NUMBER THEORETIC PROPERTIES OF WRONSKIANS OF ANDREWS-GORDON SERIES

ANTUN MILAS, ERIC MORTENSON, AND KEN ONO

Abstract. For positive integers $1 \leq i \leq k$, we consider the arithmetic properties of quotients of Wronskians in certain normalizations of the Andrews-Gordon q-series

$$\prod_{1 \leq n \not\equiv 0, \pm i \pmod{2k+1}} \frac{1}{1-q^n}.$$

This study is motivated by their appearance in conformal field theory, where these series are essentially the irreducible characters of $\mathcal{M}(2, 2k+1)$ Virasoro minimal models. We determine the vanishing of such Wronskians, a result whose proof reveals many partition identities. For example, if $P_b(a; n)$ denotes the number of partitions of n into parts which are not congruent to $0, \pm a \pmod{b}$, then for every positive integer n we have

$$P_{27}(12; n) = P_{27}(6; n-1) + P_{27}(3; n-2).$$

We also show that these quotients classify supersingular elliptic curves in characteristic p. More precisely, if $2k+1 = p$, where $p \geq 5$ is prime, and the quotient is non-zero, then it is essentially the locus of characteristic p supersingular j-invariants in characteristic p.

1. Introduction and Statement of Results

In two–dimensional conformal field theory and vertex operator algebra theory (see [Bo] [FLM]), modular functions and modular forms appear as graded dimensions, or characters, of infinite dimensional irreducible modules. As a celebrated example, the graded dimension of the Moonshine Module is the modular function

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

(see [FLM]), where $q := e^{2\pi i z}$ throughout. Although individual characters are not always modular in this way, it can be the case that the vector spaces spanned by all of the irreducible characters of a module are invariant under the modular group [Zh]. For example, to construct an automorphic form from an $\mathrm{SL}_2(\mathbb{Z})$–module, one may simply take the Wronskian of a basis of the module. In the case of the Virasoro vertex operator algebras, such Wronskians were studied by the first author (see [M1], [M2]) who obtained several classical q–series identities related to modular forms using methods from representation theory.

2000 *Mathematics Subject Classification.* 11F30, 11G05, 17B68.

The third author thanks the support of a Packard Fellowship, a Romnes Fellowship, a Guggenheim Fellowship, and grants from the National Science Foundation.

Wronskian determinants in modular forms already play many roles in number theory. For example, Rankin classified multi–linear differential operators mapping automorphic forms to automorphic forms using Wronskians [R]. As another example, the zeros of the Wronskian of a basis of weight two cusp forms for a congruence subgroup $\Gamma_0(N)$ typically are the Weierstrass points of the modular curve $X_0(N)$ [FaKr].

In view of this connection between Weierstrass points on modular curves and Wronskians of weight 2 cusp forms, it is natural to investigate the number theoretic properties of Wronskians of irreducible characters. Here we make a first step in this direction, and we consider an important class of models in vertex operator algebra theory, those associated to $\mathcal{M}(2, 2k+1)$ Virasoro minimal models. These representations are important in conformal field theory and mathematical physics and have been studied extensively in the literature (see [FF], [KW], [M2], [RC] and references therein).

We shall need some notation. Throughout, suppose that $k \geq 2$ is an integer. Define the rational number c_k by

$$c_k := 1 - \frac{3(2k-1)^2}{(2k+1)}, \tag{1.1}$$

and for each $1 \leq i \leq k$, define $h_{i,k}$ by

$$h_{i,k} := \frac{(2(k-i)+1)^2 - (2k-1)^2}{8(2k+1)}. \tag{1.2}$$

Let $L(c_k, h_{i,k})$ denote the irreducible lowest weight module for the Virasoro algebra of central charge c_k and weight $h_{i,k}$ (see [FF], [KW], [M1]). These representations are $\mathbb{N}$–gradable and have finite dimensional graded subspaces. Thus, we can define the formal q–series

$$\dim_{L(c_k,h_{i,k})}(q) := \sum_{n=0}^{\infty} \dim(L(c_k, h_{i,k})_n) q^n.$$

It is important to multiply the right hand side by the factor $q^{h_{i,k}-\frac{c_k}{24}}$. The corresponding expression is called the character of $L(c_k, h_{i,k})$ and will be denoted by $\mathrm{ch}_{i,k}(q)$. It turns out that (see [RC], [KW])

$$\mathrm{ch}_{i,k}(q) = q^{(h_{i,k}-\frac{c_k}{24})} \cdot \prod_{1 \leq n \not\equiv 0, \pm i \pmod{2k+1}} \frac{1}{1-q^n}. \tag{1.3}$$

Apart from the fractional powers of q appearing in their definition, such series have been studied extensively by Andrews, Gordon, and of course Rogers and Ramanujan (for example, see [A]). Indeed, when $k = 2$ we have that $c_5 = -\frac{22}{5}$, and the two corresponding characters are essentially the products appearing in the celebrated Rogers-Ramanujan identities

$$\mathrm{ch}_{1,2}(q) = q^{\frac{11}{60}} \prod_{n\geq 0} \frac{1}{(1-q^{5n+2})(1-q^{5n+3})},$$
$$\mathrm{ch}_{2,2}(q) = q^{-\frac{1}{60}} \prod_{n\geq 0} \frac{1}{(1-q^{5n+1})(1-q^{5n+4})}.$$

