VANISHING OF MODULAR FORMS AT INFINITY

SCOTT AHLGREN, NADIA MASRI, AND JEREMY ROUSE

Abstract. We give upper bounds for the maximal order of vanishing at ∞ of a modular form or cusp form of weight k on $\Gamma_0(Np)$ when $p \nmid N$ is prime. The results improve the upper bound given by the classical valence formula and the bound (in characteristic p) given by a theorem of Sturm. In many cases the bounds are sharp. As a corollary, we obtain a necessary condition for the existence of a non-zero form $f \in S_2(\Gamma_0(Np))$ with $\mathrm{ord}_\infty(f)$ larger than the genus of $X_0(Np)$. In particular, this gives a (non-geometric) proof of a theorem of Ogg, which asserts that ∞ is not a Weierstrass point on $X_0(Np)$ if $p \nmid N$ and $X_0(N)$ has genus zero.

1. Introduction and statement of results

Let $M_k(\Gamma_0(N))$ denote the complex vector space of holomorphic modular forms of weight k and level N, and let $S_k(\Gamma_0(N))$ denote the subspace of cusp forms (see, for example, [4] for background). If $f(z)$ is a non-zero element of $M_k(\Gamma_0(N))$, and $q := e^{2\pi i z}$, then f has a Fourier expansion at ∞ of the form

$$f(z) = \sum_{n=n_0}^{\infty} a(n)q^n \quad \text{with } a(n_0) \neq 0.$$

Given such a form f, we define

$$\mathrm{ord}_\infty(f) := n_0.$$

The following question is very natural:

> For a non-zero element $f \in M_k(\Gamma_0(N))$ (respectively $S_k(\Gamma_0(N))$, what is the largest possible value of $\mathrm{ord}_\infty(f)$?

For convenience, we define $\Gamma := \mathrm{SL}_2(\mathbb{Z})$. By the valence formula, we know that the total number of zeros of a non-zero element $f \in M_k(\Gamma_0(N))$ (counted in local coordinates in the usual way), is given by $\frac{k}{12}[\Gamma : \Gamma_0(N)]$ (see, for example, Chapter V of [12]). An element of $M_k(\Gamma_0(N))$ may (depending on the values of N and k) have forced vanishing at elliptic points. We denote by $\alpha(N, k)$ the number of zeros forced by this consideration, and by $\epsilon_\infty(N)$ the number of cusps of $\Gamma_0(N)$ (see (3.2), (3.4) for the precise definitions). Then we have

$$\begin{aligned} 0 \neq f \in M_k(\Gamma_0(N)) &\implies \mathrm{ord}_\infty(f) \leq \frac{k}{12}[\Gamma : \Gamma_0(N)] - \alpha(N, k), \\ 0 \neq f \in S_k(\Gamma_0(N)) &\implies \mathrm{ord}_\infty(f) \leq \frac{k}{12}[\Gamma : \Gamma_0(N)] - \alpha(N, k) - \epsilon_\infty(N) + 1. \end{aligned} \tag{1.1}$$

On the other hand, each of the spaces $M_k(\Gamma_0(N))$ and $S_k(\Gamma_0(N))$ has a basis consisting of forms with rational coefficients. Using this basis, one can construct an integral basis in

Date: April 4, 2008.
2000 *Mathematics Subject Classification.* 11F11, 11F33, 14H55.
The first author thanks the National Science Foundation for its support through grant DMS 01-34577.

"echelon form." To be precise, let d denote the dimension of the space in question. Then we have a basis of forms $\{f_1, \ldots, f_d\}$ with integer coefficients and with the property that

$$\begin{aligned} f_1(z) &= a_1 q^{c_1} + O(q^{c_1+1}) \\ f_2(z) &= a_2 q^{c_2} + O(q^{c_2+1}) \\ &\vdots \qquad\qquad \vdots \\ f_d(z) &= a_d q^{c_d} + O(q^{c_d+1}). \end{aligned} \tag{1.2}$$

Here each leading coefficient a_i is a non-zero integer, and $c_1 < c_2 < \cdots < c_d$. It is clear that the maximal order of vanishing at infinity of any non-zero form in the space is equal to c_d.

