alpha_t(s) \equiv 0 \pmod 4$ for which

$$S_t(z) = \sum_{s=\left\lfloor \frac{t+3}{4} \right\rfloor}^{t} \alpha_t(s) g(z)^s. \tag{5.15}$$

Therefore, by (5.12) and (5.15), there are integers $a_t(s) = \frac{\alpha_t(s)}{4}$ for which

$$h(z)^t \mid U_4 = \sum_{s=\left\lfloor \frac{t+3}{4} \right\rfloor}^{t} a_t(s) g(z)^s.$$

We now prove Lemma 5.2. Since $\alpha_t(s) = 4a_t(s)$, it suffices to show that

$$v_2(\alpha_t(s)) \geq 5s + 2 - t - \left\lfloor \frac{t+3}{4} \right\rfloor. \tag{5.16}$$

The proof is by induction on t. The explicit formulas in (5.13) show that the proposition is true for $1 \leq t \leq 4$.

We fix an integer $T \geq 4$ and suppose that (5.16) holds for all $t < T$. We will show that it holds for T. The formula (5.14) gives

$$\alpha_T(s) = 2^5\alpha_{T-1}(s-1) + 2^3 \cdot 3\alpha_{T-2}(s-1) + 2^3\alpha_{T-3}(s-1) + \alpha_{T-4}(s-1).$$

Therefore, we have

$$\begin{aligned} &v_2(\alpha_T(s)) \\ &\geq \min(5 + v_2(\alpha_{T-1}(s-1)),\ 3 + v_2(\alpha_{T-2}(s-1)),\ 3 + v_2(\alpha_{T-3}(s-1)),\ v_2(\alpha_{T-4}(s-1))). \end{aligned} \tag{5.17}$$

Lemma 5.2 follows by using the inductive hypothesis to bound each of the terms in (5.17) from below. This concludes the proof of Theorem 4.1. □

Acknowledgments. The author thanks S. Ahlgren and K. Ono for their helpful suggestions in the preparation of this paper.

References

[A-O] S. Ahlgren and K. Ono, *Arithmetic of singular moduli and class equations*, Compositio Math., to appear.

[A] A. O. L. Atkin, *Proof of a conjecture of Ramanujan*, Glasgow Math. J. **8** (1967), 14-32.

[A-L] A. O. L. Atkin and J. Lehner, *Hecke operators on* $\Gamma_0(N)$, Math. Ann. **185** (1970), 134-160.

[B-J-O] J. Bruinier, P. Jenkins, K. Ono, *Hilbert class polynomials and traces of singular moduli*, preprint.

[E] S. Edixhoven, *On the p-adic geometry of traces of singular moduli*, preprint, arXiv:math.NT/0502213 Feb. 10, 2005.

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

[G] P. Guerzhoy, *The Borcherds-Zagier isomorphism and a p-adic version of the Kohnen-Shimura map*, Inter. Math. Res. Not., to appear.

[J] P. Jenkins, *p-adic properties for traces of singular moduli*, preprint.

[Kn] M. Knopp, *Modular unctions in analytic number theory*, Chelsea New York, 2nd ed., 1993.

[K] N. Koblitz, *Introduction to elliptic curves and modular forms*, Springer-Verlag New York, GTM 97, 1993.

[O] K. Ono, *The web of modularity: Arithmetic of the coefficients of modular forms and q-series*, Amer. Math. Soc., CBMS Regional Conf. in Math., vol. 102, 2004.

[S-S] J.-P. Serre and H. Stark, *Modular forms of weight* $\frac{1}{2}$, Springer Lect. Notes in Math. **627** (1977), 29-68.

[Z] D. Zagier, *Traces of singular moduli*, Motives, polylogarithms and Hodge theory, Part I (Irvine, CA, 1998), Int. Press Lect. Ser. 3.1 (2002), Int. Press, Somerville, MA, 211-244.

Department of Mathematics, University of Illinois, Urbana, Illinois 61801
E-mail address: boylan@math.uiuc.edu