WEIERSTRASS POINTS ON $X_0(p)$ AND SUPERSINGULAR j-INVARIANTS

Scott Ahlgren and Ken Ono

1. Introduction and Statement of Results.

A point Q on a compact Riemann surface M of genus g is a *Weierstrass point* if there is a holomorphic differential ω (not identically zero) with a zero of order $\geq g$ at Q. If $Q \in M$ and $\omega_1, \omega_2, \dots, \omega_g$ form a basis for the holomorphic differentials on M with the property that

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

then the *Weierstrass weight* of Q is the non-negative integer

$$\mathrm{wt}(Q) := \sum_{j=1}^{g} (\mathrm{ord}_Q(\omega_j) - j + 1). \tag{1.1}$$

The weight is independent of the particular basis; moreover, we have $\mathrm{wt}(Q) > 0$ if and only if Q is a Weierstrass point. It is known that $\sum_{Q\in M} \mathrm{wt}(Q) = g^3 - g$; therefore Weierstrass points exist on every Riemann surface of genus $g \geq 2$ (for these and other basic facts, see [F-K]).

In this paper we study such points on modular curves; these are a class of Riemann surfaces which play an important role in Number Theory. As usual, we denote by $\mathbb{H}$ the complex upper half-plane and by $\Gamma_0(N)$ the congruence subgroup

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

We consider the modular curves $X_0(N)$ which are obtained by compactifying the quotient $Y_0(N) := \Gamma_0(N)\backslash\mathbb{H}$. These curves play a distinguished role in arithmetic; each $X_0(N)$ is the moduli space of elliptic curves with a prescribed cyclic subgroup of order N.

Works by Atkin [A], Lehner and Newman [L-N], Ogg [O1, O2] and Rohrlich [R1, R2] address a variety of questions regarding Weierstrass points on modular curves. For example, these works

---

1991 *Mathematics Subject Classification.* Primary 11F, 11G, 14H.

Key words and phrases. Weierstrass points, modular curves.

The first author thanks the National Science Foundation for its support through grants DMS 01-96443 and DMS 01-35477. The second author is grateful for the generous support of the National Science Foundation as well as the Alfred P. Sloan, David and Lucile Packard, and H. I. Romnes Fellowships.

determine some conditions under which the cusp at infinity is a Weierstrass point, and also illustrate the important role which Weierstrass points play in determining the finite list of N for which $X_0(N)$ is hyperelliptic. Apart from these works, little appears to be known. Here we consider the arithmetic of the Weierstrass points on $X_0(p)$ when p is prime. If $p \geq 5$, then the genus of $X_0(p)$ is

$$g_p := \begin{cases} (p-13)/12 & \text{if } p \equiv 1 \pmod{12}, \\ (p-5)/12 & \text{if } p \equiv 5 \pmod{12}, \\ (p-7)/12 & \text{if } p \equiv 7 \pmod{12}, \\ (p+1)/12 & \text{if } p \equiv 11 \pmod{12}. \end{cases} \tag{1.2}$$

These formulas imply that $X_0(p)$ has Weierstrass points if and only if $p \geq 23$.

Ogg [O2] studied Weierstrass points on curves $X_0(N)$ using the Igusa-Deligne-Rapoport model for the reduction of $X_0(N)$ modulo primes p. For the curves $X_0(p)$, he proved that if Q is a $\mathbb{Q}$-rational Weierstrass point, then $\widetilde{Q}$, the reduction of Q modulo p, is supersingular (i.e. the underlying elliptic curve is supersingular). In light of this, it is natural to seek a precise description of the relationship between the supersingular j-invariants and the set of $j(Q)$ for Weierstrass points $Q \in X_0(p)$. Do all supersingular j-invariants arise from Weierstrass points? If so, what is the multiplicity of such a correspondence?

To answer these questions, we investigate the degree $g_p^3 - g_p$ polynomials

$$F_p(x) := \prod_{Q \in X_0(p)} (x - j(Q))^{\mathrm{wt}(Q)}, \tag{1.3}$$

where $j(z) = q^{-1} + 744 + 196884q + \cdots$ denotes the usual elliptic modular function on $\mathrm{SL}_2(\mathbb{Z})$ ($q := e^{2\pi i z}$ throughout). Here we adopt the convention that if $Q \in Y_0(p)$, then $j(Q)$ is taken to mean $j(\tau)$, where $\tau \in \mathbb{H}$ is any point which corresponds to Q under the usual identification. We note that the product in (1.3) is well defined since it is known by work of Atkin and Ogg (see [O2]) that the cusps of $X_0(p)$ are not Weierstrass points.

