2017

Weierstrass Points on X 0+(p) and Supersingular J-invariants

Stephanie Treneer
Western Washington University, trenees@wwu.edu

Treneer *Res Math Sci(2017)4:25*
DOI 10.1186/s40687-017-0115-z

Research in the Mathematical Sciences

RESEARCH Open Access

Weierstrass points on $X_0^+(p)$ and supersingular j-invariants

Stephanie Treneer*

*Correspondence:
stephanie.treneer@wwu.edu
Department of Mathematics,
Western Washington University,
Bellingham, WA 98225, USA

Abstract

We study the arithmetic properties of Weierstrass points on the modular curves $X_0^+(p)$ for primes p. In particular, we obtain a relationship between the Weierstrass points on $X_0^+(p)$ and the j-invariants of supersingular elliptic curves in characteristic p.

Keywords: Weierstrass points, Modular curves, Supersingular elliptic curves, Modular forms

1 Introduction

A *Weierstrass point* on a compact Riemann surface M of genus g is a point $Q \in M$ at which some holomorphic differential ω vanishes to order at least g. Weierstrass points can be identified by observing their weight. Let $\mathcal{H}^1(M)$ be the g-dimensional $\mathbb{C}$-vector space of holomorphic differentials on M. If $\{\omega_1, \omega_2, \ldots, \omega_g\}$ forms a basis for $\mathcal{H}^1(M)$ adapted to $Q \in M$, so that

$$0 = \mathrm{ord}_Q(\omega_1) < \mathrm{ord}_Q(\omega_2) < \cdots < \mathrm{ord}_Q(\omega_g),$$

then we define the *Weierstrass weight* of Q to be

$$\mathrm{wt}(Q) := \sum_{j=1}^{g} (\mathrm{ord}_Q(\omega_j) - j + 1).$$

We see that $\mathrm{wt}(Q) > 0$ if and only if Q is a Weierstrass point of M. The Weierstrass weight is independent of the choice of basis, and it is known that

$$\sum_{Q \in M} \mathrm{wt}(Q) = g^3 - g.$$

Hence, each Riemann surface of genus $g \geq 2$ must have Weierstrass points. For these and other facts, see Section III.5 of [9].

We will consider Weierstrass points on modular curves, a class of Riemann surfaces which are of wide interest in number theory. Let $\mathbb{H}$ denote the complex upper half-plane. The modular group $\Gamma := \mathrm{SL}_2(\mathbb{Z})$ acts on $\mathbb{H}$ by linear fractional transformations $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) z = \frac{az+b}{cz+d}$. If $N \geq 1$ is an integer, then we define the congruence subgroup

$$\Gamma_0(N) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma : c \equiv 0 \pmod{N} \right\}.$$

The quotient of the action of $\Gamma_0(N)$ on $\mathbb{H}$ is the Riemann surface $Y_0(N) := \Gamma_0(N)\backslash\mathbb{H}$, and its compactification is $X_0(N)$. The modular curve $X_0(N)$ can be viewed as the moduli

Springer Open

space of elliptic curves equipped with a level N structure. Specifically, the points of $X_0(N)$ parameterize isomorphism classes of pairs (E, C) where E is an elliptic curve over $\mathbb{C}$ and C is a cyclic subgroup of E of order N.

Weierstrass points on $X_0(N)$ have been studied by a number of authors (see, for example, [3–6,12,13,15,17,20,22,23], and [10]). An interesting open question is to determine those N for which the cusp ∞ is a Weierstrass point. Lehner and Newman [15] and Atkin [5] showed that ∞ is a Weierstrass point for most non-squarefree N, while Atkin [6] proved that ∞ is not a Weierstrass point when N is prime.

Most central to the present paper is the connection between Weierstrass points and supersingular elliptic curves. Ogg [20] showed that for modular curves $X_0(pM)$ where p is a prime with $p \nmid M$ and with the genus of $X_0(M)$ equal to 0, the Weierstrass points of $X_0(pM)$ occur at points whose underlying elliptic curve is supersingular when reduced modulo p. So in particular, ∞ is not a Weierstrass point in these cases, extending [6]. This has recently been confirmed by Ahlgren, Masri and Rouse [2] using a non-geometric proof. Ahlgren and Ono [3] showed for the $M = 1$ case that in fact all supersingular elliptic curves modulo p correspond to Weierstrass points of $X_0(p)$, and they demonstrated a precise correspondence between the two sets. In order to state their result, we make the following definitions.

For p and M as above, let

$$F_{pM}(x) := \prod_{Q \in Y_0(pM)} (x - j(Q))^{\mathrm{wt}(Q)},$$

where $j(z) = q^{-1} + 744 + 196884q + \cdots$ is the usual elliptic modular function defined on Γ, and $j(Q) = j(\tau)$ for any $\tau \in \mathbb{H}$ with $Q = \Gamma_0(pM)\tau$. This is the divisor polynomial for the Weierstrass points of $Y_0(pM)$. Next, for a prime p we define

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

where the product is over all $\overline{\mathbb{F}}_p$-isomorphism classes of supersingular elliptic curves. It is well known that $S_p(x)$ has degree $g_p + 1$, where g_p is the genus of $X_0(p)$. Ahlgren and Ono [3] proved the following, when $M = 1$.

Theorem 1.1 *If p is prime, then $F_p(x)$ has p-integral rational coefficients and*

$$F_p(x) \equiv S_p(x)^{g_p(g_p-1)} \pmod{p}.$$

El-Guindy [8] generalized Theorem 1.1 by considering F_{pM} where M is squarefree, showing that $F_{pM}(x)$ has p-integral rational coefficients and is divisible by $\widetilde{S}_p(x)^{\mu(M)g_{pM}(g_{pM}-1)}$, where $\mu(M) := [\Gamma : \Gamma_0(M)]$ and g_{pM} is the genus of $X_0(pM)$, and where

$$\widetilde{S}_p(x) := \prod_{\substack{E/\overline{\mathbb{F}}_p \text{ supersingular} \\ j(E) \neq 0,1728}} (x - j(E)). \tag{1.1}$$

He also gave an explicit factorization of $F_{pM}(x)$ in most cases where M is prime. Generalizing Theorem 1.1 in a different direction, Ahlgren and Papanikolas [4] gave a similar result for higher-order Weierstrass points on $X_0(p)$, which are defined in relation to higher-order differentials.

In this paper we consider the modular curve $X_0^+(p)$, the quotient space of $X_0(p)$ under the action of the Atkin–Lehner involution w_p, which maps $\tau \mapsto -1/p\tau$ for $\tau \in \mathbb{H}$. There is a natural projection map $\pi : X_0(p) \to X_0^+(p)$ which sends a point $Q \in X_0(p)$ to its equivalence class $\pi(Q) = \overline{Q}$ in $X_0^+(p)$. This is a 2-to-1 mapping, ramified at those points $Q \in X_0(p)$ that remain fixed by w_p. Therefore, we set

$$\nu(Q) := \begin{cases} 2 & \text{if } w_p(Q) = Q, \\ 1 & \text{otherwise}, \end{cases} \tag{1.2}$$

so that $\nu(Q)$ is equal to the multiplicity of the map π at Q. We now define a divisor polynomial for the Weierstrass points of $X_0^+(p)$. We will set our product to be over $Y_0(p)$ to preserve the desired p-integrality of the coefficients. Let

$$\mathcal{F}_p(x) := \prod_{Q \in Y_0(p)} (x - j(Q))^{\nu(Q)\mathrm{wt}(\overline{Q})},$$

where $\mathrm{wt}(\overline{Q})$ is the Weierstrass weight of the image $\overline{Q}$ of Q in $X_0^+(p)$. The zeros of this polynomial capture those non-cuspidal points of $X_0(p)$ which map to Weierstrass points in $X_0^+(p)$. The two cusps of $X_0(p)$ at 0 and ∞ are interchanged by w_p, so that $X_0^+(p)$ has a single cusp at ∞, which may or may not be a Weierstrass point. Atkin checked all primes $p \leq 883$ and conjectured that ∞ is a Weierstrass point for all $p > 389$. Stein has confirmed this for all $p < 3000$, and his table of results can be found in [26]. Therefore, $\mathcal{F}_p(x)$ is a polynomial of degree $2((g_p^+)^3 - g_p^+ - \mathrm{wt}(\infty))$, where g_p^+ is the genus of $X_0^+(p)$.

