ILLINOIS JOURNAL OF MATHEMATICS
Volume 29, November 1, Spring 1985

WEIERSTRASS POINTS AND MODULAR FORMS

BY
DAVID E. ROHRLICH[1]

Let X be a compact Riemann surface of genus g. A point $x \in X$ is called a Weierstrass point if there is a regular differential on X, different from 0, which vanishes at x to order at least g. The concept of Weierstrass weight refines this notion: Given a point $x \in X$, let $\{\omega_1, \ldots, \omega_g\}$ be a basis for the regular differentials on X such that

$$0 = \mathrm{ord}_x \omega_1 < \mathrm{ord}_x \omega_2 < \cdots < \mathrm{ord}_x \omega_g,$$

where ord_x denotes order at x. The Weierstrass weight of x is the nonnegative integer

$$\sum_{1 \leq j \leq g} \left(\mathrm{ord}_x \omega_j + 1 - j\right).$$

Since $\mathrm{ord}_x \omega_j \geq j - 1$, this sum is 0 if and only if $\mathrm{ord}_x \omega_j = j - 1$ for all j; one deduces that x is a Weierstrass point if and only if its Weierstrass weight is positive. Furthermore, it is known that the sum of the Weierstrass weights of all points on X is $(g-1)g(g+1)$. Thus for $g \geq 2$ the set of Weierstrass points is a nonempty and finite set of intrinsically distinguished points on X.

Now let p be a prime, and put

$$\Gamma_0(p) = \left\{\gamma \in SL_2(\mathbf{Z}) \colon \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}, c \equiv 0 \pmod{p}\right\},$$

where $SL_2(\mathbf{Z})$ denotes the group of 2×2 matrices with integer coefficients and determinant 1. The group $\Gamma_0(p)$ acts on the upper half-plane H by fractional linear transformations, and the quotient space $\Gamma_0(p) \backslash H$ is a Riemann surface of finite type. Adding two cusps to $\Gamma_0(p) \backslash H$, we obtain a compact Riemann surface $X_0(p)$, which for $p \geq 23$ has genus ≥ 2. The location of the Weierstrass points on $X_0(p)$ is largely a mystery. For the known facts (including some known Weierstrass points), the reader may consult the papers of Atkin [1], Newman-Lehner [3], and Ogg [4], [5]. The point of departure of the present note is the remark (cf. [6]) that the Weierstrass points of $X_0(p)$ are essentially

Received November 12, 1982.
[1]Alfred P. Sloan Research Fellow.

the zeros of a certain modular form W for $\Gamma_0(p)$. This fact suggests that we should try to determine the modular form W more explicitly. The object of this note is to take a step in this direction by calculating W as a modular form mod p in the sense of Serre and Swinnerton-Dyer. As a corollary of the calculation we recover the theorem of Atkin (see [5]) that the cusps of $X_0(p)$ are not Weierstrass points. It should be noted, however, that this derivation of Atkin's theorem provides less information than the proof given by Ogg.

In this paper, a modular form for $\Gamma_0(p)$ of integral weight k is a holomorphic function f on H which satisfies

$$(cz+d)^{-k} f\left(\frac{az+b}{cz+d}\right) = f(z)$$

for every matrix

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(p),$$

and which has the property that $f(z)$ and $z^{-k}f(-1/z)$ are represented by absolutely convergent Fourier series of the form

$$f(z) = \sum_{n \geq 0} a(n) e^{2\pi i n z}$$

and

$$z^{-k} f(-1/z) = \sum_{n \geq 0} b(n) e^{2\pi i n z/p}$$

respectively. If $a(0)$ and $b(0)$ are both 0, then f is called a cusp form. For further facts and definitions pertaining to modular forms, the reader is referred to Shimura [8], Serre [7], and Swinnerton-Dyer [9].

1. Definition of W

Fix a prime p and let g be the genus of $X_0(p)$. We shall be concerned with a function W which we might call the Wronskian of $X_0(p)$. It is a modular form of weight $g(g+1)$ for $\Gamma_0(p)$ with the following properties:

(i) Given a basis $\{f_1, \ldots, f_g\}$ for the space of cusp forms of weight 2 on $\Gamma_0(p)$, put

$$W(f_1, \ldots, f_g)(z) = \begin{vmatrix} f_1(z) & \cdots & f_g(z) \\ \dfrac{df_1}{dz} & \cdots & \dfrac{df_g}{dz} \\ \cdot & \cdot & \cdot \\ \left(\dfrac{d}{dz}\right)^{g-1} f_1 & & \left(\dfrac{d}{dz}\right)^{g-1} f_g \end{vmatrix}.$$

Then $W(f_1, \ldots, f_g) = cW$ for some nonzero constant c.

