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 $(2, 2k + 1)$ 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 $q := e^{2\pi iz}$ 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 $[Z^2]$. For example, to construct an automorphic form from an $SL_2(\mathbb{Z})$–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.

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 $(2, 2k + 1)$ 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

\begin{equation}
    c_k := 1 - \frac{3(2k - 1)^2}{(2k + 1)},
\end{equation}

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

\begin{equation}
    h_{i,k} := \frac{(2(k - i) + 1)^2 - (2k - 1)^2}{8(2k + 1)}.
\end{equation}

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

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

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 $\text{ch}_{i,k}(q)$. It turns out that

\begin{equation}
    \text{ch}_{i,k}(q) = q^{\left(h_{i,k} - \frac{c_k}{24}\right)} \prod_{1 \leq n \neq 0, \pm i \pmod{2k+1}} \frac{1}{1 - q^n}.
\end{equation}

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

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

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

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

$$
\{\text{ch}_{1,k}(q), \text{ch}_{2,k}(q), \ldots, \text{ch}_{k,k}(q)\}.
$$
For each $k \geq 2$, define $\mathcal{W}_k(q)$ and $\mathcal{W}_k'(q)$ by

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

\begin{equation}
\mathcal{W}_k'(q) := \beta(k) \cdot \det \begin{pmatrix}
\text{ch}_{1,k}^{(1)} & \text{ch}_{2,k}^{(1)} & \cdots & \text{ch}_{k,k}^{(1)} \\
\text{ch}_{1,k}^{(2)} & \text{ch}_{2,k}^{(2)} & \cdots & \text{ch}_{k,k}^{(2)} \\
\vdots & \vdots & \ddots & \vdots \\
\text{ch}_{1,k}^{(k)} & \text{ch}_{2,k}^{(k)} & \cdots & \text{ch}_{k,k}^{(k)}
\end{pmatrix}.
\end{equation}

Here $\alpha(k)$ (resp. $\beta(k)$) is chosen so that the $q$-expansion of $\mathcal{W}_k(q)$ (resp. $\mathcal{W}_k'(q)$) has leading coefficient 1 (resp. 1 or 0), and differentiation is given by

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

which equals $\frac{1}{2\pi i} \frac{dz}{dz}$ 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 [1]), 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 $\mathcal{W}_k'(q)$, we investigate the quotient

\begin{equation}
\mathcal{F}_k(z) := \frac{\mathcal{W}_k'(q)}{\mathcal{W}_k(q)}.
\end{equation}

It turns out that these $q$-series $\mathcal{F}_k(z)$ are modular forms of weight $2k$ for the full modular group $SL_2(\mathbb{Z})$. To make this more precise, suppose that $E_4(z)$ and $E_6(z)$ are the standard Eisenstein series

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

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

\begin{equation}
\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)}.
\end{equation}

**Theorem 1.2.** If $k \geq 2$, then $\mathcal{F}_k(z)$ is a weight $2k$ holomorphic modular form on $SL_2(\mathbb{Z})$.

**Example.** For $2 \leq k \leq 5$, it turns out that

\begin{align*}
\mathcal{F}_2(z) &= E_4(z), & \mathcal{F}_3(z) &= E_6(z), \\
\mathcal{F}_4(z) &= E_4(z)^2, & \mathcal{F}_5(z) &= E_4(z)E_6(z).
\end{align*}
Some of these modular forms are identically zero. For example, we have that $F_{13}(z) = 0$, a consequence of the $q$-series identity
\begin{equation}
ch_{12,13}(q) - ch_{6,13}(q) - ch_{3,13}(q) = 1,
\end{equation}
which will be proved later. The following result completely determines those $k$ for which $F_k(z) = 0$.

