TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 355, Number 4, Pages 1521–1535
S 0002-9947(02)03204-X
Article electronically published on November 20, 2002

HIGHER WEIERSTRASS POINTS ON $X_0(p)$

SCOTT AHLGREN AND MATTHEW PAPANIKOLAS

Abstract. We study the arithmetic properties of higher Weierstrass points on modular curves $X_0(p)$ for primes p. In particular, for $r \in \{2, 3, 4, 5\}$, we obtain a relationship between the reductions modulo p of the collection of r-Weierstrass points on $X_0(p)$ and the supersingular locus in characteristic p.

1. Introduction and Statement of Results

Suppose that X is a smooth projective algebraic curve over $\mathbb{C}$ of genus $g \geq 2$. Let Ω_X denote the sheaf of holomorphic 1-forms on X and let r be a positive integer. Then let $\mathcal{H}^r(X) := H^0(X, \Omega_X^{\otimes r})$ denote the space of holomorphic r-differentials on X and let

$$d_r(X) := \dim_{\mathbb{C}}(\mathcal{H}^r(X)).$$

It follows from the Riemann-Roch theorem that

$$d_r(X) = \begin{cases} g & \text{if } r = 1, \\ (2r-1)(g-1) & \text{if } r \geq 2. \end{cases} \tag{1.1}$$

A point $Q \in X$ is called an *r-Weierstrass point* if there exists a holomorphic non-zero r-differential ω on X with the property that

$$\operatorname{ord}_Q \omega \geq d_r(X).$$

Suppose now that $Q \in X$ and that $\{\omega_1, \ldots, \omega_{d_r(X)}\}$ is a basis for $\mathcal{H}^r(X)$ such that

$$0 = \operatorname{ord}_Q \omega_1 < \operatorname{ord}_Q \omega_2 < \cdots < \operatorname{ord}_Q \omega_{d_r(X)}.$$

Then we define the Weierstrass weight of Q with respect to $\mathcal{H}^r(X)$ as

$$\operatorname{wt}_r(Q) := \sum_{j=1}^{d_r(X)} (\operatorname{ord}_Q(\omega_j) - j + 1). \tag{1.2}$$

This definition is independent of the choice of basis for $\mathcal{H}^r(X)$. Moreover, $\operatorname{wt}_r(Q)$ is positive if and only if Q is an r-Weierstrass point, and we have

$$\sum_{Q \in X} \operatorname{wt}_r(Q) = d_r(X)(g-1)(2r-1+d_r(X)). \tag{1.3}$$

Therefore, for each $r \geq 1$, the set of r-Weierstrass points is a finite, non-empty set of distinguished points on X. We remark that when $g < 2$ there are no r-Weierstrass

Received by the editors July 31, 2002 and, in revised form, September 19, 2002.
2000 *Mathematics Subject Classification.* Primary 11G18; Secondary 11F33, 14H55.
Key words and phrases. Weierstrass points, modular curves.
The first author thanks the National Science Foundation for its support through grant DMS 01-34577.

points for any r. For these and other general facts about Weierstrass points, one may consult, for instance, Chapter III of Farkas and Kra [F-K].

Higher Weierstrass points play an important role in the theory of algebraic curves. For example, one can use them to construct projective embeddings for moduli spaces of curves. Mumford has suggested that, on a curve of genus $g \geq 2$, r-Weierstrass points are analogous to r-torsion points on an elliptic curve (see §A.I-II of [M], or [Si]). Higher Weierstrass points are also important in the arithmetic of algebraic curves and their Jacobians; see for example Burnol [B].

In this paper we study the arithmetic of Weierstrass points on modular curves of level p for primes p. As usual, define the congruence subgroup $\Gamma_0(p)$ by

$$\Gamma_0(p) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \ : \ c \equiv 0 \pmod{p} \right\},$$

and denote by $\mathbb{H}$ the upper half-plane of complex numbers. Define

$$Y_0(p) := \Gamma_0(p) \backslash \mathbb{H},$$

and let the modular curve $X_0(p)$ be the compactification of $Y_0(p)$ obtained by adding cusps at 0 and ∞. Then $X_0(p)$ can be given the structure of a smooth projective curve defined over $\mathbb{Q}$ (see, for example, §6.7 of [Sh]). The genus of $X_0(p)$ grows linearly with p. To be precise, define the function $m(k)$ for $k \in \mathbb{N}$ by

$$m(k) := \begin{cases} \lfloor k/12 \rfloor & \text{if } k \not\equiv 2 \pmod{12}, \\ \lfloor k/12 \rfloor - 1 & \text{if } k \equiv 2 \pmod{12}; \end{cases} \tag{1.4}$$

then the genus g_p of $X_0(p)$ is given by

$$g_p = m(p+1). \tag{1.5}$$

Properties of 1-Weierstrass points (or simply Weierstrass points) on modular curves have been studied by a number of authors. See, for example, papers by Atkin [At], Lehner and Newman [L-N], Ogg [O1], [O2], and Rohrlich [R1], [R2]. In more recent work [A-O], the first author and Ono showed that the collection of Weierstrass points on $X_0(p)$, when reduced modulo p, covers the supersingular locus in characteristic p with multiplicity $g_p^2 - g_p$. To describe this result precisely requires the introduction of some notation. Throughout we agree that $q := e^{2\pi i z}$. Let

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

be the usual elliptic modular function on $\mathrm{SL}_2(\mathbb{Z})$ (by a slight abuse of notation, we shall also speak of $j(E)$ for elliptic curves E and of $j(Q)$ for points $Q \in Y_0(p)$; for the latter we take $j(\tau)$, where $\tau \in \mathbb{H}$ is any point which corresponds to Q under the standard identification). The supersingular polynomial in characteristic p is given by

$$S_p(x) := \prod_{\substack{E/\overline{\mathbb{F}}_p \\ \text{supersingular}}} (x - j(E)), \tag{1.6}$$

where the product runs over $\overline{\mathbb{F}}_p$-isomorphism classes of elliptic curves. Then $S_p(x) \in \mathbb{F}_p[x]$, and $S_p(x)$ splits completely over $\mathbb{F}_{p^2}$. Define the polynomial

$$F_p(x) := \prod_{Q \in X_0(p)} (x - j(Q))^{\mathrm{wt}_1(Q)}$$

(this definition makes sense, since it is known [O2] that the cusps of $\Gamma_0(p)$ are not Weierstrass points). In [A-O] the following result is obtained.