We compare the reduction of $F_p(x)$ modulo p to the polynomial

$$S_p(x) := \prod_{\substack{E/\overline{\mathbb{F}}_p \\ \text{supersingular}}} (x - j(E)) \in \mathbb{F}_p[x] \tag{1.4}$$

(the product is taken over $\overline{\mathbb{F}}_p$-isomorphism classes of elliptic curves). It is well known that the degree of $S_p(x)$ is $g_p + 1$. We obtain the following result.

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

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

Since every supersingular j-invariant lies in $\mathbb{F}_{p^2}$, it follows that the irreducible factors of $F_p(x)$ in $\mathbb{F}_p[x]$ are linear or quadratic. Theorem 1 and this phenomenon are illustrated by the following example (which is discussed at greater length in the last section).

$$\begin{aligned} F_{37}(x) = x^6 &+ 4413440825818343120655186904x^5 - 1170813143341635780411150282868x^4 \\ &+ 82273130904992951143620938110163846x^3 - 16261934011084142326646181531500240x^2 \\ &+ 58311989272495412124733786893576034567x + 2662919220569726562604951395814787027 \\ &\equiv (x+29)^2(x^2+31x+31)^2 \pmod{37} \\ &= S_{37}(x)^2. \end{aligned}$$

Theorem 1 is in part a consequence of a general phenomenon concerning modular forms modulo p. Let M_k (respectively S_k) denote the complex vector space of holomorphic modular forms (respectively cusp forms) of weight k for $\mathrm{SL}_2(\mathbb{Z})$. If $f \in M_{k_f}$ has p-integral coefficients, then let $\omega_p(f)$ denote the usual filtration

$$\omega_p(f) := \min\{k \ : \ g \equiv f \pmod{p} \text{ for some } g \in M_k\}.$$

For each such f we construct an explicit polynomial $F(f,x)$ whose roots are the values $j(\tau)$ for those $\tau \in \mathbb{H}$ with $\mathrm{ord}_f(\tau) > 0$. If k_f is large compared to $\omega_p(f)$, then we show that

$$F(f,x) \equiv R(f,x) S_p(x)^{\alpha_f} \pmod{p},$$

where $R(f,x)$ is a rational function of small degree, and α_f is a large positive integer. The precise formulation of this result is stated in Section 2 (see Theorem 2.3). In Section 3 we use this result, a theorem of Rohrlich [R1] and the 'norm' from $\Gamma_0(p)$ to $\mathrm{SL}_2(\mathbb{Z})$ of a certain Wronskian in order to prove Theorem 1. In Section 4 we consider the example of $X_0(37)$ (including the exact calculation of $F_{37}(x)$) in detail.

Acknowledgments

The authors thank Matthew Baker, Matthew Papanikolas, Joel Robbin, and David Rohrlich for their helpful comments.

2. Preliminaries

In what follows we will write $\Gamma := \mathrm{SL}_2(\mathbb{Z})$ for convenience. If $f \in M_k$, then using the classical valence formula

$$\frac{k}{12} = \frac{1}{2}\mathrm{ord}_i(f) + \frac{1}{3}\mathrm{ord}_\rho(f) + \mathrm{ord}_\infty(f) + \sum_{\tau \in \Gamma\backslash\mathbb{H} - \{i,\rho\}} \mathrm{ord}_\tau(f)$$

(throughout $\rho := e^{2\pi i/3}$), it is easy to see that

$$\mathrm{ord}_i(f) \geq \begin{cases} 1 & \text{if } k \equiv 2 \pmod{4}, \\ 0 & \text{if } k \equiv 0 \pmod{4}, \end{cases} \tag{2.1}$$

and

$$\operatorname{ord}_\rho(f) \geq \begin{cases} 2 & \text{if } k \equiv 2 \pmod 6, \\ 1 & \text{if } k \equiv 4 \pmod 6, \\ 0 & \text{if } k \equiv 0 \pmod 6. \end{cases} \tag{2.2}$$

Because of these trivial zeros (and the fact that $j(i) = 1728$ and $j(\rho) = 0$), we find it convenient to define polynomials $h_k(x)$ by

$$h_k(x) := \begin{cases} 1 & \text{if } k \equiv 0 \pmod{12}, \\ x^2(x-1728) & \text{if } k \equiv 2 \pmod{12}, \\ x & \text{if } k \equiv 4 \pmod{12}, \\ x-1728 & \text{if } k \equiv 6 \pmod{12}, \\ x^2 & \text{if } k \equiv 8 \pmod{12}, \\ x(x-1728) & \text{if } k \equiv 10 \pmod{12}. \end{cases} \tag{2.3}$$

For even integers $k \geq 2$, let E_k denote the usual Eisenstein series

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

here $\sigma_{k-1}(n) = \sum_{d|n} d^{k-1}$ and B_k is the kth Bernoulli number. As usual, let $\Delta(z)$ be the unique normalized weight 12 cusp form on Γ; we have

$$\Delta(z) = \frac{E_4(z)^3 - E_6(z)^2}{1728} = q - 24q^2 + 252q^3 - 1472q^4 + \dots. \tag{2.4}$$