Denote the maximal order of vanishing of any non-zero form in $M_k(\Gamma_0(N))$ by $m_{N,k}$ and the maximal order of vanishing of any non-zero form in $S_k(\Gamma_0(N))$ by $s_{N,k}$. Using (1.1) and the above basis, we see that

$$\begin{aligned} \dim(M_k(\Gamma_0(N))) - 1 \leq m_{N,k} &\leq \frac{k}{12}[\Gamma : \Gamma_0(N)] - \alpha(N,k), \\ \dim(S_k(\Gamma_0(N))) \leq s_{N,k} &\leq \frac{k}{12}[\Gamma : \Gamma_0(N)] - \alpha(N,k) - \epsilon_\infty(N) + 1. \end{aligned} \tag{1.3}$$

It is possible to construct examples of spaces for which $m_{N,k}$ (respectively $s_{N,k}$) falls at either end of the allowable range. However, the exact value of these quantities is in general mysterious. For example, it is conjectured that if N is squarefree, then ∞ is not a Weierstrass point on the modular curve $X_0(N)$. Letting $g(N)$ denote the genus of $X_0(N)$, this is equivalent to the assertion that $s_{N,2} = \dim(S_2(\Gamma_0(N))) = g(N)$ for such N. This has been verified by William Stein for squarefree $N \leq 3223$. On the other hand, Lehner and Newman [9] and Atkin [1] proved that $s_{N,2} > \dim(S_2(\Gamma_0(N)))$ for many families of N which are not squarefree.

Using geometric arguments in characteristic p, Ogg [10] proved that ∞ is not a Weierstrass point on $X_0(Np)$ whenever $p \nmid N$ is prime and $X_0(N)$ has genus zero. Recently, Kohnen [8] and Kilger [7] have used techniques from the theory of modular forms mod p to reprove Ogg's result for certain curves $X_0(p\ell)$ when p and ℓ are distinct primes. As a corollary to our first theorem, we obtain a proof of Ogg's result which uses only standard facts from the theory of modular forms mod p.

To state the first result, when $p \mid\mid N$ we require the Atkin-Lehner involution W_p^N on $S_2(\Gamma_0(N))$ (see (3.5) below). For a power series $f = \sum a(n)q^n$ with rational coefficients and bounded denominators, we recall that $v_p(f) := \inf\{v_p(a(n))\}$. Then we have the following, which was proved for certain N of the form $p\ell$ by Kohnen and Kilger.

Theorem 1.1. *Suppose that $p \geq 5$ is a prime with $p \mid\mid N$ and that $f \in S_2(\Gamma_0(N)) \cap \mathbb{Q}[[q]]$ has $v_p(f) = 0$ and $v_p(f \big| W_p^N) \geq 0$. Then $\mathrm{ord}_\infty(f) \leq g(N)$.*

As an easy corollary, we obtain Ogg's result.

Corollary 1.2. *If p is a prime with $p \mid\mid N$, and $g(N/p) = 0$, then ∞ is not a Weierstrass point on $X_0(N)$.*

We now state the results for general weights. If $f \in M_k(\Gamma_0(N))$ then let $\alpha_2(N,k)$ and $\alpha_3(N,k)$ denote the number of complex zeros of f which are forced at the elliptic points of order 2 and 3 (see (3.3) for the precise values). We will consider levels N of the form $N = pN'$ where $p \geq 5$ is a prime with $p \nmid N'$. For such N, and for weights k which are sufficiently small relative to p, we obtain an improvement of the upper bounds in (1.3) for each of the quantities $m_{N,k}$ and $s_{N,k}$. We note that Theorem 4.2 gives a more precise statement for any particular form f.

Theorem 1.3. *Suppose that $k \geq 2$, that $p \geq k+3$ is prime, and that N is an integer with $p||N$. Suppose that $f(z) \in M_k(\Gamma_0(N))$ and that $f \neq 0$. Then we have*

$$\mathrm{ord}_\infty(f) \leq \frac{kp}{12} \cdot [\Gamma : \Gamma_0(N/p)] - \tfrac{1}{2}\alpha_2(N/p, kp) - \tfrac{1}{3}\alpha_3(N/p, kp).$$

Theorem 1.4. *Suppose that $k \geq 2$, that $p \geq \max(5, k+1)$ is prime, and that N is an integer with $p||N$. Suppose that $f(z) \in S_k(\Gamma_0(N))$ and that $f \neq 0$. Then we have*

$$\mathrm{ord}_\infty(f) \leq \frac{kp}{12} \cdot [\Gamma : \Gamma_0(N/p)] - \tfrac{1}{2}\alpha_2(N/p, kp) - \tfrac{1}{3}\alpha_3(N/p, kp) - \epsilon_\infty(N/p) + 1.$$

The bounds in these results are sharp for many spaces of forms. Let $\eta(z)$ be the usual Dedekind eta-function, defined by

$$\eta(z) := q^{\frac{1}{24}} \prod_{n=1}^{\infty}(1-q^n).$$

For one family of examples, define $f(z) \in M_4(\Gamma_0(15))$ by

$$f(z) := \frac{\eta(z) \cdot \eta^{15}(15z)}{\eta^3(3z) \cdot \eta^5(5z)} = q^8 + \cdots,$$

and if $p > 5$ is prime, then define $g(z) \in M_4(\Gamma_0(15p))$ by

$$g(z) := f(pz) = q^{8p} + \cdots \in M_4(\Gamma_0(15p)).$$

We have $\alpha(15p, 4) = 0$, so in this case the upper bound in (1.3) is $\frac{4}{12}[\Gamma : \Gamma_0(15p)] = 8p + 8$. We see that the actual order of vanishing matches the bound $\frac{4p}{12}[\Gamma : \Gamma_0(15)] = 8p$ provided by Theorem 1.3. Infinite families of related examples will be discussed in the last section.