(ii) The Fourier expansion of W at infinity has the form

$$\sum_{n \geq n_0} c(n) e^{2\pi i n z}$$

with $c(n_0) = 1$.

(iii) Let H^* denote the union of H and the two cusps of $\Gamma_0(p)$. The Weierstrass weight of a point of $X_0(p)$ represented by $z_0 \in H^*$ is the order of vanishing of $W(z)(dz)^{g(g+1)/2}$ at z_0, measured in a local parameter for $\Gamma_0(p)$ at z_0.

(iv) The Fourier coefficients $c(n)$ in (ii) are rational.

Properties (i) and (ii) constitute the definition of W. Indeed, (i) determines W up to multiplication by a nonzero constant, and the normalization (ii) makes W unique. Elementary rules of differentiation and properties of determinants then show that W is a modular form. As regards (iii), it is apparent from the definitions that the Weierstrass points of $X_0(p)$ are precisely the zeros of $W(z)(dz)^{g(g+1)/2}$. For a proof of the sharper statement given in (iii), and for detailed proofs of the other facts just mentioned, see [2, pp. 82–85]. All these results belong to the general theory of Riemann surfaces. Property (iv), by contrast, depends on the fact that the space of cusp forms of weight 2 for $\Gamma_0(p)$ has a basis consisting of forms with rational (or even integral) Fourier coefficients at ∞ [8, p. 85]. If $\{f_1, \ldots, f_g\}$ is such a basis, then the Fourier coefficients of $W(f_1, \ldots, f_g)$ are rational multiples of $(2\pi i)^{g(g-1)/2}$, whence the Fourier coefficients of W are rational.

Example. If $p = 23$, then $g = 2$, and the Weierstrass points of $X_0(23)$ are the six fixed points of the hyperelliptic involution of $X_0(23)$. The hyperelliptic involution is the automorphism of $X_0(23)$ induced by the map $z \mapsto -1/23z$ on H. Using these facts, one can show that

$$W = D^3 G,$$

where

$$D(z) = e^{2\pi i z} \prod_{n \geq 1} (1 - e^{2\pi i n z})(1 - e^{2\pi i 23 n z})$$

and

$$G(z) = 1 - 1/24 \sum_{n \geq 1} \left(\sum_{d \mid n} \left(\frac{d}{23} \right) \left(d^2 + 23(n/d)^2 \right) \right) e^{2\pi i n z}.$$

The functions D and G are modular forms of weight 1 and 3 respectively with Nebentypus character equal to the Legendre symbol (/23). (See [7, p. 231] for the definition of a modular form of Nebentypus.) The Fourier coefficients of D and of G are integral, hence so are those of W.

2. Calculation of W mod p

As is customary, we identify a modular form for $\Gamma_0(p)$ with a formal power series in an indeterminate q by putting

$$f = \sum_{n \geq 0} a(n) q^n$$

if

$$f(z) = \sum_{n \geq 0} a(n) e^{2\pi i n z}.$$

We let Δ denote the unique normalized cusp form of weight 12 for $SL_2(\mathbf{Z})$, and if k is an even integer ≥ 4, we let E_k be the normalized Eisenstein series of weight k for $SL_2(\mathbf{Z})$. Thus

$$\Delta = q \prod_{n \geq 1} (1 - q^n)^{24}$$

and

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

where B_k is the k-th Bernoulli number and $\sigma_t(n) = \sum_{d|n} d^t$. If

$$f = \sum_{n \geq 0} a(n) q^n \quad \text{and} \quad h = \sum_{n \geq 0} b(n) q^n$$

are modular forms with rational, p-integral Fourier coefficients at ∞, then we write $f \equiv h \pmod{p}$ to denote that $a(n) \equiv b(n) \pmod{p}$ for every n.

Henceforth we assume that $p \geq 23$. If we write $p + 1 = 12g + r$, then $r = 0$, 6, 8, or 14. We define E_0 to be 1.