In view of the discussion above, we investigate, for each k, the Wronskians for the complete sets of characters

$$\{\mathrm{ch}_{1,k}(q), \mathrm{ch}_{2,k}(q), \ldots, \mathrm{ch}_{k,k}(q)\}.$$

For each $k \geq 2$, define $\mathcal{W}_k(q)$ and $\widetilde{\mathcal{W}}_k(q)$ by

$$\mathcal{W}_k(q) := \alpha(k) \cdot \det \begin{pmatrix} \mathrm{ch}_{1,k} & \mathrm{ch}_{2,k} & \cdots & \mathrm{ch}_{k,k} \\ \mathrm{ch}'_{1,k} & \mathrm{ch}'_{2,k} & \cdots & \mathrm{ch}'_{k,k} \\ \vdots & \vdots & \vdots & \vdots \\ \mathrm{ch}^{(k-1)}_{1,k} & \mathrm{ch}^{(k-1)}_{2,k} & \cdots & \mathrm{ch}^{(k-1)}_{k,k} \end{pmatrix}, \tag{1.4}$$

$$\widetilde{\mathcal{W}}_k(q) := \beta(k) \cdot \det \begin{pmatrix} \mathrm{ch}'_{1,k} & \mathrm{ch}'_{2,k} & \cdots & \mathrm{ch}'_{k,k} \\ \mathrm{ch}^{(2)}_{1,k} & \mathrm{ch}^{(2)}_{2,k} & \cdots & \mathrm{ch}^{(2)}_{k,k} \\ \vdots & \vdots & \vdots & \vdots \\ \mathrm{ch}^{(k)}_{1,k} & \mathrm{ch}^{(k)}_{2,k} & \cdots & \mathrm{ch}^{(k)}_{k,k} \end{pmatrix}. \tag{1.5}$$

Here $\alpha(k)$ (resp. $\beta(k)$) is chosen so that the q-expansion of $\mathcal{W}_k(q)$ (resp. $\widetilde{\mathcal{W}}_k(q)$) has first non-zero coefficient of 1, and differentiation is given by

$$\left(\sum a(n)q^n\right)' := \sum na(n)q^n,$$

which equals $\frac{1}{2\pi i} \cdot \frac{d}{dz}$ when $q := e^{2\pi i z}$.

It turns out that $\mathcal{W}_k(q)$ is easily described in terms of Dedekind's eta-function (see also Theorem 6.1 of [M2]), which is defined for $z \in \mathbb{H}$, $\mathbb{H}$ denoting the usual upper half-plane of $\mathbb{C}$, by

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

Theorem 1.1. *If $k \geq 2$, then*

$$\mathcal{W}_k(q) = \eta(z)^{2k(k-1)}.$$

Instead of directly computing $\widetilde{\mathcal{W}}_k(q)$, we investigate the quotient

$$\mathcal{F}_k(z) := \frac{\widetilde{\mathcal{W}}_k(q)}{\mathcal{W}_k(q)}. \tag{1.6}$$

It turns out that these q-series $\mathcal{F}_k(z)$ are modular forms of weight $2k$ for the full modular group $\mathrm{SL}_2(\mathbb{Z})$. To make this more precise, suppose that $E_4(z)$ and $E_6(z)$ are the standard Eisenstein series

$$E_4(z) = 1 + 240\sum_{n=1}^{\infty}\sum_{d|n} d^3q^n \quad \text{and} \quad E_6(z) = 1 - 504\sum_{n=1}^{\infty}\sum_{d|n} d^5q^n, \tag{1.7}$$

and that $\Delta(z)$ and $j(z)$ (as before) are the usual modular forms

$$\Delta(z) = \frac{E_4(z)^3 - E_6(z)^2}{1728} \quad \text{and} \quad j(z) = \frac{E_4(z)^3}{\Delta(z)}. \tag{1.8}$$

Theorem 1.2. *If $k \geq 2$, then $\mathcal{F}_k(z)$ is a weight $2k$ holomorphic modular form on $\mathrm{SL}_2(\mathbb{Z})$.*

Example. For $2 \leq k \leq 6$, it turns out that

$$\begin{aligned} &\mathcal{F}_2(z) = E_4(z), \qquad \mathcal{F}_3(z) = E_6(z),\\ &\mathcal{F}_4(z) = E_4(z)^2, \qquad \mathcal{F}_5(z) = E_4(z)E_6(z),\\ &\mathcal{F}_6(z) = \frac{193504E_6(z)^2 + 169971E_4(z)^3}{363475}. \end{aligned}$$

Some of these modular forms are identically zero. For example, we have that $\mathcal{F}_{13}(z) = 0$, a consequence of the q-series identity

$$\mathrm{ch}_{12,13}(q) - \mathrm{ch}_{6,13}(q) - \mathrm{ch}_{3,13}(q) = 1, \tag{1.9}$$

which will be proved later. The following result completely determines those k for which $\mathcal{F}_k(z) = 0$.