Theorem 1 ([A-O, Theorem 1])**.** *If p is prime, then $F_p(x)$ has p-integral rational coefficients and satisfies*

$$F_p(x) \equiv S_p(x)^{g_p^2 - g_p} \pmod{p}.$$

The goal in the present paper is to investigate similar phenomena related to higher Weierstrass points on $X_0(p)$. Here there are complications which are not present in the previous case. For example, the cusps can be (and often are) Weierstrass points. Moreover, the p-integrality (or non-p-integrality) of the analogue of the polynomials $F_p(x)$ becomes an issue. In the case of 1-Weierstrass points, the bijection between the space $\mathcal{H}^1(X_0(p))$ and the space of weight-two cusp forms on $\Gamma_0(p)$ plays a crucial role; the absence of such a bijection in the current situation is to blame for these complications.

If p is prime and $r \geq 2$, then we define the polynomial

$$F_p^{(r)}(x) := \prod_{Q \in Y_0(p)} (x - j(Q))^{\mathrm{wt}_r(Q)}. \tag{1.7}$$

By (1.1) and (1.3), and using the fact that 0 and ∞ are interchanged by the Atkin-Lehner involution, we see that

$$\deg(F_p^{(r)}(x)) = (2r-1)^2(g_p - 1)^2 g_p - 2 \cdot \mathrm{wt}_r(\infty).$$

Further, we define the polynomial $S_p^*(x) \in \mathbb{F}_p[x]$ by

$$S_p^*(x) := \prod_{\substack{E/\overline{\mathbb{F}}_p \\ \text{supersingular isom. class} \\ j(E) \neq 0, 1728}} (x - j(E)). \tag{1.8}$$

Then we have the simple relationship

$$S_p(x) = \begin{cases} S_p^*(x) & \text{if } p \equiv 1 \pmod{12}, \\ x \cdot S_p^*(x) & \text{if } p \equiv 5 \pmod{12}, \\ (x - 1728) \cdot S_p^*(x) & \text{if } p \equiv 7 \pmod{12}, \\ x(x - 1728) \cdot S_p^*(x) & \text{if } p \equiv 11 \pmod{12}. \end{cases} \tag{1.9}$$

We obtain an analogue of Theorem 1 for r-Weierstrass points ($2 \leq r \leq 5$) on the curves $X_0(p)$ under the assumption that $\mathcal{H}^r(X_0(p))$ is *good* at p. This assumption is necessary to ensure that the polynomial $F_p^{(r)}(x)$ has p-integral coefficients, and is described completely in the next section. Although there are some spaces which fail to be good, computations suggest that this condition is almost always satisfied. For example, the only space $\mathcal{H}^2(X_0(p))$ which fails to be good with $p < 800$ is $\mathcal{H}^2(X_0(373))$.

Suppose that $r \geq 2$ and that p is a prime with $p \geq 23$ (this ensures that $g_p \geq 2$). Then we define the polynomial

(1.10)

$$f_{p,r}(x) := \begin{cases} 1 & \text{if } p \equiv 1 \pmod{12}, \\ x^{\lceil \frac{1}{3}(2r-1)^2(g_p-1)(g_p-2) \rceil} & \text{if } p \equiv 5 \pmod{12}, \\ (x-1728)^{\frac{1}{2}(2r-1)^2(g_p-1)(g_p-2)} & \text{if } p \equiv 7 \pmod{12}, \\ x^{\lceil \frac{1}{3}(2r-1)^2(g_p-1)(g_p-2) \rceil}(x-1728)^{\frac{1}{2}(2r-1)^2(g_p-1)(g_p-2)} & \text{if } p \equiv 11 \pmod{12}. \end{cases}$$

With this notation we can state our main result.

Theorem 2. *Suppose that $p \geq 23$ is prime and that $2 \leq r \leq 5$. Suppose that $\mathcal{H}^r(X_0(p))$ is good at p. Then $F_p^{(r)}(x)$ has rational p-integral coefficients, and there exists a polynomial $H(x) \in \mathbb{F}_p[x]$ such that*

$$F_p^{(r)}(x) \equiv H(x) \cdot f_{p,r}(x) \cdot S_p^*(x)^{(2r-1)^2(g_p-1)(g_p-2)} \pmod{p}.$$

Examples. When $p = 53$, we have $g_p = 4$ and $\mathrm{wt}_2(\infty) = 0$. We have

$$S_{53}(x) = x(x+3)(x+7)(x^2+50x+39) = x \cdot S_{53}^*(x)$$

and

$$F_{53}^{(2)}(x) \equiv S_{53}(x)^{54} \cdot x^{18} \cdot H_1(x) \pmod{53},$$

where $H_1(x)$ is the square of a polynomial of degree 18.

When $p = 61$, we have $g_p = 4$ and $\mathrm{wt}_2(\infty) = 2$. We have

$$S_{61}(x) = (x+11)(x+20)(x+52)(x^2+38x+24) = S_{61}^*(x)$$

and

$$F_{61}^{(2)}(x) \equiv S_{61}(x)^{54} \cdot H_2(x) \pmod{61},$$

where $H_2(x)$ is the square of a polynomial of degree 25.

Remark 1. In view of (1.9) and (1.10), Theorem 2 shows that $F_p^{(r)}(x)$ is divisible by a large power of the full supersingular polynomial $S_p(x)$. Computations suggest that the powers of x and $x - 1728$ present in the definition of $f_{p,r}(x)$ may in fact typically be replaced by larger powers of these factors. However, we lack sufficient numerical evidence to make a precise conjecture about the correct power (possibly the full power) of $S_p(x)$ that divides $F_p^{(r)}(x)$. To obtain precise information about this would require a finer analysis of the modular form $G(z)$ which appears in Section 5.

Remark 2. The fact that the polynomials H_1 and H_2 described in the examples are squares is explained by (5.11) below. In each case, these polynomials are coprime to $S_p(x)$ in $\mathbb{F}_p[x]$. Their square roots are not irreducible.

In the next two sections we describe what it means for a space of differentials to be good and the connection to p-integrality. In Section 4 we prove some general results (which extend results of Serre) concerning congruences modulo p between modular forms on $\Gamma_0(p)$ and those on $\mathrm{SL}_2(\mathbb{Z})$. Section 5 contains the proof of Theorem 2. At the end of Section 3 we pause to give a brief overview of the proof.