THEOREM. *The Fourier coefficients of W are p-integral, and*

$$W \equiv \Delta^{g(g+1)/2} E_r^g E_{14}^{g(g-1)/2} \pmod{p}$$

Proof. Let M be the $\mathbf{Z}$-module of cusp forms of weight $p + 1$ for $SL_2(\mathbf{Z})$ with integral Fourier coefficients, and let N be the $\mathbf{Z}$-module of cusp forms of weight 2 for $\Gamma_0(p)$ with integral Fourier coefficients at ∞. Both M and N have rank g. The reduction map $\mathbf{Z}[[q]] \to \mathbf{Z}/p\mathbf{Z}[[q]]$ provides embeddings

$$M/pM \to \mathbf{Z}/p\mathbf{Z}[[q]] \quad \text{and} \quad N/pN \to \mathbf{Z}/p\mathbf{Z}[[q]],$$

and a theorem of Atkin and Serre ([7], p. 228) implies that M/pM and N/pN have the same image in $\mathbf{Z}/p\mathbf{Z}[[q]]$. It follows that if $\{F_1, \ldots, F_g\}$ is a basis for M over $\mathbf{Z}$, then there exists a basis $\{f_1, \ldots, f_g\}$ for N over $\mathbf{Z}$ such that

$$(2) \qquad F_j \equiv f_j \pmod p, \quad j = 1, \ldots, g.$$

If δ: $A \to A$ is a derivation of a commutative ring A and $h_1, \ldots, h_g$ are elements of A, we put

$$W_\delta(h_1, \ldots, h_g) = \begin{vmatrix} h_1 & \cdots & h_g \\ \delta h_1 & \cdots & \delta h_g \\ \cdot & \cdot & \cdot \\ \delta^{g-1} h_1 & \cdots & \delta^{g-1} h_g \end{vmatrix}.$$

In particular, consider Ramanujan's derivation θ: $\mathbf{C}[[q]] \to \mathbf{C}[[q]]$, given by $\theta = q d/dq$. If $\{f_1, \ldots, f_g\}$ is a $\mathbf{Z}$-basis for N as above, then

$$(2\pi i)^{-g(g-1)/2} W(f_1, \ldots, f_g) = W_\theta(f_1, \ldots, f_g),$$

because on modular forms, $d/dz = 2\pi i\theta$. Thus $cW = W_\theta(f_1, \ldots, f_g)$ for some $c \in \mathbf{Z}$, and by (2), we have

$$(3) \qquad cW \equiv W_\theta(F_1, \ldots, F_g) \pmod p.$$

Following Ramanujan, put $P = E_2$, where E_2 is the power series defined by formula (1) for $k = 2$ (this is not a modular form). Let ∂ be the derivation of the graded ring of modular forms for $SL_2(\mathbf{Z})$ which on a form of weight k is given by the formula

$$(4) \qquad \partial F = (12\theta - kP)F$$

(see [9, p. 20]). We claim that

$$(5) \qquad W_\partial(F_1, \ldots, F_g) = W_{12\theta}(F_1, \ldots, F_g),$$

i.e., that

$$(6) \qquad W_\partial(F_1, \ldots, F_g) = 12^{g(g-1)/2} W_\theta(F_1, \ldots, F_g).$$

To see this, first note that for $n \geq 0$ and any form F of weight k, we have

$$(7) \qquad \partial^n F = (12\theta)^n F + \sum_{m=0}^{n-1} h_m \theta^m F,$$

where h_m is a polynomial in $P, \theta P, \ldots, \theta^{m-1}P$ which depends on n and k but not on F. Indeed, (7) follows by induction from the Leibniz rule and formula (4). Putting $F = F_1, \ldots, F_g$ in (7) we see that the $(n+1)$-th row in the matrix defining $W_\partial(F_1, \ldots, F_g)$ is equal to the $(n+1)$-th row in the matrix defining $W_{12\theta}(F_1, \ldots, F_g)$ plus a linear combination of the preceding n rows in the latter matrix. Since a determinant is an alternating multilinear function of its rows, (5) follows, and therefore also (6). Combining (6) with the congruence (3), we see that for any $\mathbf{Z}$-basis $\{F_1, \ldots, F_g\}$ of M we have

$$(8) \qquad c'W \equiv W_\partial(F_1, \ldots, F_g) \pmod{p},$$

with $c' \in \mathbf{Z}$.

Now put

$$F_j = E_r E_4^{3(j-1)} \Delta^{g-j+1}, \quad 1 \le j \le g.$$

Then $\{F_1, \ldots, F_g\}$ is a $\mathbf{Z}$-basis for M, and we have

$$\partial^m F_j = \Delta^{g-j+1} \partial^m E_r E_4^{3(j-1)},$$

because $\partial\Delta = 0$. It follows that

$$W_\partial(F_1, \ldots, F_g) = \Delta^{g(g+1)/2} W_\partial(E_r, E_r S, \ldots, E_r S^{g-1})$$

with $S = E_4^3$. Now if $\delta\colon A \to A$ is any derivation of a commutative ring A and $h, h_1, \ldots, h_g$ are elements of A, then

$$(9) \qquad W_\delta(hh_1, \ldots, hh_g) = h^g W_\delta(h_1, \ldots, h_g)$$

(cf. [2, p. 82, equation 5.8.4]). Therefore

$$(10) \qquad W_\partial(F_1, \ldots, F_g) = \Delta^{g(g+1)/2} E_r^g W_\partial(1, S, \ldots, S^{g-1}).$$