We recall that a supersingular elliptic curve $E/\overline{\mathbb{F}}_p$ must have $j(E) \in \mathbb{F}_{p^2}$. Since those $j(E) \in \mathbb{F}_{p^2} \backslash \mathbb{F}_p$ occur in conjugate pairs, we define

$$S_p^{(l)}(x) := \prod_{\substack{E/\overline{\mathbb{F}}_p \text{ supersingular} \\ j(E) \in \mathbb{F}_p}} (x - j(E)) \quad \text{and} \quad S_p^{(q)}(x) := \prod_{\substack{E/\overline{\mathbb{F}}_p \text{ supersingular} \\ j(E) \in \mathbb{F}_{p^2} \backslash \mathbb{F}_p}} (x - j(E)),$$

so that $S_p(x) = S_p^{(l)}(x) \cdot S_p^{(q)}(x)$ and both factors lie in $\mathbb{F}_p[x]$. Our main theorem gives an analogue of Theorem 1.1 for $\mathcal{F}_p(x)$. We require an assumption that $\mathcal{H}^1(X_0^+(p))$ has a *good basis*, a condition about p-integrality which we define later in Sect. 4. Computations suggest that most, if not all, such spaces satisfy this condition. Indeed, each $\mathcal{H}^1(X_0^+(p))$ with $p < 3200$ has a good basis.

Theorem 1.2 *Let p be prime and suppose that $\mathcal{H}(X_0^+(p))$ has a good basis. Then $\mathcal{F}_p(x)$ has p-integral rational coefficients, and there exists a polynomial $H(x) \in \mathbb{F}_p[x]$ such that*

$$\mathcal{F}_p(x) \equiv S_p^{(q)}(x)^{g_p^+(g_p^+-1)} \cdot H(x)^2 \pmod{p}.$$

Note From computational evidence, it appears that $H(x)$ is always coprime to $S_p(x)$, so that contrary to the situation on $X_0(p)$, only those supersingular points with quadratic irrational j-invariants correspond to Weierstrass points of $X_0^+(p)$. We give a heuristic argument for this phenomenon in Sect. 3.

In Sect. 2 we start by reviewing some preliminary facts about divisors of polynomials of modular forms. We then consider the reduction of $X_0(p)$ modulo p in Sect. 3 in order to obtain a key result about the w_p-fixed points of $X_0(p)$. In Sect. 4 we describe our good basis condition for $\mathcal{H}^1(X_0^+(p))$. Next, in Sect. 5 we derive a special cusp form on $\Gamma_0(p)$ which encodes the Weierstrass weights of points on $X_0^+(p)$. In Sect. 6, we prove Theorem 1.2, and in Sect. 7, we demonstrate Theorem 1.2 for the curve $X_0^+(67)$.

2 Divisor polynomials of modular forms

Let M_k (resp. $M_k(p)$) denote the space of modular forms of weight k on Γ (resp. $\Gamma_0(p)$), and let S_k (resp. $S_k(p)$) be the subspace of cusp forms. For even $k \geq 4$, the Eisenstein series $E_k \in M_k$ is defined as

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

where B_k is the kth Bernoulli number, and $\sigma_{k-1}(n) = \sum_{d|n} d^{k-1}$. Then the function

$$\Delta(z) := \frac{E_4(z)^3 - E_6(z)^2}{1728} = q - 24q^2 + 252q^3 - 1472q^4 + \cdots$$

is the unique normalized cusp form in S_{12}.

We briefly recall how to build a divisor polynomial whose zeros are exactly the j-values at which a given modular form $f \in M_k$ vanishes, excluding those trivial zeros that are forced to occur at the elliptic points i and $\rho := e^{2\pi i/3}$ by the valence formula (for details, see [3] or Section 2.6 of [21]). We define

$$\widetilde{E}_k(z) := \begin{cases} 1 & \text{if } k \equiv 0 \pmod{12}, \\ E_4(z)^2E_6(z) & \text{if } k \equiv 2 \pmod{12}, \\ E_4(z) & \text{if } k \equiv 4 \pmod{12}, \\ E_6(z) & \text{if } k \equiv 6 \pmod{12}, \\ E_4(z)^2 & \text{if } k \equiv 8 \pmod{12}, \\ E_4(z)E_6(z) & \text{if } k \equiv 10 \pmod{12}, \end{cases} \tag{2.1}$$

and

$$m(k) := \begin{cases} \lfloor k/12 \rfloor & \text{if } k \not\equiv 2 \pmod{12}, \\ \lfloor k/12 \rfloor - 1 & \text{if } k \equiv 2 \pmod{12}. \end{cases} \tag{2.2}$$

Now let $f \in M_k$ have leading coefficient 1. We note that (2.1) and (2.2) are defined such that the quotient

$$\widetilde{F}(f, j(z)) := \frac{f(z)}{\Delta(z)^{m(k)}\widetilde{E}_k(z)} \tag{2.3}$$

has weight zero. Then the order of f at the elliptic points, together with the non-vanishing of $\Delta(z)$ on $\mathbb{H}$, guarantees that $\widetilde{F}(f, j(z))$ is a polynomial in $j(z)$. Therefore, we define $\widetilde{F}(f, x)$ to be the unique polynomial in x satisfying (2.3). Furthermore, if f has p-integral rational coefficients, then so does $\widetilde{F}(f, x)$.

Finally, we record a result about the divisor polynomial of the square of a modular form.

Lemma 2.1 *Let $f \in M_k$. Then*

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

Proof Using (2.3) for both f and f^2 yields

$$f(z)^2 = \Delta(z)^{2m(k)}\widetilde{E}_k(z)^2\widetilde{F}(f, j(z))^2,$$

and

$$f(z)^2 = \Delta(z)^{m(2k)}\widetilde{E}_{2k}(z)\widetilde{F}(f^2, j(z)).$$

Thus

$$\widetilde{F}(f^2, j(z)) = \Delta(z)^{2m(k)-m(2k)} \cdot \frac{\widetilde{E}_k(z)^2}{\widetilde{E}_{2k}(z)} \cdot \widetilde{F}(f, j(z))^2.$$

Then by (2.1) and (2.2) we have

$$\widetilde{F}(f^2, j(z)) = \begin{cases} \widetilde{F}(f, j(z))^2 & \text{if } k \equiv 0 \pmod{12}, \\ \Delta(z)^{-2}E_4(z)^3E_6(z)^2\widetilde{F}(f, j(z))^2 & \text{if } k \equiv 2 \pmod{12}, \\ \widetilde{F}(f, j(z))^2 & \text{if } k \equiv 4 \pmod{12}, \\ \Delta(z)^{-1}E_6(z)^2\widetilde{F}(f, j(z))^2 & \text{if } k \equiv 6 \pmod{12}, \\ \Delta(z)^{-1}E_4(z)^3\widetilde{F}(f, j(z))^2 & \text{if } k \equiv 8 \pmod{12}, \\ \Delta(z)^{-1}E_6(z)^2\widetilde{F}(f, j(z))^2 & \text{if } k \equiv 10 \pmod{12}, \end{cases}$$

Since $j(z) = \frac{E_4(z)^3}{\Delta(z)}$ and $j(z) - 1728 = \frac{E_6(z)^2}{\Delta(z)}$, the result follows. □

3 Modular curves modulo *p*

Here we recall the undesingularized reduction of $X_0(p)$ modulo p, due to Deligne and Rapoport [7]. The description below closely follows one given by Ogg [19]. The model of $X_0(p)$ modulo p consists of two copies of $X_0(1)$ which meet transversally in the supersingular points (Fig. 1). (Here we call a point supersingular if its underlying elliptic curve is supersingular.)

