Vincent *Research in the Mathematical Sciences* (2015) 2:10
DOI 10.1186/s40687-015-0026-9

Research in the Mathematical Sciences
a SpringerOpen Journal

RESEARCH Open Access

Weierstrass points on the Drinfeld modular curve $X_0(\mathfrak{p})$

Christelle Vincent

Correspondence:
cvincent@stanford.edu
Stanford University, Department of Mathematics, 450 Serra Mall; Building 380, Stanford, CA 94305, USA

Abstract

Consider the Drinfeld modular curve $X_0(\mathfrak{p})$ for $\mathfrak{p}$ a prime ideal of $\mathbb{F}_q[T]$. It was previously known that if j is the j-invariant of a Weierstrass point of $X_0(\mathfrak{p})$, then the reduction of j modulo $\mathfrak{p}$ is a supersingular j-invariant. In this paper, we show the converse: Every supersingular j-invariant is the reduction modulo $\mathfrak{p}$ of the j-invariant of a Weierstrass point of $X_0(\mathfrak{p})$.

Introduction and statement of results

Given a smooth irreducible projective curve of genus $g \geq 2$ defined over an algebraically closed field of characteristic 0, we say that a point P on X is a *Weierstrass point* if there is a nonzero rational function F on X with a pole of order less than or equal to g at P and regular everywhere else. In this case, the set of such points is non-empty and finite.

Because of the geometric significance of such points, given a curve of arithmetic import, it is natural to study its Weierstrass points. Such work was done by Atkin, Hasse, Lehner and Newman, Ogg, Petersson, and Schoeneberg for three families that are important to number theorists: the Fermat curves and the modular curves $X(N)$ and $X_0(N)$. The interested reader should see Rohrlich's 1982 paper [24] for a concise account of the results and complete references. In the same paper, Rohrlich exhibited a modular form $W(z)$ for $\Gamma_0(N)$ whose divisor encodes information about the Weierstrass points of $X_0(N)$, the modular Wronskian. In later work [25], restricting his attention to $\Gamma_0(\ell)$ for ℓ a prime, he was able to exhibit a form for $\mathrm{SL}_2(\mathbb{Z})$ congruent to $W(z)$ modulo ℓ. Building on these results, later work of Ahlgren and Ono [1] showed that not only were the elliptic curves underlying the Weierstrass points of $X_0(\ell)$ supersingular at ℓ, which was a result already obtained by Ogg [23], but furthermore that

$$\prod_{Q \in X_0(\ell)} (x - j(Q))^{\mathrm{wt}(Q)} \equiv \prod_{\substack{E/\overline{\mathbb{F}}_\ell \\ E \text{ supersingular}}} (x - j(E))^{g_\ell(g_\ell - 1)} \pmod{\ell},$$

where the quantity $\mathrm{wt}(Q)$ is a non-negative integer which is positive if and only if Q is a Weierstrass point and which we will define in Section 'Weierstrass points on $X_0(\mathfrak{p})$', Definition 7, and g_ℓ is the genus of $X_0(\ell)$.

The situation where the curve is defined over an algebraically closed field of positive characteristic is more complicated: It can be the case that for each point P, there exists a nonzero rational function with a pole of order less than or equal to the genus of the curve at P and regular elsewhere. Accordingly, to ensure that the set of Weierstrass points be finite, a modified definition of Weierstrass points must be used, which will be given in Section 'Weierstrass points in characteristic p'.

We consider in this paper the so-called Drinfeld setting, which offers for function fields some structures playing roles analogous to those played by elliptic curves, modular forms, and modular curves for number fields. More precisely, we will study the Weierstrass points on a family of Drinfeld modular curves which is denoted by $X_0(\mathfrak{p})$, where $\mathfrak{p}$ is a prime ideal of $\mathbb{F}_q[T]$. These curves are smooth, irreducible, and projective and defined over a complete, algebraically closed field of positive characteristic. As such, it is natural to wish to study their Weierstrass points. Since they are (coarse) moduli spaces of Drinfeld modules of rank 2 with a specified level structure, we may ask what can be said about the Drinfeld modules underlying the Weierstrass points of $X_0(\mathfrak{p})$.

As far as we can tell, the only result in this direction which was known previously was obtained by Baker [3] as a result of his work on the connection between linear systems on a curve and linear systems on the dual graph of a regular semistable model of the curve. As a corollary of one of his results, one can show that the Drinfeld modules underlying the Weierstrass points of $X_0(\mathfrak{p})$ have supersingular reduction at $\mathfrak{p}$.

In this paper, we prove a converse of Baker's result:

Theorem 1. *Let q be odd and let $\pi(T) \in \mathbb{F}_q[T]$ be a prime polynomial, generating the prime ideal $\mathfrak{p}$. Then each supersingular Drinfeld module over $\overline{\mathbb{F}}_{\mathfrak{p}}$ is the reduction modulo $\mathfrak{p}$ of a Weierstrass point of $X_0(\mathfrak{p})$.*

To obtain this theorem, we first introduce the necessary concepts and objects to define a form $W(z)$ analogous to the form defined by Rohrlich in [24]. By this, we mean that the divisor of $W(z)$ captures information about the Weierstrass points of $X_0(\mathfrak{p})$, and the u-series coefficients of $W(z)$ at the cusp ∞ are rational and $\mathfrak{p}$-integral. It is the study of this form, using the main theorems of [30], that allows us to use a powerful theorem on the arithmetic of the reduction of Drinfeld modular forms modulo a prime ideal $\mathfrak{p}$ and obtain Theorem 1.

Remark 1. The hypothesis that q be odd in our main theorem is a consequence of Theorem 11, in which we show that $W(z)$ is an eigenform of the Fricke involution in odd characteristic. In turn, this hypothesis is necessary to apply one of the theorems of [30] (repeated here as Theorem 5). We expect that $W(z)$ is an eigenform of the Fricke involution in even characteristic as well, but the argument in this case would most likely rely on some geometric property of $W(z)$ on $X_0(\mathfrak{p})$ instead of the argument we present here. Granting this hypothesis, the proof of Theorem 1 would carry through for $q > 2$. The exclusion of the case $q = 2$ would now come from the other main theorem of [30] (repeated here as Theorem 4); see the remark following the proof of Theorem 1.1 in [30] for a discussion of how this restriction arises.

In Section 'A special case', we show that when $q = p$ is an odd prime and $\pi(T)$ has degree 3, we can perform some explicit computations to obtain that

Theorem 2. *If p is odd, $\pi(T) \in \mathbb{F}_p[T]$ has degree 3, $\mathfrak{p}$ is the ideal generated by $\pi(T)$, and the modular Wronskian on $X_0(\mathfrak{p})$ is denoted by $W(z)$, then*

$$W(z) \equiv (-1)^{(p+1)/2} g^{\frac{p^2(p-1)}{2}} h^{\frac{p^2(p+1)}{2}} \pmod{\mathfrak{p}}.$$

Here, g and h are explicit Drinfeld modular forms which will be defined in Section 'The Drinfeld setting'. Theorem 2 is an analogue of a result obtained by Rorhlich in [25]. This explicit computation allows us to show that

Theorem 3. *If p is odd, $\pi(T) \in \mathbb{F}_p[T]$ has degree 3, and $\mathfrak{p}$ is the ideal generated by $\pi(T)$, then we have*

$$\prod_{P \in Y_0(\mathfrak{p})} (x - j(P))^{wt(P)} \equiv \prod_{\substack{\phi/\overline{\mathbb{F}}_{\mathfrak{p}} \\ \phi \text{ supersingular}}} (x - j(\phi))^{g_{\mathfrak{p}}(g_{\mathfrak{p}}-1)} \pmod{\mathfrak{p}},$$

where $g_{\mathfrak{p}}$ is the genus of the curve $X_0(\mathfrak{p})$ and $wt(P)$ is given in Definition 7.

This is an analogue of the formula from [1] quoted earlier.

The structure of the paper is the following: We begin by reviewing the theory of Weierstrass points in positive characteristic in Section 'Weierstrass points in characteristic p'. Then, we introduce the basic objects from the Drinfeld setting that we will need in Section 'The Drinfeld setting'. Section 'The Drinfeld setting' contains as well all of the statements of the results from the theory of Drinfeld modular forms that we will cite. In Section 'Hyperderivatives and quasimodular forms', we introduce Drinfeld quasimodular forms and some differentials operators that are needed in the definition of the Drinfeld modular form $W(z)$. We also prove some elementary results concerning the action of these operators on Drinfeld modular forms. The definition of $W(z)$ is finally given in Section 'Weierstrass points on $\boldsymbol{X_0(\mathfrak{p})}$', along with the properties of this form. Then, the meat of the proof of Theorem 1 is in Section 'Proof of Theorem 1' where we apply the machinery developed in the previous sections to the form $W(z)$. Finally, in Section 'The order of vanishing of $\boldsymbol{W(z)}$ at the cusps', we briefly consider the order of vanishing of $W(z)$ at ∞ and establish a result needed to study the special case which yields Theorems 2 and 3. The proofs of these last two theorems are then given in Section 'A special case'.

Weierstrass points in characteristic *p*

Since the theory of Weierstrass points in positive characteristic p is much less well known than the theory in characteristic 0, we begin with a short review of the facts we will need, based on the treatment in [27] and [17]. In particular, proofs of all facts that are stated here without proof can be found in [17].

For the duration of this section only, let k be an algebraically closed field and X a smooth projective irreducible curve over k of genus $g \geq 2$ with function field $k(X)$. A natural question to ask about X is the following: For P a point of X and n a positive integer, does there exist a nonzero rational function F on X such that F has a pole of order exactly n at P and F is regular elsewhere? If the answer to this question is negative, we say that n is a *gap* at P; otherwise n is a *pole number* at P. It is a fact that for a point P on X, there are exactly g gaps at P, and if $n_1(P), \ldots, n_g(P)$ are the gaps at P, indexed such that $n_i(P) < n_j(P)$ if $i < j$, we say that $(n_1(P), \ldots, n_g(P))$ is the gap sequence at P.

For a fixed curve X, it can be shown that there exists a sequence of positive integers $(n_1, \ldots, n_g)$ with $n_i < n_j$ if $i < j$ such that $(n_1, \ldots, n_g)$ is the gap sequence for all but finitely many points of X. We call this sequence the *canonical gap sequence* of X. There exist on X finitely many points that have a different gap sequence, and they are called the *Weierstrass points* of X. If $(n_1, \ldots, n_g)$ is the canonical gap sequence of X and $(n_1(P), \ldots, n_g(P))$ is the gap sequence at P for any point P of X, then $n_i \leq n_i(P)$ for each i.

Remark 2. We exclude the case of $g = 0$ since in that case for any point P, there is a nonzero rational function F on X such that F has a single pole at P and is regular elsewhere. There are therefore no Weierstrass points. We also exclude the case of $g = 1$ since in that case, there are no points P with a pole number of 1 (the existence of such a point would force $g = 0$, a contradiction) and for each P on X, there is a nonzero rational function F on X such that F has a double pole at P and is regular elsewhere. There are therefore again no Weierstrass points.

For any point P on X, a measure of how its gap sequence differs from the canonical gap sequence is given by the quantity

$$\sum_{i=1}^{g}(n_i(P) - n_i),$$

which is positive if and only if P is a Weierstrass point.

If X is defined over a field of characteristic 0, then the canonical gap sequence is always $(1, \ldots, g)$. When k is of characteristic $p > 0$ and X has canonical gap sequence $(1, \ldots, g)$, we say that X has a *classical* canonical gap sequence, or a classical canonical linear system (this designation will be justified shortly when we define the canonical orders of X).

Example 1. Let X be a hyperelliptic curve of genus $g \geq 2$, then its canonical gap sequence is $(1, \ldots, g)$. (In characteristic $p > 0$ this is a theorem that was implicit in [19] and stated explicitly in the seminal work of Schmidt [26] defining Weierstrass points in positive characteristic.) Furthermore, the Weierstrass points of X are exactly the branch points of f, where $f : X \to \mathbb{P}^1$ is any separable degree 2 morphism. At such a branch point P, the rational function $F = \frac{1}{f - f(P)}$ has a double pole at P and is regular elsewhere, and so at the Weierstrass points the gap sequence is $(1, 3, \ldots, 2g - 1)$.

Example 2. The projective curve of genus 3 given by $X_0^4 + X_1^4 + X_2^4 = 0$ over $\overline{\mathbb{F}}_3$ does not have a classical gap sequence. On this curve, for each point P one can construct a nonzero rational function having a pole of order ≤ 3 at P and regular elsewhere.

Because of the difficulty of computing the gap sequence of a point directly, it is often more convenient to consider a related sequence of strictly increasing positive integers $(j_1, \ldots, j_{g-1})$ called the *canonical orders* of X, which we now describe. For any element $x \in k(X)$, we will write $[x]$ for the divisor of x, $\sum_P v_P(x)P$, where the sum is taken over all points P of X. As usual, for any divisor D on X, we may define the linear system

$$L(D) = \left\{x \in k(X)^\times : [x] \geq -D\right\} \cup \{0\}.$$

We further denote by Ω_X the space of (algebraic) meromorphic differential forms on X. Because X is defined over an algebraically closed field, we have a canonical isomorphism between Ω_X and the space of Weil differentials W_X (in fact, to obtain this isomorphism, it would suffice here to require that $k' \otimes k(X)$ be a field for all finite extensions k' of k). This allows us to define the divisor $[\,\omega]$ of ω a meromorphic differential on X. We do this in the following manner: Let $\mathbb{A}_{k(X)}$ denote the ring of adèles of $k(X)$ and for D a divisor on X, write

$$\mathbb{A}_{k(X)}(D) \overset{\text{def}}{=} \left\{\alpha = (\alpha_P) \in \mathbb{A}_{k(X)} \mid \nu_P(\alpha_P) \geq -\nu_P(D) \text{ for all points } P \text{ of } X\right\}.$$

Then, a Weil differential on X is a k-linear functional with domain $\mathbb{A}_{k(X)}$ that vanishes on $\mathbb{A}_{k(X)}(D)+k(X)$ for some divisor D. For each Weil differential ω^*, there is a unique divisor D of maximum degree such that ω^* vanishes on $\mathbb{A}_{k(X)}(D)+k(X)$, and we define $[\,\omega^*] \overset{\text{def}}{=} D$. Then if ω corresponds to ω^* under the canonical isomorphism between Weil differentials and meromorphic differentials, we simply write $[\,\omega] = [\,\omega^*]$ and $\nu_P(\omega) = \nu_P([\,\omega]\,)$. One pleasant consequence of this definition is that for $x \in k(X)$ and $\omega \in \Omega_X$ we have $[\,x\omega] = [\,x] + [\,\omega]$. If ω is a meromorphic differential on X, its divisor C is called a *canonical divisor* on X, and since any two meromorphic differentials differ by a function, any two canonical divisors are linearly equivalent.

For a point P of X, consider the following sequence of spaces:

$$k = L(0) \subseteq L(P) \subseteq L(2P) \subseteq L(3P) \subseteq \dots$$

Then, we have that n is a gap at P if and only if $L((n-1)P) = L(nP)$. By the Riemann-Roch theorem, we have that for any positive integer n and any point P,

$$\dim L(nP) = n - g + 1 + \dim L(C - nP),$$

from which it follows that

$$\dim L((n+1)P)/L(nP) = 1 - \dim L(C - nP)/L(C - (n+1)P).$$

Writing $L_C(nP) = L(C - nP)$, this last equation justifies our interest in the *(canonical) osculating filtration* at P:

$$L(C) = L_C(0) \supseteq L_C(P) \supseteq L_C(2P) \supseteq L_C(3P) \supseteq \dots$$

Indeed, for a positive integer n, $n+1$ is a gap at P if and only if $L_C(nP) \supsetneq L_C((n+1)P)$. In turn, this implies the existence of a nonzero $F \in L(C)$ such that $\nu_P(F) = n - \nu_P(C)$. Whenever such a function exists, we say that n is a *canonical order* at P. The definition of the canonical orders at P does not depend on the choice of canonical divisor C: if n is a canonical order at P and C' is any canonical divisor, there will exist a nonzero $F' \in L(C')$ such that $\nu_P(F') = n - \nu_P(C')$.

From the discussion above, it follows that for a positive integer n, n is a canonical order at P if and only if $n+1$ is a gap at P. (We note that since X is a curve over an algebraically closed field, the existence of a point P such that 1 is a pole number at P implies that X has genus zero. Therefore in our case, 1 will always be a gap for any point P on X since we restrict our attention to curves of genus greater than or equal to 2, but we do not say that 0 is a canonical order.) As was the case for gap sequences, all but finitely many points of X have the same canonical orders, and we call the strictly increasing sequence of positive integers $(j_1, \dots, j_{g-1})$ formed by these integers the *canonical orders* of X.

If $(j_1, \ldots, j_{g-1})$ are the canonical orders of X and $(j_1(P), \ldots, j_{g-1}(P))$ are the canonical orders at P for any point P of X, then again $j_i \leq j_i(P)$ for each i. Furthermore if as before $(n_1, \ldots, n_g)$ is the canonical gap sequence of X and $(n_1(P), \ldots, n_g(P))$ is the gap sequence at P, then

$$\sum_{i=1}^{g}(n_i(P) - n_i) = \sum_{i=1}^{g-1}(j_i(P) - j_i).$$

The point P is called an *osculation point* of X if $j_{g-1}(P) > g - 1$. In particular, an osculation point has at least one pole number that is less than or equal to g. If X has a classical gap sequence, then the osculation points and the Weierstrass points of X exactly coincide. Otherwise, every point of X is an osculation point.

An important tool in the study of Weierstrass points is a divisor w on X, whose construction is due to Stöhr and Voloch [27]. This divisor has the property that

$$v_P(w) \geq \sum_{i=1}^{g}(n_i(P) - n_i)$$

for any point P of X, with equality

$$v_P(w) = \sum_{i=1}^{g}(n_i(P) - n_i) = 0$$

if P is not a Weierstrass point of X. We describe its construction now.

A *separating variable* for $k(X)$ is an element $s \in k(X)$ transcendental over k such that $k(X)$ is a finite, separable extension of $k(s)$. With the assumptions on X enforced in this section, we have that s is a separating variable if and only if the differential ds is not identically 0. Furthermore, s is a separating variable if s is a local parameter at a separable point of X. Since in our case X is defined over an algebraically closed field k, every point is separable.

