A mod ℓ Atkin-Lehner theorem and applications

Ken Ono and Nick Ramsey

Abstract. If $f(z)$ is a weight $k \in \frac{1}{2}\mathbb{Z}$ meromorphic modular form on $\Gamma_0(N)$ satisfying

$$f(z) = \sum_{n \geq n_0} a_n e^{2\pi i m n z},$$

where $m \nmid N$, then f is constant. If $k \neq 0$, then $f = 0$. Atkin and Lehner derived [2] the theory of integer weight *newforms* from this fact. We use the geometric theory of modular forms to prove the analog of this fact for modular forms modulo ℓ. We show that the same conclusion holds if $\gcd(N\ell, m) = 1$ and the nebentypus character is trivial at ℓ. We use this to study the parity of the partition function and the coefficients of Klein's j-function.

1. Introduction and statement of results

The Atkin-Lehner theory of newforms relies (see Theorem 1 of [2]) on the fact that a weight k meromorphic modular form f on $\Gamma_0(N)$ with a Fourier expansion of the form

$$f(z) = f(q) = \sum_{n \geq n_0} a_n q^{mn}$$

(note. $q := e^{2\pi i z}$), where $m \nmid N$, is constant. If $k \neq 0$, then $f = 0$. It is natural to ask whether this phenomenon exists for modular forms modulo ℓ. There are some obvious exceptions. For example, if ℓ is prime, then the weight 12ℓ cusp form $\Delta(z)^\ell$ on $\Gamma_0(1) = \mathrm{SL}_2(\mathbb{Z})$ satisfies

$$\Delta(z)^\ell := q^\ell \prod_{n=1}^{\infty} (1-q^n)^{24\ell} \equiv q^\ell \prod_{n=1}^{\infty} (1-q^{\ell n})^{24} \equiv \sum_{n \geq \ell} a_n q^{\ell n} \pmod{\ell}.$$

The first author is grateful for support from the NSF and the Asa Griggs Candler Fund.

Here we prove that the Atkin-Lehner theorem holds for modular forms modulo ℓ once one excludes such examples. More precisely, we prove the following theorem.

Theorem 1.1. *Suppose that f is a meromorphic modular form of weight $k \in \frac{1}{2}\mathbb{Z}$ on $\Gamma_0(N)$ which has integral Fourier coefficients at ∞. Let ℓ be a prime with the property that there is an $m > 1$ such that the Fourier expansion of f at ∞ satisfies*

$$f(q) \equiv \sum_{n \geq n_0} a_n q^{mn} \pmod{\ell}.$$

If $\gcd(N\ell, m) = 1$ and f has trivial nebentypus character at ℓ (i.e., f is fixed by the diamond operators at ℓ) if $\ell | N$, then we have that $f(q) \equiv a_0 \pmod{\ell}$.

Remark. Theorem 1.1 is a generalization of a result suggested by Serre to Mazur which appears in the classic paper on the Eisenstein ideal (see p. 83 of [7]). Naomi Jochnowitz has also informed the authors that she has obtained (in unpublished work) similar results using the classical theory of modular forms modulo p as developed by Serre.

We give two applications involving the parity of the coefficients of modular forms. The parity of the partition function $p(n)$ seems to be random, and a famous open conjecture [10] asserts that "half" of its values are even (resp. odd). Despite the difficulty of this conjecture, there are some results. For example, Subbarao's Conjecture [12] has been proved by the works of the first author and Radu [8, 11]. For every progression $r \pmod{t}$, there are infinitely many m (resp. n) for which $p(tm+r)$ (resp. $p(tn+r)$) is even (resp. odd).

We study an analog of Subbarao's Conjecture for certain quadratic polynomials. Let $h(-D)$ be the class number of the imaginary quadratic field $\mathbb{Q}(\sqrt{-D})$. Using Theorem 1.1 and *generalized* Borcherds products of the author and Bruinier [3, 9], we prove the following.

Theorem 1.2. *If $1 < D \equiv 23 \pmod{24}$ is square-free, then the following are true:*
(1) There are infinitely many m coprime to 6 for which $p\left(\frac{Dm^2+1}{24}\right)$ is even. Furthermore, the smallest one is bounded by $(12h(-D)+2)\prod_{p|D \text{ prime}}(p+1)$.
(2) There are infinitely many n coprime to 6 for which $p\left(\frac{Dn^2+1}{24}\right)$ is odd if there is at least one such n. Furthermore, the smallest one (if any) is bounded by $12h(-D)+2$.

Remark. We note that $(Dm^2+1)/24$ is an integer whenever m is coprime to 6.

Theorem 1.1 allows us to refine work of Alfes [1] on the coefficients of Klein's j-function

$$j(z) = \sum_{n=-1}^{\infty} c_n q^n = q^{-1} + 744 + 196884q + \dots. \tag{1.1}$$

Although it is simple to see that c_n is even for $n \not\equiv 7 \pmod 8$, little is known for the remaining n. Numerics suggest that "half" of these coefficients are odd. We prove the following theorem which builds on recent work of Alfes [1].