The Atkin–Lehner operator w_p is compatible with this reduction. It gives an isomorphism between the two copies of $X_0(1)$ which preserves the supersingular locus, by fixing those points with j-invariant in $\mathbb{F}_p$, and interchanging the pairs of points whose j-invariants in $\mathbb{F}_{p^2}\backslash\mathbb{F}_p$ are conjugate. Therefore, dividing out by the action of w_p glues together the two copies of $X_0(1)$. The singularities at the linear supersingular points are thus resolved, while the conjugate pairs of quadratic supersingular points are glued together. This results in a model for the reduction modulo p of $X_0^+(p)$ consisting of one copy of $X_0(1)$ which self-intersects at each point representing a pair of conjugate quadratic supersingular points (Fig. 2). This resolution at the linear supersingular points may explain their absence among the Weierstrass points of $X_0^+(p)$.

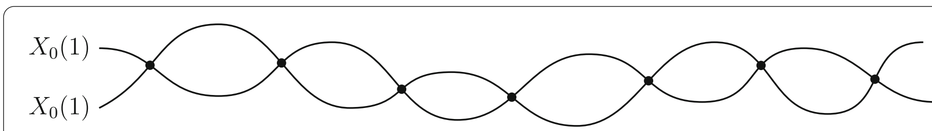

Fig. 1 Reduction of $X_0(p)$

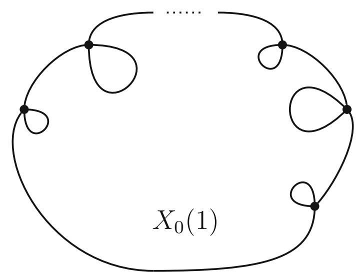

Fig. 2 Reduction of $X_0^+(p)$

To make the correspondence between fixed points and linear supersingular j-invariants more precise, for $D \equiv 0, 3 \pmod 4$, let $\mathcal{O}_D = \mathbb{Z}[\frac{1}{2}(D + \sqrt{-D})]$ be the order of the imaginary quadratic field $\mathbb{Q}[\sqrt{-D}]$ with discriminant $-D < 0$. The Hilbert class polynomial $\mathcal{H}_D(x) \in \mathbb{Z}[x]$ is the monic polynomial whose zeros are exactly the j-invariants of the distinct isomorphism classes of elliptic curves with complex multiplication by $\mathcal{O}_D$, and its degree is $h(-D)$, the class number of $\mathcal{O}_D$.

The points $Q \in Y_0(p)$ that are fixed by w_p correspond to pairs (E, C) such that E admits complex multiplication by $\sqrt{-p}$, or in other words, $\mathbb{Z}[\sqrt{-p}]$ embeds in End(E), the endomorphism ring of E over the complex numbers (see, e.g., [17]). Since End(E) must be an order in an imaginary quadratic field, we have

$$\mathrm{End}(E) \cong \begin{cases} \mathcal{O}_{4p} & \text{if } p \equiv 1 \pmod 4, \\ \mathcal{O}_p \text{ or } \mathcal{O}_{4p} & \text{if } p \equiv 3 \pmod 4. \end{cases}$$

Now define

$$H_p(x) := \prod_{\substack{\tau \in \Gamma_0(p)\backslash\mathbb{H} \\ \nu(Q_\tau)=2}} (x - j(\tau)), \tag{3.1}$$

the monic polynomial whose zeros are precisely the j-invariants of the w_p-fixed points of $Y_0(p)$. Then we have

$$\mathbb{H}_p(x) = \begin{cases} \mathcal{H}_{4p}(x) & \text{if } p \equiv 1 \pmod 4, \\ \mathcal{H}_p(x) \cdot \mathcal{H}_{4p}(x) & \text{if } p \equiv 3 \pmod 4. \end{cases} \tag{3.2}$$

The following result is due independently to Kaneko and Zagier.

Proposition 3.1 *For p prime, there exists a monic polynomial $T(x) \in \mathbb{Z}_p[x]$ with distinct roots such that $H_p(x) \equiv T(x)^2 \pmod p$.*

Proof The result follows from Kronecker's relations on the modular equation $\Phi_p(X, Y)$ and may be found in appendix of [11]. □

We can now prove the following.

Theorem 3.2 *Let p be prime. Then we have*

$$H_p(x) \equiv S_p^{(l)}(x)^2 \pmod p.$$

Proof The prime p is ramified in both $\mathbb{Q}(\sqrt{-p})$ and $\mathbb{Q}(\sqrt{-4p})$, so a result of Deuring (see, e.g., Theorem 12 in §13.4 of [14]) together with (3.2) implies that the reduction modulo p of each root of $H_p(x)$ must be a supersingular j-invariant. Since the roots of $H_p(x)$ also correspond to fixed points of w_p, these supersingular j-invariants must lie in $\mathbb{F}_p$, so by Proposition 3.1, we have $T(x) \mid S_p^{(l)}(x)$. We will show that $T(x)$ and $S_p^{(l)}(x)$ have the same degree, proving that $T(x) = S_p^{(l)}(x)$. The result then follows again by Proposition 3.1.

By the Riemann–Hurwitz formula (see, for example, Section I.2 of [9]), we have

$$2g_p^+ = g_p + 1 - \frac{\sigma}{2}, \tag{3.3}$$

where σ is the number of points of $X_0(p)$ at which the projection $\pi : X_0(p) \to X_0^+(p)$ is ramified, or in other words, the number of w_p-fixed points of $X_0(p)$. We note that the cusps are not ramified since w_p exchanges 0 and ∞, so $\sigma = \deg(H_p(x))$. On the other hand, Ogg explains in [18] that g_p^+ is equal to the number of conjugate pairs of supersingular j-invariants in $\mathbb{F}_{p^2} \backslash \mathbb{F}_p$. Since there are $g_p + 1$ total supersingular j-invariants, we have

$$2g_p^+ = g_p + 1 - \deg(S_p^{(l)}(x)). \tag{3.4}$$

Then Proposition 3.1, (3.3), and (3.4) imply that

$$\deg(T(x)) = \frac{\deg(H_p(x))}{2} = \deg(S_p^{(l)}(x)).$$

□

4 A good basis for $\mathcal{H}^1(X_0^+(p))$

For ease of notation, we will let $g := g_p^+$ for the rest of the paper, and assume that $g \geq 2$. Recall that g is the dimension of $\mathcal{H}^1(X_0^+(p))$, the space of holomorphic 1-forms on $X_0^+(p)$. Let $\{\omega_1, \omega_2, \ldots, \omega_g\}$ be a basis of $\mathcal{H}^1(X_0^+(p))$, where $\omega_i = h_i(u)du$ for some local variable u. In order to take advantage of the correspondence that exists between holomorphic 1-forms on $X_0(p)$ and weight 2 cusp forms of level p, we pull back each ω_i to a holomorphic 1-form $\pi^*\omega_i$ on $X_0(p)$ via the projection map $\pi : X_0(p) \to X_0^+(p)$ (see, for example, Chapter 2 of [16]). We can choose a local coordinate z at $Q \in X_0(p)$ so that near Q, $u = z^n$, where n is the multiplicity of π at Q, hence $n = \nu(Q)$ (1.2). Then we have $\pi^*\omega_i = H_i(z)dz$ with $H_i(z) = h_i(z^n)nz^{n-1} \in S_2(p)$. Since each $H_i(z)$ has been pulled back from $X_0^+(p)$, it must be invariant under w_p, so it is a member of $S_2^+(p)$, the subspace of w_p-invariant cusp forms of weight 2. In fact, it is straightforward to show that $\{H_1(z), H_2(z), \ldots, H_g(z)\}$ forms a basis for $S_2^+(p)$.