2. The Definition of Good

Fix an integer $r \geq 2$ (eventually we will specialize to $r \in \{2,3,4,5\}$), and, using (1.1), set

$$d := d_r(X_0(p)) = (2r-1)(g_p - 1).$$

If k is an even integer, then we denote by M_k and S_k the spaces of holomorphic modular forms and cusp forms of weight k on $\Gamma := \mathrm{SL}_2(\mathbb{Z})$, and we denote by $M_k(\Gamma_0(p))$ and $S_k(\Gamma_0(p))$ the analogous spaces on $\Gamma_0(p)$. Throughout the paper we shall identify a modular form $f(z)$ with its Fourier expansion $f(z) = \sum_{n=0}^{\infty} a(n)q^n$ at ∞. Let $S_{2r}^*(\Gamma_0(p))$ be the subspace of $S_{2r}(\Gamma_0(p))$ corresponding to $\mathcal{H}^r(X_0(p))$ under the usual identification

$$\begin{array}{ccc} \left\{\begin{array}{c}\text{Meromorphic modular forms}\\ \text{of weight } 2r \text{ on } \Gamma_0(p)\end{array}\right\} & \longleftrightarrow & \left\{\begin{array}{c}\text{Meromorphic } r\text{-differentials}\\ \text{on } X_0(p)\end{array}\right\} \\ f(z) & \longleftrightarrow & \omega = f(z)(dz)^r. \end{array} \tag{2.1}$$

Then $\mathcal{H}^r(X_0(p))$ has a basis $\{\omega_1, \ldots, \omega_d\}$ over $\mathbb{C}$, where

$$\omega_i = f_i(z)(dz)^r, \qquad 1 \leq i \leq d,$$

with

$$f_i(z) \in S_{2r}^*(\Gamma_0(p)) \cap \mathbb{Q}[\![q]\!], \qquad 1 \leq i \leq d.$$

This basis can be uniquely determined by requiring further (as we shall) that these modular forms have Fourier expansions of the form

$$\begin{aligned} f_1(z) &= q^{r_1} + O(q^{r_1+1}), \\ f_2(z) &= q^{r_2} + O(q^{r_2+1}), \\ &\vdots \qquad\qquad \vdots \\ f_d(z) &= q^{r_d} + O(q^{r_d+1}), \end{aligned} \tag{2.2}$$

where

$$r = r_1 < r_2 < r_3 < \cdots < r_d, \tag{2.3}$$

and

$$\text{the coefficient of } q^{r_i} \text{ in } f_j \text{ is } 0 \text{ if } i \neq j. \tag{2.4}$$

Definition 2.1. We call $\mathcal{H}^r(X_0(p))$ *good* at p if the modular forms $f_1, \ldots, f_d$ given in (2.2)–(2.4) have p-integral Fourier coefficients.

The question of whether or not a space $\mathcal{H}^r(X_0(p))$ is good at p is quite interesting (this question is related to a discussion of Elkies and Atkin (see p. 55 of [E]) regarding lifting modular forms in characteristic p to those in characteristic zero). In particular, computations suggest that most (but not all) such spaces are good. Here we record the results of our computations; these were carried out in MAGMA using the modular forms package developed by W. Stein [B-C-P].

Proposition 2.2.

(1) $\mathcal{H}^2(X_0(p))$ *is good at* p *for* $23 \leq p < 800$ *with the exception of* $p = 373$.
(2) $\mathcal{H}^3(X_0(p))$ *is good at* p *for* $23 \leq p < 800$ *with the exception of* $p = 373, 643$.
(3) $\mathcal{H}^4(X_0(p))$ *is good at* p *for* $23 \leq p < 800$.
(4) $\mathcal{H}^5(X_0(p))$ *is good at* p *for* $23 \leq p < 400$ *with the exception of* $p = 379$.

3. The Wronskian and p-Integrality

From the general theory of Riemann surfaces (see, for example, §III.5 of [F-K]), it is known that the collection of r-Weierstrass points on $X_0(p)$, together with their weights, is determined by the divisor of a certain differential on $X_0(p)$. In particular, if $\{h_1, \dots, h_d\}$ is any basis for $S_{2r}^*(\Gamma_0(p))$, we define

$$W(h_1, \dots, h_d)(z) := \begin{vmatrix} h_1(z) & h_2(z) & \cdots & h_d(z) \\ h_1'(z) & h_2'(z) & \cdots & h_d'(z) \\ \vdots & \vdots & & \vdots \\ h_1^{(d-1)}(z) & h_2^{(d-1)}(z) & \cdots & h_d^{(d-1)}(z) \end{vmatrix}. \tag{3.1}$$

We define the *Wronskian* $\mathcal{W}(z)$ as the unique scalar multiple of $W(h_1, \dots, h_d)(z)$ whose leading Fourier coefficient equals 1. In this way $\mathcal{W}(z)$ is independent of the particular basis and is a cusp form on $\Gamma_0(p)$ whose weight (using Proposition III.5.10 of [F-K] and (1.1)) is

$$d(2r + d - 1) = g_p(g_p - 1)(2r - 1)^2.$$

The importance of the Wronskian arises from the fact that

$$\operatorname{div}\left(\mathcal{W}(z)(dz)^{\frac{1}{2}g_p(g_p-1)(2r-1)^2}\right) = \sum_{Q \in X_0(p)} \operatorname{wt}_r(Q)Q. \tag{3.2}$$

Our next lemma gives one consequence of the existence of a good basis for $\mathcal{H}^r(X_0(p))$.

Lemma 3.1. *Suppose that $2 \le r \le 6$, and let p be a prime such that $\mathcal{H}^r(X_0(p))$ is good at p. Then $\mathcal{W} \in S_{g_p(g_p-1)(2r-1)^2}(\Gamma_0(p))$ has rational p-integral Fourier coefficients.*

Remark. When $p = 373$ and $r = 2$ (so that $\mathcal{H}^r(X_0(p))$ is bad at p) we find that the Wronskian $\mathcal{W}$ indeed has non-p-integral coefficients.

Proof. Suppose that $\mathcal{H}^r(X_0(p))$ is good at p, and that $\{f_1, \dots, f_d\}$ is a basis of $S_{2r}^*(\Gamma_0(p))$ satisfying (2.2)–(2.4). Then, if $\theta := q\frac{d}{dq}$ denotes the usual differential operator on modular forms, we see that

$$W(f_1, \dots, f_d) = (2\pi i)^{\frac{d(d-1)}{2}} \begin{vmatrix} f_1 & f_2 & \cdots & f_d \\ \theta f_1 & \theta f_2 & \cdots & \theta f_d \\ \vdots & \vdots & & \vdots \\ \theta^{d-1} f_1 & \theta^{d-1} f_2 & \cdots & \theta^{d-1} f_d \end{vmatrix}. \tag{3.3}$$

It follows that the Fourier expansion of $(\frac{1}{2\pi i})^{\frac{d(d-1)}{2}} W(f_1, \dots, f_d)$ has p-integral rational coefficients, and that the coefficient of the first term in this expansion is given by the Vandermonde determinant

$$V := \begin{vmatrix} 1 & 1 & \cdots & 1 \\ r_1 & r_2 & \cdots & r_d \\ \vdots & \vdots & & \vdots \\ r_1^{d-1} & r_2^{d-1} & \cdots & r_d^{d-1} \end{vmatrix}. \tag{3.4}$$