**Theorem 1.3.** The modular form $F_k(z)$ 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
\begin{equation}
\sum_{n=0}^{\infty} P_b(a; n) q^n = \prod_{1 \leq n \not\equiv \pm 0, a \pmod b} \frac{1}{1 - q^n},
\end{equation}
$q$-series identity (1.9) implies, for positive $n$, the shifted partition identity
\begin{equation}
P_{27}(12; n) = P_{27}(6; n - 1) + P_{27}(3; n - 2).
\end{equation}
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
\begin{equation}
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),
\end{equation}
where
\begin{align*}
a^- (t, r) &:= (2t - 1)(3t - 3r - 2), \\
a^+ (t, r) &:= (2t - 1)(3t - 3r - 1), \\
b(t) &:= 3(2t - 1)^2, \\
\omega^- (r) &:= (3r^2 - r)/2, \\
\omega^+ (r) &:= (3r^2 + r)/2.
\end{align*}

The forms $F_k(z)$ 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 $\mathcal{E}_k(z)$ by
\begin{equation}
\mathcal{E}_k(x) := \begin{cases} 
1 & \text{if } k \equiv 0 \pmod{12}, \\
E_4(z)^2 E_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}
\end{equation}
(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 $\text{SL}_2(\mathbb{Z})$. If we write $k$ as

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

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

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

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

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

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

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

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

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

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

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

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 $k = (p - 1)/2$ is not of the form $6t^2 - 6t + 1$, where $t \geq 2$, then

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

In Section 2 we prove Theorem 1.5. 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 $\tilde{F}(\mathcal{F}_k, x)$. 


Here we study the quotient

\[ F_k(q) := \frac{W'_k(q)}{W_k(q)}, \]

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

\[ W^{i_1, \ldots, i_k}(f_1, ..., f_k)(q) = \det \begin{pmatrix} f_1^{(i_1)} & f_2^{(i_1)} & \cdots & f_k^{(i_1)} \\ f_1^{(i_2)} & f_2^{(i_2)} & \cdots & f_k^{(i_2)} \\ \vdots & \vdots & \ddots & \vdots \\ f_1^{(i_k)} & f_2^{(i_k)} & \cdots & f_k^{(i_k)} \end{pmatrix}. \]

Clearly, \( W^{0,1,\ldots,k-1}(f_1, ..., f_k) \) is the ordinary Wronskian. We will write \( W^{i_1, \ldots, i_k}(f_1, ..., f_k) \) for the normalization of \( W^{i_1, \ldots, i_k}(f_1, ..., f_k) \neq 0 \), 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

\[ E_2(z) = 1 - 24 \sum_{n=1}^{\infty} \sum_{d|n} dq^n, \]

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

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

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

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

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

\[ \Theta_k := \left( q \frac{d}{dq} \right) \frac{k}{12} E_2(z) \]

It is well known that \( \Theta_k \) sends a modular form of weight \( k \) to a modular form of weight \( k + 2 \). 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

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

Clearly, \( P_0(q) = Q_0(q) \). The proof follows. \( \square \)
Proof of Theorem 1.2. Let \( \{f_1(q), \ldots, f_k(q)\} \) 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 \( \{f_1(q), \ldots, f_k(q)\} \) is a fundamental system of \( P(y) = 0 \).

Explicitly,

(2.6)

\[
P(y) = (-1)^k \frac{W^{0,1,\ldots,k}(y, f_1, \ldots, f_k)}{W^{0,1,\ldots,k-1}(f_1, \ldots, f_k)}.
\]

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,

\[
P_0(q) = \lambda_k \frac{W_k(q)}{W_k(q)},
\]

for some nonzero constant \( \lambda_k \). Now, we specialize \( f_i(q) = \text{ch}_{i,k}(q) \) and apply Theorem 2.1. □

Remark. The techniques from [M1] can be used to give explicit formulas for \( \frac{W_k(q)}{W_k(q)} \) 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