It will be helpful later on to specify a basis for $S_2^+(p)$ of a particularly nice form. First, we can guarantee a basis with rational Fourier coefficients by the following argument. The space $S_2(p)$ has a basis consisting of newforms. Let $f(z) = \sum_n a(n)q^n$ be a newform for $S_2(p)$, and let $\sigma \in \mathrm{Gal}(\mathbb{C}/\mathbb{Q})$. Then $f^\sigma(z) = \sum_n \sigma(a(n))q^n$ is also a newform for $S_2(p)$, so the action of $\mathrm{Gal}(\mathbb{C}/\mathbb{Q})$ partitions the newforms into Galois conjugacy classes. If two newforms are Galois conjugates, then they share the same eigenvalue for w_p. Let V_f be the $\mathbb{C}$-vector space spanned by the Galois conjugates of f. Standard Galois-theoretic arguments show that V_f has a basis consisting of cusp forms with rational coefficients. These are no longer newforms, but as they are linear combinations of the Galois conjugates of f, they are still eigenforms for w_p. Therefore, collecting such a basis for each Galois conjugacy class with eigenvalue 1 for w_p yields a basis for $S_2^+(p)$ with rational Fourier coefficients.

We can determine such a basis $\{f_1, f_2, \ldots, f_g\}$ uniquely by requiring that

$$\begin{aligned} f_1(z) &= q^{c_1} + O(q^{c_g+1}) \\ f_2(z) &= q^{c_2} + O(q^{c_g+1}) \\ &\vdots \\ f_g(z) &= q^{c_g} + O(q^{c_g+1}) \end{aligned} \tag{4.1}$$

where

$$c_1 < c_2 < \cdots < c_g. \tag{4.2}$$

Definition We say that $\mathcal{H}^1(X_0^+(p))$ has a *good basis* if the cusp forms $f_1, f_2, \ldots, f_g$ satisfying (4.1) and (4.2) have p-integral Fourier coefficients.

5 Wronskians and p-integrality

Given any basis $\{\omega_1, \omega_2, \ldots, \omega_g\}$ for $\mathcal{H}^1(X_0^+(p))$ with $\omega_i = h_i(u)du$, we define the Wronskian

$$W(h_1, h_2, \ldots, h_g)(u) := \begin{vmatrix} h_1 & h_2 & \cdots & h_g \\ h_1' & h_2' & \cdots & h_g' \\ \vdots & \vdots & \vdots & \vdots \\ h_1^{(g-1)} & h_2^{(g-1)} & \cdots & h_g^{(g-1)} \end{vmatrix}. \tag{5.1}$$

Let $\mathcal{W}^+(u)$ be the scalar multiple of $W(h_1, h_2, \ldots, h_g)(u)$ with leading coefficient 1, so that $\mathcal{W}^+(u)$ is independent of the choice of basis. It is well known that the Wronskian encodes the Weierstrass weights of points in $X_0^+(p)$ (see [9], page 82). Specifically,

$$\mathrm{wt}(\overline{Q}) = \mathrm{ord}_{\overline{Q}}(\mathcal{W}^+(u)(du)^{g(g+1)/2}).$$

Since it is advantageous to work on $X_0(p)$ instead of $X_0^+(p)$, we consider the pullback of $W^+ := \mathcal{W}^+(u)(du)^{g(g+1)/2}$ to $X_0(p)$ via π, which is $\pi^* W^+ = \mathcal{W}^+(z^n)(nz^{n-1}dz)^{g(g+1)/2}$. Recalling that $n = \nu(Q)$ when z is near Q, we have

$$\mathrm{ord}_Q(\pi^* W^+) = \nu(Q)\mathrm{wt}(\overline{Q}) + \frac{g(g+1)}{2}(\nu(Q) - 1). \tag{5.2}$$

Alternatively, we could pull back each ω_i individually to $\pi^*\omega_i = H_i(z)dz$ as in Sect. 4. Then we can form the Wronskian $W(H_1, H_2, \ldots, H_g)(z)$ (defined analogously to (5.1)). Since the H_i are cusp forms of weight 2 for $\Gamma_0(p)$, then $W(H_1, H_2, \ldots, H_g)(z)$ is a cusp form of weight $g(g+1)$ for $\Gamma_0(p)$. It can be shown using basic facts about determinants that

$$W(H_1, H_2, \ldots, H_g)(z)(dz)^{g(g+1)/2} = W(h_1, h_2, \ldots, h_g)(z^n)(nz^{n-1}dz)^{g(g+1)/2}.$$

Now let $\mathcal{W}_p(z)$ be the multiple of $W(H_1, H_2, \ldots, H_g)(z)$ with leading coefficient 1. Then $\mathcal{W}_p(z)$ is independent of the choice of basis for $S_2^+(p)$, and we have $\mathcal{W}_p(z)(dz)^{g(g+1)/2} = \pi^* W^+$, hence by (5.2),

$$\mathrm{ord}_Q(\mathcal{W}_p(z)(dz)^{g(g+1)/2}) = \nu(Q)\mathrm{wt}(\overline{Q}) + \frac{g(g+1)}{2}(\nu(Q) - 1). \tag{5.3}$$

We next see the advantage of having a good basis for $\mathcal{H}^1(X_0^+(p))$.

Theorem 5.1 *Let p be a prime such that $\mathcal{H}^1(X_0^+(p))$ has a good basis. Then $\mathcal{W}_p(z) \in S_{g(g+1)}(p)$ has p-integral rational coefficients.*

Proof Here we closely follow the proof of Lemma 3.1 in [4]. Let $\{f_1, f_2, \ldots, f_g\}$ be a basis for $S_2^+(p)$ satisfying (4.1) and (4.2). Let $\theta := q\frac{d}{dq}$ be the usual differential operator for modular forms, so that $\frac{d}{dz} = 2\pi i\theta$. Then by properties of determinants, we have

$$W(f_1, f_2, \ldots, f_g) = (2\pi i)^{g(g-1)/2} \begin{vmatrix} f_1 & f_2 & \cdots & f_g \\ \theta f_1 & \theta f_2 & \cdots & \theta f_g \\ \vdots & \vdots & \vdots & \vdots \\ \theta f_1^{(g-1)} & \theta f_2^{(g-1)} & \cdots & \theta f_g^{(g-1)} \end{vmatrix}.$$

We see that the Fourier expansion of $\left(\frac{1}{2\pi i}\right)^{g(g-1)/2} W(f_1, f_2, \ldots, f_g)$ has rational p-integral coefficients, with leading coefficient given by the Vandermonde determinant

$$V := \begin{vmatrix} 1 & 1 & \cdots & 1 \\ c_1 & c_2 & \cdots & c_g \\ \vdots & \vdots & \vdots & \vdots \\ c_1^{(g-1)} & c_2^{(g-1)} & \cdots & c_g^{(g-1)} \end{vmatrix} = \prod_{1 \le j < k \le g} (c_k - c_j). \tag{5.4}$$

It now suffices to show that p does not divide the leading coefficient. By Sturm's bound [27] for the order of vanishing modulo p for modular forms of weight 2 on $\Gamma_0(p)$, we have $1 \le c_i \le \frac{p+1}{6} < p$ for each $1 \le i \le g$, so $1 \le c_k - c_j \le p - 1$ for all $j < k$. Therefore, the lemma is proved. □

6 Proof of the main theorem

Let p be a prime for which $\mathcal{H}^1(X_0^+(p))$ has a good basis. We note that when $g < 2$, there are no Weierstrass points on $X_0^+(p)$. Then $\mathcal{F}_p(x) = 1$ and $g^2 - g = 0$, so the theorem holds trivially by taking $H(x) = 1$. Thus from here on, we will assume that $g \ge 2$, in which case we have $p \ge 67$.