On the polynomial ring $k[s]$, we may define the *nth* Hasse derivative with respect to s by putting

$$\mathfrak{D}_s^{(n)}(s^m) = \begin{cases} \binom{m}{n} s^{m-n} & \text{if } m \geq n, \\ 0 & \text{otherwise,} \end{cases}$$

and extending linearly to $k[s]$. It can be shown that if s is a separating variable for $k(X)$ over k, then this family of maps can be uniquely extended to a family of maps $\mathfrak{D}_s^{(n)} : k(X) \to k(X)$.

Again, let C be a canonical divisor on the curve X and consider the linear system $L(C)$ associated to it. It is a basic fact that $L(C)$ is a k-vector subspace of $k(X)$ of dimension g, and that replacing C by a different canonical divisor yields an isomorphic subspace. Fix any basis $\phi = \{\phi_1, \ldots \phi_g\}$ of $L(C)$ and define the matrix

$$H = H(\phi, s) = \left(\mathfrak{D}_s^{(j)}(\phi_i)\right)$$

for $1 \leq i \leq g$ and $0 \leq j$. Write further $H^{(j)}$ for the column of H whose *ith* entry is $\mathfrak{D}_s^{(j)}(\phi_i)$.

We are interested in the indices j such that $H^{(j)}$ is not a $k(X)$-linear combination of lower numbered columns. This is true for $j = 0$ since the ϕ_i's are not all zero. One can show that there are $g - 1$ more such indices, which we will denote by $j_1, \ldots, j_{g-1}$, and we will write $J(\phi, s) = (j_1, \ldots, j_{g-1})$.This sequence has the property that $J(\phi, s)$ in fact does not depend on our choice of s a separating variable, C a canonical divisor, or ϕ a basis for the linear system associated to C, and in fact that the j_i's are exactly the canonical orders of X defined earlier.

For any sequence $J = (j_1, j_2, \ldots)$ of positive integers, let H^J be the submatrix of H whose first column is $H^{(0)}$ and whose $(l+1)^{st}$ column is $H^{(j_l)}$. Then, we may define the nonzero rational function

$$W(\phi, s) = \det H^{J(\phi,s)},$$

the *Wronskian of ϕ with respect to s*. While not independent of the choices made above, this function behaves as well as can be expected. More precisely, put $\phi'_i = \sum_j a_{ij}\phi_j$ for $a_{ij} \in k$ such that $\phi' = (\phi'_1, \ldots, \phi'_g)$ is a different basis for $L(C)$, and let $y \in k(X)^\times$ and t be another separating variable. Then,

$$W(y\phi', t) = \det(a_{ij}) y^g \, (ds/dt)^{j_1+\ldots+j_{g-1}} \, W(\phi, s). \tag{1}$$

In light of this equation, we define the following divisor:

$$w(\phi, s) = [W(\phi, s)] + gC + \left(j_1 + \ldots + j_{g-1}\right)[ds],$$

which by Equation (1) is in fact independent of any choice we made, so that we may denote it simply by w. One can show that the points in the support of w are exactly the Weierstrass points of X, and that $\nu_P(w) \geq \sum_{i=1}^{g}(n_i(P) - n_i)$ for any point P of X, with equality $\nu_P(w) = \sum_{i=1}^{g}(n_i(P) - n_i) = 0$ if P is not a Weierstrass point of X, as claimed above.

The divisor w is effective: Fixing a point P of X, one may choose a canonical divisor C such that $\nu_P(C) = 0$, which ensures that $\nu_P(\phi_i) \geq 0$, so that $\nu_p([\,W(\phi, s)]\,) \geq 0$ since taking Hasse derivatives does not lower the valuation. Furthermore, one can choose s to be a local parameter at P, so that $\nu_P([\,ds]\,) = 0$. With these choices and because of the invariance of w, it follows that $\nu_P(w) \geq 0$ for each P.

In [27], the authors define the Weierstrass weight of a point to be $\nu_P(w)$. In Section 'Weierstrass points on $\mathbf{X_0(\mathfrak{p})}$', we will define a Drinfeld modular form $W(z)$ that will play for us a role analogous to the function $W(\phi, s)$. Because of this analogy, we will use the divisor of $W(z)$ to define the modular Weierstrass weight of a point P on the Drinfeld modular curve $X_0(\mathfrak{p})$, and study this integer in this work.

Remark 3. If X is defined over a field of characteristic 0, we have the equality $\nu_P(w) = \sum_{i=1}^{g}(n_i(P) - n_i)$ for all points P of X. In positive characteristic, this equality holds if and only if $\det \binom{J'}{J} \neq 0$, where $J' = (j_1(P), \ldots, j_{g-1}(P))$ is the sequence of canonical orders at P, $J = (j_1, \ldots, j_{g-1})$ is the sequence of canonical orders of X, and $\binom{J'}{J}$ is the $(g-1) \times (g-1)$ matrix of binomial coefficients $\binom{j'_r}{j_s}$, where $\binom{j'_r}{j_s} = 0$ if $j'_r < j_s$ and each binomial coefficient is reduced modulo p, the characteristic of k.

We will also need the following well-known fact: We have that $\dim_{k(X)} \Omega_X = 1$, so that $\Omega_X = k(X) \cdot \omega$ for any non-zero $\omega \in \Omega_X$. If C is a canonical divisor of X, by definition it is the divisor of some Weil differential ω^* and thus of a meromorphic differential ω. Then, the map

$$\begin{aligned} \Omega_X &\to k(X) \\ x\omega &\mapsto x \end{aligned}$$

is an isomorphism of k-vector spaces, and under this isomorphism, the space $L(C) \subset k(X)$ corresponds to the space $\Omega_{X,\mathrm{reg}}$ of algebraic differentials without poles.

The Drinfeld setting

Throughout when we refer to rigid analytic objects, we will mean rigid analytic in the sense of Fresnel and van der Put [9].

Drinfeld modules and Drinfeld modular forms

For a reference on Drinfeld modules and Drinfeld modular forms, we refer the reader to Gekeler's excellent *Inventiones* paper [13] or to the author's PhD thesis [29].

In this paper, we will only consider the case of the affine ring $A = \mathbb{F}_q[T]$, with fraction field $K = \mathbb{F}_q(T)$. We complete K at the infinite place $v_\infty(x) = -\deg(x)$ and write $K_\infty = \mathbb{F}_q((1/T))$ for the completion of K at this place. We will also write

$$C = \hat{\bar{K}}_\infty$$

for the completed algebraic closure of K_∞, and $\Omega = \mathbb{P}^1(C) - \mathbb{P}^1(K_\infty) = C - K_\infty$. (From now on, C will never be a canonical divisor again.) Ω has a rigid analytic structure described in [15], and we call it the Drinfeld upper half-plane. The group $\mathrm{GL}_2(A)$ acts on Ω by fractional linear transformations.

Definition 1. Let Γ be a congruence subgroup of $\mathrm{GL}_2(A)$. A function $f\colon \Omega \to C$ is called a *Drinfeld modular form of weight k and type l for* Γ, where $k \geq 0$ is an integer and l is a class in $\mathbb{Z}/(\#\det\Gamma)$, if

1. for $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma, f(\gamma z) = (\det\gamma)^{-l}(cz+d)^k f(z)$;
2. f is rigid analytic on Ω;
3. f is analytic at the cusps of Γ: at each cusp f can be written as a power series with a positive radius of convergence in a (root of) a local parameter at this cusp (this will be discussed further shortly).

For a congruence subgroup Γ of $\mathrm{GL}_2(A)$, we will denote the (finite dimensional) vector space of Drinfeld modular forms of weight k and type l for this subgroup by $M_{k,l}(\Gamma)$, the subspace of cusp forms (the forms having at least a single zero at each cusp of Γ) by $M^1_{k,l}(\Gamma)$, and the subspace of double cusp forms (the forms having at least a double zero at each cusp of Γ) by $M^2_{k,l}(\Gamma)$. We will define precisely what we mean by the order of vanishing of a Drinfeld modular form at a cusp at the very end of this section.

Although they are important to this work, we will avoid discussing Drinfeld modules as much as possible, referring rather the reader to [13] for background reading. We limit ourselves to defining the Carlitz module and presenting only the barest facts about Drinfeld modules of rank 2 that are necessary to read the text.

Definition 2. Let L be either a field extension of K or, if $\mathfrak{p}$ is a prime ideal of A, an extension of the field $\mathbb{F}_\mathfrak{p} = A/\mathfrak{p}$. Further write $\tau(X) = X^q$ and let $L\{\tau\} \subset \mathrm{End}_L(\mathbb{G}_a)$ be the subalgebra generated by τ over L, with commutation relation $l\tau = \tau l^q$ for $l \in L$. A Drinfeld module of rank r over L is a ring homomorphism $\phi\colon A \to L\{\tau\}$ such that for $a \in A$ of degree d,

$$\phi(a) = \sum_{0 \leq i \leq rd} l_i \tau^i$$

with $l_0 = a$ and $l_{rd} \neq 0$. The numbers l_i are called the *coefficients* of ϕ.

We say that two Drinfeld modules ϕ and ψ are *isogenous* if there exists a nonzero element $u \in \mathrm{End}_L(\mathbb{G}_a)$ such that $u \circ \phi = \psi \circ u$. If $u \in L^\times$, then we say that the two modules are *isomorphic* over L. One may show that there is a one-to-one correspondence between Drinfeld modules of rank r over C and rank r A-lattices in C.

In the 1930s, Carlitz studied some polynomials which had properties similar to those exhibited by the classical cyclotomic polynomials [6]. Reinterpreting his work in the context laid out by Drinfeld, his polynomials are now understood to give the action on C of a certain Drinfeld module of rank 1. We call this module the Carlitz module and it is defined by:

$$\rho(T) = T\tau^0 + \tau. \tag{2}$$

Under the correspondence mentioned above, this Drinfeld module corresponds to a certain rank 1 A-lattice $L = \tilde{\pi}A$, where the *Carlitz period* $\tilde{\pi} \in K_\infty(\sqrt[q-1]{-T})$ is defined up to multiplication by an element of $\mathbb{F}_q^\times$. We choose one such $\tilde{\pi}$ and fix it for the remainder of this work. As usual we have the Carlitz exponential function

$$e_A(z) \overset{\text{def}}{=} z \prod_{\substack{a \in A \\ a \neq 0}} \left(1 - \frac{z}{a}\right).$$

Then, we write

$$u(z) \overset{\text{def}}{=} \tilde{\pi} \frac{1}{e_A(z)} \tag{3}$$

for the parameter at infinity. This differs from Gekeler's original notation, who used $t(z)$ for this function but agrees with the notation used in more recent articles, for example, by Bosser and Pellarin in [5].

We will also consider Drinfeld modules of rank 2. For $a \in A$, ϕ a Drinfeld module over L and L' a field extension of L, write

$$\phi[a](L') = \{x \in L' : \phi(a)(x) = 0\}$$

for the a-torsion of ϕ. When ϕ is of rank 2 and defined over C, for $\pi(T)$ a prime polynomial generating the ideal $\mathfrak{p}$ of A, we have

$$\phi[\pi](C) \cong A/\mathfrak{p} \times A/\mathfrak{p}.$$

Again, if ϕ is of rank 2 but is now defined over the algebraic closure $\overline{\mathbb{F}}_\mathfrak{p}$ of $\mathbb{F}_\mathfrak{p} = A/\mathfrak{p}$, we have

$$\phi[\pi](\overline{\mathbb{F}}_\mathfrak{p}) = \begin{cases} 0 & \text{in which case we say } \phi \text{ is } \textit{supersingular}, \text{ or} \\ A/\mathfrak{p} & \text{in which case we say } \phi \text{ is } \textit{ordinary}. \end{cases}$$

There are $g_\mathfrak{p} + 1$ supersingular Drinfeld modules defined over the algebraic closure of $A/\mathfrak{p}$, where

$$g_\mathfrak{p} \overset{\text{def}}{=} \begin{cases} \frac{q^d - q}{q^2 - 1} & \text{if } d \text{ is odd,} \\ \frac{q^d - q^2}{q^2 - 1} & \text{if } d \text{ is even.} \end{cases} \tag{4}$$

Remark 4. We use $g_{\mathfrak{p}}$ to denote the quantity above because it is the genus of the modular curve $X_0(\mathfrak{p})$.

As before, let $\mathfrak{p}$ be a prime ideal of A. For a Drinfeld module ϕ of rank 2 over K, there is a notion of good reduction at $\mathfrak{p}$: First one must find a Drinfeld module ψ isomorphic to ϕ over K, such that ψ has coefficients in A and such that the reduction of ψ modulo $\mathfrak{p}$ (obtained by reducing the coefficients modulo $\mathfrak{p}$) is a Drinfeld module. If this is possible and in addition the reduction of ψ modulo $\mathfrak{p}$ has rank 2 as a Drinfeld module, then we say that ϕ has *good reduction at* $\mathfrak{p}$. Furthermore, if the reduction of ψ modulo $\mathfrak{p}$ is supersingular, then we say that ϕ is *supersingular at* $\mathfrak{p}$.

We now present some facts on Drinfeld modular forms for the full modular group $\mathrm{GL}_2(A)$. As in the classical case, the algebraic curve $Y_{\mathrm{GL}_2(A)}$ whose associated rigid analytic space is $\mathrm{GL}_2(A)\backslash\Omega$ can be compactified by adding a single cusp which we denote by ∞. This will be discussed more rigorously in the next section.

As in [13], we will write g_k for the normalized Eisenstein series of weight $q^k - 1$ and type 0 for $\mathrm{GL}_2(A)$ and set $g = g_1$ for simplicity. (From now on, we will never use g to denote the genus of a curve again.) We will also write h for the Poincaré series of weight $q + 1$ and type 1 for $\mathrm{GL}_2(A)$ which was first defined in [16]. It is well known that the graded C-algebra of Drinfeld modular forms of all weights and all types for $\mathrm{GL}_2(A)$ is the polynomial ring $C[g, h]$ (where each Drinfeld modular form corresponds to a unique isobaric polynomial), that g has leading term 1, that h has a single zero at ∞ and leading coefficient -1, and that both g and h have u-series expansions with integral coefficients.

We record here a computation which we will need later and which follows from knowing that the algebra of Drinfeld modular forms is generated by g and h:

Proposition 1. *For $q \geq 3$, the dimension of the space of modular forms of weight $q^d + 1$ and type 1 for $GL_2(A)$ is equal to $g_{\mathfrak{p}} + 1$, and the dimension of its subspace of double cusp forms is $g_{\mathfrak{p}}$, where $g_{\mathfrak{p}}$ is as in equation (4).*

We will also need a slash operator, which we define now. For any $x \in K_\infty^\times$, x can be written uniquely as

$$x = \zeta_x \left(\frac{1}{T}\right)^{v_\infty(x)} u_x \tag{5}$$

where $\zeta_x \in \mathbb{F}_q^\times$, and u_x is such that $v_\infty(u_x - 1) > 0$, or in other words u_x is a 1-unit at ∞. We call ζ_x the *leading coefficient* of x.

For $\gamma \in \mathrm{GL}_2(K)$, we have that $\det\gamma \in K^\times$. By (5), we can write

$$\det\gamma = \zeta_{\det\gamma} \left(\frac{1}{T}\right)^{v_\infty(\det\gamma)} u_{\det\gamma}.$$

For simplicity, we write

$$\zeta_{\det\gamma} = \zeta_\gamma.$$

We define a *slash operator* for $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(K)$ on a modular form of weight k and type l by

$$f|_{k,l}[\gamma] = \zeta_\gamma^l \left(\frac{\det \gamma}{\zeta_\gamma}\right)^{k/2} (cz+d)^{-k} f(\gamma z). \tag{6}$$

Note that for $\gamma \in \mathrm{GL}_2(A)$, we have that $\det \gamma = \zeta_\gamma$; thus if f is modular of weight k and type l for Γ and $\gamma \in \Gamma$, then $f|_{k,l}[\gamma] = f$.

Drinfeld modular forms modulo $\mathfrak{p}$

An important tool we will use to study the Weierstrass points of the curve $X_0(\mathfrak{p})$ is the theory of Drinfeld modular forms for $\mathrm{GL}_2(A)$ upon reduction modulo $\mathfrak{p}$. Everywhere in this paper, we will write $\pi(T) \in A$ for a monic prime polynomial of degree d and denote by $\mathfrak{p}$ the principal ideal that it generates. For $x \in K$, we write $v_\mathfrak{p}(x)$ for the valuation of x at $\mathfrak{p}$.

Definition 3. Let $f = \sum_{i=0}^{\infty} c_i u^i$ be a formal series with $c_i \in K$. Then, we define the *valuation of f at* $\mathfrak{p}$ to be

$$v_\mathfrak{p}(f) = \inf_i v_\mathfrak{p}(c_i).$$

For two formal series $f = \sum a_i u^i$ and $g = \sum b_i u^i$, we write $f \equiv g \pmod{\mathfrak{p}^m}$ if $v_\mathfrak{p}(f-g) \geq m$.

For any u-series f with rational $\mathfrak{p}$-integral coefficients, define its *filtration modulo* $\mathfrak{p}$, denoted $w_\mathfrak{p}(f)$, to be the smallest integer k such that there exists a modular form f' of weight k for $\mathrm{GL}_2(A)$ such that $f \equiv f' \pmod{\mathfrak{p}}$. We write $w_\mathfrak{p}(f) = -\infty$ if $f \equiv 0 \pmod{\mathfrak{p}}$.

As in the classical case, there is a deep connection between supersingular Drinfeld modules in characteristic $\mathfrak{p}$ and forms with lower filtration than weight. It is this connection which we will exploit to refine the connection between the Weierstrass points of $X_0(\mathfrak{p})$ and the supersingular locus.

To begin explaining the connection, let again g_k be the Drinfeld Eisenstein series of weight $q^k - 1$ and type 0 for $\mathrm{GL}_2(A)$. As shown in [13], if $\mathfrak{p}$ is an ideal generated by a prime polynomial of degree d, we have $g_d \equiv 1 \pmod{\mathfrak{p}}$. Thus, the form g_d has filtration equal to 0, which is strictly less than its weight. We note further that this is the only relation upon reducing modulo $\mathfrak{p}$.