If $k \geq 4$ is even, then define $\widetilde{E}_k(z)$ by

$$\widetilde{E}_k(z) := \begin{cases} 1 & \text{if } k \equiv 0 \pmod{12}, \\ E_4(z)^2 E_6(z) & \text{if } k \equiv 2 \pmod{12}, \\ E_4(z) & \text{if } k \equiv 4 \pmod{12}, \\ E_6(z) & \text{if } k \equiv 6 \pmod{12}, \\ E_4(z)^2 & \text{if } k \equiv 8 \pmod{12}, \\ E_4(z)E_6(z) & \text{if } k \equiv 10 \pmod{12}. \end{cases} \tag{2.5}$$

From the valence formula we see that the divisor of $E_4(z)$ (respectively $E_6(z)$) is supported on a simple zero at $\tau = \rho$ (respectively $\tau = i$). Therefore, the definitions of the polynomials $h_k(x)$ mirror the divisors of the corresponding $\widetilde{E}_k(z)$.

Lemma 2.1. *Define $m(k)$ by*

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

and suppose that $f \in M_k$ has leading coefficient 1. Let $\widetilde{F}(f,x)$ be the unique rational function in x for which

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

Then $\widetilde{F}(f,x)$ is a polynomial.

Proof. Notice that $m(k)$ is defined so that the weight of $\widetilde{E}_k(z)$ equals $k-12m(k)$. Since $\Delta(z)$ does not vanish on $\mathbb{H}$, (2.1), (2.2) and (2.5) imply that

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

is a modular function for Γ which is holomorphic on $\mathbb{H}$. Therefore it is a polynomial in $j(z)$. $\square$

If $f(z) \in M_k$ then, after Lemma 2.1, we define the polynomial $F(f,x)$ by

$$F(f,x) := h_k(x)\widetilde{F}(f,x). \tag{2.6}$$

(Note, for example, that if f vanishes to order N_0+3N at ρ, with $N_0 \in \{0,1,2\}$, then the power of x appearing in $F(f,x)$ is N_0+N.) Observe that $F(f,x)$ has p-integral rational coefficients when $f(z)$ has p-integral rational coefficients.

It is a well known result of Deligne (see, for example, [S]) that if $p \geq 5$ is prime, then

$$S_p(x) \equiv F(E_{p-1},x) \pmod{p}. \tag{2.7}$$

Before turning to the proof of Theorem 1, we develop some machinery for studying the polynomials $F(f,x)$ and $\widetilde{F}(f,x)$.

Lemma 2.2. *If $s = 1, 5, 7$ or 11 and $p \equiv s \pmod{12}$ is prime, then*

$$\frac{1}{\Delta(z)^{(p-s)/12}} \equiv \begin{cases} \widetilde{F}(E_{p-1},j(z)) \pmod{p} & \text{if } s=1, \\ E_4(z)\widetilde{F}(E_{p-1},j(z)) \pmod{p} & \text{if } s=5, \\ E_6(z)\widetilde{F}(E_{p-1},j(z)) \pmod{p} & \text{if } s=7, \\ E_4(z)E_6(z)\widetilde{F}(E_{p-1},j(z)) \pmod{p} & \text{if } s=11. \end{cases}$$

Proof. Since $E_{p-1}(z) \equiv 1 \pmod{p}$, Lemma 2.1 implies that

$$1 \equiv E_{p-1}(z) \equiv \Delta(z)^{(p-s)/12}\widetilde{E}_{p-1}(z)\widetilde{F}(E_{p-1},j(z)) \pmod{p}.$$

The congruences follow by solving for $\Delta(z)^{(p-s)/12} \pmod{p}$. $\square$

To prove Theorem 1, we shall require the following theorem.

Theorem 2.3. *If $p \geq 5$ is prime and $f \in M_k$ has p-integral coefficients, then*

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

where

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

Proof. Since $f(z) \equiv f(z)E_{p-1}(z) \pmod{p}$, it follows from Lemma 2.1 that

$$\Delta(z)^{m(k+p-1)}\widetilde{E}_{k+p-1}(z)\widetilde{F}(fE_{p-1}, j(z)) \equiv \Delta(z)^{m(k)}\widetilde{E}_k(z)\widetilde{F}(f, j(z)) \pmod{p}.$$

Therefore, we have

$$\widetilde{F}(fE_{p-1}, j(z)) \equiv \frac{1}{\Delta(z)^{m(k+p-1)-m(k)}} \cdot \frac{\widetilde{E}_k(z)}{\widetilde{E}_{k+p-1}(z)}\widetilde{F}(f, j(z)) \pmod{p}. \tag{2.8}$$