Theorem 1.3. *If $1 < D \equiv 7 \pmod 8$ is square-free, then the following are true:*
(1) There are infinitely many odd m for which c_{Dm^2} is even. Furthermore, the smallest one is bounded by $\left(h(-4D) + \frac{1}{6}\right) \cdot \prod_{p|4D \text{ prime}}(p+1)$.

(2) There are infinitely many odd n for which c_{Dn^2} is odd if there is at least one such n. Furthermore, the smallest one (if any) is bounded by $h(-4D)$.

Remark. Theorem 1.3 is equivalent to a statement about the parity of traces of certain singular moduli. By work of Zagier [13], the proof generalizes to further singular moduli.

The proof of the original Atkin-Lehner theorem [2] breaks down for modular forms modulo ℓ. Therefore, we adopt a geometric viewpoint. In Section 2 we recall features of the theory of geometric modular forms, which we use to prove Theorem 1.1 in Section 3. In Section 4 we then prove Theorems 1.2 and 1.3 by combining Theorem 1.1 with the theory of Borcherds products. These two theorems improve upon earlier work by the first author [9] and Alfes [1].

Acknowledgements

The authors thank Brian Conrad and Barry Mazur for their suggestions, and they thank Claudia Alfes and Christelle Vincent for comments on an earlier version of this paper.

2. Background on geometric modular forms

Integer weight modular forms arise as sections of line bundles on modular curves, which allows them to be interpreted in terms of relative differentials. Since modular curves are moduli spaces of generalized elliptic curves equipped with a prescribed torsion point, we may view modular forms geometrically. We prove Theorem 1.1 from this perspective. The proof essentially follows from a calculation involving the Tate elliptic curve, which allows us to geometrically study q-expansions of modular forms as moduli problems for elliptic curves.

Here we briefly recall the geometric theory of integer weight modular forms. This account is far from comprehensive, and is intended to cover the major facts that will be used to prove Theorem 1.1. We shall frequently refer to papers of Conrad, Katz, and Mazur [4, 5, 6].

2.1. Modular forms and modular curves

Denote by $\mathbb{H}$ the upper-half of the complex plane, and let $\overline{\mathbb{H}} := \mathbb{H} \cup \mathbb{Q} \cup \{\infty\}$. Let f be a classical modular form of weight $k \in \mathbb{Z}$ for $\Gamma_1(N)$. The automorphy factor by which f transforms defines a cocycle that gives rise to a natural line bundle $L(k)$ on the quotient $\Gamma_1(N)\backslash\mathbb{H}$ of which f is a section. This Riemann surface can be compactified by adding cusps to a compact Riemann surface $\Gamma_1(N)\backslash\overline{\mathbb{H}}$. The bundle $L(k)$ extends in a natural way to this compact Riemann surface and the growth condition on f imposed at the cusps is tantamount to the associated section extending to a holomorphic section on all of $\Gamma_1(N)\backslash\overline{\mathbb{H}}$. In a similar manner, a meromorphic modular form corresponds to a meromorphic section of this bundle.

The compact Riemann surface $\Gamma_1(N)\backslash\overline{\mathbb{H}}$ is the analytification of a smooth algebraic curve $X_1(N)_{\mathbb{C}}$ over $\mathbb{C}$. If $N \geq 5$, this curve can be interpreted as a moduli space of generalized elliptic curves equipped with a point of order N. In these terms, we have a complex uniformization of the non-cuspidal locus of this moduli space given by

$$\begin{array}{rcl} \Gamma_1(N)\backslash\mathbb{H} & \longrightarrow & Y_1(N)_{\mathbb{C}} \subset X_1(N)_{\mathbb{C}} \\ \tau & \longmapsto & \left(\mathbb{C}/\langle 1, \tau\rangle, \dfrac{1}{N}\right). \end{array} \tag{2.1}$$

There is a universal generalized elliptic curve $\pi : \mathcal{E} \to X_1(N)_{\mathbb{C}}$. Let ω denote the locally-free sheaf given by the push-forward $\pi_*\Omega_{\mathcal{E}/X_1(N)_{\mathbb{C}}}$ of the relative dualizing sheaf (which is simply the sheaf of relative differentials away from the cusps). Via the above uniformization, there is a natural identification of $L(k)$ with $\omega^{\otimes k}$, and this identification extends to the cusps.

The upshot is that sections of $\omega^{\otimes k}$ on $X_1(N)_{\mathbb{C}}$ give rise to classical modular forms of weight k and level N, and by Serre's GAGA, this is a one-to-one correspondence. In a similar way, meromorphic modular forms correspond to rational sections (in the sense of having poles) of $\omega^{\otimes k}$, as one can see by arguing with $\omega^{\otimes k}(D)$ for various divisors D corresponding to poles.

