WEIERSTRASS POINTS ON THE DRINFELD MODULAR CURVE $X_0(p)$

CHRISTELLE VINCENT

Abstract. Consider the Drinfeld modular curve $X_0(p)$ for $p$ a prime ideal of $\mathbb{F}_q[T]$. It was previously known that if $j$ is the $j$-invariant of a Weierstrass point of $X_0(p)$, then the reduction of $j$ modulo $p$ is a supersingular $j$-invariant. In this paper we show the converse: Every supersingular $j$-invariant is the reduction modulo $p$ of the $j$-invariant of a Weierstrass point of $X_0(p)$, except possibly the $j$-invariant $j = 0$ when the degree of the prime generating $p$ is odd.

1. 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 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 $\ell$ a prime, he was able to exhibit a form for $SL_2(\mathbb{Z})$ congruent to $W(z)$ modulo $\ell$. 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 $\ell$, which was a result already obtained by Ogg [23], but furthermore that

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

where the quantity $\text{wt}(Q)$ is a non-negative integer which is positive if and only if $Q$ is a Weierstrass point and which we will define in Section 5. Definition 5.6 and $g_\ell$ 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 [2].
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 \( X_0(p) \), where \( p \) 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 \( X_0(p) \).

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 connections 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 \( X_0(p) \) have supersingular reduction at \( p \).

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

**Theorem 1.1.** Let \( q \) be odd and let \( \pi(T) \in \mathbb{F}_q[T] \) be a prime of even degree, generating the prime ideal \( p \). Then each supersingular Drinfeld module over \( \mathbb{F}_p \) is the reduction modulo \( p \) of a Weierstrass point of \( X_0(p) \).

and also

**Theorem 1.2.** Let again \( q \) be odd and let \( \pi(T) \in \mathbb{F}_q[T] \) be a prime of odd degree, generating the prime ideal \( p \). Then each supersingular Drinfeld module over \( \mathbb{F}_p \), except possibly the Drinfeld module of \( j \)-invariant 0, is the reduction modulo \( p \) of a Weierstrass point of \( X_0(p) \).

To obtain these theorems 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 \( X_0(p) \), and the \( u \)-series coefficients of \( W(z) \) at the cusp \( \infty \) are rational and \( p \)-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 \( p \) and obtain Theorems 1.1 and 1.2.

In Section 7, 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 1.3.** If \( p \) is odd, \( \pi(T) \in \mathbb{F}_p[T] \) has degree 3, \( p \) is the ideal generated by \( \pi(T) \), and the Wronskian on \( X_0(p) \) is denoted by \( W(z) \), then

\[
W(z) \equiv (-1)^{(p+1)/2} g^{x_2(p-1)/2} h^{x_2(p+1)/2} \pmod{p}.
\]

Here \( g \) and \( h \) are explicit Drinfeld modular forms which will be defined in Section 8. Theorem 1.3 is an analogue of a result obtained by Rohrlich in \[25\]. This explicit computation allows us to show that

**Theorem 1.4.** If \( p \) is odd, \( \pi \in \mathbb{F}_p[T] \) has degree 3, \( p \) is the ideal generated by \( \pi \), then we have

\[
\prod_{P \in Y_0(p)} (x - j(P))^{wt(P)} \equiv \prod_{\phi \in \mathbb{F}_p} (x - j(\phi))^{g_p(g_p-1)} \pmod{p},
\]

where \( g_p \) is the supersingular part of the Drinfeld modular form of level \( p \).
where $g_p$ is the genus of the curve $X_0(p)$.

This is an analogue of the formula from [11] quoted earlier.

The structure of the paper is the following: We begin by reviewing the theory of Weierstrass points in positive characteristic in Section 2. Then we introduce the basic objects from the Drinfeld setting that we will need in Section 3. Section 3 contains as well all of the statements of the results from the theory of Drinfeld modular forms that we will cite. In Section 4, 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 5, along with the properties of this form. Then the meat of the proof of Theorems 1.1 and 1.2 is in Section 6 where we apply the machinery developed in the previous sections to the form $W(z)$. Finally, the special case which yields Theorems 1.3 and 1.4 is considered in Section 7.

Acknowledgments

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. Finally, the author thanks Cécelie Armana for showing her how the computation of the canonical gap sequence of $X_0(p)$ follows from one of her results.

2. Weierstrass points in characteristic $p$

Since the theory of Weierstrass points in 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 [16]. In particular, proofs of all facts that are stated here without proof can be found in [16].

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 $X$. The finitely many points that have a different gap sequence 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 $i$.

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

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

3
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 2.1.** 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 [18] 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 2.2.** The projective curve of genus 3 given by $X_0^4 + X_1^4 + X_2^4 = 0$ over $\mathbb{F}_3$ 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 $\leq 3$ 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

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

We further denote by $\Omega_X$ the space of (algebraic) meromorphic differential forms on $X$. Because $X$ is defined over an algebraically closed field, we have a canonical isomorphism between $\Omega_X$ 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 $\omega$ a meromorphic differential on $X$. We do this in the following manner: Let $A_{k(X)}$ denote the ring of ad`eles of $k(X)$ and for $D$ a divisor on $X$, write

$$A_{k(X)}(D) \overset{\text{def}}{=} \{ \alpha = (\alpha_P) \in A_{k(X)} \mid v_P(\alpha_P) \geq -v_P(D) \text{ for all points } P \text{ of } X \}.$$  