The theorem follows from a case by case analysis. For example, if $(k,p) \equiv (2,11) \pmod{12}$, then

$$\begin{aligned} \widetilde{F}(fE_{p-1}, j(z)) &\equiv \frac{1}{\Delta(z)^{(p+13)/12}} \cdot E_4(z)^2E_6(z)\widetilde{F}(f, j(z)) \pmod{p} \\ &\equiv \frac{1}{\Delta(z)^{(p-11)/12}} \cdot \frac{E_4(z)^2E_6(z)}{\Delta(z)^2} \cdot \widetilde{F}(f, j(z)) \pmod{p}. \end{aligned}$$

By Lemma 2.2, this becomes

$$\begin{aligned} \widetilde{F}(fE_{p-1}, j(z)) &\equiv \frac{E_4(z)^3}{\Delta(z)} \cdot \frac{E_6(z)^2}{\Delta(z)} \cdot \widetilde{F}(E_{p-1}, j(z))\widetilde{F}(f, j(z)) \pmod{p} \\ &\equiv j(z)(j(z)-1728)\widetilde{F}(E_{p-1}, j(z))\widetilde{F}(f, j(z)) \pmod{p}; \end{aligned}$$

here we use the identities

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

The other cases follow in a similar fashion; we omit the details for brevity. □

3. Proof of Theorem 1

In general, the Weierstrass weight of a point Q is determined by the order of vanishing of a certain Wronskian at Q (see [F-K]). In the current context, let $\{f_1(z), f_2(z), \ldots, f_{g_p}(z)\}$ be any basis for the space of cusp forms $S_2(\Gamma_0(p))$. Following Rohrlich [R1], we define $W_p(f_1, \ldots, f_{g_p})(z)$ by

$$W_p(f_1, \ldots, f_{g_p})(z) := \begin{vmatrix} f_1 & f_2 & \cdots & f_{g_p} \\ f_1' & f_2' & \cdots & f_{g_p}' \\ \vdots & \vdots & \vdots & \vdots \\ f_1^{(g_p-1)} & f_2^{(g_p-1)} & \cdots & f_{g_p}^{(g_p-1)} \end{vmatrix}. \tag{3.1}$$

Then $W_p(f_1, \ldots, f_{g_p})(z)$ is a cusp form of weight $g_p(g_p+1)$ on $\Gamma_0(p)$ (the fact that this modular form vanishes at the cusp 0 can be deduced, for example, using Lemma 3.2 below). We denote by $\mathcal{W}_p(z)$ that scalar multiple of $W_p(f_1, \ldots, f_{g_p})(z)$ whose leading coefficient equals 1. Thus $\mathcal{W}_p$ is independent of the particular choice of basis. The importance of $\mathcal{W}_p$ arises from the fact [R1] that the Weierstrass weight of a point $Q \in X_0(p)$ is given by the order of vanishing at Q of the differential $\mathcal{W}_p(z)(dz)^{g_p(g_p+1)/2}$. Rohrlich [R1] proved the following congruence for these forms.

Theorem 3.1. *If $p \geq 23$ is prime, then $\mathcal{W}_p(z) \in S_{g_p(g_p+1)}(\Gamma_0(p))$ has p-integral coefficients and satisfies*

$$\mathcal{W}_p(z) \equiv \Delta(z)^{g_p(g_p+1)/2} \widetilde{E}_{p+1}(z)^{g_p} E_{14}(z)^{g_p(g_p-1)/2} \pmod{p}.$$

If f is a function of the upper half plane, $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ is a real matrix with positive determinant, and k is a positive integer, then as usual we define

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

We recall that the spaces $S_k(\Gamma_0(p))$ admit the usual Fricke involution $f \mapsto f\big|_k w_p$, where $w_p := \left(\begin{smallmatrix} 0 & -1 \\ p & 0 \end{smallmatrix}\right)$.

We begin by proving the following lemma; for the duration of the paper we will write $g = g_p$ for simplicity.

Lemma 3.2. *We have*

$$\mathcal{W}_p(z)|_{g(g+1)} w_p = \pm \mathcal{W}_p(z). \tag{3.2}$$

Proof.