This description of modular forms opens the door for a discussion of modular forms over a host of fields and rings other than $\mathbb{C}$, since the moduli problems involved make sense in those contexts. In particular, if K is any field of characteristic zero, there is (still assuming $N \geq 5$) a fine moduli variety $X_1(N)_K$ classifying generalized elliptic curves over K-algebras equipped with a point of order N, and this variety is a smooth proper curve over K. Moreover, this claim holds verbatim if the characteristic of K is positive and relatively prime to N (see Theorems 3.2.7 and 4.2.1 of [4]). Note that this already furnishes a perfectly natural notion of modular forms in positive characteristic, at least at coprime level.

On the other hand, if the characteristic of K is positive and divides N, then the situation is less straight-forward, owing to the different nature of the N-torsion on an elliptic curve in characteristics dividing N. Here this phenomenon arises in a slightly different context, namely, *reducing* a moduli scheme defined over a certain ring of integers modulo a prime. We will also

be looking at a slightly different moduli problem. In particular, fix a rational prime $\ell \nmid N$ and let us work over the local ring $\mathbb{Z}_{(\ell)}$. Consider the $\Gamma(N;\ell^r)$ problem (in the notation of [4]) that classifies triples (E,P,C) where E is a generalized elliptic curve, P is a point of order N, and C is a cyclic subgroup of order ℓ^r. The precise definitions of these notions in this context can be found in [6] or [4]. By Theorem 4.2.1 of [4], there is a fine moduli scheme $X_1(N;\ell^r)_{\mathbb{Z}_{(\ell)}}$ representing this moduli problem. By Theorem 1.2.1 of [4], this scheme is regular and is a proper relative curve over $\mathbb{Z}_{(\ell)}$ with geometrically connected fibers.

The generic fiber of $X_1(N;\ell^r)_{\mathbb{Z}_{(\ell)}}$ is a smooth irreducible curve over $\mathbb{Q}$ as above. By Theorem 13.4.7 of [6], the reduction of $X_1(N;\ell^r)_{\mathbb{Z}_{(\ell)}}$ modulo ℓ is geometrically connected, but is comprised of $r+1$ geometrically irreducible components intersecting at the supersingular points. These components are indexed by pairs (a,b) of non-negative integers with $a+b=r$, where, roughly speaking, the "a" measures how much of the cyclic subgroup C comes from the kernel of Frobenius. In particular, on the $(r,0)$ component, C *is* the kernel of the r-iterated relative Frobenius map (away from supersingular points and cusps).

2.2. q-expansions and the Tate curve

The q-expansion of a geometric modular form at a cusp is the image of the form in the completed local ring at that cusp. Since these modular curves are moduli spaces, these completed local rings (being *points* of the scheme with values in a power series ring) themselves have a moduli interpretation. Let $\mathrm{Tate}(q)$ denote the Tate elliptic curve as defined in [5] or [4], which we will regard for the moment as being defined over the ring $\mathbb{Z}((q))$ of Laurent series over $\mathbb{Z}$ (though in general $\mathbb{Z}$ will be replaced by the ambient ring or field of definition). By [5], the N-torsion on the Tate curve is given by

$$\zeta_N^i q^{j/N}, \qquad 1 \le i,j \le N$$

and is all defined over the ring $\mathbb{Z}[\zeta_N]((q^{1/N}))$. We recall also that the curve $\mathrm{Tate}(q)$ comes equipped with a canonical differential ω_{can} (see the first Appendix A.1.2 of [5]).

Consider again the $\Gamma_1(N)$ problem in characteristic prime to N. By the moduli interpretation of $X_1(N)$ and ω, a geometric modular form f can be viewed as a rule that assigns to each pair (E,P) an element of $\Omega_E^{\otimes k}$ on E subject to some natural compatibilities (see [5]). Thus, given a point P of order N on the Tate curve, we may consider the value

$$f(\mathrm{Tate}(q),P) = \left(\sum a_n (q^{1/N})^n\right) \omega_{\mathrm{can}}^{\otimes k}.$$

These series (for varying P) *are* the q-expansions of f at the various cusps. Roughly speaking, the cusp associated to a point P is obtained as the "degenerate fiber" $q=0$ of the classifying map to $X_1(N)$ associated to the pair $(\mathrm{Tate}(q),P)$. In the geometric setting, we prefer to refer to the q-expansion at a pair $(\mathrm{Tate}(q),P)$ as above, rather than the associated cusp.