We first adapt two lemmas from [3]. For any meromorphic function $f(z)$ defined on $\mathbb{H}$ and any integer k, we define the *slash* operator $|_k$ by

$$f(z)|_k\gamma := (\det\gamma)^{k/2}(cz+d)^{-k} f(\gamma z),$$

where $\gamma := \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ is a real matrix with positive determinant, and $\gamma z := \frac{az+b}{cz+d}$. In particular, the Atkin–Lehner involution w_p is given by $f \mapsto f|_k \begin{pmatrix} 0 & -1 \\ p & 0 \end{pmatrix}$ when f is a modular form of weight k.

Lemma 6.1 *We have*

$$\mathcal{W}_p(z)|_{g(g+1)} \begin{pmatrix} 0 & -1 \\ p & 0 \end{pmatrix} = \mathcal{W}_p(z).$$

Proof The proof is identical to Lemma 3.2 of [3] except that $f|_2 \begin{pmatrix} 0 & -1 \\ p & 0 \end{pmatrix} = f$ for every newform f in $S_2^+(p)$. □

Lemma 6.2 *If p is a prime such that $X_0^+(p)$ has genus at least 2, define*

$$\widetilde{\mathcal{W}}_p(z) := \prod_{A \in \Gamma_0(p)\backslash\Gamma} \mathcal{W}_p(z)|_{g(g+1)} A,$$

normalized to have leading coefficient 1. Then $\widetilde{\mathcal{W}}_p(z)$ is a cusp form of weight $g(g+1)(p+1)$ on Γ with p-integral rational coefficients, and

$$\widetilde{\mathcal{W}}_p(z) \equiv \mathcal{W}_p(z)^2 \pmod{p}.$$

Proof This follows from our Lemma 6.1 exactly as Lemma 3.3 follows from Lemma 3.2 in [3]. □

We again consider a basis $\{f_1, f_2, \ldots, f_g\}$ for $S_2^+(p)$ satisfying (4.1) and (4.2). For each f_i, there is a cusp form $b_i \in S_{p+1}$ with p-integral rational coefficients for which $f_i \equiv b_i \pmod{p}$ ([4], Theorem 4.1(c)). Define $W(z)$ to be the multiple of $W(b_1, b_2, \ldots, b_g)$ with leading coefficient 1. By the same reasoning as in Theorem 5.1, $\left(\frac{1}{2\pi i}\right)^{g(g-1)/2} W(b_1, b_2, \ldots, b_g)$ has p-integral rational coefficients and leading coefficient V (5.4). Since the differential operator θ preserves congruences, we have

$$\left(\frac{1}{2\pi i}\right)^{g(g-1)/2} W(f_1, f_2, \ldots, f_g) \equiv \left(\frac{1}{2\pi i}\right)^{g(g-1)/2} W(b_1, b_2, \ldots, b_g) \pmod{p},$$

and hence

$$V \cdot \mathcal{W}_p(z) \equiv V \cdot W(z) \pmod{p}.$$

Since V is coprime to p, then by Lemma 6.2 we have

$$\widetilde{\mathcal{W}}_p(z) \equiv \mathcal{W}_p(z)^2 \equiv W(z)^2 \pmod{p}.$$

We now have two cusp forms $\widetilde{\mathcal{W}}_p(z)$ and $W(z)^2$ on the full modular group, but $\widetilde{\mathcal{W}}_p(z)$ has weight $\tilde{k}(p) := g(g+1)(p+1)$ while $W(z)^2$ has weight $2g(g+p)$. Using the fact that the Eisenstein series $E_{p-1}(z) \equiv 1 \pmod{p}$, we have

$$\widetilde{\mathcal{W}}_p(z) \equiv W(z)^2 \cdot E_{p-1}(z)^{g^2-g} \pmod{p}, \tag{6.1}$$

where the cusp forms on each side of the congruence in (6.1) have the same weight $\tilde{k}(p)$. By (2.3) there exist polynomials $\widetilde{F}(\widetilde{\mathcal{W}}_p(x), x)$ and $\widetilde{F}(W^2 E_{p-1}^{g^2-g}, x)$ with p-integral rational coefficients such that

$$\widetilde{\mathcal{W}}_p(z) = \Delta(z)^{m(\tilde{k}(p))} \widetilde{E}_{\tilde{k}(p)}(z) \widetilde{F}(\widetilde{\mathcal{W}}_p, j(z)),$$

and

$$W(z)^2 E_{p-1}(z)^{g^2-g} = \Delta(z)^{m(\tilde{k}(p))} \widetilde{E}_{\tilde{k}(p)}(z) \widetilde{F}(W^2 E_{p-1}^{g^2-g}, j(z)).$$

Then by (6.1), we conclude that

$$\widetilde{F}(\widetilde{\mathcal{W}}_p, x) \equiv \widetilde{F}(W^2 E_{p-1}^{g^2-g}, x) \pmod{p}. \tag{6.2}$$

We next compute each side of (6.2). To compute the right-hand side, we begin with the following.

Lemma 6.3 (Theorem 2.3 in [3]) *For a prime $p \geq 5$ and $f \in M_k$ with p-integral coefficients, we have*

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

where

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

Then using Lemma 6.3 inductively, we have

$$\widetilde{F}(W^2 \cdot E_{p-1}^{g^2-g}, x) \equiv \widetilde{F}(E_{p-1}, x)^{g^2-g} \cdot \widetilde{F}(W^2, x) \cdot \mathcal{G}_p(x) \pmod{p},$$

where

$$\mathcal{G}_p(x) := \prod_{s=1}^{g^2-g} C_p(2g(g+p) + (g^2-g-s)(p-1); x).$$

A case-by-case computation reveals that

$$\mathcal{G}_p(x) = \begin{cases} 1 & \text{if } p \equiv 1 \pmod{12}, \\ x^{\lceil \frac{g^2-g}{3} \rceil} & \text{if } p \equiv 5 \pmod{12}, \\ (x-1728)^{(g^2-g)/2} & \text{if } p \equiv 7 \pmod{12}, \\ x^{\lceil \frac{g^2-g}{3} \rceil}(x-1728)^{(g^2-g)/2} & \text{if } p \equiv 11 \pmod{12}. \end{cases}$$

By a result of Deligne (see [24]), and recalling (1.1), we have

$$\widetilde{F}(E_{p-1}, x) \equiv \widetilde{S}_p(x) \pmod{p},$$

and therefore

$$\widetilde{F}(W^2 E_{p-1}^{g^2-g}, x) \equiv \widetilde{S}_p(x)^{g^2-g} \cdot \widetilde{F}(W^2, x) \cdot \mathcal{G}_p(x) \pmod{p}. \tag{6.3}$$

Next, in the following theorem, we evaluate the left-hand side of (6.2). We recall here the definitions

$$\mathcal{F}_p(x) := \prod_{Q \in Y_0(p)} (x - j(Q))^{\nu(Q)\mathrm{wt}(\overline{Q})},$$

and

$$H_p(x) := \prod_{\substack{\tau \in \Gamma_0(p) \backslash \mathbb{H} \\ \nu(Q_\tau)=2}} (x - j(\tau)).$$