To connect g_d to the supersingular Drinfeld modules, we must first define the so-called *companion polynomial* to a Drinfeld modular form. In [7], the authors remark that the fact that the algebra of Drinfeld modular forms for $\mathrm{GL}_2(A)$ is generated by g and h implies the following: For k, a positive integer and l a class in $\mathbb{Z}/(q-1)$, define $\mu(k,l)$ and $\gamma(k,l)$ to be the unique pair of integers such that

$$\begin{aligned} \mu(k,l) &\equiv l \pmod{q-1}, \\ 0 \leq \gamma&(k,l) \leq q, \\ \text{and } k &= \mu(k,l)(q+1) + \gamma(k,l)(q-1). \end{aligned} \tag{7}$$

Then to every Drinfeld modular form of weight k and type l for $\mathrm{GL}_2(A)$, one can associate a unique polynomial $P(f,x) \in C[x]$ such that

$$f = g^{\gamma(k,l)} h^{\mu(k,l)} P(f,j) \tag{8}$$

where j is the (normalized) j-invariant, $j = \frac{g^{q+1}}{-h^{q-1}}$. Since g only has a single zero at the elliptic point with $j = 0$, the first consequence of this fact is that any form f of a given weight k and type l vanishes to order at least $\gamma(k,l)$ at $j = 0$. We will call these zeroes the *trivial zeroes of f*. The second consequence of this fact is that since h is nonzero on the Drinfeld upper half-plane, the polynomial P can be thought of as an object which keeps track of the zeroes of the form f that are not trivial.

If we define the *Drinfeld supersingular locus* to be the following polynomial:

$$S_{\mathfrak{p}}(x) = \prod_{\substack{\phi \text{ defined over } \overline{\mathbb{F}}_{\mathfrak{p}} \\ \phi \text{ supersingular}}} (x - j(\phi)),$$

then we have

$$S_{\mathfrak{p}}(x) \equiv x^{\gamma(q^d-1,0)} P(g_d, x) \pmod{\mathfrak{p}},$$

where $\gamma(q^d-1,0)$ is 0 if d is even and 1 if d is odd.

Therefore upon reduction modulo $\mathfrak{p}$, the form g_d, which has lower filtration than weight modulo $\mathfrak{p}$, has a single zero at each supersingular point. This fact is an example of a more general phenomenon:

Proposition 2 (Dobi-Wage-Wang [7]). *Assuming the notation above, let f be a Drinfeld modular form for $GL_2(A)$ of weight k and type l with rational $\mathfrak{p}$-integral u-series coefficients and finite filtration $w_{\mathfrak{p}}(f)$. Define $\alpha = \frac{k - w_{\mathfrak{p}}(f)}{q^d-1}$ and $a = \left\lfloor \frac{\alpha\gamma(q^d-1,0)q + \gamma(k,l)}{q+1} \right\rfloor$. Then, the polynomial $x^a P(f,x)$ is divisible by $S_{\mathfrak{p}}(x)^\alpha$ in $\mathbb{F}_{\mathfrak{p}}[x]$, where $\mathbb{F}_{\mathfrak{p}}$ is the field $A/\mathfrak{p}$.*

Proposition 2 when applied to a certain Drinfeld modular for $W(z)$ defined in Section ‘The modular Wronskian,’ immediately implies Theorem 1. To obtain the more precise result given in Theorem 3 we will need the following proposition:

Proposition 3. *Let f be a Drinfeld modular form of weight k and type l for $GL_2(A)$.*

1. *If d is even, then we have*

$$P\left(fg_d, x\right) \equiv P(g_d, x) P\left(f, x\right) \pmod{\mathfrak{p}}.$$

2. *If d is odd, then*

$$P\left(fg_d, x\right) \equiv \begin{cases} -xP(g_d,x)P\left(f,x\right) \pmod{\mathfrak{p}} & \text{if } \gamma(k,l) = q, \\ P(g_d,x)P\left(f,x\right) \pmod{\mathfrak{p}} & \text{otherwise.} \end{cases}$$

Proof. The case of d even: Since $g_d \equiv 1 \pmod{\mathfrak{p}}$, we have $f \equiv fg_d \pmod{\mathfrak{p}}$. Furthermore, if f is of weight k and type l, then fg_d is of weight $k + q^d - 1$ and type l. Using the statement of Equation (8), we have

$$g^{\gamma(k,l)} h^{\mu(k,l)} P\left(f, j\right) \equiv g^{\gamma(k+q^d-1,l)} h^{\mu(k+q^d-1,l)} P\left(fg_d, j\right) \pmod{\mathfrak{p}}.$$

Then,

$$P\left(fg_d, j\right) \equiv h^{\mu(k,l) - \mu(k+q^d-1,l)} g^{\gamma(k,l) - \gamma(k+q^d-1,l)} P\left(f, j\right) \pmod{\mathfrak{p}}.$$

We have $\mu(k,l) \equiv l \equiv \mu(k+q^d-1,l) \pmod{q-1}$, so let N be the integer such that $\mu(k+q^d-1,l)-\mu(k,l)=N(q-1)$. Combining the equations

$$k=\gamma(k,l)(q-1)+\mu(k,l)(q+1)$$

and

$$k+q^d-1=\gamma(k+q^d-1,l)(q-1)+\mu(k+q^d-1,l)(q+1),$$

we obtain that

$$q^d-1=\Big(\gamma(k+q^d-1,l)-\gamma(k,l)\Big)(q-1)+N(q-1)(q+1). \tag{9}$$

Since both $\gamma(k+q^d-1,l)$ and $\gamma(k,l)$ are between 0 and q inclusively, then

$$-q \le \gamma(k+q^d-1,l)-\gamma(k,l) \le q.$$

If it were the case that

$$-q \le \gamma(k+q^d-1,l)-\gamma(k,l) < 0,$$

then by the uniqueness of the integers $\mu(q^d-1,0)$ and $\gamma(q^d-1,0)$ in the Equation (9), we must have

$$\gamma(k+q^d-1,l)-\gamma(k,l)=\gamma(q^d-1,0)-q-1=-q-1,$$

a contradiction. Therefore,

$$0 \le \gamma(k+q^d-1,l)-\gamma(k,l) \le q,$$

and again using uniqueness in Equation (9),

$$0=\gamma(q^d-1,0)=\gamma(k+q^d-1,l)-\gamma(k,l),$$

and

$$N(q-1)=\mu(q^d-1,0).$$

Then,

$$P(fg_d,j) \equiv h^{-\mu(q^d-1,0)}P(f,j) \pmod{\mathfrak{p}}.$$

Solving for $P(g_d,j)$ in

$$1 \equiv g_d = h^{\mu(q^d-1,0)}P(g_d,j)$$

completes the proof.
The case of d odd: The proof proceeds as in the even case, except that we cannot rule out the case

$$-q \le \gamma(k+q^d-1,l)-\gamma(k,l) < 0.$$

In that case, we must have

$$\gamma(k+q^d-1,l)-\gamma(k,l)=\gamma(q^d-1,0)-q-1=1-q-1=-q,$$

which forces $\gamma(k,l)=q$. Furthermore, we have

$$\mu(q^d-1,0)=(N-1)(q-1),$$

where N is such that $\mu(k+q^d-1,l)-\mu(k,l)=N(q-1)$ as in the even case.

Putting this together, we have

$$\begin{aligned} P\left(fg_d,j\right) &\equiv h^{\mu(k,l)-\mu(k+q^d-1,l)} g^{\gamma(k,l)-\gamma(k+q^d-1,l)} P\left(f,j\right) \pmod{\mathfrak{p}} \\ &\equiv h^{-(N-1)(q-1)-(q-1)} g^q P\left(f,j\right) \pmod{\mathfrak{p}} \end{aligned}$$

Multiplying both sides by

$$1 \equiv g_d = gh^{\mu(q^d-1,0)} P(g_d,j) \tag{10}$$

gives

$$P\left(fg_d,j\right) \equiv \frac{g^{q+1}}{h^{q-1}} P(g_d,j) P\left(f,j\right) \pmod{\mathfrak{p}},$$

and since $j = \frac{g^{q+1}}{-h^{q-1}}$, this completes the proof of this case.

If

$$0 \leq \gamma(k+q^d-1,l) - \gamma(k,l) \leq q,$$

using uniqueness in Equation (9), we must have

$$1 = \gamma(q^d-1,0) = \gamma(k+q^d-1,l) - \gamma(k,l),$$

and

$$N(q-1) = \mu(q^d-1,0).$$

Then, we may conclude similarly as in the even case that

$$P\left(fg_d,j\right) \equiv g^{-1} h^{-\mu(q^d-1,0)} P\left(f,j\right) \pmod{\mathfrak{p}},$$

and the result follows using Equation (10) again. □

We end this subsection by recalling results from [30] for the convenience of the reader:

Theorem 4 (Theorem 1.1 of [30]). *Let $q \geq 3$. There is a one-to-one correspondence between forms of weight 2 and type 1 for $\Gamma_0(\mathfrak{p})$ with rational $\mathfrak{p}$-integral u-series coefficients at ∞ and forms of weight q^d+1 and type 1 for $GL_2(A)$ with rational $\mathfrak{p}$-integral u-series coefficients.*

We will also need a stronger version of Theorem 1.2 from [30] and take this opportunity to correct a typo in the type of the form $\widetilde{\mathrm{N}\left(f\right)}$:

Theorem 5. *Let f be a Drinfeld modular form for $\Gamma_0(\mathfrak{p})$ of weight k and type l with rational, $\mathfrak{p}$-integral u-series coefficients at ∞. Suppose further that f is an eigenform of the Fricke involution. Let*

$$\widetilde{N\left(f\right)}(z) = \pi^{q^d k/2} \prod_{\gamma \in \Gamma_0(\mathfrak{p}) \backslash GL_2(A)} f|_{k,l}[\gamma].$$

Then, $\widetilde{N\left(f\right)}$ has rational, $\mathfrak{p}$-integral u-series coefficients and

$$\widetilde{N\left(f\right)} \equiv f^2 \pmod{\mathfrak{p}}.$$

Furthermore, $\widetilde{N\left(f\right)}$ is a form of weight $(q^d+1)k$ and type $2l$.

Proof. We first note that the hypothesis in [30] that f have integral u-series coefficients at ∞ is unnecessary; it suffices that the coefficients be rational and $\mathfrak{p}$-integral for all of the arguments in the paper to work.

Corollary 5.4 of [30] asserts that for f as in the statement of the theorem,

$$f(z) \prod_{\substack{\lambda \in A \\ \deg\lambda < d}} f\left(\frac{z+\lambda}{\pi}\right) \equiv f(z)^2 \pmod{\mathfrak{p}}.$$

By Proposition 3.9 of [30],

$$\mathrm{N}(f) = \prod_{\gamma \in \Gamma_0(\mathfrak{p})\backslash \mathrm{GL}_2(A)} f|_{k,l}[\gamma] = \frac{1}{\pi^{q^d k/2}} f \prod_{\substack{\lambda \in A \\ \deg\lambda < d}} f\left(\frac{z+\lambda}{\pi}\right),$$

which proves the equivalence modulo $\mathfrak{p}$.

Because $\Gamma_0(\mathfrak{p})$ has index q^d+1 in $\mathrm{GL}_2(A)$, the weight of $\mathrm{N}(f)$ is $(q^d+1)k$, and the type is $(q^d+1)l$. However, the type of a form for $\mathrm{GL}_2(A)$ is an equivalence class in $\mathbb{Z}/(q-1)$ and

$$(q^d+1)l = (q^d-1)l + 2l \equiv 2l \pmod{q-1}.$$

□

Drinfeld modular curves

We now turn our attention to Drinfeld modular curves and more specifically to the family $X_0(\mathfrak{p})$.

For Γ a congruence subgroup of $\mathrm{GL}_2(A)$, the action of Γ on the Drinfeld upper half-plane Ω by fractional linear transformations has finite stabilizer for each $z \in \Omega$. It follows thus that the quotient $\Gamma\backslash\Omega$ is also a rigid analytic space. Moreover, it is connected and smooth of dimension one. The curve $\Gamma\backslash\Omega$ can be shown to arise from an algebraic curve:

Theorem 6 (Drinfeld [8])**.** *There exists a smooth irreducible affine algebraic curve Y_Γ defined over C such that $\Gamma\backslash\Omega$ and the underlying analytic space Y_Γ^{an} of Y_Γ are canonically isomorphic as analytic spaces over C.*

We note further that the curve Y_Γ is unique up to isomorphism and is in fact defined over a finite abelian extension of K, K_Γ. For each Y_Γ, there exists a unique smooth projective curve X_Γ over K_Γ such that Y_Γ is birationally equivalent to X_Γ. As sets, $Y_\Gamma(C)$ and $X_\Gamma(C)$ differ by finitely many points, which are in one-to-one correspondence with the points of the set $\Gamma\backslash\mathbb{P}^1(K)$, where $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$ acts on $(x_1 : x_2) \in \mathbb{P}^1(K)$ by

$$\gamma \cdot (x_1 : x_2) = (ax_1 + bx_2 : cx_1 + dx_2).$$

These points are called the cusps of Γ.

For $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$, we have

$$\frac{d(\gamma z)}{dz} = \det\gamma\ (cz+d)^{-2},$$

so that for f a modular form for Γ of weight 2 and type 1, the differential form $f(z)dz$ is Γ-invariant. A short computation, presented in [15], shows that it descends to a holomorphic differential form on X_Γ if f is a double cusp form. Since GAGA theorems hold for rigid analytic curves [21,22], we have the following theorem:

Theorem 7 (Goss [18], Gekeler-Reversat [15]). *The map $f \mapsto f(z)dz$ identifies the space of double cusp forms of weight 2 and type 1 for Γ to the space of regular differential forms on X_Γ.*

From this theorem, it follows that the dimension of the space of double cusp forms of weight 2 and type 1 for Γ is g_Γ, where g_Γ is the genus of the curve X_Γ. Furthermore, it follows by a standard argument that all spaces of Drinfeld modular forms of a fixed weight and type for a congruence group Γ are finite dimensional.

We will be interested in one family of congruence subgroups and the Drinfeld modular curves attached to these groups. Recall that $\pi(T)$ is a monic prime polynomial in A of degree d generating the ideal $\mathfrak{p}$. Then, we may define the congruence subgroups

$$\Gamma = \Gamma_0(\mathfrak{p}) \overset{\text{def}}{=} \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(A) \mid c \equiv 0 \pmod{\mathfrak{p}} \right\}.$$

In this case, $\#\det \Gamma_0(\mathfrak{p}) = q-1$. From now on, we will denote the affine curve $Y_{\Gamma_0(\mathfrak{p})}$ by $Y_0(\mathfrak{p})$ and the projective curve $X_{\Gamma_0(\mathfrak{p})}$ by $X_0(\mathfrak{p})$ to coincide with classical notation. Both $Y_0(\mathfrak{p})$ and $X_0(\mathfrak{p})$ can be defined over K, but we will most often think of them as curves over C.

As described in [15], every congruence subgroup corresponds to a certain moduli problem for Drinfeld modules of rank 2. The problem attached to $\Gamma_0(\mathfrak{p})$ classifies Drinfeld modules of rank 2 with a distinguished finite flat subgroup-scheme which is cyclic, locally free of rank q^d and contained in the $\mathfrak{p}$-torsion. We write $M_0(\mathfrak{p})$ for the coarse moduli scheme associated to this problem.

Drinfeld's work on so-called generalized Drinfeld modules, we may deduce the existence of a compactification $\overline{M}_0(\mathfrak{p})$ of $M_0(\mathfrak{p})$ over Spec A. We have that $X_0(\mathfrak{p})$ as a curve over K is $\overline{M}_0(\mathfrak{p}) \times_A K$. From [11] and [8], we know that $\overline{M}_0(\mathfrak{p})$ has the following properties:

Theorem 8.
- *$\overline{M}_0(\mathfrak{p}) \to$ Spec A is proper, normal, flat, and irreducible, of relative dimension 1.*
- *$\overline{M}_0(\mathfrak{p}) \to$ Spec A is smooth away from $\mathfrak{p}$.*
- *If d is even, $\overline{M}_0(\mathfrak{p})$ is regular. If d is odd, $\overline{M}_0(\mathfrak{p})$ has a singularity on the fiber above $\mathfrak{p}$ at the supersingular j-invariant $j = 0$ and is otherwise regular. The singularity is of type A_q.*

The last part of the theorem requires a careful study of the moduli problem 'in characteristic $\mathfrak{p}$'. To obtain it, Gekeler [11] shows that the reduction of $X_0(\mathfrak{p})$ modulo $\mathfrak{p}$ is given by two copies of $X_0(1)$ intersecting transversally at the supersingular points and interchanged by the Fricke involution $W_\mathfrak{p}$. The Fricke involution can be defined as follows: if ϕ is a Drinfeld module and H is a $\Gamma_0(\mathfrak{p})$-level structure, so that (ϕ, H) is a point of $M_0(\mathfrak{p})$, then $W_\mathfrak{p}(\phi, H) = (\phi/H, \phi[\mathfrak{p}]/H)$.

Remark 5. From Theorem 8 above, we have that $X_0(\mathfrak{p})$ is defined over K with function field $K(j, j_{\mathfrak{p}})$. In fact, because the moduli problem associated to $\Gamma_0(\mathfrak{p})$ is defined over A, the space of holomorphic differentials on $X_0(\mathfrak{p})$ has a basis that is defined over A. Therefore, the space of Drinfeld double cusp forms of weight 2 and type 1 for $\Gamma_0(\mathfrak{p})$ has a basis of forms with integral coefficients. It also follows from such considerations that Drinfeld modular forms on $\Gamma_0(\mathfrak{p})$ with rational u-series coefficients have bounded denominators.

From its action on pairs (ϕ, H), we can also see that the Fricke involution $W_{\mathfrak{p}}$ is K-rational. We note here that the analytic avatar of $W_{\mathfrak{p}}$ is the action of the matrix $\begin{pmatrix} 0 & -1 \\ \pi & 0 \end{pmatrix}$ on Ω.

Since $X_0(\mathfrak{p})$ is smooth, its arithmetic and geometric genera are the same and do not depend on the field over which we consider the curve. We denote the genus of $X_0(\mathfrak{p})$ by $g_{\mathfrak{p}}$, and it is given by

$$g_{\mathfrak{p}} = \begin{cases} \frac{q(q^{d-1}-1)}{q^2-1} & \text{if } d \text{ is odd,} \\ \frac{q^2(q^{d-2}-1)}{q^2-1} & \text{if } d \text{ is even.} \end{cases}$$

(As promised, this is the same $g_{\mathfrak{p}}$ that appears in Equation (4).) This fact can be obtained either by relating $g_{\mathfrak{p}}$ to $h_1(\Gamma_0(\mathfrak{p}))\backslash\mathcal{T})$ as in [14], or by working directly on the Drinfeld modular curve as in [10].