To prove the lemma it will therefore suffice to show that none of the differences $r_i - r_j$ for $i \neq j$ is a multiple of p. It is known that the total number of zeros of a non-zero holomorphic modular form of weight k on $\Gamma_0(p)$ (as measured in local

variables) is given by $\frac{k}{12}(p+1)$ (see, for example, §V.2.4 of [Sc]). If $r \in \{2,3,4,5,6\}$, we conclude from this that

$$r_i - r_j \leq r_i - r \leq p-1 \quad \text{if} \quad i > j,$$

from which the lemma follows immediately. □

We now give a brief outline of the proof of Theorem 2. In the case of 1-Weierstrass points, Rohrlich [R2] used the isomorphism between $\mathcal{H}^1(X_0(p))$ and $S_2(\Gamma_0(p))$ to obtain a precise description of the Wronskian $\mathcal{W}(z) \pmod p$ as a modular form modulo p on $\mathrm{SL}_2(\mathbb{Z})$. In the present situation we lack such precise information about $\mathcal{W}(z) \pmod p$. However, we can show, using the results which we develop in the next section, that $\mathcal{W}(z) \pmod p$ is the reduction modulo p of a modular form $G(z)$ on $\mathrm{SL}_2(\mathbb{Z})$ of relatively low weight. It can also be shown that $\mathcal{W}^2(z) \pmod p$ is the reduction modulo p of a modular form $\widetilde{\mathcal{W}}(z)$ on $\mathrm{SL}_2(\mathbb{Z})$ of high weight; moreover, the form $\widetilde{\mathcal{W}}(z)$ has the property that its divisor retains much of the crucial information about Weierstrass points which is contained in the divisor of $\mathcal{W}(z)$. Theorem 2 will follow from the discrepancy in the weights of the forms $G^2(z)$ and $\widetilde{\mathcal{W}}(z)$. An important ingredient is the fact (due to Deligne) that the Eisenstein series $E_{p-1}(z)$ is congruent to the Hasse invariant in characteristic p; in other words, the supersingular j-invariants in characteristic p are precisely the values of the j function at the zeros of E_{p-1}.

4. Congruences Between Spaces of Modular Forms

In this section we will develop some generalities on congruences modulo p between modular forms on $\Gamma_0(p)$ and those on $\mathrm{SL}_2(\mathbb{Z})$. In particular, we generalize the well-known fact (due to Serre [Se]) that the reductions modulo p of the spaces $M_2(\Gamma_0(p))$ and M_{p+1} are the same. Because they are of independent interest, we state results which are slightly more general then what we require for our work.

If $f(z)$ is a function of the upper half-plane, k is an integer, and $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2^+(\mathbb{R})$, then as usual we define

$$(f\big|_k\gamma)(z) := (ad-bc)^{\frac{k}{2}}(cz+d)^{-k} f\left(\frac{az+b}{cz+d}\right).$$

Further, we define

$$w_p := \begin{pmatrix} 0 & -1 \\ p & 0 \end{pmatrix},$$

and we denote by $S_k^+(\Gamma_0(p))$ the subspace of $S_k(\Gamma_0(p))$ consisting of forms which are invariant under the Fricke involution

$$f \mapsto f\big|_k w_p.$$

Also, we denote by $S_k^{\mathrm{new}}(\Gamma_0(p))$ the subspace of $S_k(\Gamma_0(p))$ spanned by newforms.

Now let $\widetilde{S}_k(\Gamma_0(p)) \subseteq \mathbb{F}_p[\![q]\!]$ be the $\mathbb{F}_p$-vector space consisting of the reductions modulo p of those forms in $S_k(\Gamma_0(p))$ with p-integral rational coefficients, and define the $\mathbb{F}_p$-vector spaces $\widetilde{S}_k^{\mathrm{new}}(\Gamma_0(p))$, $\widetilde{S}_k^+(\Gamma_0(p))$, and $\widetilde{M}_k(\Gamma_0(p))$ in the analogous fashion. In the same way, let $\widetilde{M}_k$ (respectively $\widetilde{S}_k$) be the spaces of reductions modulo p of modular forms (respectively cusp forms) on $\mathrm{SL}_2(\mathbb{Z})$.

There is a well-known isomorphism (see Serre [Se], Theorem 11)

$$\widetilde{M}_2(\Gamma_0(p)) \cong \widetilde{M}_{p+1}.$$

In fact, considering $\widetilde{M}_2(\Gamma_0(p))$ and $\widetilde{M}_{p+1}$ as $\mathbb{F}_p$-subspaces of $\mathbb{F}_p[\![q]\!]$, this isomorphism is an equality. The following theorem contains further results in this direction.

Theorem 4.1. *Let $p \geq 5$ be an odd prime.*

(a) *Suppose that $k \geq 2$. Then $\widetilde{S}_k^{\text{new}}(\Gamma_0(p)) \subseteq \widetilde{S}_{(k-1)p+1}$.*
(b) *If $k \in \{2, 4, 6, 8, 10, 14\}$, then $\widetilde{S}_k(\Gamma_0(p)) = \widetilde{S}_{(k-1)p+1}$.*
(c) *Suppose that $k \geq 2$. Then $\widetilde{S}_k^+(\Gamma_0(p)) \subseteq \widetilde{S}_{\frac{k}{2}(p+1)}$.*

The remainder of the section is devoted to the proof of Theorem 4.1. Our arguments follow those of Serre [Se], §3. For even integers $k \geq 4$, let B_k be the k-th Bernoulli number, and define the Eisenstein series $E_k(z) \in M_k$ by

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

We define operators V_p and U_p on $\mathbb{C}[\![q]\!]$ by

$$\sum_{n=0}^{\infty} a(n) q^n \big| V_p := \sum_{n=0}^{\infty} a(n) q^{pn},$$
$$\sum_{n=0}^{\infty} a(n) q^n \big| U_p := \sum_{n=0}^{\infty} a(pn) q^n.$$

For $p \geq 5$ we define

$$h(z) := E_{p-1}(z) - p^{p-1} E_{p-1}(z) \big| V_p.$$

By [Se], Lemma 8, we have

$$h(z) \equiv 1 \pmod{p}, \tag{4.1}$$

$$h(z)^{\lambda} \big|_{\lambda(p-1)} w_p \equiv 0 \pmod{p^{\frac{\lambda(p+1)}{2}}} \text{ for } \lambda \geq 0. \tag{4.2}$$

Let $A_1, \ldots, A_{p+1}$ be representatives for the coset space $\Gamma_0(p) \backslash \Gamma$. We define the *trace* of a modular form $f \in M_k(\Gamma_0(p))$ by

$$\text{Tr}(f) := \sum_{j=1}^{p+1} f \big|_k A_j.$$

By Lemma 7 of [Se], we have

$$\text{Tr}(f) = f + p^{1-\frac{k}{2}} \left(f \big|_k w_p \right) \big| U_p.$$

It is clear that $\text{Tr}(f) \in M_k$ (and that $\text{Tr}(f)$ is a cusp form if f is a cusp form). Moreover, if f has rational coefficients, then the same is true of $\text{Tr}(f)$.