Theorem 1.3. *The modular form $\mathcal{F}_k(z)$ is identically zero precisely for those k of the form $k = 6t^2 - 6t + 1$ with $t \geq 2$.*

Since the Andrews-Gordon series are the partition generating functions

$$\sum_{n=0}^{\infty} P_b(a;n)q^n = \prod_{1\leq n\not\equiv 0,\pm a \pmod b} \frac{1}{1-q^n},$$

q-series identity (1.9) implies, for positive n, the shifted partition identity

$$P_{27}(12;n) = P_{27}(6;n-1) + P_{27}(3;n-2).$$

This partition identity is a special case of the following theorem which is a corollary to the proof of Theorem 1.3.

Theorem 1.4. *If $t \geq 2$, then for every positive integer n we have*

$$P_{b(t)}(a^-(t,0);n) = \sum_{r=1}^{t-1}(-1)^{r+1}\left(P_{b(t)}(a^+(t,r);n-\omega^-(r)) + P_{b(t)}(a^-(t,r);n-\omega^+(r))\right),$$

where

$$\begin{aligned} a^-(t,r) &:= (2t-1)(3t-3r-2),\\ a^+(t,r) &:= (2t-1)(3t-3r-1),\\ b(t) &:= 3(2t-1)^2,\\ \omega^-(r) &:= \frac{3r^2-r}{2},\\ \omega^+(r) &:= \frac{3r^2+r}{2}. \end{aligned}$$

The forms $\mathcal{F}_k(z)$ also provide deeper number theoretic information. Some of them parameterize isomorphism classes of supersingular elliptic curves in characteristic p. To make this precise, suppose that K is a field with characteristic $p>0$, and let $\overline{K}$ be its algebraic closure. An elliptic curve E over K is *supersingular* if the group $E(\overline{K})$ has no p-torsion. This connection is phrased in terms of "divisor polynomials" of modular forms.

We now describe these polynomials. If $k \geq 4$ is even, then define $\tilde{E}_k(z)$ by

$$\tilde{E}_k(x) := \begin{cases} 1 & \text{if } k \equiv 0 \pmod{12},\\ E_4(z)^2E_6(z) & \text{if } k \equiv 2 \pmod{12},\\ E_4(z) & \text{if } k \equiv 4 \pmod{12},\\ E_6(z) & \text{if } k \equiv 6 \pmod{12},\\ E_4(z)^2 & \text{if } k \equiv 8 \pmod{12},\\ E_4(z)E_6(z) & \text{if } k \equiv 10 \pmod{12} \end{cases} \tag{1.10}$$

(see Section 2.6 of [O] for further details on divisor polynomials). As usual, let M_k denote the space of holomorphic weight k modular forms on $\mathrm{SL}_2(\mathbb{Z})$. If we write k as

$$k = 12m + s \quad \text{with } s \in \{0,4,6,8,10,14\}, \tag{1.11}$$

then $\dim_{\mathbb{C}}(M_k) = m+1$, and every modular form $f(z) \in M_k$ factorizes as

$$f(z) = \Delta(z)^m \tilde{E}_k(z)\tilde{F}(f, j(z)), \tag{1.12}$$

where $\tilde{F}$ is a polynomial of degree $\leq m$ in $j(z)$. Now define the polynomial $h_k(x)$ by

$$h_k(x) := \begin{cases} 1 & \text{if } k \equiv 0 \pmod{12},\\ x^2(x-1728) & \text{if } k \equiv 2 \pmod{12},\\ x & \text{if } k \equiv 4 \pmod{12},\\ x-1728 & \text{if } k \equiv 6 \pmod{12},\\ x^2 & \text{if } k \equiv 8 \pmod{12},\\ x(x-1728) & \text{if } k \equiv 10 \pmod{12}. \end{cases} \tag{1.13}$$

If $f(z) \in M_k$, then define the *divisor polynomial* $F(f,x)$ by

$$F(f,x) := h_k(x)\tilde{F}(f,x). \tag{1.14}$$

If $j(E)$ denotes the usual j-invariant of an elliptic curve E, then the *characteristic p locus of supersingular j-invariants* is the polynomial in $\mathbb{F}_p[x]$ defined by

$$S_p(x) := \prod_{E/\overline{\mathbb{F}}_p \text{ supersingular}} (x - j(E)), \tag{1.15}$$

the product being over isomorphism classes of supersingular elliptic curves. The following congruence modulo 37, when $k = 18$, is a special case of our general result

$$\begin{aligned} F(\mathcal{F}_{18}, j(z)) &= j(z)^3 - \frac{2^{13}\cdot 3^4 \cdot 89 \cdot 1915051410991641479}{17\cdot 43\cdot 83\cdot 103\cdot 113\cdot 163\cdot 523\cdot 643\cdot 919\cdot 1423}\cdot j(z)^2 + \cdots \\ &\equiv (j(z)+29)(j(z)^2+31j(z)+31) \pmod{37} \\ &= S_{37}(j(z)). \end{aligned}$$

The following result provides a general class of k for which $F(\mathcal{F}_k, j(z)) \pmod{p}$ is the supersingular locus $S_p(j(z))$.