From [10], we also note that representatives for the two distinct equivalence classes of $\Gamma_0(\mathfrak{p})\backslash\mathbb{P}^1(K)$ are $(0:1)$ and $(1:0)$, so that $X_0(\mathfrak{p})$ has two cusps, denoted 0 and ∞, respectively. Both of these cusps are K-rational points of $X_0(\mathfrak{p})$. From the same source, we have that $X_0(\mathfrak{p})(C)$ has no elliptic point when d is odd and two elliptic points when d is even. When d is even, both elliptic points have stabilizer of order $q+1$ in $\widetilde{\Gamma}_0(\mathfrak{p}) = \Gamma_0(\mathfrak{p})/\left(\Gamma_0(\mathfrak{p}) \cap Z(\mathrm{GL}_2(A))\right)$.

Expansions at the cusps

Some care is needed in discussing the behavior of Drinfeld modular forms at the cusps, so we delve into this topic now. We focus on the groups $\mathrm{GL}_2(A)$ and $\Gamma_0(\mathfrak{p})$ as this is all we will need here and leave the general case to [15] or [12].

Let us first consider the case of $\mathrm{GL}_2(A)$. The set $\mathrm{GL}_2(A)\backslash\mathbb{P}^1(K)$ consists of a single element, and we choose $(1:0)$ as the representative of this element. The stabilizer Γ_∞ of $(1:0)$ in $\mathrm{GL}_2(A)$ is the set of all upper triangular matrices. This set contains a maximal subgroup Γ_∞^{un}:

$$\Gamma_\infty^{un} = \left\{ \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} : a \in A \right\},$$

and also cyclic transformations $\begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix}$ for $a, d \in \mathbb{F}_q^\times$. The image of this group of cyclic transformations in $\mathrm{PGL}_2(A)$ has size $q-1$, the size of $\mathbb{F}_q^\times$.

Recall the function u defined in Equation (3). Now writing

$$\Omega_c = \{z \in \Omega : \inf_{x \in K_\infty} |z - x| \geq c\},$$

we have that u identifies $\Gamma_\infty^{un}\backslash\Omega_c$ with a pointed ball $B_r - \{0\}$ of radius r for some small r [15]. It can be shown that there is a constant c_0 such that for $c \geq c_0$ and $\gamma \in \mathrm{GL}_2(A)$, $\Omega_c \cap \gamma(\Omega_c) \neq \emptyset$ implies that $\gamma \in \Gamma_\infty$. Thus for such a c,

$$\begin{aligned} B_{r^{q-1}} - \{0\} &\cong \Gamma_\infty \backslash \Omega_c \hookrightarrow \mathrm{GL}_2(A)\backslash\Omega \\ u(z)^{q-1} &\leftarrow\!\shortmid z \qquad \mapsto z \end{aligned}$$

is an open immersion of analytic spaces. Thus, $u(z)^{q-1}$ is a uniformizer at the cusp ∞ for $\mathrm{GL}_2(A)\backslash\Omega$.

The subtlety involved in defining the u-series expansion of a Drinfeld modular form is that we allow them to have non-trivial type l and thus they are not invariant under the full Γ_∞ but rather only under Γ_∞^{un}. This is why in general, a Drinfeld modular form of non-trivial type will have a u-series expansion rather than a u^{q-1}-series expansion.

There is also a second subtlety that comes into play. For a general congruence subgroup Γ, to discuss the behavior of a function f at a cusp $(a : b) \in \Gamma\backslash\mathbb{P}^1(K)$, one first fixes an element $\gamma \in \mathrm{GL}_2(K)$ such that $\gamma \cdot (1 : 0) = (a : b)$. Then, the holomorphy properties and order of vanishing of f at the cusp corresponding to $(a : b)$ are the properties of $f \circ \gamma$ at ∞ and do not depend on the choice of $(a : b)$ in its equivalence class modulo Γ and on the choice of γ sending $(1 : 0)$ to $(a : b)$. However, for t a parameter at ∞ for the group Γ, one might wish to define the t-series expansion of f at the cusp corresponding to $(a : b)$ as that of $f \circ \gamma$ at ∞. This is not well defined, as the coefficients of the expansion will depend on the choice of $(a : b)$ and γ.

To remove any ambiguity, in the case of $\mathrm{GL}_2(A)$, we once and for all declare that the expansion of f at ∞ is its u-series expansion, with u as defined in Equation (3).

We now consider $\Gamma_0(\mathfrak{p})$. The cusp in the $\Gamma_0(\mathfrak{p})$-equivalence class of $(1 : 0)$, which we denote by ∞, has stabilizer Γ_∞ in $\Gamma_0(\mathfrak{p})$, where Γ_∞ is again the set of all upper-triangular matrices in $\mathrm{GL}_2(A)$. Because of this, the same argument as above shows that u^{q-1} is a parameter at ∞, and that modular forms for $\Gamma_0(\mathfrak{p})$ have a u-series expansion at ∞. As in the case of $\mathrm{GL}_2(A)$, we fix once and for all that the expansion of f at ∞ is its u-series expansion.

We now consider the other cusp of $X_0(\mathfrak{p})$, which we will denote by 0. To fix a well-defined choice of u-series expansion at 0, we fix $(0 : 1)$ as the representative of the other equivalence class, and the matrix

$$W_{\mathfrak{p}} = \begin{pmatrix} 0 & -1 \\ \pi & 0 \end{pmatrix}$$

as the matrix sending $(1 : 0)$ to $(0 : 1)$. Thus, the u-series expansion of a Drinfeld modular form of weight k and type l at the cusp 0 is defined to be that of the form

$$f|_{k,l}[\,W_{\mathfrak{p}}] = \pi^{k/2}(\pi z)^{-k} f\left(\frac{-1}{\pi z}\right)$$

at ∞.

In any case, for a Drinfeld modular form with u-series expansion $\sum_{i=0}^{\infty} a_i u(z)^i$ at a cusp c, we will write $\mathrm{ord}_c(f)$ for the least $i \geq 0$ such that $a_i \neq 0$ and call this the order of vanishing of f at c.

Hyperderivatives and quasimodular forms

In this section, we present the theory necessary to study the action of differential operators on the algebra of Drinfeld modular forms. These operators will not preserve modularity, which naturally leads us to consider a larger set of rigid analytic functions on Ω, the Drinfeld quasimodular forms. Throughout, we will use ‘analytic’ to mean ‘rigid analytic'. We will say that an analytic function f on Ω is 'analytic at ∞' to mean that there are constants $a_i \in C$, $i \in \mathbb{Z}_{\geq 0}$ such that

$$f(z) = \sum_{i=0}^{\infty} a_i u(z)^i$$

for z such that $\inf_{x \in K_\infty} |z - x|$ is large.

Drinfeld quasimodular forms

Definition 4. An analytic function $f \colon \Omega \to C$ is called a *Drinfeld quasimodular form of weight k, type l, and depth m for $GL_2(A)$*, where $k \geq 0$ and $m \geq 0$ are integers and l is a class in $\mathbb{Z}/(q-1)$. If there exist analytic functions $f_1, f_2, \ldots, f_m$ on Ω which are A-periodic and analytic at infinity such that for $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(A)$, we have

$$f(\gamma z) = (\det \gamma)^{-l} (cz + d)^k \sum_{j=0}^{m} f_j(z) \left(\frac{c}{cz+d} \right)^j .$$

For a given quasimodular form $f \neq 0$, the weight, type, and polynomial $\sum_{j=0}^{m} f_j(z) X^j$ are uniquely determined by f as shown in [4]. Furthermore, as can be seen by choosing γ to be the identity matrix, we necessarily have $f = f_0$. Finally, every modular form is a quasimodular form of depth 0 and vice-versa.

An important example of a Drinfeld quasimodular form is the function E introduced in [13]:

$$E \overset{\text{def}}{=} \frac{1}{\tilde{\pi}} \sum_{\substack{a \in \mathbb{F}_q[T] \\ a \text{monic}}} \left(\sum_{b \in \mathbb{F}_q[T]} \frac{a}{az + b} \right),$$

which can be shown to be of weight 2, type 1, and depth 1. Its importance is reflected in the fact that the graded C-algebra of Drinfeld quasimodular forms of all weights, types, and depths is the polynomial ring $C[g, h, E]$, where each form corresponds to a unique isobaric polynomial.

For a more in-depth discussion of Drinfeld quasimodular forms, we refer the interested reader to the work of Bosser and Pellarin [4] and [5].

Higher derivatives

In [28], Uchino and Satoh consider the action of the Hasse derivatives on analytic functions on Ω. We present here the results we need from their paper without proof.

We will use the fact that C is a complete field with a non-Archimedean dense valuation (which we recall is the unique extension of $v_\infty(x) = -\deg(x)$ from K to C) and that Ω is an open set. We will work in this section with analytic functions on Ω and denote the space of these functions by $\mathrm{An}(\Omega)$. For $f \in \mathrm{An}(\Omega)$ such that $f = \sum_{i=0}^{\infty} c_{i,w} (z - w)^i$ in a neighborhood of $w \in \Omega$, we define the nth hyperderivative of f at w to be

$$\mathfrak{D}_n \left(f \right) (w) = c_{n,w}. \tag{11}$$

As remarked above, this is simply the Hasse derivative.

For our purposes, it will be important that our differential operator preserves K-rationality of the u-series coefficients, which $\mathfrak{D}_n$ does not. However, the operator

$$D_n \overset{\text{def}}{=} \frac{1}{(-\tilde{\pi})^n}\mathfrak{D}_n \tag{12}$$

does [4], and so we will use this normalized operator.

Remark 6. The operator $-D_1$ was also studied by Gekeler in [13], where it was denoted by Θ, in analogy with Ramanujan's Θ-operator in the classical setting. This explains the discrepancy in sign between this work and the cited paper in our statement of Proposition 8 below.

We have the following facts:

Proposition 4 (Uchino-Satoh [28]). *For $f \in An(\Omega)$ and $w \in \Omega$ such that $f = \sum_{i=0}^{\infty} c_{i,w}(z-w)^i$ near w, we have:*

1. *Formally, in a neighborhood of w,*

$$D_nf(z) = \frac{1}{(-\tilde{\pi})^n}\sum_{i=0}^{\infty}\binom{i}{n}c_{i,w}(z-w)^{i-n}$$

and this has the same radius of convergence as $\sum_{i=0}^{\infty} c_{i,w}(z-w)^i$.

2. *In fact, D_nf is analytic on Ω.*
3. *The system of derivatives $\{D_n\}$ is a higher derivation; in other words, it satisfies:*
   (a) *$D_0f = f$,*
   (b) *D_n is C-linear,*
   (c) *for f and g in $An(\Omega)$, $D_n(fg) = \sum_{i=0}^{n} D_ifD_{n-i}g$.*
4. *This higher derivation is iterative: for all integers $i \geq 0$ and $j \geq 0$, we have:*

$$D_i \circ D_j = D_j \circ D_i = \binom{i+j}{i}D_{i+j}.$$

5. *This higher derivation has a chain rule property: For each $n \geq 1$ and each $1 \leq i \leq n$, there exist maps $F_{n,i}$ from $An(\Omega)^{n+1-i}$ to $An(\Omega)$ such that:*
   (a) *for f and g in $An(\Omega)$ such that the composition $f \circ g$ is defined, we have*

$$D_n(f\circ g) = \sum_{i=1}^{n} F_{n,i}(D_1g,\ldots,D_{n+1-i}g)(D_if)\circ g,$$

   (b) *and if $n \geq 2$, then $F_{n,1}$ is a C-linear map.*

In the case where g is a linear fractional transformation, [4, Lemma 3.3] gives the following more precise formula for the maps $F_{n,i}$ that appear in the chain rule property:

Lemma 1. *Let $f\colon \Omega \to C$ be an analytic function. For all $n \geq 1$, $z \in \Omega$, and $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(A)$, we have*

$$D_n(f\circ\gamma)(z) = (-1)^n\left(\frac{c}{cz+d}\right)^n\sum_{i=1}^{n}(-1)^i\binom{n-1}{n-i}\left(\frac{c(cz+d)}{\det\gamma}\right)^{-i}\frac{1}{(-\tilde{\pi})^{n-i}}(D_if)\left(\frac{az+b}{cz+d}\right).$$

We note here that since the D_n's are iterative and using Lucas's theorem, we have that

$$D_n = \frac{1}{n_0! \dots n_s!} D_{p^s}^{n_s} \circ \dots \circ D_p^{n_1} \circ D_1^{n_0}, \tag{13}$$

for $n = n_s p^s + \cdots + n_1 p + n_0$ the representation of n in base p, with $0 \le n_j \le p-1$ for each j, and where the exponent of n_j on D_{p^j} denotes the n_j-fold composition.

As remarked at the beginning of this section, the D_n's do not preserve modularity, but they do preserve quasimodularity, as shown in [4]. For our purposes, we shall only need this weaker version of their more general theorem:

Proposition 5. *Let f be a modular form of weight k and type l for $GL_2(A)$. Then for all $n \ge 0$ $D_n f$ is A-periodic and analytic at ∞, and for $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(A)$, we have*

$$D_n f(\gamma z) = (cz+d)^{k+2n} (\det \gamma)^{-l-n} \sum_{j=0}^{n} \binom{n+k-1}{j} \frac{D_{n-j} f(z)}{(-\tilde{\pi})^j} \left(\frac{c}{cz+d} \right)^j. \tag{14}$$

In other words, the function $D_n f$ is a quasimodular form of weight $k + 2n$, type $l + n$, and depth n.

Integrality and vanishing results

For $i \in \mathbb{N}$, write $[i] = T^{q^i} - T$, the product of all monic prime polynomials of degree dividing i, $d_i = [1]^{q^{i-1}} \cdots [i-1]^q [i]$, the product of all monics of degree i, and $d_0 = 1$. In [4], Bosser and Pellarin obtain the following result on the action of the D_n's on the u-series coefficients of quasimodular forms:

Proposition 6. *Let $f \in An(\Omega)$ be analytic at ∞ with u-series expansion $f(z) = \sum_{i \ge 0} a_i u^i$. Then for all $n \ge 0$ we have $D_n f(z) = \sum_{i \ge 2} b_{n,i} u^i$, where*

$$b_{n,i} = \sum_{r=1}^{i-1} (-1)^{n+r} \binom{i-1}{r} \left(\sum_{\substack{n_1, \dots, n_r \ge 0 \\ q^{n_1} + \cdots + q^{n_r} = n}} \frac{1}{d_{n_1} \cdots d_{n_r}} \right) a_{i-r}. \tag{15}$$

From this explicit formula, we can clearly see that

Corollary 1. *For $n < q^e$, the operator D_n preserves $\mathfrak{p}$-integrality of the u-series coefficients for all prime ideals $\mathfrak{p}$ generated by a prime polynomial of degree $\ge e$.*

Proof. Let e be a positive integer. If $n < q^e$, then we have $n_j < e$ for each n_j appearing in the sum defining the $b_{n,i}$'s in Equation (15). Since d_{n_j} is only divisible by primes of degree $\le n_j$, for $n < q^e$ D_n introduces only denominators of degree $< e$. □

From this, it easily follows that

Corollary 2. *Suppose that $f \equiv f' \pmod{\mathfrak{p}}$ for $\mathfrak{p}$ generated by a prime of degree d. Then, $D_n(f) \equiv D_n(f') \pmod{\mathfrak{p}}$ for $n < q^d$.*

We will also need:

Proposition 7. *Let $w \in \Omega$ and $f \in An(\Omega)$, then $ord_w D_n(f) \geq ord_w(f) - n$. When $n \leq ord_w(f)$, we have equality if and only if $\binom{ord_w(f)}{n} \not\equiv 0 \pmod p$.*

Proof. This follows by Proposition 4 part 1. □

A computational tool

The action of D_n quickly becomes difficult to compute explicitly as n grows. A better-behaved operator was defined by Serre in the classical case (see [20]), and we will use its analogue in the Drinfeld setting. Let n and d be non-negative integers. The nth Serre's operator of degree d is defined by the formula:

$$\partial_n^{(d)} f = D_n f + \sum_{i=1}^{n} (-1)^i \binom{d+n-1}{i} (D_{n-i} f)(D_{i-1} E). \tag{16}$$

In [5], the authors show that $\partial_n^{(k)}$ sends Drinfeld modular forms of weight k and type l to Drinfeld modular forms of weight $k + 2n$ and type $l + n$.

For simplicity, we will denote the operator $\partial_1^{(k)}$ by ∂ and make the convention that if f is a Drinfeld modular form of weight k, then $\partial(f) = \partial_1^{(k)}(f)$. Then for f a Drinfeld modular form of weight k,

$$\partial(f) = D_1(f) - kEf.$$

We have the following:

Proposition 8 (Gekeler [13]).

1. *Let f_i for $i = 1, 2$ be Drinfeld modular forms of weight k_i, then* $\partial(f_1 f_2) = \partial(f_1) f_2 + f_1 \partial(f_2)$.
2. $\partial(g) = -h$ *and* $\partial(h) = 0$.

This proposition allows us to compute the action of ∂ on all Drinfeld modular forms, since g and h generate the algebra of Drinfeld modular forms. Furthermore, since $D_n(E) = E^{n+1}$ for $1 \leq n < p$, a tedious but easy computation shows that for a Drinfeld modular form f of weight k, we have

$$\partial^n f = n!\, \partial_n^{(k)} f \tag{17}$$

for $1 \leq n < p$, where again the exponent on ∂ on the lefthand side denotes n-fold composition of the ∂ operator. This relation in fact holds for $p \leq n < q$ as well, which simply implies that the n-fold composition of ∂ beyond ∂^{p-1} is identically zero, as expected in characteristic p.

Weierstrass points on $X_0(\mathfrak{p})$

Previous results

As discussed in Section 'Weierstrass points in characteristic p', crucial to the study of Weierstrass points in positive characteristic is the knowledge of the curve's canonical gap sequence.

Proposition 9 (Armana, personal communication). *Let $\mathfrak{p}$ be a prime ideal generated by a polynomial of degree at least 3 in $\mathbb{F}_q[T]$. Then, $X_0(\mathfrak{p})$ has a classical gap sequence.*

Proof. Recall from Section 'Weierstrass points in characteristic p' that if X is a smooth projective irreducible curve defined over an algebraically closed field that has a classical gap sequence, then the osculation points and the Weierstrass points of X coincide; if X does not have a classical gap sequence, then every point of X is an osculation point.