Then a Weil differential on $X$ is a $k$-linear functional with domain $A_{k(X)}$ that vanishes on $A_{k(X)}(D) + k(X)$ for some divisor $D$. For each Weil differential $\omega^*$, there is a unique divisor $D$ of maximum degree such that $\omega^*$ vanishes on $A_{k(X)}(D) + k(X)$, and we define $[\omega^*] \overset{\text{def}}{=} D$. Then if $\omega$ corresponds to $\omega^*$ under the canonical isomorphism between Weil differentials and meromorphic differentials, we simply write $[\omega] = [\omega^*]$ and $v_P(\omega) = v_P([\omega])$. 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 $\omega$ 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:

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

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

Indeed, for a positive integer $n$, $n + 1$ is a gap at $P$ if and only if $L_C(nP) \supseteq L_C((n + 1)P)$. In turn, this implies the existence of a nonzero $F \in L(C)$ such that $v_P(F) = n - v_P(C)$. 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 $v_P(F') = n - v_P(C')$.

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 $(j_1, \ldots, j_{g-1})$ 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 $n^{th}$ Hasse derivative with respect to $s$ by putting

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

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 $\mathcal{D}^{(n)}_s : k(X) \to k(X)$.

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

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

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

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 $\phi_i$'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 $\phi$ 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 $\phi$ with respect to $s$. While not independent of the choices made above, this function behaves as well 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 $y \in k(X)^*$ and $t$ be another separating variable. Then

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

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

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

which by equation (2.1) 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 $v_p(w) \geq \sum_{i=1}^{g} (n_i(P) - n_i)$ 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 $X$, as claimed above.
The divisor $w$ is effective: Fixing a point $P$ of $X$, one may choose a canonical divisor $C$ such that $v_P(C) = 0$, which ensures that $v_P(\phi_i) \geq 0$, so that $v_P([W(\phi, s)]) \geq 0$ since taking Hasse derivatives does not lower the valuation. Furthermore, one can choose $s$ to be a local parameter at $P$, so that $v_P([ds]) = 0$. With these choices and because of the invariance of $w$, it follows that $v_P(w) \geq 0$ for each $P$.

In [27], the authors define the Weierstrass weight of a point to be $v_P(w)$. In Section 5 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 $X_0(p)$, and study this integer in this work.

Remark. If $X$ is defined over a field of characteristic 0, we have the equality $v_P(w) = \sum_{i=1}^g (n_i(P) - n_i)$ for all points $P$ of $X$. In positive characteristic, this equality holds if and only if det $(J') \neq 0$, 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 $(J')$ is the $(g-1) \times (g-1)$ matrix of binomial coefficients $(j'_r j_s)$, where $(j'_r j_s) = 0$ 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$_k(\Omega_X) = 1$, 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 $\omega^*$ and thus of a meromorphic differential $\omega$. Then the map

$$\Omega_X \to k(X)$$

$$x\omega \mapsto x$$

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

3. 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 [8].

3.1. 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 [12], 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

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

for the completed algebraic closure of $K_\infty$, 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.) $\Omega$ has a rigid analytic structure described in [13], and we call it the Drinfeld upper half-plane. The group GL$_2(A)$ acts on $\Omega$ by fractional linear transformations.
Definition 3.1. Let $\Gamma$ be a congruence subgroup of $\text{GL}_2(A)$. A function $f : \Omega \to C$ is called a Drinfeld modular form of weight $k$ and type $l$ for $\Gamma$, 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 $\Omega$;
3. $f$ is analytic at the cusps of $\Gamma$: 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 $\Gamma$ of $\text{GL}_2(A)$, 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 $\Gamma$) 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 $\Gamma$) 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 [12] 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 3.2. Let $L$ be either a field extension of $K$ or, if $p$ is a prime ideal of $A$, an extension of the field $A/p$. Further write $\tau(X) = X^q$ and let $L\{\tau\} \subset \text{End}_L(\mathbb{G}_a)$ be the subalgebra generated by $\tau$ over $L$, with commutation relation $l\tau = \tau^q l$ for $l \in L$. A Drinfeld module of rank $r$ over $L$ is a ring homomorphism $\phi : A \to L\{\tau\}$ 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 $\phi$.

We say that two Drinfeld modules $\phi$ and $\psi$ are isogenous if there exists a nonzero element $u \in \text{End}_L(\mathbb{G}_a)$ such that $u \circ \phi = \psi \circ u$. If $u \in L^*$, 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 [22]. 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:

$$\rho(T) = T \tau^0 + \tau.$$

Under the correspondence mentioned above, this Drinfeld module corresponds to a certain rank 1 $A$-lattice $L = \tilde{\pi}A$, where the Carlitz period $\tilde{\pi} \in K_\infty(\sqrt[\varphi]{-T})$ is defined up to multiplication by an element of $F_q^*$. 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

\[(3.2)\]

\[u(z) \overset{\text{def}}{=} \frac{1}{e_A(z)}\]

for the parameter at infinity. This differs from Gekeler's original notation, who used \(t(z)\) for this function. The new notation has the advantage that it reduces confusion with Anderson's \(t\)-motives.