Theorem 1.5. *If $p \geq 5$ is prime and $k = \frac{p-1}{2}$, then*

$$F(\mathcal{F}_k, j(z)) \equiv S_p(j(z)) \pmod{p}.$$

In Section 2 we prove Theorem 1.2. In Section 3 we provide the preliminaries required for the proofs of Theorems 1.3 and 1.5. These theorems, along with Theorem 1.4, are then proved in Sections 4 and 5 respectively. In Section 6 we give a conjecture concerning the zeros of $\widetilde{F}(\mathcal{F}_k, x)$.

2. Differential operators and the proof of Theorem 1.2

Here we study the quotient

$$\mathcal{F}_k(q) := \frac{\widetilde{\mathcal{W}}_k(q)}{\mathcal{W}_k(q)}, \tag{2.1}$$

and prove Theorem 1.2. Needless to say, the previous expression can be defined for an arbitrary set $\{f_1(q), ..., f_k(q)\}$ of holomorphic functions in $\mathbb{H}$, where each $f_i(q)$ has a q–expansion. In the $k = 1$ case, (2.1) is just the logarithmic derivative of f_1. We also introduce generalized Wronskian determinants. For $0 \leq i_1 < i_2 < \cdots < i_k$, let

$$W^{i_1,\dots,i_k}(f_1, ..., f_k)(q) = \det \begin{pmatrix} f_1^{(i_1)} & f_2^{(i_1)} & . & . & f_k^{(i_1)} \\ f_1^{(i_2)} & f_2^{(i_2)} & . & . & f_k^{(i_2)} \\ . & . & . & . & . \\ . & . & . & . & . \\ f_1^{(i_k)} & f_2^{(i_k)} & . & . & f_k^{(i_k)} \end{pmatrix}. \tag{2.2}$$

Clearly, $W^{0,1,\dots,k-1}(f_1, ..., f_k)$ is the ordinary Wronskian. We will write $\mathcal{W}^{i_1,\dots,i_k}(f_1, ..., f_k)$ for the normalization of $W^{i_1,\dots,i_k}(f_1, ..., f_k) \neq 0$, where the leading coefficient in the q-expansion is one.

Before we prove Theorem 1.2, we recall the definition of the "quasi-modular" form

$$E_2(z) = 1 - 24 \sum_{n=1}^{\infty} \sum_{d|n} dq^n, \tag{2.3}$$

which plays an important role in the proof of the following result (also see [M1]).

Theorem 2.1. *For $k \geq 2$, the set $\{\mathrm{ch}_{1,k}(q), ..., \mathrm{ch}_{k,k}(q)\}$ is a fundamental system of a k-th order linear differential equation of the form*

$$\left(q\frac{d}{dq}\right)^k y + \sum_{i=0}^{k-1} P_i(q) \left(q\frac{d}{dq}\right)^i y = 0, \tag{2.4}$$

where $P_i(q) \in \mathbb{Q}[E_2, E_4, E_6]$. Moreover, $P_0(q)$ is a modular form for $\mathrm{SL}_2(\mathbb{Z})$.

Proof. The first part was already proven in [M2], Theorem 6.1. Let

$$\Theta_k := \left(q\frac{d}{dq}\right) - \frac{k}{12}E_2(z) \tag{2.5}$$

It is well known that Θ_k sends a modular form of weight k to a modular form of weight $k+2$ [Z]. Then Theorem 5.3 in [M1] implies that the equation (2.4) can be rewritten as

$$\Theta^k y + \sum_{i=1}^{k-1} Q_i(q)\Theta^i y + Q_0(q)y = 0,$$

where for $i \geq 1$

$$\Theta^i := \Theta_{2i-2} \circ \cdots \circ \Theta_2 \circ \Theta_0,$$

and

$$Q_i(q) \in \mathbb{Q}[E_4, E_6].$$

We note that $Q_0(q)$ is the "modular part" $P_0(q)$, but that $P_0(q)$ itself is modular. Thus $P_0(q) = Q_0(q)$, and the proof follows. □

Proof of Theorem 1.2. Let $\{f_1(q), ..., f_k(q)\}$ be a linearly independent set of holomorphic functions in the upper half-plane. Then there is a unique $k-$th order linear differential operator with meromorphic coefficients

$$P = \left(q\frac{d}{dq}\right)^k + \sum_{i=0}^{k-1} P_i(q) \left(q\frac{d}{dq}\right)^i,$$

such that $\{f_1(q), ..., f_k(q)\}$ is a fundamental system of

$$P(y) = 0.$$

Explicitly,

$$P(y) = (-1)^k \frac{W^{0,1,...,k}(y, f_1, ..., f_k)}{W^{0,1,...,k-1}(f_1, ..., f_k)}. \tag{2.6}$$

In particular,

$$P_0(q) = (-1)^k \frac{W^{1,2,\ldots,k}(f_1,\ldots,f_k)}{W^{0,1,\ldots,k-1}(f_1,\ldots,f_k)}.$$

Thus,

$$P_0(q) = \lambda_k \frac{\widetilde{\mathcal{W}}_k(q)}{\mathcal{W}_k(q)},$$

for some nonzero constant λ_k. Now, we specialize $f_i(q) = \mathrm{ch}_{i,k}(q)$ and apply Theorem 2.1. $\square$

Remark. The techniques from [M1] can be used to give explicit formulas for $\frac{\widetilde{\mathcal{W}}_k(q)}{\mathcal{W}_k(q)}$ in terms of Eisenstein series. However, this computation becomes very tedious for large k.