We fix a basis $\{f_1, f_2, \ldots, f_g\}$ of newforms for the space $S_2(\Gamma_0(p))$, and we write

$$W_p(z) = W_p(f_1, \ldots, f_g)(z). \tag{3.3}$$

It clearly suffices to establish (3.2) with $\mathcal{W}_p(z)$ replaced by $W_p(z)$. By [A-L, Th. 3] we have, for $1 \leq i \leq g$,

$$f_i\big|_2 w_p = \lambda_i f_i, \quad \text{with} \quad \lambda_i \in \{\pm 1\}. \tag{3.4}$$

For each i, (3.4) shows that
$$f_i(-1/pz) = \lambda_i p z^2 f_i(z). \tag{3.5}$$

Therefore, from the definition (3.1) we have

$$\begin{aligned} W_p(-1/pz) &= \begin{vmatrix} f_1(-1/pz) & \dots & f_g(-1/pz) \\ f_1'(-1/pz) & \dots & f_g'(-1/pz) \\ \vdots & \vdots & \vdots \\ f_1^{(g-1)}(-1/pz) & \dots & f_g^{(g-1)}(-1/pz) \end{vmatrix} \\ &= pz^2 \begin{vmatrix} \lambda_1 f_1(z) & \dots & \lambda_g f_g(z) \\ f_1'(-1/pz) & \dots & f_g'(-1/pz) \\ \vdots & \vdots & \vdots \\ f_1^{(g-1)}(-1/pz) & \dots & f_g^{(g-1)}(-1/pz) \end{vmatrix}. \end{aligned} \tag{3.6}$$

Using (3.5) and induction, we find that for each i and for all $n \geq 1$ we have

$$f_i^{(n)}(-1/pz) = \lambda_i \left\{ p^{n+1} z^{2n+2} f_i^{(n)}(z) + \sum_{j=0}^{n-1} A_{n,j}(p,z) f_i^{(j)}(z) \right\}, \tag{3.7}$$

where each $A_{n,j}$ is a polynomial in p and z which is independent of the value of i. Using (3.6), (3.7), and properties of determinants, we find that

$$W_p(-1/pz) = p^{\frac{g^2+g}{2}} z^{g^2+g} \lambda_1 \dots \lambda_g W_p(z).$$

The lemma follows. □

We use the preceding lemma to construct a modular form $\widetilde{\mathcal{W}}_p(z)$ on Γ whose divisor encodes the pertinent information regarding Weierstrass points on $X_0(p)$. A crucial fact for our proof is that the form we construct also preserves the arithmetic of the relevant Fourier expansions. This is described precisely in the following lemma.

Lemma 3.3. *If $p \geq 23$ is prime and $\widetilde{k}(p) := g(g+1)(p+1)$, then let $\widetilde{\mathcal{W}}_p(z) \in S_{\widetilde{k}(p)}$ be the cusp form*

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

normalized to have leading coefficient 1. Then $\widetilde{\mathcal{W}}_p(z)$ has p-integral rational coefficients and satisfies

$$\widetilde{\mathcal{W}}_p(z) \equiv \mathcal{W}_p(z)^2 \equiv \Delta(z)^{g(g+1)} \widetilde{E}_{p+1}(z)^{2g} E_{14}(z)^{g(g-1)} \pmod{p}.$$

Proof. That $\widetilde{\mathcal{W}}_p(z)$ is a weight $\widetilde{k}(p)$ cusp form on Γ follows easily from the fact that

$$[\Gamma : \Gamma_0(p)] = p + 1.$$

To prove the congruence, begin by observing that the matrices $A_j = \begin{pmatrix} 0 & -1 \\ 1 & j \end{pmatrix}$, for $0 \leq j \leq p-1$, together with the identity matrix, form a complete set of representatives for the coset space $\Gamma_0(p)\backslash\Gamma$. We may write $A_j = w_p B_j$, where $B_j = \begin{pmatrix} 1/p & j/p \\ 0 & 1 \end{pmatrix}$. Using Lemma 3.2 we obtain

$$\prod_{j=0}^{p-1} \mathcal{W}_p(z)|_{g(g+1)} A_j = \pm \prod_{j=0}^{p-1} \mathcal{W}_p(z)|_{g(g+1)} B_j. \tag{3.8}$$

For $n \geq 1$, let $c(n)$ denote the exponents which uniquely express $\mathcal{W}_p(z)$ as an infinite product of the form

$$\mathcal{W}_p(z) = q^{\frac{g(g+1)}{2}} \prod_{n=1}^{\infty} (1-q^n)^{c(n)}. \tag{3.9}$$

Since $\mathcal{W}_p(z)$ has p-integral rational coefficients, it follows that the exponents $c(n)$ are p-integral rational numbers. Indeed, it is clear that the $c(n)$ are rational. To see that they are p-integral, notice that the first non p-integral exponent in (3.9) would produce a non p-integral coefficient of $\mathcal{W}_p(z)$.