Theorem 6.4 *Let p be a prime such that the genus of $X_0^+(p)$ is at least 2. Define $\epsilon_p(i)$ and $\epsilon_p(\rho)$ by*

$$\epsilon_p(i) = \frac{(g^2+g)\left(1 + \left(\frac{-1}{p}\right)\right)}{4},$$

and

$$\epsilon_p(\rho) = \frac{(g^2+g)\left(1 + \left(\frac{-3}{p}\right)\right) - k^*}{3},$$

where $k^* \in \{0,1,2\}$ with $k^* \equiv \tilde{k}(p) \pmod{3}$. Then we have

$$\widetilde{F}(\widetilde{\mathcal{W}}_p, x) = x^{\epsilon_p(\rho)}(x-1728)^{\epsilon_p(i)} \mathcal{F}_p(x) H_p(x)^{g(g+1)/2}.$$

Proof If $\tau_0 \in \mathbb{H}$ and $A \in \Gamma$, then

$$\mathrm{ord}_{\tau_0}(\mathcal{W}_p(z) \mid_{g(g+1)} A) = \mathrm{ord}_{A(\tau_0)}(\mathcal{W}_p(z)),$$

so that

$$\mathrm{ord}_{\tau_0}(\widetilde{\mathcal{W}}_p(z)) = \sum_{A \in \Gamma_0(p)\backslash\Gamma} \mathrm{ord}_{A(\tau_0)}(\mathcal{W}_p(z)). \tag{6.4}$$

Now recall by (5.3) that for $Q \in Y_0(p)$, we have

$$\mathrm{ord}_Q(\mathcal{W}_p(z)(dz)^{g(g+1)/2}) = \nu(Q)\mathrm{wt}(\overline{Q}) + \frac{g(g+1)}{2}(\nu(Q)-1).$$

Let $\ell_\tau \in \{1,2,3\}$ be the order of the isotropy subgroup of τ in $\Gamma_0(p)/\{\pm I\}$, where τ is an elliptic fixed point if and only if $\ell(\tau) \neq 1$. If $Q_\tau \in Y_0(p)$ is associated with $\tau \in \mathbb{H}$ in the usual way, then we have

$$\begin{aligned}\mathrm{ord}_\tau(\mathcal{W}_p(z)) &= \ell_\tau \mathrm{ord}_{Q_\tau}(\mathcal{W}_p(z)(dz)^{g(g+1)/2}) + \frac{g(g+1)}{2}(\ell_\tau - 1)\\ &= \ell_\tau \nu(Q_\tau)\mathrm{wt}(\overline{Q_\tau}) + \frac{g(g+1)}{2}(\ell_\tau\nu(Q_\tau)-1). \end{aligned} \tag{6.5}$$

If τ_0 is not equivalent to i or ρ under Γ, then $\{A(\tau_0)\}_{A\in\Gamma_0(p)\backslash\Gamma}$ consists of $p+1$ points which are $\Gamma_0(p)$-inequivalent, so by (6.4) and (6.5),

$$\begin{aligned}\mathrm{ord}_{\tau_0}(\widetilde{\mathcal{W}}_p(z)) &= \sum_{\substack{\tau\in\Gamma_0(p)\backslash\mathbb{H}\\ \tau \overset{\Gamma}{\sim} \tau_0}} \mathrm{ord}_\tau(\mathcal{W}_p(z))\\ &= \sum_{\substack{\tau\in\Gamma_0(p)\backslash\mathbb{H}\\ \tau \overset{\Gamma}{\sim} \tau_0}} \left(\nu(Q_\tau)\mathrm{wt}(\overline{Q_\tau}) + \frac{g(g+1)}{2}(\nu(Q_\tau)-1)\right).\end{aligned}$$

When $\tau_0 \overset{\Gamma}{\sim} \rho$, then $\mathrm{ord}_{\tau_0}(\widetilde{\mathcal{W}}_p(z)) = \mathrm{ord}_\rho(\widetilde{\mathcal{W}}_p(z))$, and $\{A(\rho)\}_{A\in\Gamma_0(p)\backslash\Gamma}$ contains $1+(\frac{-3}{p})$ elliptic fixed points of order 3 which are $\Gamma_0(p)$-inequivalent, and $p-(\frac{-3}{p})$ additional points which are partitioned into $\Gamma_0(p)$-orbits of size 3. Then by (6.5) we have

$$\begin{aligned}\mathrm{ord}_\rho(\widetilde{\mathcal{W}}_p(z)) &= 3\sum_{\substack{\tau\in\Gamma_0(p)\backslash\mathbb{H}\\ \tau \overset{\Gamma}{\sim} \rho,\ \ell(\tau)=1}} \mathrm{ord}_\tau(\mathcal{W}_p(z)) + \sum_{\substack{\tau\in\Gamma_0(p)\backslash\mathbb{H}\\ \tau \overset{\Gamma}{\sim} \rho,\ \ell(\tau)=3}} \mathrm{ord}_\tau(\mathcal{W}_p(z))\\ &= 3\sum_{\substack{\tau\in\Gamma_0(p)\backslash\mathbb{H}\\ \tau \overset{\Gamma}{\sim} \rho,\ \ell(\tau)=1}} \left(\nu(Q_\tau)\mathrm{wt}(\overline{Q_\tau}) + \frac{g(g+1)}{2}(\nu(Q_\tau)-1)\right)\\ &\quad + \sum_{\substack{\tau\in\Gamma_0(p)\backslash\mathbb{H}\\ \tau \overset{\Gamma}{\sim} \rho,\ \ell(\tau)=3}} \left(3\nu(Q_\tau)\mathrm{wt}(\overline{Q_\tau}) + \frac{g(g+1)}{2}(3\nu(Q_\tau)-1)\right)\\ &= 3\left(\sum_{\substack{\tau\in\Gamma_0(p)\backslash\mathbb{H}\\ \tau \overset{\Gamma}{\sim} \rho}} \nu(Q_\tau)\mathrm{wt}(\overline{Q_\tau}) + \frac{g(g+1)}{2}(\nu(Q_\tau)-1)\right)\\ &\quad + (g^2+g)\left(1+\left(\frac{-3}{p}\right)\right).\end{aligned} \tag{6.6}$$

When $\tau_0 \overset{\Gamma}{\sim} i$, then $\mathrm{ord}_{\tau_0}(\widetilde{\mathcal{W}}_p(z)) = \mathrm{ord}_i(\widetilde{\mathcal{W}}_p(z))$, and $\{A(i)\}_{A\in\Gamma_0(p)\backslash\Gamma}$ contains $1+(\frac{-1}{p})$ elliptic fixed points of order 2 which are $\Gamma_0(p)$-inequivalent, and $p-(\frac{-1}{p})$ additional points which are partitioned into $\Gamma_0(p)$-orbits of size 2. We then have

$$\begin{aligned}
\mathrm{ord}_i(\widetilde{\mathcal{W}}_p(z)) &= 2\sum_{\substack{\tau\in\Gamma_0(p)\backslash\mathbb{H}\\ \tau\overset{\Gamma}{\sim}i,\ \ell(\tau)=1}} \mathrm{ord}_\tau(\mathcal{W}_p(z)) + \sum_{\substack{\tau\in\Gamma_0(p)\backslash\mathbb{H}\\ \tau\overset{\Gamma}{\sim}i,\ \ell(\tau)=2}} \mathrm{ord}_\tau(\mathcal{W}_p(z))\\
&= 2\sum_{\substack{\tau\in\Gamma_0(p)\backslash\mathbb{H}\\ \tau\overset{\Gamma}{\sim}i,\ \ell(\tau)=1}} \left(\nu(Q_\tau)\mathrm{wt}(\overline{Q_\tau}) + \frac{g(g+1)}{2}(\nu(Q_\tau)-1)\right)\\
&\quad + \sum_{\substack{\tau\in\Gamma_0(p)\backslash\mathbb{H}\\ \tau\overset{\Gamma}{\sim}i,\ \ell(\tau)=2}} \left(2\nu(Q_\tau)\mathrm{wt}(\overline{Q_\tau}) + \frac{g(g+1)}{2}(2\nu(Q_\tau)-1)\right)\\
&= 2\left(\sum_{\substack{\tau\in\Gamma_0(p)\backslash\mathbb{H}\\ \tau\overset{\Gamma}{\sim}i}} \nu(Q_\tau)\mathrm{wt}(\overline{Q_\tau}) + \frac{g(g+1)}{2}(\nu(Q_\tau)-1)\right)\\
&\quad + \frac{g^2+g}{2}\left(1+\left(\frac{-1}{p}\right)\right).
\end{aligned} \tag{6.7}$$