3. Preliminaries for Proofs of Theorems 1.3 and 1.5

In this section we recall essential preliminaries regarding q-series and divisor polynomials of modular forms.

3.1. **Classical q-series identities.** We begin by recalling Jacobi's triple product identity and Euler's pentagonal number theorem.

Theorem 3.1. *(Jacobi's Triple Product Identity) For $y \neq 0$ and $|q| < 1$, we have*

$$\sum_{m=-\infty}^{\infty} y^m q^{m^2} = \prod_{n=1}^{\infty} (1-q^{2n})(1+yq^{2n-1})(1+y^{-1}q^{2n-1}).$$

Theorem 3.2. *(Euler's Pentagonal Number Theorem) The following q-series identity is true:*

$$\sum_{m=-\infty}^{\infty} (-1)^m q^{\frac{1}{2}m(3m-1)} = \prod_{n=1}^{\infty}(1-q^n).$$

3.2. **Divisor polynomials and Deligne's theorem.** If $p \geq 5$ is prime, then the supersingular loci $S_p(x)$ and $\widetilde{S}_p(x)$ are defined in $\mathbb{F}_p[x]$ by the following products over isomorphism classes of supersingular elliptic curves:

$$S_p(x) := \prod_{E/\overline{\mathbb{F}}_p \text{ supersingular}} (x - j(E)),$$

$$\widetilde{S}_p(x) := \prod_{\substack{E/\overline{\mathbb{F}}_p \text{ supersingular} \\ j(E)\notin\{0,1728\}}} (x - j(E)). \tag{3.1}$$

For such primes p, let $\mathfrak{S}_p$ denote the set of those supersingular j-invariants in characteristic p which are in $\mathbb{F}_p - \{0, 1728\}$, and let $\mathfrak{M}_p$ denote the set of monic irreducible quadratic polynomials in $\mathbb{F}_p[x]$ whose roots are supersingular j-invariants. The polynomial $S_p(x)$ splits completely in $\mathbb{F}_{p^2}$ ([Si]). Define $\epsilon_\omega(p)$ and $\epsilon_i(p)$ by

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

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

The following proposition relates $S_p(x)$ to $\tilde{S}_p(x)$ ([Si]).

Proposition 3.3. *If $p \geq 5$ is prime, then*

$$\begin{aligned} S_p(x) &= x^{\epsilon_\omega(p)}(x-1728)^{\epsilon_i(p)} \cdot \prod_{\alpha \in \mathfrak{S}_p} (x-\alpha) \cdot \prod_{g \in \mathfrak{M}_p} g(x) \\ &= x^{\epsilon_\omega(p)}(x-1728)^{\epsilon_i(p)} \tilde{S}_p(x). \end{aligned}$$

Deligne found the following explicit description of these polynomials (see [Dw], [Se]).

Theorem 3.4. *If $p \geq 5$ is prime, then*

$$F(E_{p-1}, x) \equiv S_p(x) \pmod p.$$

Remark. In a beautiful paper [KZ], Kaneko and Zagier provide a simple proof of Theorem 3.4.

Remark. The Von-Staudt congruences imply for primes p, that $\frac{2(p-1)}{B_{p-1}} \equiv 0 \pmod p$, where B_n denotes the usual nth Bernoulli number. It follows that if

$$E_k(z) = 1 - \frac{2k}{B_k} \sum_{n=1}^{\infty} \sum_{d|n} d^{k-1} q^n$$

is the usual weight k Eisenstein series, then

$$E_{p-1}(z) \equiv 1 \pmod p.$$

If $p \geq 5$ is prime, then Theorem 3.4 combined with the definition of divisor polynomials, implies that if $f(z) \in M_{p-1}$ and $f(z) \equiv 1 \pmod p$, then

$$F(f, j(z)) \equiv S_p(j(z)) \pmod p.$$

4. The Vanishing of $\mathcal{F}_k(z)$

Here we prove Theorem 1.3 and Theorem 1.4. To prove these results, we first require some notation and two technical lemmas. For simplicity, we will write $\mathrm{ch}_i(q)$ for $\mathrm{ch}_{i,k}(q)$ when k is understood.