Via (2.1), the classical cusp ∞ corresponds to the pair $(\mathrm{Tate}(q), e^{2\pi i/N})$, and this pair is defined over the ring $\mathbb{C}(\!(q)\!)$. In particular, if f is a classical modular form of level N, its classical q-expansion at ∞ is obtained as

$$f(\mathrm{Tate}(q), e^{2\pi i/N}) = \left(\sum a_n q^n\right) \omega_{\mathrm{can}}^{\otimes k}.$$

We embed the cyclotomic field $\mathbb{Q}(\zeta_N)$ in $\mathbb{C}$ by sending the primitive root ζ_N to $e^{2\pi i/N}$. The q-expansion principle ([5], Corollary 1.6.2) implies that, if $a_n \in \mathbb{Q}(\zeta_N)$ for all n, then f is defined over $\mathbb{Q}(\zeta_N)$. Moreover, the classical q-expansion of f is recovered from $f(\mathrm{Tate}(q), \zeta_N)$.

Remark. We have considered the $\Gamma_1(N)$ problem for simplicity. We note that analogous results hold for all of the usual moduli problems (in particular for $\Gamma_1(N; \ell^r)$).

3. The proof of Theorem 1.1

First observe that we may assume that k is an integer, since we can replace f by a power to reduce to this case. Second, we may assume that the prime-to-ℓ part of the level N is at least 5, since we may artificially inflate the level without interfering with the conditions in the theorem. From here, the flow of the argument consists of two steps, namely:

1. We construct from f a section $\tilde{f}$ of $\omega^{\otimes k}(D_0)$ (with k an integer and D_0 a divisor) over the ordinary locus in $X_1(N')_F$, where $N' \geq 5$ is relatively prime to $m\ell$, with the property that its q-expansion at $(\mathrm{Tate}(q), \zeta_{N'})$ (for some primitive N'-th root $\zeta_{N'}$) is the reduction modulo ℓ of f. Here $F/\mathbb{F}_\ell$ is a finite extension.
2. We prove that such forms (still assuming that $\ell \nmid m$) have constant q-expansion.

With our assumption on N, we have a fine moduli curve $X_1(N)_{\mathbb{C}}$ and our form f can be realized via GAGA as a rational section of the sheaf $\omega^{\otimes k}$. Let $N = N'\ell^r$ where $\ell \nmid N'$ (and $N' \geq 5$ by the above). Since f is fixed by the diamond action at ℓ, we can view f as a section on the curve $X_1(N'; \ell^r)_{\mathbb{C}}$. The q-expansion of f at ∞ is given by evaluating f at the triple

$$(\mathrm{Tate}(q), e^{2\pi i/N'}, \langle e^{2\pi i/\ell^r} \rangle).$$

Embed $\mathbb{Q}(\zeta_N)$ into $\mathbb{C}$ by sending ζ_N to $e^{2\pi i/N}$. Then the q-expansion principle applied at the $\mathbb{Q}(\zeta_{N'})$-rational triple $(\mathrm{Tate}(q), \zeta_{N'}, \langle \zeta_{\ell^r} \rangle)$ implies that the form f actually arises as a rational section of $\omega^{\otimes k}$ on the curve $X_1(N'; \ell^r)_{\mathbb{Q}(\zeta_{N'})}$. In particular, it is a section of $\omega^{\otimes k}(D)$ for an appropriate effective divisor D corresponding to the poles of f.

Let $\lambda \subseteq \mathbb{Z}[\zeta_{N'}]$ be a prime dividing ℓ. We wish to further cut the ring of definition of f down to the localization $\mathbb{Z}[\zeta_{N'}]_\lambda$. This is not *a priori* possible since the moduli scheme $X_1(N'; \ell^r)_{\mathbb{Z}[\zeta_{N'}]_\lambda}$ has bad reduction if $r > 0$. We only have knowledge of the integrality of f at one cusp, and therefore only

on one irreducible component of the reduction of $X_1(N';\ell^r)_{\mathbb{Z}[\zeta_{N'}]_\lambda}$ mod λ. The solution is simply to remove the remaining components.

Recall that this reduction consists of $r+1$ irreducible components indexed by pairs (a,b) of non-negative integers with $a+b=r$. The datum $(\mathrm{Tate}(q), \zeta_{N'}, \langle\zeta_{\ell^r}\rangle)$ reduces to the $(r,0)$ component, since $\langle\zeta_{\ell^r}\rangle$ is the kernel of the r-power relative Frobenius map on $\mathrm{Tate}(q)$.

Notation. Let $\mathcal{X}$ denote the subscheme of $X_1(N';\ell^r)_{\mathbb{Z}[\zeta_{N'}]_\lambda}$ obtained by removing the irreducible components of the special fiber indexed by (a,b) with $b>0$ (there are none if $r=0$).

In particular, we have removed the supersingular points if $r>0$, so $\mathcal{X}$ is smooth over $\mathbb{Z}[\zeta_{N'}]_\lambda$ in any case. It is proper if and only if $r=0$.