We also remark that the hypothesis on the size of p is necessary. For example, in the space $M_6(\Gamma_0(35))$, there is a form whose q-expansion begins with $q^{21} + \cdots$. On the other hand, we have $\frac{6\cdot 7}{12}[\Gamma : \Gamma_0(5)] - \frac{1}{2}\alpha_2(5, 42) = 20$, from which we see that the conclusion does not hold when $p = 7$.

To see that Theorem 1.4 is sharp, consider the space $S_4(\Gamma_0(60))$. We have $\alpha(60, 4) = 0$ and $\epsilon_\infty(60) = 12$, so the upper bound provided by (1.3) is 37. On the other hand, we have $[\Gamma : \Gamma_0(12)] = 24$ and $\epsilon_\infty(12) = 6$, so the bound in Theorem 1.4 is $\frac{4\cdot 5}{12} \cdot 24 - 5 = 35$. In fact, there is a form in this space whose q-expansion is $q^{35} + \cdots$. More examples will be provided in the last section. Again, the assumption on p is necessary; to see this note that there is a form $f \in S_8(\Gamma_0(35))$ whose q-expansion is $f = q^{26} + \cdots$.

A computation using (1.1) shows that $s_{N,k}$ attains values in an interval, considered asymptotically with respect to N, of length $\frac{p+1}{12}[\Gamma : \Gamma_0(N/p)]$. Theorem 1.4 implies that $s_{N,k}$ lies in the narrower range

$$\dim(S_k(\Gamma_0(N))) \leq s_{N,k} \leq \frac{kp}{12}[\Gamma : \Gamma_0(N/p)] - \tfrac{1}{2}\alpha_2(N/p, kp) - \tfrac{1}{3}\alpha_3(N/p, kp) - \epsilon_\infty(\tfrac{N}{p}) + 1. \tag{1.4}$$

Considered asymptotically with respect to N, this interval has length $\frac{-k+p+1}{12}[\Gamma : \Gamma_0(N/p)]$. So the result of Theorem 1.4 is optimized when p is as close to k as possible. For example, when $k = 4$ and $p = 5$, then the length of the interval (1.4) is asymptotically one-third the length of the interval in (1.1).

The proofs of these results use techniques similar to those in [8], [7]. In order to prove these theorems, we will establish the analogous results in characteristic p. In particular, we give an improvement of a well-known theorem of Sturm on the maximal order of vanishing of a modular form in characteristic p. The tools involve facts on the integrality of modular forms, a modification of Sturm's original result to account for forced vanishing at the elliptic points, the trace map, the theory of modular forms mod p, and a recent result of Kilbourn [6] which, extending results of Deligne-Rapaport [3] and Weissauer [14] for weight 2, gives bounds for the p-adic valuation of the image of a cusp form $f \in S_k(\Gamma_0(N))$ under the Atkin-Lehner operator W_p^N. We begin in the next section by stating the characteristic p results and deducing from them Theorems 1.3 and 1.4. The following sections contain background material, the proof of the characteristic p results, and examples.

2. A result modulo p

If $f(z) = \sum_{n=0}^{\infty} a(n)q^n \in M_k(\Gamma_0(N)) \cap \mathbb{Q}[[q]]$ and p is prime, then define

$$v_p(f) := \inf\{v_p(a(n)\} \tag{2.1}$$

(this infimum exists by the principle of bounded denominators). If p is prime, then let $\mathbb{Z}_{(p)}$ denote the ring of p-integral rational numbers. If $f \in \mathbb{Z}_{(p)}[[q]]$, then we write $\overline{f}$ for its (coefficientwise) reduction modulo p, and if $v_p(f) = 0$ then we denote by $\text{ord}_\infty(\overline{f})$ the index of the first coefficient which does not vanish modulo p.

A well-known theorem of Sturm [13] gives bounds for the maximal order of vanishing of a modular form modulo p. Theorems 1.3 and 1.4 will follow from the next results, which improve Sturm's theorem in the cases under consideration.