Now set $\zeta_p := e^{\frac{2\pi i}{p}}$. After renormalizing, we find that the product in (3.8) is given by

$$\begin{aligned} q^{\frac{g(g+1)}{2}} \prod_{n=1}^{\infty} \prod_{j=0}^{p-1} (1 - q^{\frac{n}{p}} \zeta_p^{nj})^{c(n)} &= q^{\frac{g(g+1)}{2}} \prod_{p \nmid n} (1-q^n)^{c(n)} \prod_{p \mid n} (1 - q^{\frac{n}{p}})^{pc(n)} \\ &\equiv q^{\frac{g(g+1)}{2}} \prod_{n=1}^{\infty} (1-q^n)^{c(n)} \pmod{p}. \end{aligned}$$

The desired congruence follows. $\square$

The next lemma gives the precise relation between the order of vanishing of $\widetilde{\mathcal{W}}_p(z)$ and the Weierstrass weights of the corresponding points on $X_0(p)$. We will use the standard identification of points $\tau \in \mathbb{H} \cup \{0, \infty\}$ with points $Q_\tau \in X_0(p)$.

Lemma 3.4. *For primes $p \geq 23$, define $\epsilon_p(i)$ and $\epsilon_p(\rho)$ by*

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

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

where

$$\alpha(p) := \begin{cases} 2 & \text{if } p \equiv 19, 25 \pmod{36}, \\ 0 & \text{otherwise.} \end{cases}$$

Then we have

$$F(\widetilde{\mathcal{W}}_p, x) = x^{\epsilon_p(\rho)} (x-1728)^{\epsilon_p(i)} \cdot F_p(x). \tag{3.10}$$

Proof. For $A \in \Gamma$ and $\tau \in \mathbb{H}$, we have

$$\mathrm{ord}_\tau(\mathcal{W}_p|_{g(g+1)}A) = \mathrm{ord}_{A(\tau)}(\mathcal{W}_p). \tag{3.11}$$

If τ_0 is neither Γ-equivalent to ρ nor to i, then the set $\{A(\tau_0)\}_{A\in\Gamma_0(p)\backslash\Gamma}$ consists of $p+1$ points which are $\Gamma_0(p)$-inequivalent. For $\tau \in \mathbb{H}$ we define $\ell_\tau \in \{1,2,3\}$ as the order of the isotropy subgroup of τ in $\Gamma_0(p)/\{\pm I\}$. Then we have

$$\begin{aligned}\frac{1}{\ell_\tau}\mathrm{ord}_\tau(\mathcal{W}_p) &= \mathrm{ord}_{Q_\tau}(\mathcal{W}_p(z)(dz)^{(g^2+g)/2}) + \frac{(g^2+g)}{2}(1-1/\ell_\tau)\\ &= \mathrm{wt}(Q_\tau) + \frac{(g^2+g)}{2}(1-1/\ell_\tau).\end{aligned} \tag{3.12}$$

Using the definition of $\widetilde{\mathcal{W}}_p$ together with (3.11) and (3.12), we see that if τ_0 is Γ-equivalent neither to ρ nor to i, then

$$\mathrm{ord}_{\tau_0}(\widetilde{\mathcal{W}}_p) = \sum_{\tau\in\Gamma_0(p)\backslash\mathbb{H},\ \tau\overset{\Gamma}{\sim}\tau_0} \mathrm{ord}_\tau(\mathcal{W}_p) = \sum_{\tau\in\Gamma_0(p)\backslash\mathbb{H},\ \tau\overset{\Gamma}{\sim}\tau_0} \mathrm{wt}(Q_\tau). \tag{3.13}$$

By (3.13) we conclude that, for such τ_0, the power of $x - j(\tau_0)$ appearing in the polynomials on either side of (3.10) is the same.

We next verify that the powers of x on either side are the same. Define $k^* \in \{0,1,2\}$ by $k^* \equiv \widetilde{k}(p) \pmod 3$. Then if

$$\mathrm{ord}_\rho(\widetilde{\mathcal{W}}_p) = k^* + 3N, \tag{3.14}$$

we see that

$$\text{the power of } x \text{ in } F(\widetilde{\mathcal{W}}_p, x) \text{ is } k^* + N. \tag{3.15}$$

The list $[A(\rho)]_{A\in\Gamma_0(p)\backslash\Gamma}$ contains $1 + \left(\frac{-3}{p}\right)$ elliptic fixed points of order 3 which are $\Gamma_0(p)$-inequivalent. The remainder of the list is comprised of the three $\Gamma_0(p)$-equivalent points ρ, $\frac{-1}{\rho+1} = \rho$, and $\frac{-1}{\rho}$, together with $\frac{1}{3}\left(p - 3 - \left(\frac{-3}{p}\right)\right)$ orbits, each of which contains three points of the form

$$\frac{-1}{\rho+j} \overset{\Gamma_0(p)}{\sim} \frac{-1}{\rho+j'} \overset{\Gamma_0(p)}{\sim} \frac{-1}{\rho+j''},$$