We will also consider Drinfeld modules of rank 2. For \(a \in A\), \(\phi\) 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 \(\phi\). When \(\phi\) is of rank 2 and defined over \(C\), for \(\pi(T)\) a prime polynomial generating the ideal \(p\) of \(A\), we have

\[\phi[\pi](C) \cong A/p \times A/p.\]

Again, if \(\phi\) is of rank 2, but is now defined over the algebraic closure of \(A/p\), we have

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

There are \(g_p + 1\) supersingular Drinfeld modules defined over the algebraic closure of \(A/p\), where

\[(3.3)\]

\[g_p \overset{\text{def}}{=} \begin{cases} \frac{q^d - q}{q^2 - 1} & \text{if } d \text{ is odd,} \\ \frac{q^d - q^2}{q^2 - 1} & \text{if } d \text{ is even.} \end{cases}\]

**Remark.** We use \(g_p\) for the quantity above because it is the genus of the modular curve \(X_0(p)\).

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

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

As in \([12]\), we will write \(g_k\) for the normalized Eisenstein series of weight \(q^k - 1\) and type 0 for \(\text{GL}_2(A)\) 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 \(\text{GL}_2(A)\) which was first defined in \([15]\). It is well-known that the graded \(C\)-algebra of Drinfeld modular forms of all weights and all types for \(\text{GL}_2(A)\) 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 \(\infty\) 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 3.3. For \( q \geq 3 \), the dimension of the space of modular forms of weight \( q^d + 1 \) and type 1 for \( \text{GL}_2(A) \) is equal to \( q_p + 1 \), and the dimension of its subspace of double cusp forms is \( g_p \), where \( g_p \) is as in equation (3.3).

We will also need a slash operator, which we define now. For any \( x \in K^*_\infty \), \( x \) can be written uniquely as

\[
 x = \zeta_x \left( \frac{1}{T} \right)^{v_\infty(x)} u_x
\]

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

For \( \gamma \in \text{GL}_2(K) \) we have that \( \det \gamma \in K^* \). By (3.4), 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 \( \gamma = (a \ b \ c \ d) \in \text{GL}_2(K) \) on a modular form of weight \( k \) and type \( l \) by

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

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

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

Definition 3.4. 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 \( p \) to be

\[
 v_p(f) = \inf_i v_p(c_i).
\]

For two formal series \( f = \sum a_i u^i \) and \( g = \sum b_i u^i \), we write \( f \equiv g \) (mod \( p^m \)) if \( v_p(f - g) \geq m \).

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

As in the classical case, there is a deep connection between supersingular Drinfeld modules in characteristic \( p \) and forms with lower filtration than weight. It is this connection which we will exploit to refine the connection between the Weierstrass points of \( X_0(p) \) 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 \( \text{GL}_2(A) \). As shown in [12], if \( p \) is an ideal generated by a prime polynomial of degree \( d \), we have \( g_d \equiv 1 \) (mod \( p \)). 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 \( p \).

To connect \( g_d \) to the supersingular Drinfeld modules, we must first define the so-called \emph{companion polynomial} to a Drinfeld modular form. In [6], the authors remark that the fact that the algebra of Drinfeld modular forms for 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 the unique functions \( \mu(k,l) \) and \( \gamma(k,l) \) such that

\[
\mu(k,l) \equiv l \pmod{q - 1},
\]

\[
0 \leq \gamma(k,l) \leq q,
\]

and

\[
k = \mu(k,l)(q + 1) + \gamma(k,l)(q - 1).
\]

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

\[
f = g^\gamma(k,l)h^\mu(k,l)P(f, j)
\]

where \( j \) is the (normalized) \emph{j}-invariant, \( j = \frac{g^{q+1}}{f^{1/q}} \). 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 \emph{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 \emph{Drinfeld supersingular locus} to be the following polynomial:

\[
S_p(x) = \prod_{\phi \text{ defined over } \mathbb{F}_p \atop \phi \text{ supersingular}} (x - j(\phi)),
\]

then we have

\[
S_p(x) \equiv x^{\gamma(q^d - 1, 0)}P(g_d, x) \pmod{p},
\]

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

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

**Proposition 3.5** (Dobi-Wage-Wang [6]). Assuming the notation above, let \( f \) be a Drinfeld modular form for GL\(_2(A)\) of weight \( k \) and type \( l \) with rational \( p \)-integral \( u \)-series coefficients and finite filtration \( w_p(f) \). Define \( \alpha = \frac{k - w_p(f)}{q^d - 1} \) and \( a = \frac{\alpha^\gamma(q^d - 1, 0) + \gamma(w_p(f), l)}{q + 1} \). Then the polynomial \( x^aP(f, x) \) is divisible by \( S_p(x)^\alpha \) in \( \mathbb{F}_p[x] \).

Proposition 3.5 when applied to a certain Drinfeld modular for \( W(z) \) defined in Section 5.2 immediately implies Theorems 1.1 and 1.2. To obtain the more precise result given in Theorem 1.3 we will need the following proposition:

**Proposition 3.6.** 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

\[
P(f g_d, x) \equiv P(g_d, x)P(f, x) \pmod{p}.
\]
(2) If $d$ is odd, then

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

Proof. (1) Suppose first that $d$ is even. Since $g_d \equiv 1 \pmod{p}$, we have $f \equiv fg_d \pmod{p}$. 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 (3.6), we have

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

Then

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

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

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

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

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

If it were the case that

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

then by the uniqueness of the integers $\mu(q^d - 1, 0)$ and $\gamma(q^d - 1, 0)$ in the equation (3.7), we must have

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

a contradiction. Therefore

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

and again using uniqueness in equation (3.7),

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

and

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

Then

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

Solving for $P(g_d, j)$ in

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

completes the proof.
(2) Suppose now that \(d\) is odd. The proof proceeds as in the even case, except that we cannot rule out the case

\[-q \leq \gamma (k + q^d - 1, l) - \gamma (k, l) < 0.\]

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.