Theorem 2.1. *Suppose that $k \geq 2$ is an even integer, that $p \geq k+3$ is prime, and that N is a positive integer with $p||N$. Suppose that $f(z) \in M_k(\Gamma_0(N)) \cap \mathbb{Z}_{(p)}[[q]]$ and that $f \not\equiv 0 \pmod p$. Then*

$$\text{ord}_\infty(\overline{f}) \leq \frac{kp}{12} \cdot [\Gamma : \Gamma_0(N/p)] - \tfrac{1}{2}\alpha_2(N/p, kp) - \tfrac{1}{3}\alpha_3(N/p, kp).$$

Theorem 2.2. *Suppose that $k \geq 2$ is an even integer, that $p \geq \max(5, k+1)$ is prime, and that N is a positive integer with $p||N$. Suppose that $f(z) \in S_k(\Gamma_0(N)) \cap \mathbb{Z}_{(p)}[[q]]$ and that $f \not\equiv 0 \pmod p$. Then*

$$\text{ord}_\infty(\overline{f}) \leq \frac{kp}{12} \cdot [\Gamma : \Gamma_0(N/p)] - \tfrac{1}{2}\alpha_2(N/p, kp) - \tfrac{1}{3}\alpha_3(N/p, kp) - \epsilon_\infty(N/p) + 1.$$

To deduce Theorem 1.3, we argue as follows. It suffices to prove the result for the form f_d in the basis (1.2). Assume without loss of generality that $v_p(f_d) = 0$. Since $\text{ord}_\infty(f_d) \leq \text{ord}_\infty(\overline{f}_d)$, Theorem 1.3 follows. Theorem 1.4 follows in the same manner. □

3. Preliminaries

We first recall the values of some of the quantities introduced in the first section. A good reference is thet table on p. 107 of the book of Diamond and Shurman [4]. We have

$$[\Gamma : \Gamma_0(N)] = N \prod_{p|N} (1 + \tfrac{1}{p}). \tag{3.1}$$

The number of cusps on $X_0(N)$ is given by

$$\epsilon_\infty(N) = \sum_{d|N} \phi(\gcd(d, N/d)). \tag{3.2}$$

Let $\epsilon_2(N)$, $\epsilon_3(N)$ denote the numbers of elliptic points of orders 2 and 3 on $X_0(N)$, respectively. Then we have

$$\epsilon_2(N) = \begin{cases} 0 & \text{if } 4 \mid N, \\ \prod_{p|N} \left(1 + \left(\frac{-4}{p}\right)\right) & \text{otherwise,} \end{cases}$$

$$\epsilon_3(N) = \begin{cases} 0 & \text{if } 9 \mid N, \\ \prod_{p|N} \left(1 + \left(\frac{-3}{p}\right)\right) & \text{otherwise.} \end{cases}$$

If $\alpha_2(N,k)$ and $\alpha_3(N,k)$ count the number of forced complex zeroes of a form $f \in M_k(\Gamma_0(N))$ at the elliptic points of order 2 and order 3 respectively, then

$$(\alpha_2(N,k), \alpha_3(N,k)) := \begin{cases} (\epsilon_2(N), 2\epsilon_3(N)) & \text{if } k \equiv 2 \pmod{12}, \\ (0, \epsilon_3(N)) & \text{if } k \equiv 4 \pmod{12}, \\ (\epsilon_2(N), 0) & \text{if } k \equiv 6 \pmod{12}, \\ (0, 2\epsilon_3(N)) & \text{if } k \equiv 8 \pmod{12}, \\ (\epsilon_2(N), \epsilon_3(N)) & \text{if } k \equiv 10 \pmod{12}, \\ (0,0) & \text{if } k \equiv 0 \pmod{12}. \end{cases} \tag{3.3}$$

Then the quantity $\alpha(N,k)$ used in the introduction is given by

$$\alpha(N,k) := \tfrac{1}{2}\alpha_2(N,k) + \tfrac{1}{3}\alpha_3(N,k). \tag{3.4}$$

We next recall some basic operators (a good reference is [2]). For any prime p, we define the linear operators U_p and V_p on Fourier expansions by

$$\left(\sum a(n)q^n\right) \big| U_p := \sum a(pn)q^n,$$
$$\left(\sum a(n)q^n\right) \big| V_p := \sum a(n)q^{pn}.$$

We will always assume that p is a prime with $p \mid\mid N$. For such primes, we define the Atkin-Lehner involution W_p^N on $M_k(\Gamma_0(N))$ by

$$f\big|_k W_p^N := f\big|_k \begin{pmatrix} pa & 1 \\ Nb & p \end{pmatrix} \tag{3.5}$$

where $a, b \in \mathbb{Z}$ and $p^2a - Nb = p$. We then have

$$f\big|_k W_p^N = p^{\frac{k}{2}} f\big|V_p \quad \text{for } f \in M_k(\Gamma_0(N/p)). \tag{3.6}$$