The closure $\overline{D}$ of D in $\mathcal{X}$ is a relative effective Cartier divisor over $\mathbb{Z}[\zeta_{N'}]_\lambda$, since its support consists of codimension one points on the regular scheme $\mathcal{X}$ and the ideals of such points are locally principal (since regular local rings are unique factorization domains). Thus we may consider the invertible sheaf $\omega^{\otimes k}(\overline{D})$. The following is the q-expansion in spirit, but we know of no reference that covers this case. We are grateful to Brian Conrad for explaining to us the following argument.

Proposition 3.1. *The form f extends to a section of $\omega^{\otimes k}(\overline{D})$ over $\mathcal{X}$.*

Proof. The section f on the generic fiber can be viewed as a rational section of $\omega^{\otimes k}(\overline{D})$ on all of $\mathcal{X}$. We claim that in order to prove that it is an integral section, it suffices to check that it is integral at each codimension 1 point of $\mathcal{X}$. To see this, note that this can be checked locally on $\mathcal{X}$, so we may trivialize $\omega^{\otimes k}(\overline{D})$ and prove the analogous statement for the structure sheaf of an affine open. Since $\mathcal{X}$ is regular, it is normal, and the result now follows from the fact that a Noetherian normal domain is the intersection (in its fraction field) of its localizations at height 1 primes.

Since f is a regular section on the generic fiber, we have only to check that it is integral at the unique irreducible component of the special fiber. Let x denote the reduction modulo λ of the cusp associated to $(\mathrm{Tate}(q), \zeta_{N'}, \langle\zeta_{\ell^r}\rangle)$ on the generic fiber, and let $\mathrm{Spec}(A)$ be an affine open in $\mathcal{X}$ containing x on which $\omega^{\otimes k}(\overline{D})$ is trivial, so we may regard our rational section as an element (which we will also call f) of the field of fractions K of A. It suffices to show that f lies in the localization A_x. From the q-expansion, we know that the image of f in the field of fractions of the completion $\mathrm{Frac}(\hat{A}_x)$ lies in $\hat{A}_x$ itself. The result will now follow if we can show that the intersection of K and $\hat{A}_x$ in $\mathrm{Frac}(\hat{A}_x)$ is A_x. Writing $f=a/b\in K$, we note that we have an inclusion of ideals $(b)\hat{} \subseteq (a)\hat{}$ upon passing to completion, and by faithful flatness of completion the inclusion $(b)\subseteq(a)$ holds in A_x, so $f=a/b\in A_x$. □

In particular, if D_0 denotes the reduction of $\overline{D}$ modulo λ on $\mathcal{X}$, we obtain by reduction a section of $\omega^{\otimes k}(D_0)$ on said fiber. The ordinary locus in this fiber is identified with (on non-cuspidal points) the moduli space over $F=F(\lambda)$ (the residue field of the prime λ) classifying elliptic curves

with a point of order N' and a type $(r, 0)$ cyclic subgroup of order ℓ^r. But there is one and only one such subgroup, namely the kernel of the r-iterated relative Frobenius map. The result is that the ordinary locus in this fiber is canonically identified with the ordinary locus in $X_1(N')_F$, which we will denote by $X_1(N')_F^{\mathrm{ord}}$.

Thus our form f has given rise to a section $\tilde{f}$ of $\omega^{\otimes k}(D_0)$ on $X_1(N')_F^{\mathrm{ord}}$. Its q-expansion at the cusp associated to the datum $(\mathrm{Tate}(q), \zeta_{N'})$ is the reduction modulo ℓ of the q-expansion of f at $(\mathrm{Tate}(q), \zeta_{N'}, \langle\zeta_{\ell^r}\rangle)$, since $\langle\zeta_{\ell^r}\rangle$ reduces to the kernel of the r-iterated Frobenius.

This completes step (1). We have a section $\tilde{f}$ of $\omega^{\otimes k}(D_0)$ on $X_1(N')_F^{\mathrm{ord}}$ whose q-expansion at the cusp associated to the datum $(\mathrm{Tate}(q), \zeta_{N'})$ has the form

$$\sum_n a_n q^{nm} \in F(\!(q)\!)$$

for an integer $m > 1$. We claim that such a section is necessarily constant.

Let $X_1(N'; m, m)_F$ denote the moduli curve over F that classifies (on non-cuspidal points) isomorphism classes of quadruples (E, P, C_1, C_2) consisting of an elliptic curve E with a point of order N' and a pair of cyclic subgroups C_1 and C_2 of order m intersecting trivially. This curve arises as a quotient of the space classifying points of order N' and full level m (in the sense of $\Gamma(m)$) structures via the group

$$\left\{ \begin{pmatrix} * & 0 \\ 0 & * \end{pmatrix} \right\} \subseteq \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$$

in the natural fashion. Since ℓ is coprime to N' and m, this is an irreducible curve over F, since it is connected and smooth (by Theorem 3.2.7 of [4]).