\[P(fg^d, j) \equiv h^{\mu (k, l) - \mu (k + q^d - 1, l)} g^{\gamma (k, l) - \gamma (k + q^d - 1, l)} P(f, j) \pmod{p}\]

\[\equiv h^{-(N - 1)(q - 1)} g^{q - 1} P(f, j) \pmod{p}\]

Solving for \(P(g^d, j)\) in

\[1 \equiv g^d = gh^\mu (q^d - 1, 0) P(g^d, j)\]

gives

\[P(fg^d, j) \equiv g^{q + 1} P(g^d, j) P(f, j) \pmod{p},\]

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 \((3.7)\), 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

\[P(fg^d, j) \equiv g^{-1} h^{-\mu (q^d - 1, 0)} P(f, j) \pmod{p},\]

and the result follows.

\[\square\]

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

**Theorem 3.7** (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 \(\Gamma_0(p)\) with rational \(p\)-integral \(u\)-series coefficients at \(\infty\) and forms of weight \(q^d + 1\) and type 1 for \(GL_2(A)\) with rational \(p\)-integral \(u\)-series coefficients.

We will also need a stronger version of Theorem 1.2 from \([30]\).
**Theorem 3.8.** Let $f$ be a Drinfeld modular form for $\Gamma_0(p)$ of weight $k$ and type $l$ with rational, $p$-integral $u$-series coefficients at $\infty$. Suppose further that $f$ is an eigenform of the Fricke involution. Let

$$\widetilde{N}(f)(z) = \pi^{q^d k/2} \prod_{\gamma \in \Gamma_0(p) \setminus \text{GL}_2(A)} f|_{k,l}[\gamma].$$

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

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

**Proof.** We first note that the hypothesis in [30] that $f$ have integral $u$-series coefficients at $\infty$ is unnecessary; it suffices that the coefficients be rational and $p$-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,

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

By Proposition 3.9 of [30],

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

and the result follows. $\square$

**3.3. Drinfeld modular curves.** We now turn our attention to Drinfeld modular curves, and more specifically to the family $X_0(p)$.

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

**Theorem 3.9 (Drinfeld [7]).** There exists a smooth irreducible affine algebraic curve $Y_\Gamma$ defined over $\mathbb{C}$ such that $\Gamma \setminus \Omega$ and the underlying analytic space $Y_\Gamma^{an}$ of $Y_\Gamma$ are canonically isomorphic as analytic spaces over $\mathbb{C}$.

We note further that the curve $Y_\Gamma$ is unique up to isomorphism, and is in fact defined over a finite abelian extension of $K$, $K_\Gamma$. For each $Y_\Gamma$ there exists a unique smooth projective curve $X_\Gamma$ over $K_\Gamma$ such that $Y_\Gamma$ is birationally equivalent to $X_\Gamma$. 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 $\Gamma \setminus \mathbb{P}^1(K)$, where $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma$ 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 $\Gamma$.

For $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma$, we have

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

so that for $f$ a modular form for $\Gamma$ of weight 2 and type 1, the differential form $f(z)dz$ is $\Gamma$-invariant. A short computation, presented in [14], shows that it descends to a holomorphic
differential form on $X_\Gamma$ if $f$ is a double cusp form. Since GAGA theorems hold for rigid analytic curves [20] [21], we have the following theorem:

**Theorem 3.10** (Goss [17], Gekeler-Reversat [14]). The map $f \mapsto f(z)dz$ identifies the space of double cusp forms of weight 2 and type 1 for $\Gamma$ to the space of regular differential forms on $X_\Gamma$.

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

We will be interested in one family of congruence subgroups, and the Drinfeld modular curves attached to these groups. Recall that $\pi$ congruence group $\Gamma$ are finite-dimensional. It also follows from such considerations that Drinfeld modular forms on $K$ curves attached to these groups. Recall that $\pi$ congruence group $\Gamma$ are finite-dimensional.

Remark. From Theorem 3.11 above, we have that $X_0(\mathfrak{p})$ is defined over $K$ with function field $K(j, j_0)$. 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 \((\phi, H)\), we can also see that the Fricke involution \(W_p\) is \(K\)-rational. We note here that the analytic avatar of \(W_p\) is the action of the matrix \(\begin{pmatrix} 0 & -1 \\ \pi & 0 \end{pmatrix}\) on \(\Omega\).

Since \(X_0(p)\) 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 \(X_0(p)\) by \(g_p\), and it is given by
\[
g_p = \begin{cases} \frac{q(q^d-1)}{q^2-1} & \text{if } d \text{ is odd}, \\ \frac{q^2(q^d-2)}{q^2-1} & \text{if } d \text{ is even}. \end{cases}
\]

(As promised, this is the same \(g_p\) that appears in equation (3.3).) This fact can be obtained either by relating \(g_p\) to \(h_1(\Gamma_0(p))\) as in [13], or by working directly on the Drinfeld modular curve as in [9].

From [9], we also note that representatives for the two distinct equivalence classes of \(\Gamma_0(p)\) are \((0 : 1)\) and \((1 : 0)\), so we delve into this topic now. We focus on the groups \(\text{GL}_2\) and \(\Gamma_0(p)\) as this is all we will need here, and leave the general case to [14] or [10].