In general, if $f(z) = \sum_{n=0}^{\infty} a(n) q^n$ is a holomorphic modular form with rational coefficients, then we take

$$\text{ord}_p(f) := \inf_n \text{ord}_p(a(n)).$$

We record three lemmas for convenience.

Lemma 4.2. *Suppose that $f \in M_k(\Gamma_0(p))$ has rational Fourier coefficients and that λ is a non-negative integer. Then*

$$\text{ord}_p \left(\text{Tr}(f h^{\lambda}) - f h^{\lambda} \right) \geq 1 - \tfrac{k}{2} + \lambda + \text{ord}_p \left(f \big|_k w_p \right).$$

Proof. We have

$$\mathrm{Tr}(fh^\lambda) - fh^\lambda = p^{1-\frac{1}{2}(k+\lambda(p-1))}\left(f\big|_k w_p \cdot h^\lambda\big|_{\lambda(p-1)} w_p\right)|U_p.$$

From this and (4.2) we obtain

$$\mathrm{ord}_p\left(\mathrm{Tr}(fh^\lambda) - fh^\lambda\right) \geq 1 - \tfrac{1}{2}(k+\lambda(p-1)) + \frac{\lambda(p+1)}{2} + \mathrm{ord}_p\left(f\big|_k w_p\right).$$

The result follows. □

Lemma 4.3. *Suppose that $f \in S_k^{\mathrm{new}}(\Gamma_0(p))$ and that f has rational p-integral coefficients. Then $\mathrm{Tr}(fh^{k-1}) \in S_{(k-1)p+1}$ has rational p-integral coefficients and satisfies*

$$\mathrm{Tr}(fh^{k-1}) \equiv f \pmod{p}.$$

Proof. That $\mathrm{Tr}(fh^{k-1}) \in S_{(k-1)p+1}$ is clear. To prove the congruence, we write

$$\mathrm{Tr}(fh^{k-1}) - f = \left(\mathrm{Tr}(fh^{k-1}) - fh^{k-1}\right) + f(h^{k-1}-1).$$

In view of (4.1), we only need to show that

$$\mathrm{ord}_p\left(\mathrm{Tr}(fh^{k-1}) - fh^{k-1}\right) > 0.$$

By Lemma 4.2, we have

$$\mathrm{ord}_p\left(\mathrm{Tr}(fh^{k-1}) - fh^{k-1}\right) \geq \tfrac{k}{2} + \mathrm{ord}_p\left(f\big|_k w_p\right). \tag{4.3}$$

Because $f \in S_k^{\mathrm{new}}(\Gamma_0(p))$, we have $\mathrm{Tr}\left(f\big|_k w_p\right) = 0$. Together with the fact that

$$\mathrm{Tr}\left(f\big|_k w_p\right) = f\big|_k w_p + p^{1-\frac{k}{2}} f|U_p,$$

this shows that

$$\mathrm{ord}_p\left(f\big|_k w_p\right) \geq 1 - \tfrac{k}{2}. \tag{4.4}$$

The lemma then follows from (4.3) and (4.4). □

Lemma 4.4. *Suppose that $f \in M_k(\Gamma_0(p))$ has rational coefficients, and suppose further that f and $f\big|_k w_p$ are both p-integral. Then the modular form $\mathrm{Tr}(fh^{\frac{k}{2}})$ is in $M_{\frac{k}{2}(p+1)}$ and satisfies*

$$\mathrm{Tr}(fh^{\frac{k}{2}}) \equiv f \pmod{p}.$$

Proof. This follows from Lemma 4.2 in the same manner as Lemma 4.3. □

Proof of Theorem 4.1. Part (a) follows immediately from Lemma 4.3. Part (c) follows in a similar manner from Lemma 4.4, since $f|_k w_p = f$ for all $f \in S_k^+(\Gamma_0(p))$.

To prove part (b), suppose that $k \in \{2,4,6,8,10,14\}$. Then $S_k(\Gamma_0(p)) = S_k^{\mathrm{new}}(\Gamma_0(p))$; therefore by part (a) we need only show that $\dim_{\mathbb{F}_p} \widetilde{S}_k(\Gamma_0(p)) = \dim_{\mathbb{F}_p} \widetilde{S}_{(k-1)p+1}$, or equivalently that

$$\dim_{\mathbb{C}} S_k(\Gamma_0(p)) = \dim_{\mathbb{C}} S_{(k-1)p+1}. \tag{4.5}$$

By classical dimension formulas we have

$$\dim_{\mathbb{C}} S_{(k-1)p+1} = m((k-1)p+1), \tag{4.6}$$

where $m(k)$ is defined in (1.4). For $k = 2$, (4.5) can be verified using (1.5) and (4.6). Suppose then that $k \geq 4$. By combining Proposition 1.43 and Theorem 2.24 of [Sh], we observe that for all even $k \geq 4$ we have

$$\dim_{\mathbb{C}} S_k(\Gamma_0(p)) = g_p(k-1) - 1 + \left(1 + \left(\frac{-1}{p}\right)\right)\left\lfloor \frac{k}{4} \right\rfloor + \left(1 + \left(\frac{-3}{p}\right)\right)\left\lfloor \frac{k}{3} \right\rfloor. \tag{4.7}$$

It is now a matter of checking the various cases to confirm that the values in (4.6) and (4.7) are the same for $k \in \{4, 6, 8, 10, 14\}$ and for all p, and we do not include the details here. □

5. Proof of Theorem 2

We begin with a lemma.