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

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

\[
\prod_{n=1}^{\infty} (1 - q^n) = \sum_{m=-\infty}^{\infty} (-1)^m q^{\frac{1}{2}m(3m-1)}
\]
3.2. **Divisor polynomials and Deligne’s theorem.** If \( p \geq 5 \) is prime, then the supersingular loci \( S_p(x) \) and \( \tilde{S}_p(x) \) are defined in \( \mathbb{F}_p[x] \) by the following products over isomorphism classes of supersingular elliptic curves:

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

\[
(3.1) \quad \tilde{S}_p(x) := \prod_{E/\mathbb{F}_p \text{ supersingular}} (x - j(E)).
\]

For such primes \( p \), let \( \mathcal{S}_p \) 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 \( \mathbb{F}_p^2 [\{S_i\}] \). 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

\[
S_p(x) = x^{\epsilon_\omega(p)}(x - 1728)^{\epsilon_i(p)} \cdot \prod_{\alpha \in \mathcal{S}_p} (x - \alpha) \cdot \prod_{g \in \mathfrak{M}_p} g(x)
\]

\[
= x^{\epsilon_\omega(p)}(x - 1728)^{\epsilon_i(p)} \tilde{S}_p(x).
\]

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 \( n \)th 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 $\text{ch}_i(q)$ for $\text{ch}_{i,k}(q)$ when $k$ is understood.

We define

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

and we consider the sum

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

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

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

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

$$\Theta(-q^{\frac{1}{2}(2t-1)}, q^{\frac{3}{2}(2t-1)^2})$$

$$= \prod_{n=1}^{\infty} (1 - q^{3(2t-1)^2n}) (1 - q^{\frac{1}{2}(2t-1)+\frac{3}{2}(2t-1)^2(2n-1)}) (1 - q^{-\frac{1}{2}(2t-1)+\frac{3}{2}(2t-1)^2(2n-1)})$$

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

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

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

Arguing with Theorem 3.1 again, we find that

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

and

$$\Psi_{r,t}^+(q) = \prod_{n=1}^{\infty} (1 - q^n) \cdot \text{ch}_{(2t-1)(3t-3r-2)}((2t-1)(3t-3r-2)) (q).$$
The lemma follows easily.

**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 $A_t(q)$

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

$= \sum_{n=-\infty}^{\infty} (-1)^n q^{\frac{1}{2}((2t-1)n(3(2t-1)n-1))}$,

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

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

$$(-1)^r \Psi_{r,t}^-(q) = \sum_{n=-\infty}^{\infty} (-1)^{n+r} q^{\frac{1}{2}r(3r+1)+\frac{1}{2}(6r+1)(2t-1)n+\frac{3}{2}(2t-1)^2n^2}$$

$= \sum_{n=-\infty}^{\infty} (-1)^{(2t-1)n+r} q^{\frac{1}{2}((2t-1)n+r)(3((2t-1)n+r)-1)},$

and we have

$$(-1)^r \Psi_{r,t}^+(q) = \sum_{n=-\infty}^{\infty} (-1)^{n+r} q^{\frac{1}{2}r(3r+1)+\frac{1}{2}(6r+1)(2t-1)n+\frac{3}{2}(2t-1)^2n^2}$$

$= \sum_{n=-\infty}^{\infty} (-1)^{(2t-1)n+(2t-1)\frac{1}{2}r} q^{\frac{1}{2}((2t-1)n+2t-1)(3((2t-1)n+(2t-1)-r)-1)},$

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* We first show that if $k = 6t^2 - 6t + 1$, then $W_k(q)$ vanishes. Recalling that $2k+1 = 3(2t-1)^2$ and using the above lemmas, we obtain