Finally, we recall that $j(z)$ vanishes to order 3 at $z=\rho$, that $j(z)-1728$ vanishes to order 2 at $z=i$, and that $j(z)-j(\tau_0)$ vanishes to order 1 at all other points $\tau_0 \in \Gamma\backslash\mathbb{H}$. Therefore the exponent of $x-j(\tau_0)$ in $\widetilde{F}(\widetilde{\mathcal{W}}_p, x)$ is equal to

$$\begin{cases} \mathrm{ord}_{\tau_0}\widetilde{\mathcal{W}}_p & \text{if } \tau_0 \neq i, \rho,\\ \frac{1}{2}\mathrm{ord}_i\widetilde{\mathcal{W}}_p & \text{if } \tau_0 = i,\\ \frac{1}{3}(\mathrm{ord}_\rho\widetilde{\mathcal{W}}_p - k^*) & \text{if } \tau_0 = \rho. \end{cases} \tag{6.8}$$

Therefore, by (3.1), (6.5), (6.6), (6.7), and (6.8), we have

$$\begin{aligned}
\widetilde{F}(\widetilde{\mathcal{W}}_p, x) &= x^{\epsilon_p(\rho)}(x-1728)^{\epsilon_p(i)}\mathcal{F}_p(x)\prod_{\substack{\tau\in\Gamma_0(p)\backslash\mathbb{H}\\ \nu(Q_\tau)=2}}(x-j(\tau))^{g(g+1)/2}\\
&= x^{\epsilon_p(\rho)}(x-1728)^{\epsilon_p(i)}\mathcal{F}_p(x)H_p(x)^{g(g+1)/2}.
\end{aligned}$$

□

Combining (6.2), (6.3), Theorem 3.2 and Theorem 6.4 now yields

$$x^{\epsilon_p(\rho)}(x-1728)^{\epsilon_p(i)}\mathcal{F}_p(x)S_p^{(l)}(x)^{g^2+g} \equiv \widetilde{S}_p(x)^{g^2-g}\cdot\widetilde{F}(W^2,x)\cdot\mathcal{G}_p(x) \pmod{p}. \tag{6.9}$$

We next define

$$\widetilde{S}_p^{(l)}(x) := \prod_{\substack{E/\overline{\mathbb{F}}_p \text{ supersingular}\\ j(E)\in\mathbb{F}_p\backslash\{0,1728\}}}(x-j(E)).$$

In Table 1 below, we compare certain factors appearing in (6.9) for each choice of p modulo 12.

Since both $\lceil \frac{g^2-g}{3} \rceil$ and $\frac{g^2-g}{2}$ are less than g^2+g, we see from Table 1 that $\mathcal{G}_p(x)$ always divides $S_p^{(l)}(x)^{g^2+g}$. Then since x and $(x-1728)$ are coprime to $\widetilde{S}_p(x)$, we have

$$\mathcal{F}_p(x)\frac{S_p^{(l)}(x)^{g^2+g}}{\mathcal{G}_p(x)} \equiv \widetilde{S}_p(x)^{g^2-g}\frac{\widetilde{F}(W^2,x)}{x^{\epsilon_p(\rho)}(x-1728)^{\epsilon_p(i)}} \pmod{p}, \tag{6.10}$$

where the two quotients reduce to polynomials.

Now on the left of (6.10), we write $S_p^{(l)}(x) = x^{\alpha_p(\rho)}(x-1728)^{\alpha_p(i)}\widetilde{S}_p^{(l)}(x)$ with $\alpha_p(\rho), \alpha_p(i) \in \{0,1\}$ according to p modulo 12, as in Table 1. On the right, we write $\widetilde{S}_p(x) = \widetilde{S}_p^{(l)}(x)S^{(q)}(x)$. Then (6.10) becomes

$$\begin{aligned}\mathcal{F}_p(x)\widetilde{S}_p^{(l)}(x)^{g^2+g}&\frac{(x^{\alpha_p(\rho)}(x-1728)^{\alpha_p(i)})^{g^2+g}}{\mathcal{G}_p(x)}\\ &\equiv \widetilde{S}_p^{(l)}(x)^{g^2-g}S_p^{(q)}(x)^{g^2-g}\frac{\widetilde{F}(W^2,x)}{x^{\epsilon_p(\rho)}(x-1728)^{\epsilon_p(i)}} \pmod{p}.\end{aligned} \tag{6.11}$$

Now the quotient on the left of (6.11) must divide $\widetilde{F}(W^2,x)$. Then canceling $\widetilde{S}_p^{(l)}(x)^{g^2-g}$ on each side leaves $\widetilde{S}_p^{(l)}(x)^{2g}$ on the left, which must then divide $\widetilde{F}(W^2,x)$ as well. So (6.11) becomes

$$\mathcal{F}_p(x) \equiv S_p^{(q)}(x)^{g^2-g}H_1(x) \pmod{p},$$

where $H_1(x)$ is the polynomial given in non-reduced form by the quotient

$$H_1(x) := \frac{\mathcal{G}_p(x)\widetilde{F}(W^2,x)}{x^{\epsilon_p(\rho)}(x-1728)^{\epsilon_p(i)}(x^{\alpha_p(\rho)}(x-1728)^{\alpha_p(i)})^{g^2+g}\widetilde{S}_p^{(l)}(x)^{2g}}.$$

It remains to show that $H_1(x)$ is a perfect square. By Lemma 2.1, we write $\widetilde{F}(W^2,x) = x^{\delta_p(\rho)}(x-1728)^{\delta_p(i)}\widetilde{F}(W,x)^2$, where $\delta_p(\rho), \delta_p(i) \in \{0,1\}$ according to $g(g+p)$ modulo 12. We then decompose $H_1(x)$ into a product of two quotients,

$$H_1(x) = \frac{\mathcal{G}_p(x)x^{\delta_p(\rho)}(x-1728)^{\delta_p(i)}}{x^{\epsilon_p(\rho)}(x-1728)^{\epsilon_p(i)}} \cdot \frac{\widetilde{F}(W,x)^2}{(x^{\alpha_p(\rho)}(x-1728)^{\alpha_p(i)})^{g^2+g}\widetilde{S}_p^{(l)}(x)^{2g}}.$$

Note that the exponents in the right-hand quotient are all even. The quotient on the left is of the form $x^a(x-1728)^b$, where a and b are integers, possibly negative. It is sufficient to show that a and b are both even. An examination of the exponents reveals that the parity of a and b depend only on p and g modulo 12. A check of all possible combinations of these values using Table 1 and Lemma 2.1 confirms that a and b are indeed even in all cases, and therefore we can write $H_1(x) = H(x)^2$ for some polynomial $H(x) \in \mathbb{F}_p$. This concludes the proof of Theorem 1.2. □