Lemma 5.1. *If $p \geq 23$ is prime and $\mathcal{W}$ is the Wronskian of $\mathcal{H}^r(X_0(p))$, then*

$$\mathcal{W}\big|_{g_p(g_p-1)(2r-1)^2} w_p = \pm \mathcal{W}.$$

Proof. Let $S_{2r}^*(\Gamma_0(p))$ be the subspace of $S_{2r}(\Gamma_0(p))$ corresponding to $\mathcal{H}^r(X_0(p))$ as described in Section 2. Since the Atkin-Lehner involution w_p is an automorphism of $X_0(p)$, it acts also on the space $\mathcal{H}^r(X_0(p))$; therefore the map $f \mapsto f\big|_{2r} w_p$ defines an action on $S_{2r}^*(\Gamma_0(p))$. Since $w_p^2 = 1$ (and the characteristic is not two), the operator defined by this action is diagonalizable on $S_{2r}^*(\Gamma_0(p))$. We may therefore choose a basis $\{h_1, \dots, h_d\}$ of $S_{2r}^*(\Gamma_0(p))$ such that

$$h_i\big|_{2r} w_p = \lambda_i h_i \quad \text{with} \quad \lambda_i \in \{\pm 1\}, \qquad 1 \leq i \leq d. \tag{5.1}$$

It clearly suffices to prove the assertion in the lemma with $\mathcal{W}$ replaced by $W := W(h_1, \dots, h_d)$. From (5.1) it follows that for each i we have

$$h_i(-1/pz) = \lambda_i p^r z^{2r} h_i(z). \tag{5.2}$$

Using (5.2) and induction, we find that for each i and for all $n \geq 1$ we have

$$h_i^{(n)}(-1/pz) = \lambda_i \left(p^{r+n} z^{2r+2n} h_i^{(n)}(z) + \sum_{j=0}^{n-1} A_{n,j}(p,z) h_i^{(j)}(z) \right), \tag{5.3}$$

where each $A_{n,j}$ is a polynomial in p and z which is independent of i. From the definition (3.1) together with (5.3) and properties of determinants, we conclude that

$$W(-1/pz) = \left(\prod_{i=1}^{d} \lambda_i \right) \cdot p^{\frac{1}{2} g_p (g_p-1)(2r-1)^2} z^{g_p(g_p-1)(2r-1)^2} W(z).$$

The lemma follows. □

Our next proposition is a general version of [A-O, Lemma 3]. For the remainder we agree that $\rho := e^{\frac{2\pi i}{3}}$.

Proposition 5.2. *Suppose that*

$$W(z) = q^h + \sum_{n=h+1}^{\infty} a(n) q^n \in S_k(\Gamma_0(p))$$

has rational p-integral coefficients and that $W\big|_k w_p = \pm W$. *Let* $\widetilde{W}(z)$ *be the modular form*

$$\prod_{A\in\Gamma_0(p)\backslash\Gamma} W\big|_k A,$$

normalized to have leading coefficient 1. *Then* $\widetilde{W} \in S_{k(p+1)}$, $\widetilde{W}$ *has rational p-integral coefficients, and*

$$\widetilde{W} \equiv W^2 \pmod{p}.$$

Moreover, if $\tau \in \mathbb{H}$, *then let* $Q_\tau \in Y_0(p)$ *be the point corresponding to* τ *under the natural identification. Then we have*

$$\begin{aligned}
\operatorname{ord}_{\tau_0} \widetilde{W} &= \sum_{\substack{\tau\in\Gamma_0(p)\backslash\mathbb{H}\\ \tau\overset{\Gamma}{\sim}\tau_0}} \operatorname{ord}_{Q_\tau} W(z)(dz)^{\frac{k}{2}} \quad \text{if } \tau_0 \in \mathbb{H}, \quad \tau_0 \overset{\Gamma}{\not\sim} i, \rho,\\
\operatorname{ord}_i \widetilde{W} &= 2\sum_{\substack{\tau\in\Gamma_0(p)\backslash\mathbb{H}\\ \tau\overset{\Gamma}{\sim} i}} \operatorname{ord}_{Q_\tau} W(z)(dz)^{\frac{k}{2}} + \left(1+\left(\tfrac{-1}{p}\right)\right)\tfrac{k}{2},\\
\operatorname{ord}_\rho \widetilde{W} &= 3\sum_{\substack{\tau\in\Gamma_0(p)\backslash\mathbb{H}\\ \tau\overset{\Gamma}{\sim}\rho}} \operatorname{ord}_{Q_\tau} W(z)(dz)^{\frac{k}{2}} + \left(1+\left(\tfrac{-3}{p}\right)\right)k.
\end{aligned} \tag{5.4}$$

Proof. Since $[\Gamma : \Gamma_0(p)] = p+1$, it is clear that $\widetilde{W} \in S_{k(p+1)}$. The identity matrix together with the matrices $A_j := \left(\begin{smallmatrix} 0 & -1 \\ 1 & j\end{smallmatrix}\right)$, $0 \le j \le p-1$, form a complete set of coset representatives for the space $\Gamma_0(p)\backslash\Gamma$. Moreover, for each j we have $A_j = w_p B_j$, where $B_j = \left(\begin{smallmatrix} 1/p & j/p \\ 0 & 1\end{smallmatrix}\right)$. Therefore

$$\prod_{j=0}^{p-1} W\big|_k A_j = \pm \prod_{j=0}^{p-1} W\big|_k B_j. \tag{5.5}$$

Now let $\{c(n)\}_{n=1}^\infty$ denote the unique sequence of exponents which (in a small neighborhood of infinity) express $W(z)$ as an infinite product of the form

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

(see Lemma 2.1 of [B-K-O]). Then each $c(n)$ is a p-integral rational number. Therefore, setting $\zeta_p := e^{\frac{2\pi i}{p}}$, we find that the product in (5.5) (after normalization) is given by

$$\begin{aligned}
q^h \prod_{n=1}^\infty \prod_{j=0}^{p-1} (1-q^{\frac{n}{p}}\zeta_p^{nj})^{c(n)} &= q^h \prod_{p\nmid n} (1-q^n)^{c(n)} \prod_{p\mid n} (1-q^{\frac{n}{p}})^{pc(n)}\\
&\equiv q^h \prod_{n=1}^\infty (1-q^n)^{c(n)} \pmod{p}.
\end{aligned}$$

The asserted congruence follows.

To prove the remaining statements, we begin with the fact that for $A \in \Gamma$ and $\tau \in \mathbb{H}$, we have

$$\operatorname{ord}_\tau (W\big|_k A) = \operatorname{ord}_{A(\tau)} W. \tag{5.6}$$

For $\tau \in \mathbb{H}$, let $\ell_\tau \in \{1,2,3\}$ denote the order of the isotropy subgroup of τ in $\Gamma_0(p)/\{\pm I\}$. Then we have

$$\operatorname{ord}_\tau W = \ell_\tau \cdot \operatorname{ord}_{Q_\tau} W(z)(dz)^{\frac{k}{2}} + \tfrac{k}{2}(\ell_\tau - 1) \tag{5.7}$$

(see, for example, §2.4 of [Sh]). The first assertion in (5.4) follows immediately from (5.6) and (5.7).