We recall also the trace operator

$$\mathrm{Tr}^N_{N/p} : M_k(\Gamma_0(N)) \to M_k(\Gamma_0(N/p))$$

defined by

$$\mathrm{Tr}^N_{N/p}(f) := f + p^{1-\frac{k}{2}} f\big|_k W_p^N \big| U_p. \tag{3.7}$$

The trace takes cusp forms to cusp forms. Finally, we define the familiar modular form

$$E^*_{p-1} := E_{p-1} - p^{p-1} E_{p-1}|V_p \in M_{p-1}(\Gamma_0(p)).$$

We have $E^*_{p-1} \equiv 1 \pmod{p}$ and

$$E^*_{p-1}|_{p-1} W_p^N \equiv 0 \pmod{p^{\frac{p+1}{2}}} \quad \text{for all } N \text{ with } p \mid\mid N. \tag{3.8}$$

We will make use of the following recent result of Kilbourn [6]. This generalizes the result of Weissauer [14] in the case of weight 2.

Theorem 3.1 (Kilbourn)**.** *Suppose that $f \in S_k(\Gamma_0(N)) \cap \mathbb{Q}[[q]]$ and that p is a prime with $p \mid\mid N$ and $p \geq \max(5, k+1)$. Then $|v_p(f|_k W_p^N) - v_p(f)| \leq \frac{k}{2}$.*

We also require a minor modification of this theorem for modular forms.

Theorem 3.2. *Suppose that $f \in M_k(\Gamma_0(N)) \cap \mathbb{Q}[[q]]$ and that p is a prime with $p \mid\mid N$ and $p \geq k+3$. Then $|v_p(f|_k W_p^N) - v_p(f)| \leq \frac{k}{2}$.*

In the case of prime level, this result is proven in [3], Proposition 3.20.

For the convenience of the reader, we will sketch Kilbourn's method as applied to Theorem 3.2. We seek a contradiction from the assumption (made without loss of generality after renormalization) that $f \in M_k(\Gamma_0(N)) \cap \mathbb{Z}_{(p)}[[q]]$ has $v_p(f) = 0$ and $v_p(f\big|_k W_p^N) \geq k/2 + 1$. Defining $h := \mathrm{Tr}^N_{N/p}(f) \in M_k(\Gamma_0(N/p))$, we find from (3.7) that $h \equiv f \pmod{p^2}$. Let $m := v_p(h - f) \geq 2$ and define $g := (h-f)/p^m \in M_k(\Gamma_0(N)) \cap \mathbb{Z}_{(p)}[[q]]$. Using the hypotheses and (3.6), it can be shown that $h|V_p \equiv p^{m-k/2} g\big|_k W_p^N \pmod{p}$. Defining

$$h' := \mathrm{Tr}^N_{N/p}(p^{m-k/2}(g\big|_k W_p^N)(E^*_{p-1})^{k-2}) \in M_{(k-2)p+2}(\Gamma_0(N/p)), \tag{3.9}$$

we find after a computation that $h' \equiv h|V_p \pmod{p}$.

If $F \in M_k(\Gamma_0(N/p)) \cap \mathbb{Z}_{(p)}[[q]]$, define

$$\omega(F) = \inf\{k : \text{ there exists } G \in M_k(\Gamma_0(N/p)) \cap \mathbb{Z}_{(p)}[[q]] \text{ with } F \equiv G \pmod{p}\}.$$

The theory of modular forms modulo p (see Section 4 of [5]) implies that $\omega(h') = \omega(h^p) = p\omega(h)$. Since $k \leq p-3$ and h is not identically zero, it follows that $\omega(h') = pk$, contradicting (3.9).

4. Proof of Theorem 2.1

We require a slight sharpening of Sturm's theorem [13]. We follow Sturm's proof, but take account of forced vanishing at the elliptic points.