where for $2 \le j \le p-1$ we set $j' = -1/(j-1)$ and $j'' = 1 - 1/j$. From this together with (3.11) we see that

$$\mathrm{ord}_\rho(\widetilde{\mathcal{W}}_p) = 3 \sum_{\substack{\tau\in\Gamma_0(p)\backslash\mathbb{H},\ \tau\overset{\Gamma}{\sim}\rho \\ \tau \text{ not elliptic fixed point}}} \mathrm{ord}_\tau(\mathcal{W}_p) + \sum_{\substack{\tau\in\Gamma_0(p)\backslash\mathbb{H},\ \tau\overset{\Gamma}{\sim}\rho \\ \tau \text{ elliptic fixed point}}} \mathrm{ord}_\tau(\mathcal{W}_p). \tag{3.16}$$

Using (3.11), (3.12), (3.14), and (3.16) we see that

$$k^* + 3N = 3 \sum_{\tau\in\Gamma_0(p)\backslash\mathbb{H},\ \tau\overset{\Gamma}{\sim}\rho} \mathrm{wt}(Q_\tau) + \left(1 + \left(\tfrac{-3}{p}\right)\right)(g^2+g),$$

from which

$$k^* + N = \sum_{\tau \in \Gamma_0(p)\backslash \mathbb{H},\ \tau \overset{\Gamma}{\sim} \rho} \mathrm{wt}(Q_\tau) + \frac{\left(1 + \left(\frac{-3}{p}\right)\right)(g^2+g) + 2k^*}{3}. \qquad (3.17)$$

Now if $p \equiv 2 \pmod 3$ then $k^* = 0$, while if $p \equiv 1 \pmod 3$ then an easy calculation using (1.2) and the valence formula shows that $k^* = 0$ except when $p \equiv 19, 25 \pmod{36}$, in which case $k^* = 1$. Therefore, using (3.15) and (3.17), we see that the powers of x in the polynomials given in (3.10) indeed agree.

The verification that the powers of $x - 1728$ agree follows similar lines, and we omit the details for brevity. $\square$

Proof of Theorem 1. Since the theorem is trivial for $p < 23$ (i.e. both sides of the congruence are identically 1), we assume that $p \geq 23$. In view of Lemma 3.4 and (2.7), it suffices to prove that

$$F(\widetilde{\mathcal{W}}_p, x) \equiv x^{\epsilon_p(\rho)}(x-1728)^{\epsilon_p(i)} \cdot F(E_{p-1}, x)^{g^2-g} \pmod p. \qquad (3.18)$$

If $k(p)$ denotes the weight of

$$G_p(z) := \Delta(z)^{g(g+1)} \widetilde{E}_{p+1}(z)^{2g} E_{14}(z)^{g(g-1)}$$

(this is the form appearing in Lemma 3.3), then $\widetilde{k}(p) = k(p) + (g^2-g)(p-1)$. Therefore we have the following congruence between two weight $\widetilde{k}(p)$ modular forms:

$$\widetilde{\mathcal{W}}_p(z) \equiv G_p(z) E_{p-1}(z)^{g^2-g} \pmod p.$$

Since these forms have the same weight, we have

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

If we define $\mathcal{G}_p(x)$ by

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

then arguing inductively with Theorem 2.3 gives

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

Therefore we have

$$\begin{aligned} F(\widetilde{\mathcal{W}}_p, x) &= h_{\widetilde{k}(p)}(x) \widetilde{F}(\widetilde{\mathcal{W}}_p, x) \\ &\equiv h_{\widetilde{k}(p)}(x) \mathcal{G}_p(x) \widetilde{F}(G_p, x) \widetilde{F}(E_{p-1}, x)^{g^2-g} \pmod p. \end{aligned} \qquad (3.19)$$

We must determine the first three factors appearing in the right hand side of (3.19). The polynomial $\widetilde{F}(G_p, x)$ can be computed using the facts that

$$\operatorname{ord}_\rho(G_p) = 2g\left(g + \left(\frac{-3}{p}\right)\right) \quad \text{and} \quad \operatorname{ord}_i(G_p) = g\left(g + \left(\frac{-1}{p}\right)\right). \tag{3.20}$$

Using Theorem 2.3, a straightforward (albeit tedious) case by case analysis gives the following:

$$h_{\widetilde{k}(p)}(x)\mathcal{G}_p(x) = \begin{cases} 1 & \text{if } p \equiv 1, 13 \pmod{36}, \\ x & \text{if } p \equiv 25 \pmod{36}, \\ x^{(g^2-g)/3} & \text{if } p \equiv 5, 17 \pmod{36}, \\ x^{(g^2-g+1)/3} & \text{if } p \equiv 29 \pmod{36}, \\ (x-1728)^{(g^2-g)/2} & \text{if } p \equiv 7, 31 \pmod{36}, \\ x(x-1728)^{(g^2-g)/2} & \text{if } p \equiv 19 \pmod{36}, \\ x^{(g^2-g)/3}(x-1728)^{(g^2-g)/2} & \text{if } p \equiv 11, 35 \pmod{36}, \\ x^{(g^2-g+1)/3}(x-1728)^{(g^2-g)/2} & \text{if } p \equiv 23 \pmod{36}. \end{cases} \tag{3.21}$$