We define

$$\Theta(y,q) := \sum_{n=-\infty}^{\infty} y^n q^{n^2}, \tag{4.1}$$

and we consider the sum

$$A_t(q) := \Theta(-q^{\frac{1}{2}(2t-1)}, q^{\frac{3}{2}(2t-1)^2}) + \sum_{r=1}^{t-1}(-1)^r\Psi^-_{r,t}(q) + \sum_{r=1}^{t-1}(-1)^r\Psi^+_{r,t}(q), \tag{4.2}$$

where

$$\Psi^-_{r,t}(q) := q^{\frac{1}{2}r(3r-1)}\Theta(-q^{\frac{1}{2}(6r-1)(2t-1)}, q^{\frac{3}{2}(2t-1)^2}),$$

and

$$\Psi^+_{r,t}(q) := q^{\frac{1}{2}r(3r+1)}\Theta(-q^{\frac{1}{2}(6r+1)(2t-1)}, q^{\frac{3}{2}(2t-1)^2}).$$

Lemma 4.1. *If $t \geq 2$ and $k = 6t^2 - 6t + 1$, then we have the following q-series identity*

$$\begin{aligned}\prod_{n=1}^{\infty}(1-q^n)^{-1} \cdot A_t(q) =& \mathrm{ch}_{((2t-1)(3t-2))}(q)\\ &+ \sum_{r=1}^{t-1}(-1)^r\mathrm{ch}_{((2t-1)(3t-3r-1))}(q) + \sum_{r=1}^{t-1}(-1)^r\mathrm{ch}_{((2t-1)(3t-3r-2))}(q).\end{aligned}$$

Proof. We examine the summands in $A_t(q)$. Using Theorem 3.1, the first term is

$$\begin{aligned}&\Theta(-q^{\frac{1}{2}(2t-1)}, q^{\frac{3}{2}(2t-1)^2})\\ &= \prod_{n=1}^{\infty}(1-q^{3(2t-1)^2n})(1-q^{\frac{1}{2}(2t-1)+\frac{3}{2}(2t-1)^2(2n-1)})(1-q^{-\frac{1}{2}(2t-1)+\frac{3}{2}(2t-1)^2(2n-1)})\\ &= \prod_{n=1}^{\infty}(1-q^{3(2t-1)^2n})(1-q^{-(\frac{3}{2}(2t-1)^2-\frac{1}{2}(2t-1))+3(2t-1)^2n})(1-q^{\frac{3}{2}(2t-1)^2-\frac{1}{2}(2t-1)+3(2t-1)^2(n-1)}).\end{aligned}$$

Noting that $\frac{1}{2}(3(2t-1)^2 - (2t-1)) = (2t-1)(3t-2)$, we have that

$$\Theta(-q^{\frac{1}{2}(2t-1)}, q^{\frac{3}{2}(2t-1)^2}) = \prod_{n=1}^{\infty}(1-q^n) \cdot \mathrm{ch}_{((2t-1)(3t-2))}(q).$$

Arguing with Theorem 3.1 again, we find that

$$\Psi^-_{r,t}(q) = \prod_{n=1}^{\infty}(1-q^n) \cdot \mathrm{ch}_{((2t-1)(3t-3r-1))}(q),$$

and

$$\Psi^+_{r,t}(q) = \prod_{n=1}^{\infty}(1-q^n) \cdot \mathrm{ch}_{((2t-1)(3t-3r-2))}(q).$$

The lemma follows easily. $\square$

Lemma 4.2. *If $t \geq 2$, then we have the following q-series identity*

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

Proof. It suffices to show that $A_t(q)$ is the q-series in Euler's Pentagonal Number Theorem. Write $A_t(q)$ in a more recognizable form beginning with the first term in $A_t(q)$

$$\begin{aligned}\Theta(-q^{\frac{1}{2}(2t-1)}, q^{\frac{3}{2}(2t-1)^2}) &= \sum_{n=-\infty}^{\infty} (-1)^n q^{\frac{1}{2}(2t-1)n+\frac{3}{2}(2t-1)^2n^2}\\ &= \sum_{n=-\infty}^{\infty} (-1)^n q^{\frac{1}{2}(2t-1)n(3(2t-1)n-1)},\end{aligned}$$

where we have replaced n by $-n$ in the final sum.

For $\Psi^-_{r,t}(q)$ and $\Psi^+_{r,t}(q)$ we have

$$\begin{aligned}(-1)^r\Psi^-_{r,t}(q) &= \sum_{n=-\infty}^{\infty} (-1)^{n+r} q^{\frac{1}{2}r(3r-1)+\frac{1}{2}(6r-1)(2t-1)n+\frac{3}{2}(2t-1)^2n^2}\\ &= \sum_{n=-\infty}^{\infty} (-1)^{(2t-1)n+r} q^{\frac{1}{2}((2t-1)n+r)(3((2t-1)n+r)-1)},\end{aligned}$$

and we have

$$\begin{aligned}(-1)^r\Psi^+_{r,t}(q) &= \sum_{n=-\infty}^{\infty} (-1)^{n+r} q^{\frac{1}{2}r(3r+1)+\frac{1}{2}(6r+1)(2t-1)n+\frac{3}{2}(2t-1)^2n^2}\\ &= \sum_{n=-\infty}^{\infty} (-1)^{n+r} q^{\frac{1}{2}((2t-1)n+r)(3((2t-1)n+r)+1)}\\ &= \sum_{n=-\infty}^{\infty} (-1)^{(2t-1)n+(2t-1)-r} q^{\frac{1}{2}((2t-1)n+(2t-1)-r)(3((2t-1)n+(2t-1)-r)-1)},\end{aligned}$$

where in the last line we substituted $-n$ for n and then $n+1$ for n. By combining these series, the claim follows easily from Theorem 3.2. □