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

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

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

$$a(i, k) := h_{i,k} - \frac{c_k}{24}.$$
If \( k \neq 6t^2 - 6t + 1 \), it is straightforward to show that \( a(i, k) \neq 0 \). Noting that

\[
\text{ch}_{i,k}(q) = q^{a(i,k)} + \ldots
\]

and making a few simple observations such as \( a(i, k) > a(i + 1, k) \) and \( a(k, k) > -1 \), it follows that \( W_k'(q) \) 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

\[
\prod_{n \neq 0, \pm(2t-1)(3t-2)} \frac{1}{1 - q^n} + \sum_{r=1}^{t-1} (-1)^r q^{\frac{1}{2}r(3r-1)} \cdot \prod_{n \neq 0, \pm(2t-1)(3t-3r-1)} \frac{1}{1 - q^n} + \sum_{r=1}^{t-1} (-1)^r q^{\frac{1}{2}r(3r+1)} \cdot \prod_{n \neq 0, \pm(2t-1)(3t-3r-2)} \frac{1}{1 - q^n} = 1.
\]

The proof now follows by inspection. \( \square \)

5. SUPERSINGULAR POLYNOMIAL CONGRUENCES

Here we prove Theorem 1.5: the congruence

\[
F(F_k, j(z)) \equiv S_p(j(z)) \pmod{p},
\]

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, and \( k \) not of the form \( 6t^2 - 6t + 1 \), \( t \geq 2 \), then \( F_k(z) \) has \( p \)-integral coefficients, and satisfies the congruence

\[
F_k(z) \equiv 1 \pmod{p}.
\]

Proof. If we expand \( W_k'(q) \) by minors along its bottom row, and if we expand \( W_k(q) \) by minors along its top row, we have that the quotient of the Wronskians is the normalization of

\[
\sum_{i=1}^{k} \frac{\chi^{(k)}_{i,k}(q) \det(M_i)}{\sum_{i=1}^{k} \chi_{i,k}(q) \det(M_i)},
\]

where the \( M(i) \)'s are the respective minors. We fix an \( i \) and consider the term

\[
\chi^{(k)}_{i,k}(q) = \sum_{n=0}^{\infty} (n + a(i, k))^k b_{i,k}(n) q^{n+a(i,k)},
\]

where

\[
\chi_{i,k}(q) = \sum_{n=0}^{\infty} b_{i,k}(n) q^{n+a(i,k)}.
\]
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
\[
\sum_{i=1}^{k} \sum_{n=0}^{\infty} \left(12(2k + 1)n + (2k + 1)(3k + 1 - 6i) + 6i^2\right)^k b_{i,k}(n)q^{n+a(i,k)} \det(M_i)
\]

However if we compute this modulo \(p\), and note that \(k = \frac{p-1}{2}\), we have
\[
\left(12(2k + 1)n + (2k + 1)(3k + 1 - 6i) + 6i^2\right)^k \equiv \left(\frac{6}{p}\right) \quad \text{(mod } p).\]

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 \(F_k(z) \equiv 1 \quad \text{(mod } p)\), with \(2k+1 \neq p\). It would 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 \(F_k(z)\) 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 \(F(F_k, j) \mod p\). For example, if \((k, p) \in \{(10, 17), (16, 29), (17, 31), (22, 41), (23, 43), (28, 53)\}\), we have that
\[ F(F_k, j(z)) \equiv j(z) \cdot S_p(j(z)) \quad \text{(mod } p).\]

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 \(F(F_k, x)\)

Our Theorem 1.5 shows that the divisor polynomial modulo \(p\), for certain \(F_k(z)\), is the locus of supersingular \(j\)-invariants in characteristic \(p\). We proved this theorem by showing that
\[ F_{-p-1}(z) \equiv E_{p-1}(z) \equiv 1 \quad \text{(mod } p), \]
and we then obtained the desired conclusion by applying a famous result of Deligne. In view of such close relationships between certain \(F_k(z)\) and \(E_{2k}(z)\), it is natural to investigate other
properties of $E_{2k}(z)$ which may be shared by $F_k(z)$. 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 $F(F_k, x)$ 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 Sci. 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 orthogonal polynomials*, 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, *Congrues et formes modulaires (d’apres 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