To prove the second assertion, we must consider the list of points $[A(i)]_{A\in\Gamma_0(p)\backslash\Gamma}$. We first note that the point $i = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right) i$ appears twice in this list. Since i is stabilized in $\Gamma/\pm I$ by I and $\left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$, we see that the list contains $1 + \left(\frac{-1}{p}\right)$ elliptic fixed points of order 2 which are $\Gamma_0(p)$-inequivalent; these are the points $-1/(i+j)$, where $j^2 \equiv -1 \pmod p$. Finally, if $1 \le j \le p-1$ has $j^2 \not\equiv -1 \pmod p$, and we define j' by $jj' \equiv -1 \pmod p$, then we see that the points $-1/(i+j)$ and $-1/(i+j')$ are $\Gamma_0(p)$-equivalent; the remainder of the list above therefore consists of $\frac{1}{2}\left(p - \left(\frac{-1}{p}\right) - 2\right)$ orbits, each of which contains such a pair. After this discussion, we conclude, using (5.6), that

$$\operatorname{ord}_i \widetilde{W} = \sum_{A\in\Gamma_0(p)\backslash\Gamma} \operatorname{ord}_{A(i)} W = 2 \sum_{\substack{\tau\in\Gamma_0(p)\backslash\mathbb{H} \\ \tau \overset{\Gamma}{\sim} i,\ \ell_\tau = 1}} \operatorname{ord}_\tau W + \sum_{\substack{\tau\in\Gamma_0(p)\backslash\mathbb{H} \\ \tau \overset{\Gamma}{\sim} i,\ \ell_\tau = 2}} \operatorname{ord}_\tau W.$$

The second assertion now follows from (5.7). The third follows in a similar fashion, and we do not include the details here. □

Now suppose that $2 \le r \le 5$. Let $\{f_1, \dots, f_d\}$ be the basis of $S^*_{2r}(\Gamma_0(p))$ described in (2.2)–(2.4), and let V be the Vandermonde determinant displayed in (3.4). Since we assume that $\mathcal{H}^r(X_0(p))$ is good at p, we conclude by part (b) of Theorem 4.1 that there exist forms $F_1, \dots, F_d \in S_{(2r-1)p+1}$ with rational p-integral coefficients and such that

$$f_i \equiv F_i \pmod p, \qquad 1 \le i \le d.$$

Therefore, recalling (3.3) and using Lemma 3.1, we see that

$$\mathcal{W} = \frac{1}{V}\left(\frac{1}{2\pi i}\right)^{\frac{d(d-1)}{2}} W(f_1, \dots, f_d) \equiv \frac{1}{V}\left(\frac{1}{2\pi i}\right)^{\frac{d(d-1)}{2}} W(F_1, \dots, F_d) \pmod p.$$

We now define

$$G(z) := \frac{1}{V}\left(\frac{1}{2\pi i}\right)^{\frac{d(d-1)}{2}} W(F_1, \dots, F_d)(z).$$

An argument using properties of determinants as in Lemma 3.1 shows that $G \in S_{d(2rp-p+d)}$. Moreover, if $\widetilde{\mathcal{W}} \in S_{(p+1)g_p(g_p-1)(2r-1)^2}$ is the form

$$\prod_{A\in\Gamma_0(p)\backslash\Gamma} \mathcal{W}\big|_{g_p(g_p-1)(2r-1)^2} A$$

(after normalization) described in Proposition 5.2, then we have

$$\widetilde{\mathcal{W}} \equiv G^2 \pmod p.$$

Using the fact that $d = (2r-1)(g_p-1)$, we conclude that

$$\widetilde{\mathcal{W}} \equiv G^2 E_{p-1}^{(2r-1)^2(g_p-1)(g_p-2)} \pmod p, \tag{5.8}$$

where these forms have the same weight.

To complete the proof requires some introduction of notation. In particular, if $k \geq 4$ is even, then define $\widetilde{E}_k(z)$ by

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

Also, let

$$\Delta(z) := \frac{E_4(z)^3 - E_6(z)^2}{1728}$$

be the unique normalized cusp form of weight 12 on $\mathrm{SL}_2(\mathbb{Z})$. If $f \in M_k$ has leading coefficient 1, then we define $\widetilde{F}(f, x)$ as the unique rational function in x for which

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

where $m(k)$ is defined as in (1.4). A straightforward argument (see, for example, Lemma 2.1 of [A-O]) shows that $\widetilde{F}(f, x)$ is in fact a polynomial. Moreover, it is not hard to show that $\widetilde{F}(f, x)$ has p-integral rational coefficients whenever the modular form f does.

Since the forms appearing in (5.8) have the same weight, we conclude that

$$\widetilde{F}(\widetilde{\mathcal{W}}, x) \equiv \widetilde{F}(G^2 E_{p-1}^{(2r-1)^2(g_p-1)(g_p-2)}, x) \pmod{p}. \tag{5.9}$$

We now require a result from [A-O] (cf. [G], Theorem 2.4).

Proposition 5.3 ([A-O], Theorem 2.3)**.** *Suppose that $p \geq 5$ is prime and that $f \in M_k$ has p-integral rational coefficients. Define the polynomial $C_p(k; x)$ by*

$$C_p(k; x) := \begin{cases} x & \text{if } (k, p) \equiv (2, 5), (8, 5), (8, 11) \pmod{12}, \\ x - 1728 & \text{if } (k, p) \equiv (2, 7), (6, 7), (10, 7), (6, 11), (10, 11) \pmod{12}, \\ x(x - 1728) & \text{if } (k, p) \equiv (2, 11) \pmod{12}, \\ 1 & \text{otherwise.} \end{cases}$$

Then

$$\widetilde{F}(f E_{p-1}, x) \equiv \widetilde{F}(E_{p-1}, x) \cdot \widetilde{F}(f, x) \cdot C_p(k; x) \pmod{p}.$$

Recalling that the weight of the modular form G^2 appearing in (5.8) is $2d(2rp - p + d)$, we define the polynomial $G_{p,r}(x)$ by

$$G_{p,r}(x) := \prod_{j=1}^{(2r-1)^2(g_p-1)(g_p-2)} C_p\left(2d(2rp-p+d) + \left((2r-1)^2(g_p-1)(g_p-2) - j\right)(p-1); x\right).$$

Then, using (5.9) and Proposition 5.3, we see that

$$\widetilde{F}(\widetilde{\mathcal{W}}, x) \equiv G_{p,r}(x) \cdot \widetilde{F}(E_{p-1}, x)^{(2r-1)^2(g_p-1)(g_p-2)} \cdot \widetilde{F}(G^2, x) \pmod{p}. \tag{5.10}$$

Using (1.1), we may write

$$G_{p,r}(x) = \prod_{j=1}^{(2r-1)^2(g_p-1)(g_p-2)} C_p((2r-1)^2 g_p(g_p-1)(p+1) - j(p-1)\ ; x).$$

A case-by-case computation using Proposition 5.3 shows that $G_{p,r}(x) = f_{p,r}(x)$, where $f_{p,r}(x)$ is defined in (1.10). We now require another lemma.