There are two natural degeneracy maps

$$\pi_1, \pi_2 : X_1(N'; m, m)_F \longrightarrow X_1(N')_F$$

given (on non-cuspidal points) by passage to quotient by C_1 and C_2, respectively, and forgetting the other subgroup. Pull-back of differentials gives a canonical identification $\pi_1^*\omega \cong \pi_2^*\omega$.

Lemma 3.2. *The pull-backs $\pi_1^*\tilde{f}$ and $\pi_2^*\tilde{f}$ coincide under this identification.*

Proof. Since $X_1(N'; m, m)_F$ is irreducible, it suffices to check that these forms have the same q-expansion at a single cusp, that is, that they have the same value on the Tate curve with some level structure. Consider the quadruple $(\mathrm{Tate}(q), \zeta_{N'}, \langle q^{1/m}\rangle, \langle\zeta_m q^{1/m}\rangle)$ for some primitive m-th root of unity ζ_m. We

have

$$\begin{aligned}\pi_1^*\tilde{f}(\mathrm{Tate}(q),\zeta_{N'},\langle q^{1/m}\rangle,\langle\zeta_m q^{1/m}\rangle) &= \tilde{f}(\mathrm{Tate}(q)/\langle q^{1/m}\rangle,\zeta_{N'})\\ &= \tilde{f}(\mathrm{Tate}(q^{1/m}),\zeta_{N'})\\ &= \left(\sum_n a_n (q^{1/m})^{mn}\right)\omega_{\mathrm{can}}^{\otimes k}\\ &= \left(\sum_n a_n q^n\right)\omega_{\mathrm{can}}^{\otimes k}\end{aligned}$$

and

$$\begin{aligned}\pi_2^*\tilde{f}(\mathrm{Tate}(q),\zeta_{N'},\langle q^{1/m}\rangle,\langle\zeta_m q^{1/m}\rangle) &= \tilde{f}(\mathrm{Tate}(q)/\langle\zeta_m q^{1/m}\rangle,\zeta_{N'})\\ &= \tilde{f}(\mathrm{Tate}(\zeta_m q^{1/m}),\zeta_{N'})\\ &= \left(\sum_n a_n (\zeta_m q^{1/m})^{mn}\right)\omega_{\mathrm{can}}^{\otimes k}\\ &= \left(\sum_n a_n q^n\right)\omega_{\mathrm{can}}^{\otimes k}.\end{aligned}$$

Here, we are implicitly using the fact that the pull-backs of the canonical differentials ω_{can} on the quotient curves (the latter having been identified with base-changes of $\mathrm{Tate}(q)$ as indicated) coincide under the natural identification $\pi_1^*\omega \cong \pi_2^*\omega$. □

Unraveling this, we have shown that if E is any elliptic curve over an F-algebra, P is a point of order N' on E, C_1 and C_2 are cyclic subgroups of E of order m intersecting trivially, and $p_i : E \longrightarrow E/C_i$ denote the quotient maps, then

$$p_1^*\tilde{f}(E/C_1, P/C_1) = p_2^*\tilde{f}(E/C_2, P/C_2). \tag{3.1}$$

For each non-negative integer d, let

$$\tilde{f}(\mathrm{Tate}(q),\zeta_{N'}^{m^d}) = \left(\sum_n b_n(d) q^n\right)\omega_{\mathrm{can}}^{\otimes k}.$$

We apply (3.1) to $(\mathrm{Tate}(q),\zeta_{N'}^{m^d})$ and the subgroups $C_1 = \langle\zeta_m\rangle$ and $C_2 = \langle q^{1/m}\rangle$. We have

$$\begin{aligned}p_1^*\tilde{f}(\mathrm{Tate}(q)/\langle\zeta_m\rangle,\zeta_{N'}^{m^d}) &= p_1^*\tilde{f}(\mathrm{Tate}(q^m),\zeta_{N'}^{m^{d+1}})\\ &= p_1^*\left(\left(\sum_n b_n(d+1)(q^m)^n\right)\omega_{\mathrm{can}}^{\otimes k}\right)\\ &= \left(\sum_n b_n(d+1) q^{nm}\right) m^k \omega_{\mathrm{can}}^{\otimes m}\end{aligned}$$

and

$$\begin{aligned} p_2^*\tilde{f}(\mathrm{Tate}(q)/\langle q^{1/m}\rangle, \zeta_{N'}^{m^d}) &= p_2^*\tilde{f}(\mathrm{Tate}(q^{1/m}), \zeta_{N'}^{m^d}) \\ &= p_2^*\left(\left(\sum_n b_n(d)(q^{1/m})^n\right)\omega_{\mathrm{can}}^{\otimes k}\right) \\ &= \left(\sum_n b_n(d)q^{n/m}\right)\omega_{\mathrm{can}}^{\otimes m}, \end{aligned}$$

and thus

$$\sum_n b_n(d)q^{n/m} = m^k \sum_n b_n(d+1)q^{mn}$$

for all $d \geq 0$. If s denotes the order of m modulo N', then we may successively use this with $d = 0, 1, \ldots, s$ (noting that $b_n(0) = b_n(s) = a_{n/m}$ for all n) to conclude that

$$\sum_n a_n q^n = m^{ks} \sum_n a_{n/m^{2s}} q^{m^2 n}.$$

It follows (consider the "least" m-divisible n with $a_n \neq 0$) that $a_n = 0$ for all non-zero n. This completes step (2) and the proof of Theorem 1.1.