Let us first consider the case of \(\text{GL}_2\). The set \(\text{GL}_2(K)\) consists of a single element, and we choose \((1 : 0)\) as the representative of this element. The stabilizer \(\Gamma_\infty\) of \((1 : 0)\) in \(\text{GL}_2\) is the set of all upper-triangular matrices. This set contains a maximal subgroup \(\Gamma^\infty\):
\[
\Gamma^\infty = \left\{ \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} : a \in A \right\},
\]
and also cyclic transformations \((a, q, q^2)\) for \(a, d \in \mathbb{F}_q^*\). The image of this group of cyclic transformations in \(\text{PGL}_2\) has size \(q-1\), the size of \(\mathbb{F}_q^*\).

Recall the function \(u\) defined in equation (3.2). Now writing
\[
\Omega_c = \{z \in \Omega : \inf_{x \in K_\infty} |z - x| \geq c \},
\]
we have that \(u\) identifies \(\Gamma^\infty / \Omega_c\) with a pointed ball \(B_r \setminus \{0\}\) of radius \(r\) for some small \(r\) [14]. It can be shown that there is a constant \(c_0\) such that for \(c \geq c_0\) and \(\gamma \in \text{GL}_2\), \(\Omega_c \cap \gamma(\Omega_c) \neq \emptyset\) implies that \(\gamma \in \Gamma_\infty\). Thus for such a \(c\),
\[
B_{rq^{-1}} \setminus \{0\} \cong \Gamma_\infty / \Omega_c \hookrightarrow \text{GL}_2(K) \\
u(z)^{q-1} \leftarrow z \rightarrow z
\]
is an open immersion of analytic spaces. Thus \(u(z)^{q-1}\) is a uniformizer at the cusp \(\infty\) for \(\text{GL}_2(K)\).

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 \(\Gamma_\infty\), but rather only under \(\Gamma^\infty\). 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 \(\Gamma\), to discuss the behavior of a function \(f\) at a cusp \(a : b \in \Gamma \setminus \mathbb{P}^1(K)\), one first fixes an
element $\gamma \in \text{GL}_2(K)$ 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 $\infty$, and do not depend on the choice of $(a : b)$ in its equivalence class modulo $\Gamma$ and on the choice of $\gamma$ sending $(1 : 0)$ to $(a : b)$. However, for $t$ a parameter at $\infty$ for the group $\Gamma$, 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 $\infty$. This is not well-defined, as the coefficients of the expansion will depend on the choice of $(a : b)$ and $\gamma$.

To remove any ambiguity, in the case of $\text{GL}_2(A)$ we once and for all declare that the expansion of $f$ at $\infty$ is its $u$-series expansion, with $u$ as defined in equation (3.2).

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

We now consider the other cusp of $X_0(p)$, 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

$$W_p = \begin{pmatrix} 0 & -1 \\ \pi & 0 \end{pmatrix}$$

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

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

at $\infty$.

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

### 4. 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 $\Omega$, the Drinfeld quasimodular forms. Throughout, we will use “analytic” to mean “rigid analytic”. We will say that an analytic function $f$ on $\Omega$ is “analytic at $\infty$” 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. As we did for Drinfeld modular forms, we will write $\text{ord}_{\infty}(f)$ for the least $i \geq 0$ such that $a_i \neq 0$. 

17
4.1. Drinfeld quasimodular forms.

**Definition 4.1.** An analytic function \( f : \Omega \to C \) is called a *Drinfeld quasimodular form of weight* \( k \), *type* \( l \), and *depth* \( m \) for \( \text{GL}_2(A) \), 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 \( \Omega \) which are \( A \)-periodic and analytic at infinity such that for \( \gamma = \left( \begin{array}{cc} a & b \\ c & d \end{array} \right) \in \text{GL}_2(A) \), 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 \( \gamma \) 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 [12]:

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

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].

4.2. Higher derivatives. In [28], Uchino and Satoh consider the action of the Hasse derivatives on analytic functions on \( \Omega \). 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 \( \Omega \) is an open set. We will work in this section with analytic functions on \( \Omega \) and denote the space of these functions by \( \text{An}(\Omega) \). For \( f \in \text{An}(\Omega) \) such that \( f = \sum_{i=0}^{\infty} c_{i,w} (z-w)^i \) in a neighborhood of \( w \in \Omega \), we define the \( n^{th} \) hyperderivative of \( f \) at \( w \) to be

\[
\mathfrak{D}_n(f)(w) = c_{n,w}.
\]

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

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

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

**Remark.** The operator \(-D_1\) was also studied by Gekeler in [12], where it was denoted by \( \Theta \), in analogy with Ramanujan’s \( \Theta \)-operator in the classical setting. This explains the discrepancy in sign between this work and the cited paper in our statement of Proposition 4.10 below.
We have the following facts:

**Proposition 4.2 (Uchino-Satoh [23]).** For \( f \in \text{An}(\Omega) \) 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 \( w \),
   \[
   D_n f(z) = \frac{1}{(-\pi)^n} \sum_{i=0}^{\infty} \binom{i}{n} c_{i,w}(z-w)^{i-n}
   \]
   and this has the same radius of convergence as \( \sum_{i=0}^{\infty} c_{i,w}(z-w)^i \).

2. In fact, \( D_n f \) is analytic on \( \Omega \).

3. The system of derivatives \( \{D_n\} \) is a higher derivation; in other words it satisfies:
   a. \( D_0 f = f \),
   b. \( D_n \) is \( C \)-linear,
   c. for \( f \) and \( g \) in \( \text{An}(\Omega) \), \( D_n(fg) = \sum_{i=0}^{n} D_i f D_{n-i} g \).