Lemma 5.4. *Define* $k^* \in \{0, 1, 2\}$ *by*

$$k^* \equiv (p+1)g_p(g_p-1)(2r-1)^2 \pmod 3.$$

Then

$$\widetilde{F}(\widetilde{\mathcal{W}}, x) = F_p^{(r)}(x) \cdot x^{\epsilon_p(\rho)}(x-1728)^{\epsilon_p(i)},$$

where

$$\epsilon_p(\rho) := \frac{\left(1 + \left(\frac{-3}{p}\right)\right) g_p(g_p-1)(2r-1)^2 - k^*}{3},$$
$$\epsilon_p(i) := \frac{\left(1 + \left(\frac{-1}{p}\right)\right) g_p(g_p-1)(2r-1)^2}{4}.$$

Proof. Recall that $j(z)$ vanishes to order 3 at $z = \rho$ and that $j(z) - 1728$ vanishes to order 2 at $z = i$; at all other points $\tau_0 \in \Gamma\backslash\mathbb{H}$ we have $\operatorname{ord}_{z=\tau_0}(j(z) - j(\tau_0)) = 1$. Using this together with the definition of the polynomial $\widetilde{F}$, we see that if $\tau_0 \in \Gamma\backslash\mathbb{H}$, then the exponent of $(x - j(\tau_0))$ in the factorization of $\widetilde{F}(\widetilde{W}, x)$ is given by

$$\begin{cases} \operatorname{ord}_{\tau_0} \widetilde{W} & \text{if } \tau_0 \neq i, \rho, \\ \frac{1}{2} \operatorname{ord}_i \widetilde{W} & \text{if } \tau_0 = i, \\ \frac{1}{3}(\operatorname{ord}_\rho \widetilde{W} - k^*) & \text{if } \tau_0 = \rho. \end{cases}$$

The lemma follows from this fact together with (1.7), (3.2), and (5.4). □

Deligne (see, for example, [Sw] or Theorem 2.2 of [G]) showed that E_{p-1} is congruent to the Hasse invariant in characteristic p. In the present language (see also [K-Z]), we have

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

Combining this fact with (5.10) and Lemma 5.4, we see that

(5.11)
$$F_p^{(r)}(x) \cdot x^{\epsilon_p(\rho)}(x-1728)^{\epsilon_p(i)} \equiv f_{p,r}(x) \cdot S_p^*(x)^{(2r-1)^2(g_p-1)(g_p-2)} \cdot \widetilde{F}(G^2, x) \pmod p.$$

In every case we see that $x^{\epsilon_p(\rho)}(x-1728)^{\epsilon_p(i)}$ is coprime to $f_{p,r}(x) \cdot S_p^*(x)$. Therefore Theorem 2 follows from (5.11).

Acknowledgments

The authors thank Matt Baker, Ken Ono, Joseph Silverman, and the referee for their helpful comments and suggestions.

References

[A-O] S. Ahlgren and K. Ono, *Weierstrass points on $X_0(p)$ and supersingular j-invariants*, Math. Ann., to appear.

[At] A. O. L. Atkin, *Weierstrass points at cusps of $X_0(N)$*, Ann. of Math. (2) **85** (1967), 42–45. MR **36:**1646

[B-C-P] W. Bosma, J. Cannon, and C. Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997), 235–265.

[B-K-O] J. Bruinier, W. Kohnen, and K. Ono, *The arithmetic of the values of modular functions and the divisors of modular forms*, Compositio Math., to appear.

[B] J.-F. Burnol, *Weierstrass points on arithmetic surfaces*, Invent. Math. **107** (1992), 421–432. MR **93b:**14040

[E] N. D. Elkies, *Elliptic and modular curves over finite fields and related computational issues*, Computational perspectives on number theory (Chicago, IL, 1995), AMS/IP Stud. Adv. Math., vol. 7, Amer. Math. Soc., Providence, RI, 1998, pp. 21–76. MR **99a:**11078

[F-K] H. M. Farkas and I. Kra, *Riemann surfaces*, Springer-Verlag, New York, 1992. MR **93a:**30047

[G] E.-U. Gekeler, *Some observations on the arithmetic of Eisenstein series for the modular group* $\mathrm{SL}_2(\mathbb{Z})$, Arch. Math. (Basel) **77** (2001), 5–21. MR **2002f:**11050

[L-N] J. Lehner and M. Newman, *Weierstrass points on $\Gamma_0(N)$*, Ann. of Math. (2) **79** (1964), 360–368. MR **28:**5045

[K-Z] 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 Stud. Adv. Math., vol. 7, Amer. Math. Soc., Providence, RI, 1998, pp. 97–126. MR **99b:**11064

[M] D. Mumford, *The red book of varieties and schemes*, 2nd ed., Springer-Verlag, New York, 1999. MR **2001b:**14001

[O1] A. Ogg, *Hyperelliptic modular curves*, Bull. Soc. Math. France **102** (1974), 449–462. MR **51:**514

[O2] A. Ogg, *On the Weierstrass points of $X_0(N)$*, Illinois J. Math. **22** (1978), 31–35. MR **57:**3136

[R1] D. Rohrlich, *Some remarks on Weierstrass points*, Number Theory Related to Fermat's Last Theorem (ed. N. Koblitz), Birkhäuser, Prog. Math. **26** (1982), 71–78. MR **84d:**14008

[R2] D. Rohrlich, *Weierstrass points and modular forms*, Illinois J. Math. **29** (1985), 134–141. MR **86e:**11032

[Sc] B. Schoeneberg, *Elliptic modular functions*, Springer-Verlag, New York, Heidelberg, Berlin, 1974. MR **54:**236

[Se] J.-P. Serre, *Formes modulaires et fonctions zêta p-adiques*, Modular functions of one variable, III, Lecture Notes in Math., Vol. 350, Springer-Verlag, Berlin, 1973, pp. 191–268. MR **53:**7949b

[Sh] G. Shimura, *Introduction to the arithmetic theory of automorphic functions*, Princeton University Press, Princeton, NJ, 1994, reprint of the 1971 original. MR **95e:**11048; MR **47:**3318

[Si] J. H. Silverman, *Some arithmetic properties of Weierstrass points: hyperelliptic curves*, Bol. Soc. Brasil. Mat. (N.S.) **21** (1990), 11–50. MR **92k:**11066

[Sw] H. P. F. Swinnerton-Dyer, *On ℓ-adic representations and congruences for modular forms*, Modular functions of one variable, III, Lecture Notes in Math., Vol. 350, Springer-Verlag, Berlin, 1973, pp. 1–55. MR **53:**10717a

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

Department of Mathematics, Brown University, Providence, Rhode Island 02912
E-mail address: map@math.brown.edu