4. The proofs of Theorems 1.2 and 1.3

We now prove Theorems 1.2 and 1.3 using the strategy outlined in [9].

Proof of Theorem 1.2. Theorem 1.2 (2) is Theorem 1.2 (2) of [9]. Moreover, Theorem 1.2 (1) of [9] asserts that if there are any m coprime to 6 for which $p\left(\frac{Dm^2+1}{24}\right)$ is even, then there are infinitely many such m. Furthermore, this result bounds the smallest such m (if any). Therefore, it suffices to show that there is at least one such m.

We employ Theorem 1.1 of [9], which depends on generalized Borcherds products constructed by the first author and Bruinier (see Section 8.2 of [3]). This theorem asserts that

$$\widehat{F}(D;z) := \sum_{\substack{m\geq 1 \\ \gcd(m,6)=1}} p\left(\frac{Dm^2+1}{24}\right) \sum_{\substack{n\geq 1 \\ \gcd(n,D)=1}} q^{mn} \pmod 2 \tag{4.1}$$

is the reduction modulo 2 of a weight 2 meromorphic modular form on $\Gamma_0(6)$ whose poles are simple and are supported on CM points of discriminant $-D$.

Suppose that $p\left(\frac{Dm^2+1}{24}\right)$ is odd for every m coprime to 6. Then we have

$$\widehat{F}(D;z) \equiv \sum_{\substack{m\geq 1 \\ \gcd(m,6)=1}} \sum_{\substack{n\geq 1 \\ \gcd(n,D)=1}} q^{mn} \pmod 2. \tag{4.2}$$

This form can be described in terms of $E_2(z) := 1 - 24\sum_{d|n} dq^n$, the quasi-modular weight 2 Eisenstein series. Although $E_2(z)$ is not a modular form,

it is well known that if $t \geq 2$, then $E_2(z) - tE_2(tz)$ is a holomorphic weight 2 modular form on $\Gamma_0(t)$. If we let

$$\mathcal{E}(z) := \frac{(E_2(z) - 3E_2(3z)) - 2(E_2(z) - 2E_2(2z))}{24} = q - q^2 + 7q^3 - 5q^4 - \dots,$$

then $\mathcal{E}(z)$ is a holomorphic weight 2 modular form on $\Gamma_0(6)$ with integer coefficients satisfying

$$\mathcal{E}(z) \equiv \sum_{\substack{m \geq 1 \\ \gcd(m,6)=1}} \sum_{n \geq 1} q^{mn} \pmod 2. \tag{4.3}$$

Since D is square-free, we then have that

$$\widehat{F}(D; z) \equiv \sum_{\delta | D} \mathcal{E}(\delta z) \pmod 2.$$

Now let $p \geq 5$ be any prime dividing D. Such primes exist since $D \equiv 23 \pmod{24}$. Then we have the weight 2 holomorphic modular form

$$\mathcal{E}_p(D; z) := \sum_{1 \leq \delta | \frac{D}{p}} \mathcal{E}(\delta z) \equiv \sum_{\substack{m \geq 1 \\ \gcd(m,6)=1}} \sum_{\substack{n \geq 1 \\ \gcd(n, D/p)=1}} q^{mn} \pmod 2$$

on $\Gamma_0(6D/p)$. Consequently, we find that

$$\widehat{F}_p(D; z) := \widehat{F}(D; z) - \mathcal{E}_p(D; z) \equiv \sum_{\delta | D/p} \mathcal{E}(\delta p z) \pmod 2.$$

This q-series is a nonconstant meromorphic weight 2 modular form modulo 2 on $\Gamma_0(6D/p)$ whose odd coefficients are supported on exponents which are multiples of p. By Theorem 1.1, with $N = 6D/p$, $\ell = 2$, and $m = p$, we have a contradiction, and this completes the proof. □

Alfes [1] recently applied this strategy to certain twisted Borcherds products constructed by Zagier [13]. Combining her results with Theorem 1.1 proves Theorem 1.3.

Proof of Theorem 1.3. Theorem 1.3 (2) is Theorem 1.3 (2) of [1]. Moreover, Theorem 1.3 (1) of [1] implies that there are infinitely many odd m for which c_{Dm^2} is even provided that there is at least one such m. Furthermore, this result gives the stated bound for the first such m (if any). Therefore, here it suffices to show that there is at least one such m.