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 \( \text{An}(\Omega)^{n+1-i} \) to \( \text{An}(\Omega) \) such that:
   a. for \( f \) and \( g \) in \( \text{An}(\Omega) \) such that the composition \( f \circ g \) is defined, we have
   \[
   D_n(f \circ g) = \sum_{i=1}^{n} F_{n,i}(D_1 g, \ldots, D_{n+1-i} g)(D_i f) \circ g,
   \]
   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 map \( F_{n,i} \) that appears in the chain rule property:

**Lemma 4.3.** Let \( f : \Omega \to C \) be an analytic function. For all \( n \geq 1, z \in \Omega, \) and \( \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{GL}_2(A) \), we have

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

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

\[
D_n = \frac{1}{n_0! \cdots n_q!} D_{p^j}^{n_j} \circ \cdots \circ D_{p^1}^{n_1} \circ D_{p^0}^{n_0},
\]
for \( n = n_p p^q + \cdots + n_1 p + n_0 \) the representation of \( n \) in base \( p \), with \( 0 \leq n_j \leq p - 1 \) 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 4.4. Let $f$ be a modular form of weight $k$ and type $l$ for $\text{GL}_2(A)$. Then for all $n \geq 0$ $D_n f$ is $A$-periodic and analytic at $\infty$, and for $\gamma = \left( \begin{array}{cc} a & b \\ c & d \end{array} \right) \in \text{GL}_2(A)$, we have

\begin{equation}
D_n f(\gamma z) = (cz + d)^{k+2n}(\text{det } \gamma)^{-l-n} \sum_{j=0}^{n} \binom{n+k-1}{j} D_{n-j}f(z) \left( \frac{c}{cz + d} \right)^j.
\end{equation}

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

4.3. An integrality result. 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 4.5. Let $f \in \text{An}(\Omega)$ be analytic at $\infty$ with $u$-series expansion $f(z) = \sum_{i \geq 0} a_i u^i$. Then for all $n \geq 0$ we have $D_n f(z) = \sum_{i \geq 2} b_{n,i} u^i$, where

\begin{equation}
b_{n,i} = \sum_{r=1}^{i-1} (-1)^{n+r} \binom{i-1}{r} \left( \sum_{n_1, \ldots, n_r \geq 0, q^{n_1+\cdots+q^{n_r}}=n} \frac{1}{d_{n_1} \cdots d_{n_r}} \right) a_{i-r}.
\end{equation}

From this explicit formula we can clearly see that

Corollary 4.6. For $n < q^e$, the operator $D_n$ preserves $p$-integrality of the $u$-series coefficients for all prime ideals $p$ generated by a prime polynomial of degree $\geq e$.

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 (4.5). Since $d_{n_j}$ is only divisible by primes of degree $\leq n_j$, for $n < q^e$ $D_n$ introduces only denominators of degree $< e$.

From this it easily follows that

Corollary 4.7. Suppose that $f \equiv f' \pmod{p}$ for $p$ generated by a prime of degree $d$. Then $D_n(f) \equiv D_n(f') \pmod{p}$ for $n < q^d$.

4.4. Vanishing results. For $w \in \Omega$ and $f \in \text{An}(\Omega)$, write $\text{ord}_w f$ for the order of vanishing of $f$ at $w$. We recall that if $f$ is analytic at $\infty$ with $u$-series expansion $f = \sum_{i=0}^{\infty} a_i u^i$ and $a_j \neq 0$, then we say $\text{ord}_\infty f = j$.

Proposition 4.8. Let $w \in \Omega$ and $f \in \text{An}(\Omega)$, then $\text{ord}_w D_n(f) \geq \text{ord}_w(f) - n$. When $n \leq \text{ord}_w(f)$, we have equality if and only if $(\text{ord}_n(f) \neq 0 \pmod{p})$.

Proof. This follows by Proposition 4.2 part II.

Proposition 4.9. Let $f$ be analytic at $\infty$, then $\text{ord}_\infty D_n(f) \geq \max(\text{ord}_\infty(f) + 1, 2)$. If $\text{ord}_\infty(f) \geq 1$, we have $\text{ord}_\infty D_n(f) = \text{ord}_\infty(f) + 1$ if and only if $\text{ord}_\infty(f) \neq 0 \pmod{p}$.

Proof. This follows from Proposition 4.5.
4.5. 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 [19]), and we will use its analogue in the Drinfeld setting. Let $n$ and $d$ be non-negative integers. The $n^{th}$ Serre’s operator of degree $d$ is defined by the formula:

\begin{equation}
\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).
\end{equation}

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 $\partial$, 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 4.10 (Gekeler [12]).**

1. Let $f_i$ for $i = 1, 2$ be Drinfeld modular forms of weight $k_i$, then $\partial(f_1f_2) = \partial(f_1)f_2 + f_1\partial(f_2)$.
2. $\partial(g) = -h$ and $\partial(h) = 0$.

This proposition allows us to compute the action of $\partial$ 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

\begin{equation}
\partial^{n}f = n!\partial_{n}^{(k)}f
\end{equation}

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

5. Weierstrass points on $X_0(p)$

5.1. Previous results. As discussed in Section 2, crucial to the study of Weierstrass points in positive characteristic is the knowledge of the curve’s canonical gap sequence.

**Proposition 5.1 (Armana, personal communication).** Let $p$ be a prime ideal generated by a polynomial of degree at least 3 in $\mathbb{F}_q[T]$. Then $X_0(p)$ has a classical gap sequence.

**Proof.** Recall from Section 2 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 $X_0(p)$ such that its unique extension to a section of $\overline{X}_0(p)$ over $A$ is not supersingular at $p$, and denote by $c \geq 1$ the smallest pole number at $P$. Then $c \geq 1 + g_p$, where as before $g_p$ is the genus of $X_0(p)$.