Theorem 4.1. *Suppose that $k \geq 2$ is an even integer and that N is a positive integer. Suppose that $f(z) \in M_k(\Gamma_0(N)) \cap \mathbb{Z}_{(p)}[[q]]$ and that $f \not\equiv 0 \pmod{p}$. Then*

$$\mathrm{ord}_\infty(\overline{f}) \leq \frac{k}{12} \cdot [\Gamma : \Gamma_0(N)] - \tfrac{1}{3}\alpha_3(N,k) - \tfrac{1}{2}\alpha_2(N,k).$$

If in fact $f(z) \in S_k(\Gamma_0(N)) \cap \mathbb{Z}_{(p)}[[q]]$, then

$$\mathrm{ord}_\infty(\overline{f}) \leq \frac{k}{12} \cdot [\Gamma : \Gamma_0(N)] - \tfrac{1}{3}\alpha_3(N,k) - \tfrac{1}{2}\alpha_2(N,k) - \epsilon_\infty(N) + 1.$$

Proof. Define $m := [\Gamma : \Gamma_0(N)]$ and let γ_v, $v = 1, \ldots, m$ (where γ_1 is the identity) be the representatives of $\Gamma\backslash\Gamma_0(N)$. Following Sturm's argument, we fix a number field K containing the coefficients of each form $f\big|_k\gamma_v$, and denote by $\mathcal{O}$ the ring of integers of K. Let λ be any place above p. For each v, we find $A_v \in K^\times$ such that $v_\lambda(A_v f\big|_k\gamma_v) = 0$, and consider the form

$$G := f \prod_{v=2}^{m} A_v f\big|_k\gamma_v \in S_{km}(\Gamma).$$

Note that $G \not\equiv 0 \pmod{\lambda}$. For $h = 2, 3$, we see that for each complex zero of f at an elliptic fixed point of order h on a fundamental domain for $\Gamma_0(N)$, the function G has precisely one zero at an elliptic fixed point of order h on a fundamental domain for Γ. Since E_4 and E_6 have simple zeros at the points of order 3, 2 for Γ, we conclude that

$$G' := \frac{G}{E_4^{\alpha_3(N,k)} E_6^{\alpha_2(N,k)}} \in S_{km-4\alpha_3(N,k)-6\alpha_2(N,k)}(\Gamma).$$

Since f is a cusp form, we see that for each $v \geq 2$, we have an expansion of the form

$$A_v f\big|_k\gamma_v = c_v q^{1/h_v} + \cdots,$$

where h_v is the width of the cusp corresponding to γ_v. Since each such cusp corresponds to exactly h_v of the elements γ_v, we conclude that G' vanishes mod λ at ∞ to order at least

$$\mathrm{ord}_\lambda(\overline{f}) + \epsilon_\infty(N) - 1.$$

By Sturm's result in level one, this quantity is at most one-twelfth the weight of G', which gives the theorem for cusp forms. The proof for modular forms is the same. □

We will now prove the following.

Theorem 4.2. *Suppose that N and k are positive integers and that $p \geq 5$ is a prime with $p \mid\mid N$. Suppose that $f \in M_k(\Gamma_0(N)) \cap \mathbb{Z}_{(p)}[[q]]$ has*

$$v_p(f) = 0, \quad v_p(f\big|_k W_p^N) \geq a.$$

(1) *If $p \geq k + 3$, then*

$$\mathrm{ord}_\infty(\overline{f}) \leq \frac{k + (\frac{k}{2} - a)(p-1)}{12}[\Gamma : \Gamma_0(N/p)] - \tfrac{1}{3}\alpha_2(N/p, k + (\tfrac{k}{2} - a)(p-1)) - \tfrac{1}{2}\alpha_3(N/p, k + (\tfrac{k}{2} - a)(p-1)).$$

(2) *If $p \geq k + 1$ and $f \in S_k(\Gamma_0(N))$, then*

$$\mathrm{ord}_\infty(\overline{f}) \leq \frac{k + (\frac{k}{2} - a)(p-1)}{12}[\Gamma : \Gamma_0(N/p)] - \tfrac{1}{3}\alpha_2(N/p, k + (\tfrac{k}{2} - a)(p-1)) - \tfrac{1}{2}\alpha_3(N/p, k + (\tfrac{k}{2} - a)(p-1)) - \epsilon_\infty(N/p) + 1.$$

Theorems 2.1 and 2.2 follow immediately since by Theorems 3.1 and 3.2 we have $a \geq -k/2$ in each case.

Proof of Theorem 4.2. Let f be as in the hypotheses of the first part. Then consider the form

$$F := \mathrm{Tr}^N_{N/p}\left(f(E^*_{p-1})^{\frac{k}{2}-a}\right)$$
$$= f(E^*_{p-1})^{\frac{k}{2}-a} + p^{1-\frac{k+(\frac{k}{2}-a)(p-1)}{2}}\left(f\big|_k W^N_p \cdot (E^*_{p-1})^{\frac{k}{2}-a}\big|_{(p-1)(\frac{k}{2}-a)} W^N_p\right)\big|U_p.$$