Alfes (see the proof of Theorem 1.1 of [1]) uses Zagier's Borcherds products to prove that

$$\mathfrak{F}(D; z) \equiv \sum_{\substack{m \geq 1 \\ \text{odd}}} c_{Dm^2} \sum_{\substack{n \geq 1 \\ \gcd(n, 2D)=1}} q^{mn} \pmod 2 \tag{4.4}$$

is the reduction modulo 2 of a weight 2 meromorphic modular form modulo 2 on $\mathrm{SL}_2(\mathbb{Z})$ whose poles are simple and are supported on CM points with

discriminant $-D$. Suppose that c_{Dm^2} is odd for every odd m. Then we have

$$\mathfrak{F}(D;z) \equiv \sum_{\substack{m\geq 1\\ \text{odd}}} \sum_{\substack{n\geq 1\\ \gcd(n,2D)=1}} q^{mn} \pmod 2. \tag{4.5}$$

This form is easily described in terms of the weight 2 Eisenstein series on $\Gamma_0(4)$ given by

$$\mathfrak{E}(z) := \frac{\eta(4z)^8}{\eta(2z)^4} = \sum_{\substack{n\geq 1\\ \text{odd}}} \sum_{d|n} dq^n = q + 4q^3 + 6q^5 + \dots. \tag{4.6}$$

Here $\eta(z) := q^{\frac{1}{24}} \prod_{n=1}^{\infty}(1-q^n)$ is Dedekind's eta-function. Since D is square-free, we have

$$\mathfrak{F}(D;z) \equiv \sum_{\delta|D} \mathfrak{E}(\delta z) \pmod 2.$$

Now let p be any odd prime dividing D. Such primes exist since $D \equiv 7 \pmod 8$. Then we have the weight 2 holomorphic modular form on $\Gamma_0(4D/p)$ given by

$$\mathfrak{E}_p(D;z) := \sum_{1\leq\delta|D/p} \mathfrak{E}(\delta z) \equiv \sum_{\substack{m\geq 1\\ \text{odd}}} \sum_{\substack{n\geq 1\\ \gcd(n,2D/p)=1}} q^{mn} \pmod 2.$$

Consequently, we find that

$$\mathfrak{F}(D;z) - \mathfrak{E}_p(D;z) \equiv \sum_{1\leq\delta|D/p} \mathfrak{E}(\delta p z) \pmod 2$$

is a nonconstant weight 2 modular form modulo 2 on $\Gamma_0(4D/p)$ with the property that its odd coefficients are supported on exponents which are multiples of p. By Theorem 1.1, where $N = 4D/p$, $\ell = 2$ and $m = p$, we have a contradiction, and this completes the proof. □

References

[1] C. Alfes. Parity of the coefficients of Klein's j-function. *Proc. Amer. Math. Soc.*, in press.

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

[3] J. H. Bruinier and K. Ono. Heegner divisors, L-functions, and harmonic weak Maass forms. *Ann. Math.* **172** (2010), pages 2135-2181.

[4] B. Conrad. Arithmetic moduli of generalized elliptic curves. *J. Inst. Math. Jussieu* **6** (2007), pages 209–278.

[5] N. M. Katz. p-adic properties of modular schemes and modular forms. In *Modular functions of one variable, III (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972)*, pages 69–190. Lecture Notes in Mathematics, Vol. 350. Springer, Berlin, 1973.

[6] N. M. Katz and B. Mazur. *Arithmetic moduli of elliptic curves*, volume 108 of *Annals of Mathematics Studies*. Princeton University Press, Princeton, NJ, 1985.

[7] B. Mazur, *Modular curves and the Eisenstein ideal*, Inst. Hautes Études Sci. Publ. Math. No. 47 (1977), pages 33-186.

[8] K. Ono. Parity of the partition function in arithmetic progressions. *J. reine Angew. Math.* **472** (1996), pages 1-15.

[9] K. Ono. The parity of the partition function. Adv. Math. **225** (2010), pages 349-366.

[10] T. R. Parkin and D. Shanks. On the distribution of parity in the partition function. *Math. Comp.* **21** (1967), pages 466-480.

[11] S. Radu. A proof of Subbarao's conjecture. *J. reine Angew. Math.*, in press.

[12] M. Subbarao. Some remarks on the partition function. *Amer. Math. Monthly* **73** (1966), pages 851-854.

[13] D. Zagier. Traces of singular moduli. Motives, polylogarithms and Hodge theory, Part I. Intl. Press, Somerville (2002), pages 211-244.

Ken Ono and Nick Ramsey
Department of Mathematics and Computer Science, Emory University, Atlanta, GA 30322
e-mail: ono@mathcs.emory.edu
Department of Mathematics, DePaul University, Chicago, IL 60614
e-mail: nramsey@depaul.edu