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
A function possibly with poles will be said to be meromorphic. 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 [20], [21]. 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 [8] for the construction of $X^{an}$). Then there is an equivalence of category between the category of algebraic coherent sheaves on $X$ and 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 $\ast^{an}$ 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

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

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

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

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 $F \in \mathcal{L}(C_{can})(X^{an})$ such that $v_{P}(F) = j - v_{P}(C_{can})$.

We now start our work on $X_{0}(p)$ in earnest. We first compute the divisor of $dz$, where $z$ is a parameter on $\Omega$: From explicit computations [14], we have that $\frac{1}{u}du = -\pi dz$. Recall from Section 3.4 the function $t = u^{q-1}$, which is a uniformizer at the cusps $0$ and $\infty$ for $X_{0}(p)$. Then we have

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

and $dz$ has a pole of order

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

at the cusps $0$ and $\infty$. Now let $P$ be a point of $X_{0}(p)$ that is not a cusp, and choose $\tau \in \Omega$ to be a representative of $P$ in the Drinfeld upper half-plane. Throughout we write $e_{r}$ for the order of the stabilizer of $\tau$ in

$$\tilde{\Gamma}_{0}(p) = \Gamma_{0}(p)/\Gamma_{0}(p) \cap Z(GL_{2}(A)).$$

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

$$dz = \frac{1}{e_{r}}t^{(e_{r}-1)/e_{r}}dt.$$
\( e_\tau \) is either 1 or \( q + 1 \) \([14]\) 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 \( \tau \).

**Proposition 5.3.** Let \( P \) be a point on \( X_0(p) \), and write \( j_0(P) = 0 \), and \( (j_1(P), \ldots, j_{g_p - 1}(P)) \) for the canonical orders at \( P \). If \( P \) is not a cusp, choose \( \tau \in \Omega \) to be a representative of \( P \) in the Drinfeld upper half-plane, and write \( e_\tau \) for the order of the stabilizer of \( \tau \) in \( \Gamma_0(p) \). If \( P \) is a cusp we write \( \tau = 0 \) or \( \tau = \infty \). Then there is a basis \( \{ f_i \}_{i=0}^{g_p - 1} \) of \( M_{2,1}(\Gamma_0(p)) \) such that:

\[
\text{ord}_\tau(f_i) = \begin{cases} 
  e_\tau j_1(P) + e_\tau - 1 & \text{if } \tau \in \Omega, \\
  (q - 1) j_1(P) + q & \text{if } \tau = 0, \infty.
\end{cases}
\]

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

Suppose first that \( P \) is not a cusp, and choose \( \tau \in \Omega \) to be a representative of \( P \) in the Drinfeld upper half-plane. We write as before \( e_\tau \) for the order of the stabilizer of \( \tau \) in \( \Gamma_0(p) \). Then

\[
\text{ord}_P(f_i(z)dz) = \frac{\text{ord}_\tau(f_i)}{e_\tau} = \frac{e_\tau - 1}{e_\tau}.
\]

If \( P \) is a cusp, we write \( \tau = \infty \) or \( \tau = 0 \) as appropriate, and then

\[
\text{ord}_P(f_i(z)dz) = \frac{\text{ord}_\tau(f_i(z))}{q - 1} = \frac{q - 1}{q - 1}.
\]

The result follows. \( \square \)

For any basis \( \{ f_0, f_1, \ldots, f_{g_p - 1} \} \) of \( M_{2,1}^2(\Gamma_0(p)) \), we define

\[
W(f_0, \ldots, f_{g_p - 1}) = \begin{vmatrix} 
  f_0(z) & D_1(f_0(z)) & \cdots & D_{g_p - 1}(f_0(z)) \\
  \vdots & \vdots & \ddots & \vdots \\
  f_{g_p - 1}(z) & D_1(f_{g_p - 1}(z)) & \cdots & D_{g_p - 1}(f_{g_p - 1}(z)) 
\end{vmatrix},
\]

where \( D_n \) is the normalized Hasse derivative introduced in Section 4. This is a modular form of weight \( g_p(g_p + 1) \) and type \( \frac{g_p(g_p + 1)}{2} \) for \( \Gamma_0(p) \).

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

**Lemma 5.4.** There exists a basis \( \{ f_0, \ldots, f_{g_p - 1} \} \) of \( M_{2,1}^2(\Gamma_0(p)) \) with integral u-series coefficients at \( \infty \) such that \( W(f_0, \ldots, f_{g_p - 1}) \) has rational, \( p \)-integral u-series coefficients at \( \infty \) and

\[
v_p(W(f_0, \ldots, f_{g_p - 1})) = 0.
\]
Proof. By Remark 3.3 there is a basis \( \{ f_1, \ldots, f_g \} \) for the space \( M^2_{2,1}(\Gamma_0(p)) \) that has integral \( u \)-series coefficients at \( \infty \).

When computing \( W(f_1, \ldots, f_g) \), we will compute \( D_n \) for \( n \leq g_p - 1 \). From the explicit formula (3.3), we have \( g_p \leq 2q^{d-2} \), so that \( n \leq 2q^{d-2} - 1 < q^d \). In this case, Proposition 4.6 says that \( D_n \) preserves \( p \)-integrality of the \( u \)-series coefficients, so \( W(f_1, \ldots, f_g) \) has rational, \( p \)-integral \( u \)-series coefficients.