Then $F \in M_{k+(\frac{k}{2}-a)(p-1)}(\Gamma_0(N/p)) \cap \mathbb{Q}[[q]]$. Moreover, a computation using (3.8) shows that we have $F \equiv f \pmod{p}$. By Theorem 4.1 we conclude that

$$\mathrm{ord}_\infty(\overline{f}) = \mathrm{ord}_\infty(\overline{F}) \le \frac{k+(\frac{k}{2}-a)(p-1)}{12}[\Gamma : \Gamma_0(N/p)]$$
$$- \tfrac{1}{3}\alpha_2(N/p,\, k+(\tfrac{k}{2}-a)(p-1)) - \tfrac{1}{2}\alpha_3(N/p,\, k+(\tfrac{k}{2}-a)(p-1)).$$

The second assertion follows in a similar manner. □

Finally, we prove Theorem 1.1. If $f \in S_2(\Gamma_0(N))$ is as in the hypothesis, then, taking $k = 2$ and $a = 0$ in Theorem 4.2, we find that

$$\mathrm{ord}_\infty(\overline{f}) \le \frac{p+1}{12}[\Gamma : \Gamma_0(N/p)] - \epsilon_\infty(N/p) - \tfrac{1}{2}\alpha_2(N/p, p+1) - \tfrac{1}{3}\alpha_3(N/p, p+1) + 1.$$

A computation shows that we have $\alpha_2(N/p, p+1) = \frac{1}{2}\epsilon_2(N)$, $\alpha_3(N/p, p+1) = \epsilon_3(N)$, and $\epsilon_\infty(N/p) = \frac{1}{2}\epsilon_\infty(N)$. Thus,

$$\mathrm{ord}_\infty(\overline{f}) \le \frac{[\Gamma : \Gamma_0(N)]}{12} - \tfrac{1}{2}\epsilon_\infty(N) - \tfrac{1}{4}\epsilon_2(N) - \tfrac{1}{3}\epsilon_3(N) + 1.$$

The right hand side is precisely the genus of $X_0(N)$, which proves Theorem 1.1.

Corollary 1.2 can be checked explicitly when $p = 2, 3$. For other primes, we note that if $g(N/p) = 0$ and $f \in S_2(\Gamma_0(N)) \cap \mathbb{Z}_{(p)}[[q]]$, then $\mathrm{Tr}^N_{N/p}(f\big|W^N_p) = 0$, so that we must have $v_p(f\big|W^N_p) = v_p(f\big|U_p) \ge 0$.

5. Examples

We provide more examples of spaces for which Theorems 1.3 and 1.4 are sharp. Let $N' \ge 1$ be a squarefree integer. Define the form

$$f_{N'}(z) := \left(\prod_{d|N'} \eta(dz)^{\mu(N'/d)d}\right)^\alpha,$$

where $\mu(n)$ is the Möbius function and

$$\alpha := \begin{cases} 24 & \text{if } N' = 1,\\ 8 & \text{if } N' = 2,\\ 6 & \text{if } N' = 3,\\ 2 & \text{if } N' = 6,\ p, \text{ or } 2p \text{ where } p \ge 5 \text{ is prime},\\ 1 & \text{otherwise.}\end{cases}$$

Set

$$k := \frac{\alpha\phi(N')}{2}.$$

Using standard criteria (a convenient reference is Section 1.4 of [11]) it can be checked that $f_{N'}(z) \in M_k(\Gamma_0(N'))$ and that

$$\mathrm{ord}_\infty(f_{N'}(z)) = \frac{\alpha\phi(N')\sigma_1(N')}{24} = \frac{k}{12}[\Gamma : \Gamma_0(N')].$$

If N' is not squarefree then write $N' = N_1 N_2$ where N_1 is the largest squarefree divisor of N'. Then define the form $f_{N'}(z) := f_{N_1}(z)|V_{N_2} \in M_{\alpha\phi(N_1)/2}(\Gamma_0(N'))$.

For all $N' \geq 1$ it follows that

$$\mathrm{ord}_\infty(f_{N'}(z)) = \frac{k}{12}[\Gamma : \Gamma_0(N')]. \tag{5.1}$$

If $p \geq k+3$, let $N = pN'$. Theorem 1.3 asserts that each non-zero form $f \in M_k(\Gamma_0(N))$ has

$$\mathrm{ord}_\infty(f) \leq \frac{kp}{12}[\Gamma : \Gamma_0(N)]. \tag{5.2}$$

We see from (5.1) that equality holds in (5.2) for the form $f_{N'}(pz) \in M_k(\Gamma_0(N))$. Therefore Theorem 1.3 is sharp for these spaces.

We turn to Theorem 1.4. Suppose that $k \geq 2$, and that $p \geq 12k+1$ is prime. Then the order of vanishing of the form $F(z) := \Delta(pz)^k = q^{kp} + \cdots \in S_{12k}(\Gamma_0(p))$ agrees with the upper bound provided by Theorem 1.4.