Using an argument analogous to Ogg's argument in the classical case, Armana [2] shows the following: Let P be a K-rational point of $X_0(\mathfrak{p})$ such that its unique extension to a section of $\overline{M}_0(\mathfrak{p})$ over A is not supersingular at $\mathfrak{p}$, and denote by $c \geq 1$ the smallest pole number at P. Then $c \geq 1 + g_{\mathfrak{p}}$, where, as before, $g_{\mathfrak{p}}$ is the genus of $X_0(\mathfrak{p})$.

We repeat her argument here since [2] is in French: Let P be such a point, and let $c \geq 1$ be an integer such that c is a pole number of P; recall that this means that there is a function F on X that has a pole of order c at P and is regular elsewhere. Since P is K-rational, we may suppose that F is defined over K as well. The Fricke involution $W_{\mathfrak{p}}$ of $X_0(\mathfrak{p})$ is also defined over K, and we write $P' = W_{\mathfrak{p}}(P)$; P' is also K-rational. Up to adding to F a constant belonging to K, we may suppose that $f(P') = 0$.

As stated in Section 'Drinfeld modular curves,' the reduction of $X_0(\mathfrak{p})$ modulo $\mathfrak{p}$ is given by two copies Z and Z' of $X_0(1)$ intersecting transversally at the $g_{\mathfrak{p}}+1$ supersingular points over the algebraic closure of $A/\mathfrak{p}$ and interchanged by the Fricke involution $W_{\mathfrak{p}}$. Without loss of generality, suppose that the reduction modulo $\mathfrak{p}$ of P, which we denote $\tilde{P}$, belongs to Z and the reduction modulo $\mathfrak{p}$ of P', denoted $\tilde{P'}$, belongs to Z'. Up to multiplication by a constant in $K^{\times}$, we may suppose that the reduction modulo $\mathfrak{p}$ of F, $\tilde{F}$, is reduced and non-constant.

On Z', $\tilde{F}$ has a zero at $\tilde{P'}$ and no pole since $\tilde{P}$ is not supersingular and therefore does not belong to Z'. Therefore, $\tilde{F}$ is identically zero on Z'. In particular, $\tilde{F}$ vanishes at each supersingular point. On Z, the restriction of $\tilde{F}$ has at least $g_{\mathfrak{p}} + 1$ zeroes and at most a pole at P of order c. Since the degree of the divisor of a function is zero, it follows that $g_{\mathfrak{p}} + 1 \leq c$.

It suffices now to notice that such a point is not an osculation point of the curve. Either one of the cusps of $X_0(\mathfrak{p})$ satisfies the conditions on the point P above. Thus, $X_0(\mathfrak{p})$ has a point that is not an osculation point, and the result follows. □

Remark 7. The requirement that $\mathfrak{p}$ be generated by a prime polynomial of degree at least 3 ensures that $X_0(\mathfrak{p})$ has genus at least 2. (See Equation (4) for an expression giving the genus of $X_0(\mathfrak{p})$ as it depends on the degree d of the prime polynomial generating $\mathfrak{p}$ and Remark 2 for an explanation of the requirement that the genus be at least 2.)

It is immediate from the proof of Proposition 9 above that the K-rational Weierstrass points of $X_0(\mathfrak{p})$ have supersingular reduction modulo $\mathfrak{p}$. A stronger result can be deduced using the following theorem:

Theorem 9 (Baker [3]). *Let R be a complete discrete valuation ring with algebraically closed residue field k. Let X be a smooth, proper, geometrically connected curve defined over the fraction field of R, and denote by $\mathfrak{X}$ a proper model for X over R. (In other words, $\mathfrak{X}$ is a proper flat scheme over* Spec *R such that its generic fiber is X.) Suppose that the special fiber of $\mathfrak{X}$ consists of two genus 0 curves intersecting transversally at 3 or more points. Then, every Weierstrass point of X defined over the fraction field of R specializes to a singular point of the special fiber of $\mathfrak{X}$.*

The proof of this theorem is a corollary of a specialization lemma proved in the same paper, which roughly says that the dimension of a linear system can only increase under specialization from the curve X to the dual graph of the model $\mathfrak{X}$.

Let $K_{\mathfrak{p}}^{un}$ denote the maximal unramified extension of the field $K_{\mathfrak{p}}$, where $K_{\mathfrak{p}}$ the completion of K at $\mathfrak{p}$. Baker's theorem implies that the $K_{\mathfrak{p}}^{un}$-rational Weierstrass points of $X_0(\mathfrak{p})$ have supersingular reduction modulo $\mathfrak{p}$ since $\overline{M}_0(\mathfrak{p})$ satisfies the hypothesis of the theorem when considered as a scheme over the ring of integers of $K_{\mathfrak{p}}^{un}$.

The modular Wronskian

It is natural to ask whether it is possible to say more about the connection between the supersingular locus at $\mathfrak{p}$ and the Weierstrass points of $X_0(\mathfrak{p})$, as was done in the classical case by Rohrlich [25] and Ahlgren and Ono [1]. To refine the connection, we now develop the ideas of Section 'Weierstrass points in characteristic p' for the curve $X_0(\mathfrak{p})$ over C using Drinfeld modular forms, as Rohrlich did in the classical setting.

We consider the rigid analytic structure on $X_0(\mathfrak{p})$, so that we can compute with Drinfeld modular forms. For ease of reading, we will continue to write analytic below to mean rigid analytic. An analytic function without poles will be a holomorphic function, and an analytic function possibly with poles will be said to be meromorphic.

We first note that GAGA theorems hold for rigid analytic geometry [21,22]. More precisely, we will need the following: Let X be a smooth projective algebraic curve defined over a complete non-Archimedean field k of positive characteristic p, and let X^{an} be the rigid analytic space associated to X. (See for example [9] for the construction of X^{an}.) Then, there is an equivalence of category between the algebraic coherent sheaves on X and the analytic coherent sheaves on X^{an}. Using this correspondence, we will associate to an algebraic coherent sheaf F on X an analytic coherent sheaf denoted F^{an} on X^{an}.

We note that the sets of points (throughout, we will consider only C-valued points) of X and X^{an} coincide, so that we will not make a distinction between a divisor on X and a divisor on X^{an}. We denote by O the sheaf of algebraic regular functions on X and by $\mathcal{O}$ the sheaf of holomorphic functions on X^{an}.

The linear space $L(D)$ associated to a divisor D on X is the space of global sections of an algebraic sheaf which we will also denote by $L(D)$. The sheaf $L(D)$ is coherent and thus corresponds to a sheaf $L(D)^{an}$ on X^{an}.

Because the operation $*^{an}$ commutes with duals and tensor products, $L(D)^{an}$ is none other than $\mathcal{L}(D)$, the subsheaf of meromorphic functions $\mathcal{M}$ on X^{an} such that for U an open set of X^{an}, we have

$$\mathcal{L}(D)(U) = \{f \in \mathcal{M}(U) \,|\, [f] \geq -D|_U\} \cup \{0\}.$$

In particular, by GAGA, the space of global sections of $L(D)$ is isomorphic to the space of global sections of $\mathcal{L}(D)$, and for a point P of X^{an}, we may instead consider the sequence of spaces

$$k = \mathcal{L}(0)(X^{an}) \subseteq \mathcal{L}(P)(X^{an}) \subseteq \mathcal{L}(2P)(X^{an}) \subseteq \mathcal{L}(3P)(X^{an}) \subseteq \dots$$

Then, $L((n-1)P)(X) = L(nP)(X)$ if and only if $\mathcal{L}((n-1)P)(X^{an}) = \mathcal{L}(nP)(X^{an})$, so that the gap sequences can be computed analytically.

Denote by C_{can} a canonical divisor on X. Arguing as in the algebraic case, if j is a canonical order at P, there is $F \in \mathcal{L}(C_{\text{can}})(X^{an})$ such that $\nu_P(F) = j - \nu_P(C_{\text{can}})$.

We now start our work on $X_0(\mathfrak{p})$ in earnest. Our task now is to define a Drinfeld modular form $W(z)$ for $\Gamma_0(\mathfrak{p})$ whose divisor will capture information about the Weierstrass points of $X_0(\mathfrak{p})$. We note that since the cusps of $X_0(\mathfrak{p})$ are not Weierstrass points, to obtain our main result, it is enough to consider the divisor of $W(z)$ away from the cusps. In Section 'The order of vanishing of $\boldsymbol{W(z)}$ at the cusps,' we will collect what we know of the divisor of $W(z)$ at the cusp ∞. We recall that $Y_0(\mathfrak{p})$ denotes the affine curve whose C-points are exactly those of $X_0(\mathfrak{p})$ but with the cusps excluded.

We first compute the divisor of dz away from the cusps, where z is a parameter on Ω: Let $P \in Y_0(\mathfrak{p})$ and choose $\tau \in \Omega$ to be a representative of P in the Drinfeld upper half-plane. Throughout, we write e_τ for the order of the stabilizer of τ in

$$\widetilde{\Gamma}_0(\mathfrak{p}) = \Gamma_0(\mathfrak{p})/\,\Gamma_0(\mathfrak{p}) \cap Z(\mathrm{GL}_2(A)).$$

Then, we may choose $t = (z-\tau)^{e_\tau}$ as an analytic parameter at P. We have

$$dz = \frac{1}{e_\tau} t^{(e_\tau - 1)/e_\tau} dt$$

(e_τ is either 1 or $q+1$ [15] so it is prime to the characteristic p of C) and so dz has a pole of order

$$\frac{e_\tau - 1}{e_\tau}$$

at τ.

Proposition 10. *Let P be a point on $Y_0(\mathfrak{p})$, and write $j_0(P) = 0$ and $(j_1(P), \ldots, j_{g_\mathfrak{p}-1}(P))$ for the canonical orders at P. Choose $\tau \in \Omega$ to be a representative of P in the Drinfeld upper half-plane, and write e_τ for the order of the stabilizer of τ in $\widetilde{\Gamma}_0(\mathfrak{p})$. Then, there is a basis $\{f_i\}_{i=0}^{g_\mathfrak{p}-1}$ of $M_{2,1}^2(\Gamma_0(\mathfrak{p}))$ such that:*

$$ord_\tau(f_i) = e_\tau j_i(P) + e_\tau - 1.$$

for each i.

Proof. Fix a point P on $Y_0(\mathfrak{p})$, and let s be a parameter at P. We choose as our canonical divisor the divisor $[ds]$. There is a basis $\{F_0, \ldots, F_{g_\mathfrak{p}-1}\}$ of $\mathcal{L}([ds])$ such that $\mathrm{ord}_P(F_i) = j_i(P)$. Furthermore, $\{F_i ds\}$ is a basis for the space of analytic regular differentials $H^0(X_0(\mathfrak{p})^{an}, \Omega^1_{an})$ on $X_0(\mathfrak{p})$. Because of the correspondence between the space $M_{2,1}^2(\Gamma_0(\mathfrak{p}))$ of double cusp forms of weight 2 and type 1 for $\Gamma_0(\mathfrak{p})$ and the space of analytic regular differentials on $X_0(\mathfrak{p})$, we have that there is a basis $\{f_i\}$ for $M_{2,1}^2(\Gamma_0(\mathfrak{p}))$ such that $f_i(z)dz = F_i ds$. In particular, $\mathrm{ord}_P(f_i(z)dz) = \mathrm{ord}_P(F_i ds) = \mathrm{ord}_P(F_i) = j_i(P)$.

We now use the fact that for $P \in Y_0(\mathfrak{p})$, $\tau \in \Omega$ a representative of P in the Drinfeld upper half-plane and a Drinfeld modular form f, we have

$$\mathrm{ord}_P(f) = \frac{\mathrm{ord}_\tau(f)}{e_\tau}.$$

Then,

$$\mathrm{ord}_P(f_i(z)dz) = \mathrm{ord}_P(f_i) + \mathrm{ord}_P(dz) = \frac{\mathrm{ord}_\tau(f_i)}{e_\tau} - \frac{e_\tau - 1}{e_\tau},$$

and the result follows. □

Definition 5. For any basis $\{f_0,f_1,\ldots f_{g_\mathfrak{p}-1}\}$ of $M^2_{2,1}(\Gamma_0(\mathfrak{p}))$, we define

$$W\left(f_0,\ldots,f_{g_\mathfrak{p}-1}\right)=\begin{vmatrix} f_0(z) & D_1(f_0(z)) & \ldots & D_{g_\mathfrak{p}-1}(f_0(z)) \\ \vdots & & \vdots & \\ f_{g_\mathfrak{p}-1}(z) & D_1(f_{g_\mathfrak{p}-1}(z)) & \ldots & D_{g_\mathfrak{p}-1}(f_{g_\mathfrak{p}-1}(z)) \end{vmatrix},$$

where D_n is the normalized Hasse derivative introduced in Section 'Hyperderivatives and quasimodular forms'. This is a modular form of weight $g_\mathfrak{p}(g_\mathfrak{p}+1)$ and type $\frac{g_\mathfrak{p}(g_\mathfrak{p}+1)}{2}$ for $\Gamma_0(\mathfrak{p})$.

If $\left\{f_0,\ldots f_{g_\mathfrak{p}-1}\right\}$ and $\left\{f'_0,\ldots f'_{g_\mathfrak{p}-1}\right\}$ are two bases for $M^2_{2,1}(\Gamma_0(\mathfrak{p}))$, then $W\left(f_0,\ldots,f_{g_\mathfrak{p}-1}\right) = aW\left(f'_0,\ldots,f'_{g_\mathfrak{p}-1}\right)$ for $0\neq a\in C$.

Lemma 2. *There exists a basis* $\left\{f_0,\ldots,f_{g_\mathfrak{p}-1}\right\}$ *of* $M^2_{2,1}(\Gamma_0(\mathfrak{p}))$ *with integral u-series coefficients at* ∞ *such that* $W(f_0,\ldots,f_{g_\mathfrak{p}-1})$ *has rational,* $\mathfrak{p}$*-integral u-series coefficients at* ∞ *and*

$$v_\mathfrak{p}(W(f_0,\ldots,f_{g_\mathfrak{p}-1}))=0.$$

Proof. By Remark 5, there is a basis $\left\{f_1,\ldots,f_{g_\mathfrak{p}}\right\}$ for the space $M^2_{2,1}(\Gamma_0(\mathfrak{p}))$ that has integral u-series coefficients at ∞.

When computing $W(f_1,\ldots,f_{g_\mathfrak{p}})$, we will compute D_n for $n\leq g_\mathfrak{p}-1$. From the explicit formula (4), we have $g_\mathfrak{p}\leq 2q^{d-2}$, so that $n\leq 2q^{d-2}-1<q^d$. In this case, Proposition 1 says that D_n preserves $\mathfrak{p}$-integrality of the u-series coefficients, so $W(f_1,\ldots,f_{g_\mathfrak{p}})$ has rational, $\mathfrak{p}$-integral u-series coefficients.

Suppose that

$$v_\mathfrak{p}(W(f_0,\ldots,f_{g_\mathfrak{p}-1}))>0.$$

Then, there exist $a_0,\ldots,a_{g_\mathfrak{p}-1}$ with each $a_i\in A$ such that

$$a_0f_0+\ldots+a_{g_\mathfrak{p}-1}f_{g_\mathfrak{p}-1}\equiv 0 \pmod{\mathfrak{p}},$$

and for at least one i such that $0\leq i\leq g_\mathfrak{p}-1$,

$$a_i\not\equiv 0 \pmod{\mathfrak{p}}.$$

Without loss of generality, suppose that

$$a_0\not\equiv 0 \pmod{\mathfrak{p}}.$$

Then, we have

$$v_\mathfrak{p}\left(f_0+\frac{1}{a_0}\left(a_1f_1+\ldots+a_{g_\mathfrak{p}-1}f_{g_\mathfrak{p}-1}\right)\right)=m>0,$$

for some $m\in\mathbb{Z}$. Putting

$$f'_0=\frac{1}{\pi^m}\left(f_0+\frac{1}{a_0}\left(a_1f_1+\ldots+a_{g_\mathfrak{p}-1}f_{g_\mathfrak{p}-1}\right)\right),$$

we have that f'_0 has integral u-series coefficients at ∞, $W(f'_0,f_1,\ldots f_{g_\mathfrak{p}-1})$ has rational, $\mathfrak{p}$-integral u-series coefficients at ∞, and

$$v_\mathfrak{p}(W(f_0,\ldots,f_{g_\mathfrak{p}-1}))>v_\mathfrak{p}(W(f'_0,\ldots,f_{g_\mathfrak{p}-1})).$$

If

$$\nu_{\mathfrak{p}}(W(f_0',\ldots,f_{g_{\mathfrak{p}}-1}))>0,$$

we may repeat the procedure above. We can continue this process until the valuation is 0. □

Definition 6. As a consequence of Lemma 2, there is a unique Drinfeld modular form $W(f_0,\ldots,f_{g_{\mathfrak{p}}-1})$ such that

$$\nu_{\mathfrak{p}}(W(f_0,\ldots,f_{g_{\mathfrak{p}}-1}))=0$$

and the leading coefficient of $W(f_0,\ldots,f_{g_{\mathfrak{p}}-1})$ is a power of π. We denote this form by $W(z)$ and call it the *modular Wronskian* of $X_0(\mathfrak{p})$.

We note that the forms $\{f_0,\ldots,f_{g_{\mathfrak{p}}-1}\}$ which give us $W(z)$ can be chosen to have rational, $\mathfrak{p}$-integral u-series coefficients at ∞.

We are interested in $W(z)$ because of its relation to the Weierstrass points of $X_0(\mathfrak{p})$:

Theorem 10. *Let $(n_1,\ldots,n_{g_{\mathfrak{p}}})=(1,\ldots,g_{\mathfrak{p}})$ denote the canonical gap sequence of $X_0(\mathfrak{p})$, P be a point of $Y_0(\mathfrak{p})$, and $(n_1(P),\ldots,n_{g_{\mathfrak{p}}}(P))$ be the gap sequence at P. Then, we have*

$$\mathrm{ord}_P\left(W(z)(dz)^{g_{\mathfrak{p}}(g_{\mathfrak{p}}+1)/2}\right)\geq\sum_{i=1}^{g_{\mathfrak{p}}}(n_i(P)-n_i).$$

In addition, when P is not an elliptic point nor a Weierstrass point, we have equality:

$$\mathrm{ord}_P\left(W(z)(dz)^{g_{\mathfrak{p}}(g_{\mathfrak{p}}+1)/2}\right)=0.$$

Proof. Let P be a point on $Y_0(\mathfrak{p})$, and choose a basis $\{f_i\}$ of $M_{2,1}^2(\Gamma_0(\mathfrak{p}))$ that satisfies the conclusion of Proposition 10. We also continue to use the notation introduced in the statement of Proposition 10. Then

$$\mathrm{ord}_P\left(W(f_0,\ldots,f_{g_{\mathfrak{p}}-1})(dz)^{g_{\mathfrak{p}}(g_{\mathfrak{p}}+1)/2}\right)=\mathrm{ord}_P\left(W(z)(dz)^{g_{\mathfrak{p}}(g_{\mathfrak{p}}+1)/2}\right),$$

so we may work with $W(f_0,\ldots,f_{g_{\mathfrak{p}}-1})$ for convenience.