Table 1 Factors arising from elliptic points

$p \pmod{12}$	$x^{\epsilon_p(\rho)}$	$(x-1728)^{\epsilon_p(i)}$	$\mathcal{G}_p(x)$	$S_p^{(l)}(x)$
1	$x^{\lfloor \frac{2(g^2+g)}{3} \rfloor}$	$(x-1728)^{(g^2+g)/2}$	1	$\widetilde{S}_p^{(l)}(x)$
5	1	$(x-1728)^{(g^2+g)/2}$	$x^{\lceil \frac{g^2-g}{3} \rceil}$	$x \cdot \widetilde{S}_p^{(l)}(x)$
7	$x^{\lfloor \frac{2(g^2+g)}{3} \rfloor}$	1	$(x-1728)^{(g^2-g)/2}$	$(x-1728) \cdot \widetilde{S}_p^{(l)}(x)$
11	1	1	$x^{\lceil \frac{g^2-g}{3} \rceil}(x-1728)^{(g^2-g)/2}$	$x(x-1728) \cdot \widetilde{S}_p^{(l)}(x)$

7 The example for $X_0^+(67)$

Here we compute $\mathcal{F}_{67}(x)$, the divisor polynomial corresponding to the modular curve $X_0^+(67)$, which has genus 2. A basis for $S_2^+(67)$ is given by $\{f_1, f_2\}$, with

$$f_1 = q - 3q^3 - 3q^4 - 3q^5 + q^6 + 4q^7 + 3q^8 + \cdots,$$

and

$$f_2 = q^2 - q^3 - 3q^4 + 3q^7 + 4q^8 + \cdots.$$

The associated Wronskian is

$$\mathcal{W}_{67}(z) = q^3 - 2q^4 - 6q^5 + 6q^6 + 15q^7 + 8q^8 + \cdots \in S_6(67).$$

Then by Lemma 6.2 and (2.3), we have

$$\widetilde{F}(\widetilde{\mathcal{W}}_{67}, x) \equiv x^4(x+1)^6(x+14)^6(x^2+8x+45)^2(x^2+44x+24)^2 \times (x^2+10x+62)^2 \pmod{67}.$$

But $\epsilon_{67}(i) = 0$, $\epsilon_{67}(\rho) = 4$, and

$$S_{67}(x) = (x+1)(x+14)(x^2+8x+45)(x^2+44x+24).$$

Therefore, by Theorem 6.4, we have

$$\begin{aligned}\mathcal{F}_{67}(x) &\equiv (x^2+8x+45)^2(x^2+44x+24)^2(x^2+10x+62)^2 \pmod{67}\\ &\equiv S_{67}^{(q)}(x)^2(x^2+10x+62)^2 \pmod{67}.\end{aligned}$$

Note In general, $H(x)$ may not be irreducible.

Acknowledgements
The author thanks the reviewers for their helpful comments and gratefully acknowledges Scott Ahlgren for his invaluable mentoring and for suggesting this problem in the first place.

Publisher's Note

Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Received: 14 February 2017 Accepted: 11 July 2017
Published online: 06 December 2017

References

1. Ahlgren, S.: The arithmetic of Weierstrass points on modular curves $X_0(p)$. In: Galois Theory and Modular Forms, Dev. Math., vol. 11, pp. 3–12. Kluwer Acad. Publ., Boston (2004)
2. Ahlgren, S., Masri, N., Rouse, J.: Vanishing of modular forms at infinity. Proc. Am. Math. Soc. **137**(4), 1205–1214 (2009)
3. Ahlgren, S., Ono, K.: Weierstrass points on $X_0(p)$ and supersingular j-invariants. Math. Ann. **325**, 355–368 (2003)
4. Ahlgren, S., Papanikolas, M.: Higher Weierstrass points on $X_0(p)$. Trans. Am. Math. Soc. **355**, 1521–1535 (2003)
5. Atkin, A.O.L.: Weierstrass points at cusps of $\Gamma_0(n)$. Ann. Math. **85**, 42–45 (1967)
6. Atkin, A.O.L.: Modular forms of weight 1 and supersingular equations. In: US: Japan Seminar on Applications of Automorphic Forms to Number Theory. Ann Arbor (1975)
7. Deligne, P., Rapoport, M.: Les schémas de modules de courbes elliptiques. In: Modular Functions of One Variable, II, (Proceedings of the International Summer School, University Antwerp, Antwerp, 1972), Lecture Notes in Mathematics, vol. 349, pp. 143–316. Springer, Berlin (1973)
8. El-Guindy, A.: Weierstrass points on $X_0(pM)$ and supersingular j-invariants. J. Lond. Math. Soc. (2) **70**(1), 1–22 (2004)
9. Farkas, H.M., Kra, I.: Riemann Surfaces. Springer, New York (1992)
10. Im, B.-H., Jeon, D., Kim, C.H.: Notes on Weierstrass points of modular curves $X_0(N)$. Taiwanese J. Math. **20**(6), 1275–1293 (2016)
11. Kaneko, M.: Supersingular j-invariants as singular moduli mod p. Osaka J. Math. **26**, 849–855 (1989)
12. Kohnen, W.: A short remark on Weierstrass points at infinity on $X_0(N)$. Monatshefte Math. **143**(2), 163–167 (2004)
13. Kohnen, W.: Weierstrass points at cusps on special modular curves. Abh. Math. Sem. Univ. Hamburg **73**, 241–251 (2003)
14. Lang, S.: Elliptic Functions, 2nd edn. Springer, New York (1987)
15. Lehner, J., Newman, M.: Weierstrass points of $\Gamma_0(n)$. Ann. Math. **79**, 360–368 (1964)

16. Miranda, R.: Algebraic Curves and Riemann Surfaces, Graduate Studies in Mathematics 5. Amer. Math. Soc, Providence (1995)
17. Ogg, A.: Hyperelliptic modular curves. Bull. Soc. Math. Fr. **102**, 449–462 (1974)
18. Ogg, A.: Modular functions. In: The Santa Cruz Conference on Finite Groups (Univ. California, Santa Cruz, Calif., 1979), Proceedings of the Symposium Pure Mathematics, vol. 37, pp. 521–532. Amer. Math. Soc., Providence (1980)
19. Ogg, A.: On the reduction modulo p of $X_0(pM)$. In: US: Japan Seminar on Applications of Automorphic Forms to Number Theory. Ann Arbor (1975)
20. Ogg, A.: On the Weierstrass points of $X_0(N)$. Ill. J. Math. **22**, 31–35 (1978)
21. Ono, K.: The web of modularity: arithmetic of the coefficients of modular forms and q-series. In: CBMS Regional Conference Series in Mathematics, 102, Published for the Conference Board of the Mathematical Sciences, Washington, DC, by the American Mathematical Society. Providence (2004)
22. Rohrlich, D.E.: Some remarks on Weierstrass points. In: Number Theory Related to Fermat's Last Theorem (Cambridge, MA, 1981), Progress in Mathematics, vol. 26, pp. 71–78. Birkhuser, Boston (1982)
23. Rohrlich, D.E.: Weierstrass points and modular forms. Ill. J. Math. **29**, 134–141 (1985)
24. Serre, J.-P.: Congruences et formes modulaires (d'après H. P. F. Swinnerton-Dyer). Sm. Bourbaki, **416**, 74–88 (1971–1972)
25. Serre, J.-P.: Formes modulaires et fonctions zêta p-adiques. In: Modular Functions of One Variable, III (Proceedings of the International Summer School, Univ. Antwerp, 1972). Lecture Notes in Mathematics, vol. 350, pp. 191–268. Springer, Berlin (1973)
26. Stein, W.: Weierstrass points on $X_0(p)^+$, http://wstein.org/Tables/weierstrass_point_plus. Accessed 13 Feb 2017
27. Sturm, J.: On the congruence of modular forms. In: Number Theory (New York, 1984–1985), Lecture Notes in Mathematics, vol. 1240, pp. 275–280. Springer, Berlin (1987)