There are other examples where Theorem 1.4 is sharp. For example, define

$$F(z) := \frac{\eta(6z)\eta(9z)\eta^6(21z)\eta^{34}(126z)}{\eta^2(18z)\eta^{11}(42z)\eta^{17}(63z)} \in S_6(\Gamma_0(126)).$$

Then we have $\alpha_2(18,42)/2 = \alpha_3(18,42)/3 = 0$ and

$$\mathrm{ord}_\infty(F) = 119 = \frac{6\cdot 7}{12}[\Gamma : \Gamma_0(18)] - \epsilon_\infty(18) + 1.$$

Another example is provided by the form

$$F = 2q^{99} + 2q^{101} - 3q^{104} + \cdots \in S_6(\Gamma_0(175)).$$

Then, $\alpha_2(25,42)/2 = 1$, $\alpha_3(25,42)/3 = 0$ and

$$\mathrm{ord}_\infty(F) = 99 = \frac{6\cdot 7}{12}[\Gamma : \Gamma_0(25)] - \alpha_2(25,42)/2 - \alpha_3(25,42)/3 - \epsilon_\infty(25) + 1.$$

In closing, we mention several other forms for which equality holds in Theorem 1.4 (there are other examples of the same sort). For example, this occurs for the following forms:

$$\frac{\eta(z)\eta^{13}(77z)}{\eta(7z)\eta(11z)} \in S_6(\Gamma_0(77)),$$
$$\frac{\eta^{30}(44z)\eta^2(2z)}{\eta^2(4z)\eta^{14}(22z)} \in S_8(\Gamma_0(44)),$$
$$\frac{\eta^{29}(99z)\eta(3z)}{\eta^9(33z)\eta(9z)} \in S_{10}(\Gamma_0(99)),$$
$$\frac{\eta^{47}(46z)\eta(z)}{\eta^{23}(23z)\eta(2z)} \in S_{12}(\Gamma_0(46)).$$

References

[1] A. O. L. Atkin. Weierstrass points at cusps of $\Gamma_0(n)$. *Ann. of Math. (2)*, 85:42–45, 1967.

[2] A. O. L. Atkin and J. Lehner. Hecke operators on $\Gamma_0(m)$. *Math. Ann.*, 185:134–160, 1970.

[3] P. Deligne and M. Rapoport. Les schémas de modules de courbes elliptiques. In *Modular functions of one variable, II (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972)*, pages 143–316. Lecture Notes in Math., Vol. 349. Springer, Berlin, 1973.

[4] Fred Diamond and Jerry Shurman. *A first course in modular forms*, volume 228 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2005.

[5] Benedict H. Gross. A tameness criterion for Galois representations associated to modular forms (mod p). *Duke Math. J.*, 61(2):445–517, 1990.

[6] Tim Kilbourn. Congruence properties of Fourier coefficients of modular forms. Preprint.

[7] Kilian Kilger. Weierstrass points on $X_0(p\ell)$ and arithmetic properties of Fourier coffficients of cusp forms. *Ramanujan J.*

[8] Winfried Kohnen. A short remark on Weierstrass points at infinity on $X_0(N)$. *Monatsh. Math.*, 143(2):163–167, 2004.

[9] J. Lehner and M. Newman. Weierstrass points of $\Gamma_0\,(n)$. *Ann. of Math. (2)*, 79:360–368, 1964.

[10] A. P. Ogg. On the Weierstrass points of $X_0(N)$. *Illinois J. Math.*, 22(1):31–35, 1978.

[11] Ken Ono. *The web of modularity: arithmetic of the coefficients of modular forms and q-series*, volume 102 of *CBMS Regional Conference Series in Mathematics*. Published for the Conference Board of the Mathematical Sciences, Washington, DC, 2004.

[12] Bruno Schoeneberg. *Elliptic modular functions: an introduction*. Springer-Verlag, New York, 1974. Translated from the German by J. R. Smart and E. A. Schwandt, Die Grundlehren der mathematischen Wissenschaften, Band 203.

[13] Jacob Sturm. On the congruence of modular forms. In *Number theory (New York, 1984–1985)*, volume 1240 of *Lecture Notes in Math.*, pages 275–280. Springer, Berlin, 1987.

[14] R. Weissauer. Integral forms on $\Gamma_0\,(pn)$. Preprint (2002).

Department of Mathematics, University of Illinois, Urbana, IL 61801

E-mail address: ahlgren@math.uiuc.edu

E-mail address: nmasri@math.uiuc.edu

E-mail address: jarouse@math.uiuc.edu