Choose $\tau\in\Omega$ to be a representative of P in the Drinfeld upper half-plane. By Proposition 7, for $k=0,\ldots,g_{\mathfrak{p}}-1$, we have that

$$\mathrm{ord}_\tau(D_k(f_l))\geq e_\tau j_l(P)+e_\tau-1-k$$

with equality if and only if $\binom{e_\tau j_l(P)+e_\tau-1}{k}\not\equiv 0 \pmod p$. When computing the determinant $W(f_0,\ldots,f_{g_{\mathfrak{p}}-1})$, we will be adding terms all of whose order of vanishing at τ is $\geq\sum_{i=0}^{g_{\mathfrak{p}}-1}(e_\tau j_i(P)-i+e_\tau-1)$. Thus,

$$\mathrm{ord}_\tau W(f_0,\ldots,f_{g_{\mathfrak{p}}-1})\geq\sum_{i=0}^{g_{\mathfrak{p}}-1}(e_\tau j_i(P)-i+e_\tau-1).$$

Since $X_0(\mathfrak{p})$ has canonical orders $(j_1,\ldots,j_{g_{\mathfrak{p}}-1})=(1,\ldots,g_{\mathfrak{p}}-1)$ and

$$\sum_{i=1}^{g_{\mathfrak{p}}}(n_i(P)-n_i)=\sum_{i=1}^{g_{\mathfrak{p}}-1}(j_i(P)-j_i),$$

for any point P on $X_0(\mathfrak{p})$, we have

$$\sum_{i=0}^{g_\mathfrak{p}-1}(e_\tau j_i(P)-i+e_\tau-1)=e_\tau\sum_{i=1}^{g_\mathfrak{p}}(n_i(P)-n_i)+\frac{g_\mathfrak{p}(g_\mathfrak{p}+1)}{2}(e_\tau-1).$$

Thus,

$$\begin{aligned}\operatorname{ord}_P\left(W(f_0,\ldots,f_{g_\mathfrak{p}-1})(dz)^{g_\mathfrak{p}(g_\mathfrak{p}+1)/2}\right)&\geq\sum_{i=1}^{g_\mathfrak{p}}(n_i(P)-n_i)+\frac{g_\mathfrak{p}(g_\mathfrak{p}+1)}{2}\frac{e_\tau-1}{e_\tau}\\&\quad-\frac{g_\mathfrak{p}(g_\mathfrak{p}+1)}{2}\frac{e_\tau-1}{e_\tau}\\&=\sum_{i=1}^{g_\mathfrak{p}}(n_i(P)-n_i).\end{aligned}$$

In the case where P is not elliptic and P is not a Weierstrass point, the terms on the diagonal of $W(f_0,\ldots,f_{g_\mathfrak{p}-1})$ have order of vanishing exactly 0, and all of the terms below the diagonal have order of vanishing strictly greater than 0. Thus, $\operatorname{ord}_\tau W(f_0,\ldots,f_{g_\mathfrak{p}-1})=0=\sum_{i=1}^{g_\mathfrak{p}}(n_i(P)-n_i)$.

□

The significance of the previous theorem is that away from the cusps, the divisor

$$[W(z)]+\frac{g_\mathfrak{p}(g_\mathfrak{p}+1)}{2}[dz]$$

is the modular avatar of the invariant divisor w constructed by Stöhr and Voloch [27]. Consequently, we make the following definition:

Definition 7. The (modular) Weierstrass weight of a point P on $Y_0(\mathfrak{p})$ is

$$\operatorname{wt}(P)=\operatorname{ord}_P\left(W(z)(dz)^{g_\mathfrak{p}(g_\mathfrak{p}+1)/2}\right).$$

Finally, to apply Theorem 5, we will need:

Proposition 11. *Suppose that q is odd. Then, $W(z)$ is an eigenform of the Fricke involution.*

Proof. Since we are in odd characteristic, the Fricke involution is diagonalizable. Let $\{f_1,\ldots,f_{g_\mathfrak{p}}\}$ be a basis of eigenforms of $W_\mathfrak{p}$ of the space $M_{2,1}^2(\Gamma_0(\mathfrak{p}))$, say with $f_i|[W_\mathfrak{p}]=\lambda_i f_i$.

We compute

$$\begin{aligned}W(f_0,\ldots,f_{g_\mathfrak{p}-1})\left(\frac{-1}{\pi z}\right)&=\begin{vmatrix}f_0\left(\frac{-1}{\pi z}\right)&(D_1f_0)\left(\frac{-1}{\pi z}\right)&\ldots&(D_{g_\mathfrak{p}-1}f_0)\left(\frac{-1}{\pi z}\right)\\\vdots&&\vdots&\\f_{g_\mathfrak{p}-1}\left(\frac{-1}{\pi z}\right)&(D_1f_{g_\mathfrak{p}-1})\left(\frac{-1}{\pi z}\right)&\ldots&(D_{g_\mathfrak{p}-1}f_{g_\mathfrak{p}-1})\left(\frac{-1}{\pi z}\right)\end{vmatrix}\\&=\begin{vmatrix}\lambda_0\pi z^2f_0(z)&(D_1f_0)\left(\frac{-1}{\pi z}\right)&\ldots&(D_{g_\mathfrak{p}-1}f_0)\left(\frac{-1}{\pi z}\right)\\\vdots&&\vdots&\\\lambda_{g_\mathfrak{p}-1}\pi z^2f_{g_\mathfrak{p}-1}(z)&(D_1f_{g_\mathfrak{p}-1})\left(\frac{-1}{\pi z}\right)&\ldots&(D_{g_\mathfrak{p}-1}f_{g_\mathfrak{p}-1})\left(\frac{-1}{\pi z}\right)\end{vmatrix}.\end{aligned}$$

By Proposition 1, we have for each i and n:

$$D_n\left(f_i\left(\frac{-1}{\pi z}\right)\right) = z^{-n}\sum_{j=1}^{n}(-1)^j\binom{n-1}{n-j}\frac{1}{(\pi z)^j}\frac{1}{(-\tilde{\pi})^{n-j}}(D_jf_i)\left(\frac{-1}{\pi z}\right). \tag{18}$$

Furthermore using the product rule, we have

$$D_n\left(\lambda_i\pi z^2 f_i(z)\right) = \lambda_i\pi\left(z^2(D_nf)(z) + 2z(D_{n-1}f)(z) + (D_{n-2}f)(z)\right). \tag{19}$$

Combining Equations (18) and (19) and using induction on n, we obtain that

$$(D_nf_i)\left(\frac{-1}{\pi z}\right) = (-1)^n\lambda_i\pi^{n+1}z^{2n+2}(D_nf_i)(z) + \lambda_i\left(\sum_{j=0}^{n-1}A_{n,j}(\pi,z)(D_nf_i)(z)\right),$$

where $A_{n,j}$ is a polynomial that depends only on n and j. Therefore, we may successively add to column C_n linear combinations of earlier columns to obtain

$$W(f_0,\ldots,f_{g_{\mathfrak{p}}-1})\left(\frac{-1}{\pi z}\right) = |\ \lambda_i\pi^{n+1}z^{2n+2}(D_nf_i)(z)\ |,$$

where $0 \le i \le g_{\mathfrak{p}} - 1$ indexes the rows and $0 \le n \le g_{\mathfrak{p}} - 1$ indexes the columns of the matrix.

Pulling out the constant λ_i from each row and $\pi^{n+1}z^{2n+2}$ from each column gives

$$W(f_0,\ldots,f_{g_{\mathfrak{p}}-1})\left(\frac{-1}{\pi z}\right) = \left(\prod_{i=0}^{g_{\mathfrak{p}}-1}\lambda_i\right)\pi^{g_{\mathfrak{p}}(g_{\mathfrak{p}}+1)/2}z^{g_{\mathfrak{p}}(g_{\mathfrak{p}}+1)}W(f_0,\ldots,f_{g_{\mathfrak{p}}-1})(z).$$

Since $W(z)$ is a constant multiple of $W(f_0,\ldots,f_{g_{\mathfrak{p}}-1})(z)$, we conclude that $W(z)$ is an eigenform of the Fricke involution with eigenvalue $\prod_{i=0}^{g_{\mathfrak{p}}-1}\lambda_i$. □

Proof of Theorem 1

We are now in a position to prove our main theorem.

For simplicity throughout this section, we will write

$$\mathcal{W} = \widetilde{N(W)} = \pi^{q^dk/2}\prod_{\gamma\in\Gamma_0(\mathfrak{p})\backslash\mathrm{GL}_2(A)} W|_{k,l}[\gamma], \tag{20}$$

which is the form appearing in the statement of Theorem 5. It has weight $(q^d+1)g_{\mathfrak{p}}(g_{\mathfrak{p}}+1)$ and type $g_{\mathfrak{p}}(g_{\mathfrak{p}}+1)$. We also write

$$F_{\mathfrak{p}}(x) \overset{\mathrm{def}}{=} \prod_{P\in Y_0(\mathfrak{p})}(x - j(P))^{\mathrm{wt}(P)}. \tag{21}$$

We note that this is a polynomial since only finitely many points P have $\mathrm{wt}(P) \neq 0$, where $\mathrm{wt}(P)$ is as in Definition 7, and that we have excluded the cusps from consideration in this product, so that the quantity $j(P)$ is not infinite.

The strategy to prove Theorem 1 is to relate the companion polynomial of $\mathcal{W}(z)$ to the polynomial $F_{\mathfrak{p}}(x)$. Then applying Theorems 4 and 5 to $W(z)$, we show that $\mathcal{W}$ has lower filtration than weight, and conclude that its divisor is supported on all of the supersingular locus.

Theorem 11. *Let $\mathcal{W}(z)$ be as in Equation (20). Let $P(\mathcal{W},x)$ be the companion polynomial of the form $\mathcal{W}(z)$ defined in Equation (8). Then,*

$$P(\mathcal{W},x) = x^{\epsilon(d)}F_{\mathfrak{p}}(x).$$

for

$$\epsilon(d) = \begin{cases} \frac{1}{q+1}(qg_{\mathfrak{p}}(g_{\mathfrak{p}}+1) - \gamma((q^d+1)g_{\mathfrak{p}}(g_{\mathfrak{p}}+1), g_{\mathfrak{p}}(g_{\mathfrak{p}}+1))) & \text{if } d \text{ is even,} \\ \frac{1}{q+1}\gamma((q^d+1)g_{\mathfrak{p}}(g_{\mathfrak{p}}+1), g_{\mathfrak{p}}(g_{\mathfrak{p}}+1)) & \text{if } d \text{ is odd.} \end{cases}$$

Proof. Our strategy to relate $P(\mathcal{W}, x)$ to $F_{\mathfrak{p}}(x)$ is to first relate the Weierstrass weight $\mathrm{wt}(P)$ of a point to the order of vanishing at τ of $W(z)$, where τ is a representative of P in the upper half-plane. We then relate the order of vanishing of $\mathcal{W}(z)$ at $\tau_0 \in \Omega$ to the order of vanishing of $W(z)$ at points τ that are $\mathrm{GL}_2(A)$-equivalent to τ_0.

Let τ be any element of the Drinfeld upper half-plane Ω, and let P_τ be the point on $Y_0(\mathfrak{p})$ corresponding to τ. Further, let e_τ be the order of the stabilizer of τ in $\widetilde{\Gamma}_0(\mathfrak{p})$. Then, we have

$$\frac{1}{e_\tau}\mathrm{ord}_\tau W(z) = \mathrm{ord}_{P_\tau}\left(W(z)(dz)^{g_{\mathfrak{p}}(g_{\mathfrak{p}}+1)/2}\right) + \frac{g_{\mathfrak{p}}(g_{\mathfrak{p}}+1)}{2}\left(1 - \frac{1}{e_\tau}\right).$$

In the case where P_τ is not elliptic, since $e_\tau = 1$, we simply obtain that

$$\mathrm{ord}_\tau W(z) = \mathrm{wt}(P_\tau), \tag{22}$$

whereas if P is elliptic, in which case $e_\tau = q+1$, we have

$$\mathrm{ord}_\tau W(z) = (q+1)\mathrm{wt}(P_\tau) + q\frac{g_{\mathfrak{p}}(g_{\mathfrak{p}}+1)}{2}. \tag{23}$$

We now proceed to the second step of the proof.

Let first τ_0 be a point in the Drinfeld upper-half space Ω that is not in the equivalence class of the elliptic point of $X_0(1)$. Since $\mathcal{W}$ is a multiple of

$$\prod_{\gamma \in \Gamma_0(\mathfrak{p})\backslash \mathrm{GL}_2(A)} W|_{k,l}[\gamma],$$

and the map $X_0(\mathfrak{p}) \to X_0(1)$ is unramified above τ_0, we have

$$\mathrm{ord}_{\tau_0}\mathcal{W}(z) = \sum_{\substack{P_\tau \in Y_0(\mathfrak{p}),\\ \tau\sim\tau_0}} \mathrm{ord}_\tau W(z) = \sum_{\substack{P_\tau \in Y_0(\mathfrak{p}),\\ \tau\sim\tau_0}} \mathrm{wt}(P_\tau), \tag{24}$$

where $\sim$ denotes $\mathrm{GL}_2(A)$-equivalence.

We note that in Equation (24), the left-hand side is exactly the power of $(x - j(\tau_0))$ appearing in $P(\mathcal{W}, x)$ and the right-hand side is exactly the power of $(x - j(\tau_0))$ in $x^{\epsilon(d)}F_{\mathfrak{p}}(x)$.

We now consider the case of τ_0 in the equivalence class of the elliptic point of $X_0(1)$, i.e., $j(\tau_0) = 0$.

The case of d even: If the degree d of the prime polynomial generating $\mathfrak{p}$ is even, then $X_0(\mathfrak{p})$ has two elliptic points, both of which are unramified over $X_0(1)$. The fiber above the elliptic point of $X_0(1)$ in $X_0(\mathfrak{p})$ contains in addition $\frac{q^d-1}{q+1}$ non-elliptic points, each ramified above $P_{\tau_0} \in X_0(1)$ with index $q+1$ ([10], pages 77-78).

Thus if $\tau_0 \in \Omega$ is in the $\mathrm{GL}_2(A)$-equivalence class of the elliptic point on $X_0(1)$, using Equations (22) and (23), we have

$$\mathrm{ord}_{\tau_0}\mathcal{W}(z) = 2q\frac{g_{\mathfrak{p}}(g_{\mathfrak{p}}+1)}{2} + (q+1)\sum_{\substack{\tau \in Y_0(\mathfrak{p}),\\ \tau\sim\tau_0}} \mathrm{wt}(P_\tau).$$

On the other hand, by Equation (8), we have

$$\mathrm{ord}_{\tau_0}\mathcal{W}(z) = \gamma((q^d+1)g_{\mathfrak{p}}(g_{\mathfrak{p}}+1), g_{\mathfrak{p}}(g_{\mathfrak{p}}+1)) + (q+1)M,$$

where M is the order of vanishing of $P(\mathcal{W}, x)$ at $j(\tau_0) = 0$.

Combining these two equations, we obtain

$$M = \frac{1}{q+1}(qg_{\mathfrak{p}}(g_{\mathfrak{p}}+1) - \gamma((q^d+1)g_{\mathfrak{p}}(g_{\mathfrak{p}}+1), g_{\mathfrak{p}}(g_{\mathfrak{p}}+1))) + \sum_{\substack{\tau\in Y_0(\mathfrak{p}),\\ \tau\sim\tau_0}} \mathrm{wt}(P_\tau). \quad (25)$$

For d even, let $\epsilon(d) = \frac{1}{q+1}(qg_{\mathfrak{p}}(g_{\mathfrak{p}}+1) - \gamma((q^d+1)g_{\mathfrak{p}}(g_{\mathfrak{p}}+1), g_{\mathfrak{p}}(g_{\mathfrak{p}}+1)))$.

Equations (24) and (25) imply the equality of polynomials

$$P(\mathcal{W}, x) = x^{\epsilon(d)} F_{\mathfrak{p}}(x).$$

The case of d odd: If the degree d of the prime polynomial generating $\mathfrak{p}$ is odd, then $X_0(\mathfrak{p})$ has no elliptic points, and the fiber above the elliptic point of $X_0(1)$ in $X_0(\mathfrak{p})$ contains $\frac{q^d+1}{q+1}$ non-elliptic points, each ramified above $X_0(1)$ with index $q+1$. Thus if τ_0 is in the $\mathrm{GL}_2(A)$-equivalence class of the elliptic point on $X_0(1)$, we have

$$\mathrm{ord}_{\tau_0}\mathcal{W}(z) = (q+1)\sum_{\substack{\tau\in Y_0(\mathfrak{p}),\\ \tau\sim\tau_0}} \mathrm{wt}(P_\tau).$$

On the other hand, by Equation (8), we have

$$\mathrm{ord}_{\tau_0}\mathcal{W}(z) = \gamma((q^d+1)g_{\mathfrak{p}}(g_{\mathfrak{p}}+1), g_{\mathfrak{p}}(g_{\mathfrak{p}}+1)) + (q+1)M,$$

where M is the order of vanishing of $P(\mathcal{W}, x)$ at $j(\tau_0) = 0$.

Combining these two equations, we obtain that

$$M = \frac{1}{q+1}\gamma((q^d+1)g_{\mathfrak{p}}(g_{\mathfrak{p}}+1), g_{\mathfrak{p}}(g_{\mathfrak{p}}+1)) + \sum_{\substack{\tau\in Y_0(\mathfrak{p}),\\ \tau\sim\tau_0}} \mathrm{wt}(P_\tau). \quad (26)$$

For d odd, let $\epsilon(d) = \frac{1}{q+1}\gamma((q^d+1)g_{\mathfrak{p}}(g_{\mathfrak{p}}+1), g_{\mathfrak{p}}(g_{\mathfrak{p}}+1))$.