By (2.3) we have

$$h_{p-1}(x)^{g^2-g} = \begin{cases} 1 & \text{if } p \equiv 1 \pmod{12}, \\ x^{g^2-g} & \text{if } p \equiv 5 \pmod{12}, \\ (x-1728)^{g^2-g} & \text{if } p \equiv 7 \pmod{12}, \\ x^{g^2-g}\cdot(x-1728)^{g^2-g} & \text{if } p \equiv 11 \pmod{12}. \end{cases} \tag{3.22}$$

A calculation using (3.20), (3.21) and (3.22) reveals that in every case we have

$$x^{\epsilon_p(\rho)}(x-1728)^{\epsilon_p(i)}h_{p-1}(x)^{g^2-g} \equiv h_{\widetilde{k}(p)}(x)\mathcal{G}_p(x)\widetilde{F}(G_p, x) \pmod{p}.$$

In view of (3.19), the last congruence is equivalent to (3.18). This completes the proof of Theorem 1. □

4. The $X_0(37)$ example

Here we compute the polynomial $F_{37}(x)$ corresponding to the genus 2 modular curve $X_0(37)$. The space $S_2(\Gamma_0(37))$ is generated by the two newforms

$$f_1(z) = q - 2q^2 - 3q^3 + 2q^4 - 2q^5 + 6q^6 - q^7 + \cdots,$$
$$f_2(z) = q + q^3 - 2q^4 - q^7 - 2q^9 + \cdots;$$

these correspond to the two isogeny classes of elliptic curves with conductor 37 in the usual way. The Wronskian $\mathcal{W}_{37}(z)$ is the weight 6 cusp form in $S_6(\Gamma_0(37))$ whose expansion is

$$\mathcal{W}_{37}(z) = q^3 + 4q^4 - 7q^5 + 8q^6 - 13q^7 + 2q^8 - \cdots.$$

We find that the cusp form $\widetilde{\mathcal{W}}_{37}(z) \in S_{228}$ begins with the terms

$$\begin{aligned}\widetilde{\mathcal{W}}_{37}(z) &= \mathcal{W}_{37}(z) \cdot \prod_{j=1}^{37} \mathcal{W}_{37}\left(\frac{z+j}{37}\right) \\ &= q^6 + 4413440825818343120655190936q^7 + 28032620018743543766031107247 40q^8 - \cdots .\end{aligned}$$

Then by Lemma 2.1 and Lemma 3.4, we find that

$$\begin{aligned}F_{37}(x) &= x^6 + 4413440825818343120655186904x^5 - 117081314334163578041111502828 68x^4 \\ &+ 8227313090499295114362093811016384x^3 - 1626193401108414232664618153150 0240x^2 \\ &+ 58311989272495412124733786893576034 56x + 2662919220569726562604951395814787 0272.\end{aligned}$$

By Lemma 2.1 we have

$$F(E_{36}, x) \equiv S_{37}(x) \equiv (x+29)(x^2+31x+31) \pmod{37}.$$

Then, as asserted by Theorem 1, we have

$$F_{37}(x) \equiv S_{37}(x)^2 \pmod{37}.$$

References

[A] A. O. L. Atkin, *Weierstrass points at cusps of $X_0(N)$*, Ann. of Math. **85** (1967), 42-45.
[A-L] A. O. L. Atkin and J. Lehner, *Hecke operators on $\Gamma_0(m)$*, Math. Ann. **185** (1970), 134-160.
[F-K] H. M. Farkas and I. Kra, *Riemann surfaces*, Springer-Verlag, New York, 1992.
[L-N] J. Lehner and M. Newman, *Weierstrass points on $\Gamma_0(N)$*, Ann. of Math. **79** (1964), 360-368.
[O1] A. Ogg, *Hyperelliptic modular curves*, Bull. Soc. Math. France **102** (1974), 449-462.
[O2] A. Ogg, *On the Weierstrass points of $X_0(N)$*, Illinois J. Math. **22** (1978), 31-35.
[R1] D. Rohrlich, *Weierstrass points and modular forms*, Illinois J. Math. **29** (1985), 134-141.
[R2] 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.
[S] J.-P. Serre, *Congruences et formes modulaires (d'après H. P. F. Swinnerton-Dyer)*, Sem. Bourbaki **416** (1971-1972), 74-88.

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

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