Proof of Theorem 1.3. We first show that if $k = 6t^2 - 6t + 1$, then $\widetilde{\mathcal{W}}_k(q)$ vanishes. Recalling that $2k + 1 = 3(2t-1)^2$ and using the above lemmas, we obtain

$$\mathrm{ch}_{((2t-1)(3t-2))}(q) + \sum_{r=1}^{t-1}(-1)^r\mathrm{ch}_{((2t-1)(3t-3r-1))}(q) + \sum_{r=1}^{t-1}(-1)^r\mathrm{ch}_{((2t-1)(3t-3r-2))}(q) = 1.$$

This gives us a linear relationship among the columns, and the Wronskian is then identically zero.

Define, for $1 \le i \le k$, the rational number

$$a(i,k) := h_{i,k} - \tfrac{c_k}{24}.$$

If $k \ne 6t^2 - 6t + 1$, it is straightforward to show that $a(i,k) \ne 0$. Noting that

$$\mathrm{ch}_{i,k}(q) = q^{a(i,k)} + \dots$$

and making a few simple observations such as $a(i,k) > a(i+1,k)$ and $a(k,k) > -1$, it follows that $\widetilde{\mathcal{W}}_k(q)$ cannot vanish. Specifically, if the Wronskian vanished, then we would have a linear dependence of the characters. However, because $a(i,k) \neq 0$ and $a(i,k) > -1$, this is not possible. □

Proof of Theorem 1.4. For $t \geq 2$ and $k = 6t^2 - 6t + 1$, the proof of Theorem 1.3 gives the following identity

$$\prod_{n \not\equiv 0, \pm(2t-1)(3t-2) \pmod{2k+1}}^{\infty} \frac{1}{1-q^n} + \sum_{r=1}^{t-1} (-1)^r q^{\frac{1}{2}r(3r-1)} \cdot \prod_{n \not\equiv 0, \pm(2t-1)(3t-3r-1) \pmod{2k+1}}^{\infty} \frac{1}{1-q^n}$$
$$+ \sum_{r=1}^{t-1} (-1)^r q^{\frac{1}{2}r(3r+1)} \cdot \prod_{n \not\equiv 0, \pm(2t-1)(3t-3r-2) \pmod{2k+1}}^{\infty} \frac{1}{1-q^n} = 1.$$

The proof now follows by inspection. □

5. Supersingular Polynomial Congruences

Here we prove Theorem 1.5: the congruence

$$F(\mathcal{F}_k, j(z)) \equiv S_p(j(z)) \pmod{p},$$

which holds for primes $5 \leq p = (2k+1)$, where $k \neq 6t^2 - 6t + 1$ with $t \geq 2$.

We begin with a technical lemma.

Lemma 5.1. *For k with $2k+1 = p$, p a prime, then $\mathcal{F}_k(z)$ has p-integral coefficients, and satisfies the congruence*

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

Proof. If we expand $\widetilde{\mathcal{W}}_k(q)$ by minors along its bottom row, and if we expand $\mathcal{W}_k(q)$ by minors along its top row, we have that the quotient of the Wronskians is the normalization of

$$\frac{\sum_{i=1}^{k} \mathrm{ch}_{i,k}^{(k)}(q) \det(N_i)}{\sum_{i=1}^{k} \mathrm{ch}_{i,k}(q) \det(N_i)},$$

where the N_i's are the respective minors. We fix an i and consider the term

$$\mathrm{ch}_{i,k}^{(k)}(q) = \sum_{n=0}^{\infty} (n + a(i,k))^k b_{i,k}(n) q^{n+a(i,k)},$$

where

$$\mathrm{ch}_{i,k}(q) = \sum_{n=0}^{\infty} b_{i,k}(n) q^{n+a(i,k)}.$$

We note that

$$a(i,k) = \frac{(2k+1)(3k+1-6i)+6i^2}{12(2k+1)}.$$

Multiplying the numerator by $(12(2k+1))^k$ to clear out the denominators in the $a(i,k)$'s, the quotient of the Wronskians is then just the normalization of

$$\frac{\displaystyle\sum_{i=1}^{k}\sum_{n=0}^{\infty}\big(12(2k+1)n+(2k+1)(3k+1-6i)+6i^2\big)^k\, b_{i,k}(n)q^{n+a(i,k)}\det(N_i)}{\displaystyle\sum_{i=1}^{k}\mathrm{ch}_{i,k}(q)\det(N_i)}$$

However if we compute this modulo p, and note that $k=\frac{p-1}{2}$, we have

$$\big(12(2k+1)n+(2k+1)(3k+1-6i)+6i^2\big)^k \equiv \left(\frac{6}{p}\right) \pmod{p}.$$

The p-integrality follows from Theorem 1.1, and it then follows that modulo p, the quotient is just 1. ☐

Proof of Theorem 1.3. Here we simply combine Theorem 1.2, Lemma 5.1 and the second remark at the end of Section 3. ☐

Remark. There are cases for which

$$\mathcal{F}_k(z) \equiv 1 \pmod{p},$$

with $2k+1 \neq p$. It would be interesting to completely determine all the conditions for which such a congruence holds. By the theory of modular forms 'mod p', it follows that such k must have the property that $2k = a(p-1)$ for some positive integer a. A resolution of this problem requires determining conditions for which $\mathcal{F}_k(z)$ has p-integral coefficients, and also the extra conditions guaranteeing the above congruence.