Equations (24) and (26) now imply

$$P(\mathcal{W}, x) = x^{\epsilon(d)} F_{\mathfrak{p}}(x),$$

as in the even case but with a different $\epsilon(d)$. □

We now use the trace map to obtain a form of low weight for $\mathrm{GL}_2(A)$ that is congruent to $W(z)$ modulo $\mathfrak{p}$.

Theorem 12. *Let $q \geq 3$, then there exists a Drinfeld modular form F of weight $g_{\mathfrak{p}}(g_{\mathfrak{p}}+q^d)$ and type $\frac{g_{\mathfrak{p}}(g_{\mathfrak{p}}+1)}{2}$ for $GL_2(A)$ such that*

$$W(z) \equiv F(z) \pmod{\mathfrak{p}}.$$

Proof. We choose a basis $\{f_0, \ldots, f_{g_{\mathfrak{p}}-1}\}$ for the space $M^2_{2,1}(\Gamma_0(\mathfrak{p}))$ such that

$$W(z) = W(f_0, \ldots, f_{g_{\mathfrak{p}}-1}),$$

and such that for each i, f_i has rational, $\mathfrak{p}$-integral u-series coefficients at ∞.

By Theorem 4, there is a basis $\{F_0, \ldots, F_{g_{\mathfrak{p}}-1}\}$ for the space $M^2_{q^d+1,1}(\mathrm{GL}_2(A))$, all of whose elements have rational, $\mathfrak{p}$-integral u-series coefficients and such that $f_i \equiv F_i \pmod{\mathfrak{p}}$.

As we remarked in the proof of Proposition 2, when computing the forms $W(f_0, \ldots, f_{g_{\mathfrak{p}}-1})$ and $W(F_0, \ldots, F_{g_{\mathfrak{p}}-1})$, one needs to compute D_n for $n < q^d$. Thus in all of the cases we will consider, we have that $f_i \equiv F_i \pmod{\mathfrak{p}}$ implies that $D_n(f_i) \equiv D_n(F_i) \pmod{\mathfrak{p}}$ by Corollary 2.

Therefore, we have

$$W(f_0,\dots,f_{g_\mathfrak{p}-1}) \equiv W(F_0,\dots,F_{g_\mathfrak{p}-1}) \pmod{\mathfrak{p}}.$$

The form $W(F_0,\dots,F_{g_\mathfrak{p}-1})$ is modular for $\mathrm{GL}_2(A)$ of weight $g_\mathfrak{p}(g_\mathfrak{p}+q^d)$ and type $\frac{g_\mathfrak{p}(g_\mathfrak{p}+1)}{2}$, and we denote it F for simplicity. □

We can now prove Theorem 1:

Proof. Since W has rational, $\mathfrak{p}$-integral u-series coefficients at ∞ and is an eigenform of the Fricke involution, Theorem 5 states that

$$\mathcal{W} = \widetilde{\mathrm{N}(W)} \equiv W^2 \pmod{\mathfrak{p}},$$

As remarked earlier, $\mathcal{W}$ is a form of weight $(q^d+1)g_\mathfrak{p}(g_\mathfrak{p}+1)$ and type $g_\mathfrak{p}(g_\mathfrak{p}+1)$ for $\mathrm{GL}_2(A)$.

By Theorem 12, we have

$$\mathcal{W} \equiv F^2 \pmod{\mathfrak{p}}. \tag{27}$$

The form F^2 is of weight $2g_\mathfrak{p}(g_\mathfrak{p}+q^d)$ and type $g_\mathfrak{p}(g_\mathfrak{p}+1)$.

We note now that the proof of Proposition 2 can be adapted say the following: Let f and f' be two Drinfeld modular forms for $\mathrm{GL}_2(A)$ of weights $k > k'$ and of types l and l', respectively, both with rational $\mathfrak{p}$-integral u-series coefficients and not $\equiv 0 \pmod{\mathfrak{p}}$. Then for $\alpha = \frac{k-k'}{q^d-1}$ and $a = \left\lfloor \frac{\alpha\gamma(q^d-1,0)q+\gamma(k,l)}{q+1} \right\rfloor$, the polynomial $x^a P(f,x)$ is divisible by $S_\mathfrak{p}(x)^\alpha$ in $\mathbb{F}_\mathfrak{p}[x]$. (We recall that $\mathbb{F}_\mathfrak{p}$ is the field $A/\mathfrak{p}$.)

Applying this to Equation (27), we have $\alpha = g_\mathfrak{p}(g_\mathfrak{p}-1)$. Then in $\mathbb{F}_\mathfrak{p}[x]$, we have that

$$S_\mathfrak{p}(x)^{g_\mathfrak{p}(g_\mathfrak{p}-1)} \mid x^a P(\mathcal{W},x) = x^{a+\epsilon(d)} F_\mathfrak{p}(x),$$

where

$$a = \left\lfloor \frac{g_\mathfrak{p}(g_\mathfrak{p}-1)\gamma(q^d-1,0)q + \gamma((q^d+1)g_\mathfrak{p}(g_\mathfrak{p}+1), g_\mathfrak{p}(g_\mathfrak{p}+1))}{q+1} \right\rfloor. \tag{28}$$

The case of d even: In this case, $j=0$ is not supersingular at $\mathfrak{p}$, so x does not divide $S_\mathfrak{p}(x)$, and we conclude that

$$S_\mathfrak{p}(x)^{g_\mathfrak{p}(g_\mathfrak{p}-1)} \mid F_\mathfrak{p}(x).$$

Thus, each supersingular j-invariant is the reduction modulo $\mathfrak{p}$ of a root of $F_\mathfrak{p}(x)$.

By Theorem 10, for $P \in Y_0(\mathfrak{p})$,

$$\mathrm{wt}(P) = \mathrm{ord}_P(W(z)(dz)^{g_\mathfrak{p}(g_\mathfrak{p}+1)/2}) \geq \sum_{i=1}^{g_\mathfrak{p}} (n_i(P)-n_i),$$

with $\mathrm{wt}(P)=0$ if P is neither a Weierstrass point nor an elliptic point. Recall also that a Weierstrass point is a point such that

$$\sum_{i=1}^{g_\mathfrak{p}} (n_i(P)-n_i) > 0.$$

By definition (Equation (21)), the polynomial $F_\mathfrak{p}(x)$ has zeroes at the Weierstrass points and possibly also at the elliptic points of $X_0(\mathfrak{p})$, which have $j=0$. Since $j=0$ is not supersingular when d is even, then each supersingular j-invariant is the reduction modulo $\mathfrak{p}$ of the j-invariant of a Weierstrass point.

The case of d odd: As argued in the case of d even, the zeroes of $F_{\mathfrak{p}}$ are either Weierstrass points or elliptic points. Since $X_0(\mathfrak{p})$ does not have elliptic points when d is odd, the zeroes of $F_{\mathfrak{p}}$ are exactly the Weierstrass points.

Since

$$S_{\mathfrak{p}}(x)^{g_{\mathfrak{p}}(g_{\mathfrak{p}}-1)} \mid x^{a+\epsilon(d)}F_{\mathfrak{p}}(x),$$

where a is as in Equation (28) and $\epsilon(d)$ is as in the statement of Theorem 11, we conclude that each supersingular j-invariant in characteristic $\mathfrak{p}$ except possibly $j = 0$ is the reduction modulo $\mathfrak{p}$ of the j-invariant of a Weierstrass point.

To conclude that $j = 0$ is also the j-invariant of a Weierstrass point, we must show that

$$g_{\mathfrak{p}}(g_{\mathfrak{p}} - 1) > a + \epsilon(d),$$

from which it will follow that $x \mid F_{\mathfrak{p}}(x)$.

We first investigate the number $\epsilon(d) = \frac{1}{q+1}\gamma((q^d + 1)g_{\mathfrak{p}}(g_{\mathfrak{p}} + 1), g_{\mathfrak{p}}(g_{\mathfrak{p}} + 1))$. Since $(q^d + 1)g_{\mathfrak{p}}(g_{\mathfrak{p}} + 1)$ is divisible by $q + 1$ and by the uniqueness of the numbers $\gamma((q^d + 1)g_{\mathfrak{p}}(g_{\mathfrak{p}} + 1), g_{\mathfrak{p}}(g_{\mathfrak{p}} + 1))$ and $\mu((q^d + 1)g_{\mathfrak{p}}(g_{\mathfrak{p}} + 1), g_{\mathfrak{p}}(g_{\mathfrak{p}} + 1))$, satisfying the conditions of (7), we must have

$$\mu((q^d + 1)g_{\mathfrak{p}}(g_{\mathfrak{p}} + 1), g_{\mathfrak{p}}(g_{\mathfrak{p}} + 1)) = \frac{(q^d + 1)g_{\mathfrak{p}}(g_{\mathfrak{p}} + 1)}{q + 1}$$

and

$$\gamma((q^d + 1)g_{\mathfrak{p}}(g_{\mathfrak{p}} + 1), g_{\mathfrak{p}}(g_{\mathfrak{p}} + 1)) = 0,$$

so $\epsilon(d) = 0$ when d is odd.

Since d is odd, we have that $\gamma(q^d - 1, 0) = 1$ and in light of the work above, the formula for a simplifies to

$$a = \left\lfloor \frac{g_{\mathfrak{p}}(g_{\mathfrak{p}} - 1)q}{q + 1} \right\rfloor.$$

Since

$$\left\lfloor \frac{g_{\mathfrak{p}}(g_{\mathfrak{p}} - 1)q}{q + 1} \right\rfloor \leq \frac{g_{\mathfrak{p}}(g_{\mathfrak{p}} - 1)q}{q + 1} < g_{\mathfrak{p}}(g_{\mathfrak{p}} - 1),$$

it follows that $j = 0$ is also the reduction modulo $\mathfrak{p}$ of the j-invariant of a Weierstrass point of $X_0(\mathfrak{p})$. □

A refinement of the statement

Since $\mathcal{W}$ is of weight $(q^d + 1)g_{\mathfrak{p}}(g_{\mathfrak{p}} + 1)$ and type $g_{\mathfrak{p}}(g_{\mathfrak{p}} + 1)$, F^2 is of weight $2g_{\mathfrak{p}}(g_{\mathfrak{p}} + q^d)$ and type $g_{\mathfrak{p}}(g_{\mathfrak{p}} + 1)$, and

$$\mathcal{W} \equiv F^2 \pmod{\mathfrak{p}},$$

we have that $\mathcal{W}$ and $F^2 g_d^{g_{\mathfrak{p}}(g_{\mathfrak{p}}-1)}$ are two forms of the same weight and type that are congruent modulo $\mathfrak{p}$, and therefore their companion polynomials are congruent modulo $\mathfrak{p}$:

$$P(\mathcal{W}, x) \equiv P(F^2 g_d^{g_{\mathfrak{p}}(g_{\mathfrak{p}}-1)}, x) \pmod{\mathfrak{p}}.$$

The case of d even: Applying Proposition 3 part 1 $g_{\mathfrak{p}}(g_{\mathfrak{p}} - 1)$times, we have

$$P(\mathcal{W}, x) \equiv P(F^2, x)P(g_d, x)^{g_{\mathfrak{p}}(g_{\mathfrak{p}}-1)} \pmod{\mathfrak{p}}.$$

Since $P(\mathcal{W},x) = x^{\epsilon(d)}F_{\mathfrak{p}}(x)$ and $P(g_d,x) = S_{\mathfrak{p}}(x)$, we have

$$x^{\epsilon(d)}F_{\mathfrak{p}}(x) \equiv P(F^2,x)S_{\mathfrak{p}}(x)^{g_{\mathfrak{p}}(g_{\mathfrak{p}}-1)} \pmod{\mathfrak{p}}.$$

The case of d odd: Applying Proposition 3 part 2 $g_{\mathfrak{p}}(g_{\mathfrak{p}}-1)$times, we have

$$P(\mathcal{W},x) \equiv x^b P(F^2,x)P(g_d,x)^{g_{\mathfrak{p}}(g_{\mathfrak{p}}-1)} \pmod{\mathfrak{p}},$$

where $b = \left\lfloor \frac{g_{\mathfrak{p}}(g_{\mathfrak{p}}-1)+\gamma(k,l)}{q+1} \right\rfloor$.

Then, we have

$$F_{\mathfrak{p}}(x) \equiv x^b P(F^2,x)P(g_d,x)^{g_{\mathfrak{p}}(g_{\mathfrak{p}}-1)} \pmod{\mathfrak{p}},$$

since $\epsilon(d) = 0$ when d is odd.

Therefore, the extent to which we can understand the polynomial $P(F^2,x)$ will determine how much more we can understand about the Weierstrass points of $X_0(\mathfrak{p})$ and the quantity $\mathrm{wt}(P)$ defined in this paper. In addition, it is this polynomial which keeps us from obtaining the main result of [1] in full generality in this setting.

The order of vanishing of $W(z)$ at the cusps

In the discussion surrounding the definition of modular weight (Definition 7), we avoided considering the valuation of the divisor

$$[\,W(z)] + \frac{g_{\mathfrak{p}}(g_{\mathfrak{p}}+1)}{2}[\,dz]$$

at the two cusps of $X_0(\mathfrak{p})$. From the algebraic theory of Weierstrass points developed in Section 'Weierstrass points in characteristic p,' we would expect this divisor to have valuation 0 or at worst positive valuation at the cusps. Unfortunately, at present we cannot show this directly but we proceed to say what we can.

We begin by considering the divisor of dz at the cusps. From explicit computations [15], we have that $\frac{1}{u^2}du = -\tilde{\pi}dz$. Recall from Section 'Expansions at the cusps' the function $t = u^{q-1}$, which is a uniformizer at the cusps 0 and ∞ for $X_0(\mathfrak{p})$. Then, we have

$$\frac{1}{t^{q/(q-1)}}dt = \tilde{\pi}dz,$$

and dz has a pole of order

$$\frac{q}{q-1}$$

at the cusps 0 and ∞.

Proposition 12. *Let P be a cusp of $X_0(\mathfrak{p})$, and write $\tau = 0$ or $\tau = \infty$. Then, there is a basis $\{f_i\}_{i=0}^{g_{\mathfrak{p}}-1}$ of $M^2_{2,1}(\Gamma_0(\mathfrak{p}))$ such that:*

$$ord_{\tau}(f_i) = (q-1)i + q$$

for each i.

Proof. As in the proof of Proposition 10, since the canonical orders at P are $(1,\ldots,g_{\mathfrak{p}}-1)$ (recall that the cusps are not Weierstrass points), we have that there is a basis of $M^2_{2,1}(\Gamma_0(\mathfrak{p}))$ with

$$\mathrm{ord}_P(f_i(z)dz) = i.$$

If P is a cusp of $X_0(\mathfrak{p})$, $\tau = 0$ or ∞, and f is a Drinfeld modular form for $\Gamma_0(\mathfrak{p})$, we have

$$\mathrm{ord}_P(f) = \frac{\mathrm{ord}_\tau(f)}{q-1}.$$

Then, since

$$\mathrm{ord}_P(f_i(z)dz) = \mathrm{ord}_P(f_i) + \mathrm{ord}_P(dz) = \frac{\mathrm{ord}_\tau(f_i(z))}{q-1} - \frac{q}{q-1},$$

the result follows. □

For the next result, we will need the following definition: Let n be a positive integer and q be a power of a prime such that the expansion of n in base q is $n = \sum_{i=0}^{r} n_i q^i$, where each $0 \leq n_i \leq q-1$ for each i. Then, we write $\|n\|_q = \sum_{i=0}^{r} n_i$.

Proposition 13. *Let f be analytic at ∞, then $ord_\infty D_n(f) \geq ord_\infty(f) + \|n\|_q$.*

Proof. Let

$$\alpha_{n,j} = \sum_{\substack{n_1,\ldots,n_j \geq 0 \\ q^{n_1}+\cdots+q^{n_j}=n}} \frac{1}{d_{n_1}\cdots d_{n_j}},$$

where d_i was defined at the beginning of Section 'Hyperderivatives and quasimodular forms'. Then, we have that $\alpha_{n,j} \neq 0$ if and only if $j \equiv \|n\|_q \pmod{q-1}$ and $j \leq n$. Indeed, the least j such that there exists $n_1, \ldots n_j \geq 0$ with $q^{n_1}+\cdots+q^{n_j} = n$ is $\|n\|_q$. Furthermore, given a tuple $(n_1, \ldots, n_j)$ such that $q^{n_1} + \cdots + q^{n_j} = n$ and at least one $n_i > 0$, we can write another tuple $(m_1, \ldots, m_{j+q-1})$ such that $q^{m_1} + \cdots + q^{m_{j+q-1}} = n$ by 'unbundling' a term q^{n_i} into q terms of the form q^{n_i-1} if $n_i > 0$. This process is no longer possible when each $n_i = 0$, in which case we have $q^0 + \ldots + q^0 = n$. This shows that for each j between $\|n\|_q$ and n such that $j \equiv \|n\|_q \pmod{q-1}$, $\alpha_{n,j} \neq 0$. Conversely if there is $(n_1, \ldots, n_j)$ such that $q^{n_1} + \cdots + q^{n_j} = n$, then

$$n = (q^{n_1} - 1) + \cdots + (q^{n_j} - 1) + j \equiv j \pmod{q-1}.$$

But applying this same trick to the sum $n = \sum_{i=0}^{r} n_i q^i$, we have $n \equiv \|n\|_q \pmod{q-1}$.

Using the explicit formula given in Proposition 6, we have that if $f = \sum_{i=0}^{\infty} a_i u^i$ and $D_n f = \sum_{i=0}^{\infty} b_{n,i} u^i$, then

$$b_{n,i} = \sum_{r=1}^{i-1} (-1)^{n+r} \binom{i-1}{r} \alpha_{n,r} a_{i-r}.$$

In light of the remarks above, the only terms that can possibly appear in this sum are those with $r \equiv \|n\|_q \pmod{q-1}$. Therefore, the least i for which $b_{n,i}$ is possibly nonzero is one where $i - \|n\|_q \geq \mathrm{ord}_\infty(f)$. □

Proposition 14. *Let $\mathfrak{p}$ be generated by a prime polynomial of degree 3, so that $g_\mathfrak{p} = q$. Then if P is the cusp ∞ of $X_0(\mathfrak{p})$, we have*

$$ord_P\left(W(z)(dz)^{g_\mathfrak{p}(g_\mathfrak{p}+1)/2}\right) \geq 0.$$

Proof. We choose a basis $\{f_i\}$ of $M^2_{2,1}(\Gamma_0(\mathfrak{p}))$ that satisfies the conclusion of Proposition 12 at ∞. Then,

$$\mathrm{ord}_P\left(W\left(f_0,\ldots,f_{g_\mathfrak{p}-1}\right)(dz)^{g_\mathfrak{p}(g_\mathfrak{p}+1)/2}\right)=\mathrm{ord}_P\left(W(z)(dz)^{g_\mathfrak{p}(g_\mathfrak{p}+1)/2}\right),$$

so we may work with $W(f_0,\ldots,f_{g_\mathfrak{p}-1})$ for convenience.