To evaluate the right-hand side of (10), we note that

$$\begin{aligned} W_\partial(1, S, \ldots, S^{g-1}) &= W_\partial(\partial S, 2S\partial S, \ldots, (g-1)S^{g-2}\partial S) \\ &= (\partial S)^{g-1}(g-1)!\, W_\partial(1, S, \ldots, S^{g-2}), \end{aligned}$$

by (9). Applying induction, we obtain

$$W_\partial(1, S, \ldots, S^{g-1}) = \left(\prod_{j=1}^{g-1} j!\right)(\partial S)^{g(g-1)/2}.$$

Since $\partial S = 3E_4^2 \partial E_4 = -12E_4^2 E_6 = -12E_{14}$, substitution in (10) gives

$$W_\partial(F_1, \ldots, F_g) = c'' \Delta^{g(g+1)/2} E_r^g (E_{14})^{g(g-1)/2}$$

with

$$c'' = (-12)^{g(g-1)/2} \prod_{j=1}^{g-1} j!.$$

Now p does not divide c'', because $1 \leq g - 1 < 12g + r - 1 = p$. Thus the congruence (8) implies

$$c'(c'')^{-1} W \equiv \Delta^{g(g+1)/2} E_r^g E_{14}^{g(g-1)/2} \pmod{p}. \tag{11}$$

To complete the proof of the theorem, let q^{n_0} be the smallest power of $q = e^{2\pi iz}$ which occurs with a nonzero coefficient in the Fourier expansion of W at ∞ (cf. (ii) in the definition of W in Section 1). Making the substitutions $q = e^{2\pi iz}$, $dq/q = 2\pi i dz$, we see that

$$\operatorname{ord}_\infty W(z)(dz)^{g(g+1)/2} = n_0 - g(g+1)/2.$$

Thus the Weierstrass weight of the cusp ∞ is $n_0 - g(g+1)/2$; in particular, $n_0 \geq g(g+1)/2$. On the other hand, by (11), the coefficient of $q^{g(g+1)/2}$ in $c'(c'')^{-1}W$ is congruent to 1 $(\operatorname{mod} p)$, and is therefore not equal to 0. We conclude that n_0 is equal to $g(g+1)/2$ and that $c'(c'')^{-1}$ is congruent to 1 $(\operatorname{mod} p)$; the theorem now follows from (11). At the same time we have recovered Atkin's theorem that the cusp ∞ (hence also the conjugate cusp 0) is not a Weierstrass point of $X_0(p)$.

Finally, we remark that our congruence can be written in the more concise form

$$W \equiv \Phi_s^g \Phi_{26}^{g(g-1)/2} \pmod{p},$$

where $s = r + 12$ and Φ_j ($j = 12, 18, 20$, or 26) denotes the unique normalized cusp form for $SL_2(\mathbf{Z})$ of weight j.

References

1. A.O.L. Atkin, *Weierstrass points at cusps of* $\Gamma_0(N)$, Ann. of Math., vol. 85 (1967), pp. 42–45.
2. H.M. Farkas and I. Kra, *Riemann surfaces*, Graduate Texts in Math., vol. 71, Springer, New York, 1980.
3. J. Lehner and M. Newman, *Weierstrass points of* $\Gamma_0(N)$, Ann. of Math., vol. 79 (1964), pp. 360–368.
4. A.P. Ogg, *Hyperelliptic modular curves*, Bull. Soc. Math. France, vol. 102 (1974), pp. 449–462.
5. ______, *On the Weierstrass points of* $X_0(N)$, Illinois J. Math., vol. 22 (1978), pp. 31–35.

6. D.E. ROHRLICH, "Some remarks on Weierstrass points" in *Number theory related to Fermat's last theorem*, Birkhauser, Boston, 1982.
7. J.-P. SERRE, "Formes modulaires et fonctions zêta p-adiques" in *Modular functions of one variable III*, Lecture Notes in Math., vol. 350, Springer, New York, 1973.
8. G. SHIMURA, *Introduction to the arithmetic theory of automorphic functions*, Iwanami Shoten and Princeton University Press, Princeton, 1971.
9. H.P.F. SWINNERTON-DYER, "On l-adic representations and congruences for coefficients of modular forms" in *Modular functions of one variable III*, Lecture Notes in Math., vol. 350, Springer, New York, 1973.

RUTGERS UNIVERSITY
NEW BRUNSWICK, NEW JERSEY