Remark. The methods of this paper can be used to reveal many more congruences relating supersingular j-invariants to the divisor polynomials $F(\mathcal{F}_k, j) \pmod{p}$. For example, if

$$(k,p) \in \{(10,17),(16,29),(17,31),(22,41),(23,43),(28,53)\},$$

we have that

$$F(\mathcal{F}_k, j(z)) \equiv j(z)\cdot S_p(j(z)) \pmod{p}.$$

Such congruences follow from the multiplicative structure satisfied by divisor polynomials as described in Section 2.8 of [O].

6. A conjecture on the zeros of $F(\mathcal{F}_k, x)$

Our Theorem 1.5 shows that the divisor polynomial modulo p, for certain $\mathcal{F}_k(z)$, is the locus of supersingular j-invariants in characteristic p. We proved this theorem by showing that

$$\mathcal{F}_{\frac{p-1}{2}}(z) \equiv E_{p-1}(z) \equiv 1 \pmod{p},$$

and we then obtained the desired conclusion by applying a famous result of Deligne. In view of such close relationships between certain $\mathcal{F}_k(z)$ and $E_{2k}(z)$, it is natural to investigate other properties of $E_{2k}(z)$ which may be shared by $\mathcal{F}_k(z)$. A classical result of Rankin and Swinnerton-Dyer proves that every $F(E_{2k}, x)$ has simple roots, all of which are real and lie in the interval $[0, 1728]$. Numerical evidence strongly supports the following conjecture.

Conjecture. If $k \geq 2$ is a positive integer for which $k \neq 6t^2 - 6t + 1$ with $t \geq 2$, then $F(\mathcal{F}_k, x)$ has simple roots, all of which are real and are in the interval $[0, 1728]$.

References

[A] G. Andrews, *The Theory of Partitions*, Cambridge University Press, Cambridge, 1998.

[Bo] R. Borcherds, Vertex algebras, Kac-Moody algebras, and the Monster, *Proc. Nat. Acad. Sci. U.S.A.* **83** (1986), pages 3068–3071.

[Dw] B. Dwork, *p-adic cycles*, Inst. Hautes Études Scie. Publ. Math. **37** (1969), pages 27-115.

[FaKr] H. M. Farkas and I. Kra, *Riemann surfaces*, Springer-Verlag, New York, 1980.

[FF] B. Feigin and E. Frenkel, Coinvariants of nilpotent subalgebras of the Virasoro algebra and partition identities, in: *I.M. Gelfand Seminar*, Adv. Soviet Math. **16** (1993), Part I, pages 139-148.

[FLM] I. Frenkel, J. Lepowsky and A. Meurman, *Vertex Operator Algebras and the Monster*, Pure and Appl. Math., Vol 134, Academic Press, New York, 1988.

[KW] V. Kac and M. Wakimoto, Modular invariant representations of infinite-dimensional Lie algebras and superalgebras, *Proc. Nat. Acad. Sci. USA* **85** (1988), pages 4956-4960.

[KZ] M. Kaneko and D. Zagier, *Supersingular j-invariants, hypergeometric series, and Atkin's othogonal ploynomials*, Computational perspectives on number theory (Chicago, Il., 1995), AMS/IP **7** (1998), pages 97-126.

[M1] A. Milas, Ramanujan's "Lost Notebook" and the Virasoro algebra, *Comm. Math. Phys.* **251** (2004), pages 657-678.

[M2] A. Milas, Virasoro algebra, Dedekind eta-function and specialized Macdonald's identities, *Transf. Groups* **9** (2004), pages 273-288.

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

[R] R.A. Rankin, The construction of automorphic forms from the derivatives of given forms, *J. Indian Math. Soc.* **20**, (1956), pages 103-116.

[RC] A. Rocha-Caridi, Vacuum vector representations of the Virasoro algebra, in *Vertex operators in mathematics and physics* (Berkeley, 1983), Math. Sci. Res. Inst. Publ., 3, 1985, pages 451-473.

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

[Si] J. Silverman, *The arithmetic of elliptic curves*, Springer-Verlag, New York, 1986.

[Z] D. Zagier, Modular forms and differential operators, K. G. Ramanathan memorial issue, *Proc. Indian Acad. Sci. Math. Sci.* **104** (1994), pages 57-75.

[Zh] Y. Zhu, Modular invariance of characters of vertex operator algebras, *J. Amer. Math. Soc.* **9** (1996), pages 237–307.

Department of Mathematics and Statistics, SUNY Albany, Albany, New York 12222
E-mail address: `amilas@math.albany.edu`

Department of Mathematics, Penn State University, University Park, Pennsylvania 16802
E-mail address: `mort@math.psu.edu`

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