By Proposition 13, for $k=0,\ldots,g_\mathfrak{p}-1=q-1$, we have that

$$\mathrm{ord}_\infty(D_k(f_l))\geq(q-1)l+q+\|k\|_q=(q-1)l+q+k,$$

since $\|k\|_q=k$ because $0\leq k\leq q-1$. When computing the determinant $W(f_0,\ldots,f_{g_\mathfrak{p}-1})$, we will be adding terms all of whose order of vanishing at ∞ is $\geq \sum_{i=0}^{g_\mathfrak{p}-1}((q-1)i+q+i)$. Thus,

$$\mathrm{ord}_\tau W(f_0,\ldots,f_{g_\mathfrak{p}-1})\geq\sum_{i=0}^{g_\mathfrak{p}-1}q(i+1).$$

We have

$$\sum_{i=0}^{g_\mathfrak{p}-1}q(i+1)=q\frac{g_\mathfrak{p}(g_\mathfrak{p}+1)}{2}.$$

And so

$$\mathrm{ord}_P\left(W(f_0,\ldots,f_{g_\mathfrak{p}-1})(dz)^{g_\mathfrak{p}(g_\mathfrak{p}+1)/2}\right)\geq\frac{q}{q-1}\frac{g_\mathfrak{p}(g_\mathfrak{p}+1)}{2}-\frac{q}{q-1}\frac{g_\mathfrak{p}(g_\mathfrak{p}+1)}{2}=0.$$

□

Remark 8. To obtain Proposition 14 for all $\mathfrak{p}$, it would be sufficient to show that for a basis of $M^2_{2,1}(\Gamma_0(\mathfrak{p}))$ satisfying the conclusion of Proposition 12 at ∞,

$$\mathrm{ord}_\infty(D_k(f_l))\geq\mathrm{ord}_\infty(f_l)+k=(q-1)l+q+k,$$

but that is not true. For example, fixing $q=3$ and any $d>3$, we have that $\mathrm{ord}_\infty(f_1)=5$ but

$$\mathrm{ord}_\infty(D_3(f_1))=6<5+3=8.$$

For this reason, we expect that to show that the divisor of $W(z)(dz)^{g_\mathfrak{p}(g_\mathfrak{p}+1)/2}$ is effective at the cusps will require an intricate and precise study of the action of D_n, beyond the scope of what we wish to accomplish in this paper.

Remark 9. We note that it should be straightforward to obtain a result similar to Proposition 14 for the cusp 0 using Lemma 1, but we do not need it at the moment.

A special case

As remarked in Section 'A refinement of the statement', because of its significance, it would be of great interest to compute the reduction modulo $\mathfrak{p}$ of the form F explicitly or even just its divisor modulo $\mathfrak{p}$. This task, however, involves computing the action of D_n for large n, which quickly gets complicated. However, under some rather restrictive conditions, we are able to prove Theorem 2 which provides an explicit form which is congruent to F modulo $\mathfrak{p}$ and gives us an analogue of the main theorem of [25]. This in turns allows us to prove Theorem 3, which is an analogue of the main theorem of [1].

We will need some notation: For a system of derivatives $\{\delta_n\}$ which is a higher derivation and a positive integer n, we will write $W_\delta(f_1,\ldots,f_n)$ for the quantity

$$\begin{vmatrix} f_1 & \delta_1(f_1) & \ldots & \delta_{n-1}(f_1) \\ \vdots & & \vdots & \\ f_n & \delta_1(f_g) & \ldots & \delta_{n-1}(f_n) \end{vmatrix}.$$

We note that $W_D(f_1,\ldots,f_n) = W(f_1,\ldots,f_n)$.

Recall from the proof of Theorem 12 that there exists a basis $\{F_0,\ldots,F_{g_\mathfrak{p}-1}\}$ for the space $M^2_{q^d+1,1}(\mathrm{GL}_2(A))$, all of whose elements have rational, $\mathfrak{p}$-integral u-series coefficients and such that

$$W(z) \equiv W_D(F_0,\ldots,F_{g_\mathfrak{p}-1}) \pmod{\mathfrak{p}}. \tag{29}$$

Furthermore, $W_D(F_0,\ldots,F_{g_\mathfrak{p}-1})$ was the form which we denoted by F.

Let $\partial_n^{(d)}$ be the Serre operator from Section 'A computational tool,' we have that $D_n(f)$ and $\partial_n^{(k)}(f)$, for k the weight of f, differ by the sum

$$\sum_{i=1}^{n}(-1)^i\binom{k+n-1}{i}(D_{i-1}E)(D_{n-i}f).$$

We note that the quantity $(-1)^i\binom{k+n-1}{i}(D_{i-1}E)$ depends on k and n, but not on f. To ease notation, we write M_D for the matrix appearing in the definition of $W_D(F_0,\ldots,F_{g_\mathfrak{p}-1})$, and M_∂ for the matrix appearing in the definition of $W_\partial(F_0,\ldots,F_{g_\mathfrak{p}-1})$. Then, we have that the $(n+1)$st column of M_∂ is equal to the $(n+1)$st column of M_D plus a linear combination of earlier columns of M_D. Since we are taking a determinant, we conclude that

$$W_D(F_0,\ldots,F_{g_\mathfrak{p}-1}) = W_\partial(F_0,\ldots,F_{g_\mathfrak{p}-1}). \tag{30}$$

In order to proceed with the computation, we first restrict our attention to the case where $d=3$. In that case, $g_\mathfrak{p} = q$ and the canonical orders of $X_0(\mathfrak{p})$ are $(1,\ldots,q-1)$.

We now give a basis for the space $M^2_{q^3+1,1}(\mathrm{GL}_2(A))$. We recall that the algebra of Drinfeld modular forms for $\mathrm{GL}_2(A)$ is generated by g, a Drinfeld modular form of weight $q-1$ and type 0 which is not a cusp form, and h, a Drinfeld modular form of weight $q+1$ and type 1 with a simple zero at the cusp. We note that both g and h have integral u-series coefficients at ∞. To give a basis for $M^2_{q^3+1,1}(\mathrm{GL}_2(A))$ with integral u-series coefficients is thus simply equivalent to enumerating all monomials g^ah^b with $a\geq 0$, $b\geq 2$ and such that

$$a(q-1)+b(q+1) = q^3+1$$

and $b\equiv 1 \pmod{q-1}$. This is easily done, and we get that

$$g^{n(q+1)}h^{q^2-q+1-n(q-1)}, \qquad 0\leq n\leq q-1$$

is a basis of Drinfeld modular forms with integral u-series coefficients for the space we are interested in.

Therefore, there is a constant $a\in K$ such that

$$\begin{aligned} W_D(F_0,\ldots,F_{g_\mathfrak{p}-1}) &= W_\partial(F_0,\ldots,F_{g_\mathfrak{p}-1}) \\ &= aW_\partial\left(h^{q^2-q+1},\ldots,g^{q^2-1}h^q\right), \end{aligned}$$

where the first equality is Equation (30) and so

$$W(z) \equiv aW_\partial \left(h^{q^2-q+1}, \dots, g^{q^2-1}h^q\right) \pmod{\mathfrak{p}} \tag{31}$$

by Equation (29).

As before, we make the convention that if f is a Drinfeld modular form of weight k, then $\partial(f) = \partial_1^{(k)}(f)$. Then if $1 \leq n < p$ for p odd, we have $\partial^n f = n!\,\partial_n^{(k)} f$, where as before the exponent of n on ∂ denotes the n-fold iteration. Therefore, when $q = p$, the computation of $W_\partial \left(h^{p^2-p+1}, \dots, g^{p^2-1}h^p\right)$ can be performed using the fact that $\partial(g) = -h$ and $\partial(h) = 0$, and we get

$$W_\partial \left(h^{p^2-p+1}, \dots, g^{p^2-1}h^p\right) = g^{\frac{p^2(p-1)}{2}} h^{\frac{p^2(p+1)}{2}}.$$

Thus, Equation (31) becomes

$$W(z) \equiv ag^{\frac{p^2(p-1)}{2}} h^{\frac{p^2(p+1)}{2}} \pmod{\mathfrak{p}} \tag{32}$$

We now investigate the value of the constant a. The first non-zero u-series coefficient of $g^{\frac{p^2(p-1)}{2}} h^{\frac{p^2(p+1)}{2}}$ has index $\frac{p^2(p+1)}{2}$. Since the leading coefficient of h is -1 and the leading coefficient of g is 1, the leading coefficient of $g^{\frac{p^2(p-1)}{2}} h^{\frac{p^2(p+1)}{2}}$ is $(-1)^{(p+1)/2}$.

Denote by n_0 the index of the first non-zero coefficient of the u-series expansion of $W(z)$ at ∞. Then, the order of vanishing of $W(z)(dz)^{\frac{p(p+1)}{2}}$ at ∞ is

$$\frac{n_0}{p-1} - \frac{p}{p-1}\left(\frac{p(p+1)}{2}\right).$$

Since this quantity must be non-negative by Proposition 14, we have that $n_0 \geq \frac{p^2(p+1)}{2}$.

Equation (32) then forces $n_0 = \frac{p^2(p+1)}{2}$. Since the leading coefficient of $W(z)$ is a power of π by definition and $(-1)^{(p+1)/2}$ is not zero modulo $\mathfrak{p}$, this forces the leading coefficient of $W(z)$ to be 1 and

$$1 \equiv a(-1)^{(p+1)/2} \pmod{\mathfrak{p}},$$

from which it follows that

$$a \equiv (-1)^{(p+1)/2} \pmod{\mathfrak{p}}.$$

This proves the following theorem:

Theorem 2. *If p is odd, $\pi \in \mathbb{F}_p[T]$ has degree 3, $\mathfrak{p}$ is the ideal generated by π, and the Wronskian on $X_0(\mathfrak{p})$ is denoted by $W(z)$, then $W(z)$ has leading coefficient 1 and rational, $\mathfrak{p}$-integral u-series coefficients at ∞ and furthermore we have*

$$W(z) \equiv (-1)^{(p+1)/2} g^{\frac{p^2(p-1)}{2}} h^{\frac{p^2(p+1)}{2}} \pmod{\mathfrak{p}}.$$

Thanks to this congruence, we may now prove:

Theorem 3. *If p is odd, $\pi \in \mathbb{F}_p[T]$ has degree 3, $\mathfrak{p}$ is the ideal generated by π, then we have*

$$\prod_{P \in Y_0(\mathfrak{p})} (x - j(P))^{wt(P)} \equiv \prod_{\substack{\phi/\overline{\mathbb{F}}_{\mathfrak{p}} \\ \phi \text{ supersingular}}} (x - j(\phi))^{g_{\mathfrak{p}}(g_{\mathfrak{p}}-1)} \pmod{\mathfrak{p}},$$

where $g_{\mathfrak{p}}$ is the genus of the curve $X_0(\mathfrak{p})$.

Proof. Still in the case where $d = 3$ and $q = p$ is an odd prime, we have that

$$G \overset{\text{def}}{=} \left((-1)^{(p+1)/2} g^{\frac{p^2(p-1)}{2}} h^{\frac{p^2(p+1)}{2}} \right)^2$$

is of weight $2p(p^3 + p)$ and type $p(p+1) \equiv 2 \pmod{p-1}$. We have

$$\mu(2p(p^3 + p), 2) = 2p^3 - 2p^2 + 3p - 1$$

and

$$\gamma(2p(p^3 + p), 2) = p - 1.$$

In turn, this allows us to compute

$$P(G, x) = x^{(p-1)^2}.$$

We also have that $\epsilon(d) = 0$ since d is odd, as shown at the end of the proof of Theorem 1.

We apply Proposition 3 part 2, $g_{\mathfrak{p}}(g_{\mathfrak{p}} - 1) = p(p-1)$ times. Since $p(p-1) = 2 + (p-2)(p+1)$ and $\gamma(2p(p^3+p), 2) = p - 1$, we will be in the case where $\gamma(k + p^3 - 1, 2) = p$ exactly $p - 1$ times. Therefore,

$$\begin{aligned} F_{\mathfrak{p}}(x) &\equiv P(\mathcal{W}, x) \pmod{\mathfrak{p}} \\ &\equiv (-x)^{p-1} P(G, x) P(g_3, x)^{p(p-1)} \pmod{\mathfrak{p}} \\ &\equiv x^{p(p-1)} P(g_3, x)^{p(p-1)} \pmod{\mathfrak{p}} \\ &\equiv S_{\mathfrak{p}}(x)^{p(p-1)}, \end{aligned}$$

since $p - 1$ is even.

This concludes the proof since $g_{\mathfrak{p}} = p$ in this case. □

Acknowledgements

The author thanks the support of an NSERC graduate fellowship.

A lot of this work is part of the author's PhD thesis, and the author is grateful to her adviser Ken Ono, who suggested the problem. The author also thanks Matt Baker for many helpful reading suggestions and Cécile Armana for showing her how the computation of the canonical gap sequence of $X_0(\mathfrak{p})$ follows from one of her results. Finally, the author thanks the referee for their thoughtful comments and suggestions.

Received: 30 September 2014 Accepted: 12 April 2015
Published online: 10 July 2015

References

1. Ahlgren, S, Ono, K: Weierstrass points on $X_0(p)$ and supersingular j-invariants. Mathematische Ann. **325**, 355–368 (2003)
2. Armana, C: Torsion rationelle des modules de Drinfeld. PhD thesis, Université Paris Diderot - Paris 7 (2008)
3. Baker, M: Specialization of linear systems from curves to graph. With an appendix by Brian Conrad. Algebra Number Theory. **2**(6), 613–653 (2008)
4. Bosser, V, Pellarin, F: Hyperdifferential properties of Drinfeld quasi-modular forms. International Mathematics Research Notices. **11** (2008)
5. Bosser, V, Pellarin, F: On certain families of Drinfeld quasi-modular forms. J. Number Theory, 2952–2990 (2009)
6. Carlitz, L: On certain functions connected with polynomials in a Galois field. Duke Math. J. **1**, 137–168 (1935)
7. Dobi, D, Wage, N, Wang, I: Supersingular rank two Drinfel'd modules and analogs of Atkin's orthogonal polynomials. Int. J. Number Theory. **5**, 885–895 (2009)
8. Drinfel'd, VG: Elliptic modules (Russian). Matematicheskii Sbornik (Novaya Seriya). **94**, 594–627 (1974)
9. Fresnel, J, van der Put, M: Géométrie analytique rigide et applications, Vol. 18. Progress in Mathematics, Birkhäuser, Boston (1981)
10. Gekeler, E-U: Drinfeld-Moduln und Modulare Formen Über Rationalen Funktionenkörpern, Vol. 119. Bonner Mathematische Schriften, Bonn (1980)
11. Gekeler, E-U: Über Drinfeld'sche Modulkurven vom Hecke-Typ. Compositio Math. **57**, 219–236 (1986)
12. Gekeler, E-U: Drinfeld Modular Curves. Lecture Notes in Mathematics, Vol. 1231. Springer, Berlin (1986)
13. Gekeler, E-U: On the coefficients of Drinfeld modular forms. Inventiones Mathematicae. **93**, 667–700 (1988)
14. Gekeler, E-U, Nonnengardt, U: Fundamental domains of some arithmetic groups over function fields. Int. J. Math. **6**, 689–708 (1995)
15. Gekeler, E-U, Reversat, M: Jacobians of Drinfeld modular curves. J. für die reine und angewandte Mathematik. **476**, 27–93 (1996)

16. Gerritzen, L, van der Put, M: Schottky Groups and Mumford Curves. Lecture Notes in Mathematics, Vol. 817. Springer, Berlin (1980)
17. Goldschmidt, DM: Algebraic Functions and Projective Curves. Graduate Texts in Mathematics, Vol. 215. Springer, New York (2003)
18. Goss, D: π-adic Eisenstein series for function fields. Compositio Math. **41**, 3–38 (1980)
19. Hasse, H, Schmid, HL: Über die Ausnahmeklassen bei abstrakten hyperelliptischen Funktionenkörpern. J. für die reine und angewandte Mathematik. **176**, 184 (1937)
20. Kaneko, M, Koike, M: On extremal quasimodular forms. Kyushu J. Math. **60**, 457–470 (2006)
21. Kiehl, R: Der Endlichkeitssatz für eigentliche Abbildungen in der nichtarchimedischen Funktionentheorie. Inventiones Mathematicae. **2**, 191–214 (1967)
22. Kiehl, R: Theorem A und Theorem B in der nichtarchimedischen Funktionentheorie. Inventiones Mathematicae. **2**, 256–273 (1967)
23. Ogg, AP: On the Weierstrass points of $X_0(n)$. Ill. J. Math. **22**(1), 31–35 (1978)
24. Rohrlich, DE: Some remarks on Weierstrass points. Progress in Mathematics, Vol. 26. Birkhäuser, Boston (1982)
25. Rohrlich, DE: Weierstrass points and modular forms. Ill. J. Math. **29**(1), 134–141 (1985)
26. Schmidt, FK: Zur arithmetischen Theorie der algebraischen Funktionen. II, Allgemeine Theorie der Weierstraßpunkte. Mathematische Zeitschrift. **45**(1), 75–96 (1939)
27. Stöhr, K, Voloch, JF: Weierstrass points and curves over finite fields. Proc. Lond. Math. Soc. Third Series. **52**, 1–19 (1986)
28. Uchino, Y, Satoh, T: Function field modular forms and higher derivations. Mathematische Ann. **311**, 439–466 (1998)
29. Vincent, C: Drinfeld modular forms modulo $\mathfrak{p}$ and Weierstrass points on Drinfeld modular curves. PhD thesis, University of Wisconsin – Madison (2012)
30. Vincent, C: On the trace and norm map from $\Gamma_0(\mathfrak{p})$ to $\mathrm{GL}_2(A)$. J. Number Theory. **142**, 18–43 (2014)