Suppose that
\[
v_p(W(f_0, \ldots, f_{g_p-1})) > 0.
\]
Then there exist \( a_0, \ldots, a_{g_p-1} \) with each \( a_i \in A \) such that
\[
a_0f_0 + \ldots + a_{g_p-1}f_{g_p-1} \equiv 0 \pmod{p},
\]
and for at least one \( i \) such that \( 0 \leq i \leq g_p - 1 \),
\[
a_i \not\equiv 0 \pmod{p}.
\]
Without loss of generality, suppose that
\[
a_0 \not\equiv 0 \pmod{p}.
\]
Then we have
\[
v_p\left( f_0 + \frac{1}{a_0} (a_1f_1 + \ldots + a_{g_p-1}f_{g_p-1}) \right) = m > 0,
\]
for some \( m \in \mathbb{Z} \). Putting
\[
f'_0 = \frac{1}{\pi^m} \left( f_0 + \frac{1}{a_0} (a_1f_1 + \ldots + a_{g_p-1}f_{g_p-1}) \right),
\]
we have that \( f'_0 \) has integral \( u \)-series coefficients at \( \infty \), \( W(f'_0, f_1, \ldots, f_{g_p-1}) \) has rational, \( p \)-integral \( u \)-series coefficients at \( \infty \), and
\[
v_p(W(f_0, \ldots, f_{g_p-1})) > v_p(W(f'_0, \ldots, f_{g_p-1})).
\]
If
\[
v_p(W(f'_0, \ldots, f_{g_p-1})) > 0,
\]
we may repeat the procedure above. We can continue this process until the valuation is 0. \( \square \)

As a consequence of this lemma, there is a unique Drinfeld modular form \( W(f_0, \ldots, f_{g_p-1}) \) such that
\[
v_p(W(f_0, \ldots, f_{g_p-1})) = 0
\]
and the leading coefficient of \( W(f_0, \ldots, f_{g_p-1}) \) is a power of \( \pi \). We denote this form by \( W(z) \) and call it the modular Wronskian of \( X_0(p) \). We note that the forms \( \{ f_0, \ldots, f_{g_p-1} \} \) which give us \( W(z) \) can be chosen to have rational, \( p \)-integral \( u \)-series coefficients at \( \infty \).

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

**Theorem 5.5.** Let \( (n_1, \ldots, n_{g_p}) = (1, \ldots, g_p) \) denote the canonical gap sequence of \( X_0(p) \), and for any point \( P \) of \( X_0(p) \), write \( (n_1(P), \ldots, n_{g_p}(P)) \) for the gap sequence at \( P \). Then we have
\[
\text{ord}_P(W(z)(dz)^{g_p(g_p+1)/2}) \geq \sum_{i=1}^{g_p} (n_i(P) - n_i).
\]
In addition, when \( P \) is not a cusp, an elliptic point, nor a Weierstrass point, we have equality:
\[
\text{ord}_P(W(z)(dz)^{g_p(g_p+1)/2}) = 0.
\]

**Proof.** Let \( P \) be a point on \( X_0(\mathfrak{p}) \), and choose a basis \( \{f_i\} \) of \( M^2_{\mathfrak{p}}(\Gamma_0(\mathfrak{p})) \) that satisfies the conclusion of Proposition 5.3. We also continue to use the notation introduced in the statement of Proposition 5.3. Then
\[
\text{ord}_P(W(f_0, \ldots, f_{g_p-1})(dz)^{g_p(g_p+1)/2}) = \text{ord}_P(W(z)(dz)^{g_p(g_p+1)/2}),
\]
so we may work with \( W(f_0, \ldots, f_{g_p-1}) \) for convenience.

First, suppose that \( P \) is not a cusp of \( X_0(\mathfrak{p}) \), and choose \( \tau \in \Omega \) to be a representative of \( P \) in the Drinfeld upper half-plane. By Proposition 4.8, for \( k = 0, \ldots, g_p - 1 \), we have that
\[
\text{ord}_\tau(D_k(f_i)) \geq e_{\tau,j_i}(P) + e_\tau - 1 - k
\]
with equality if and only if \( (e_{\tau,j_i}(P) + e_\tau - 1) \neq 0 \pmod{p} \). When computing the determinant \( W(f_0, \ldots, f_{g_p-1}) \), we will be adding terms all of whose order of vanishing at \( \tau \) is
\[
\sum_{i=0}^{g_p-1} (e_{\tau,j_i}(P) - i + e_\tau - 1).
\]

Thus
\[
\text{ord}_\tau W(f_0, \ldots, f_{g_p-1}) \geq \sum_{i=0}^{g_p-1} (e_{\tau,j_i}(P) - i + e_\tau - 1).
\]

Since \( X_0(\mathfrak{p}) \) has canonical orders \( (j_1, \ldots, j_{g_p-1}) = (1, \ldots, g_p - 1) \) and
\[
\sum_{i=1}^{g_p} (n_i(P) - n_i) = \sum_{i=1}^{g_p-1} (j_i(P) - j_i),
\]
for any point \( P \) on \( X_0(\mathfrak{p}) \), we have
\[
\sum_{i=0}^{g_p-1} (e_{\tau,j_i}(P) - i + e_\tau - 1) = e_\tau \sum_{i=1}^{g_p} (n_i(P) - n_i) + \frac{g_p(g_p + 1)}{2} (e_\tau - 1).
\]

Thus
\[
\text{ord}_P(W(f_0, \ldots, f_{g_p-1})(dz)^{g_p(g_p+1)/2}) \geq \sum_{i=1}^{g_p} (n_i(P) - n_i) + \frac{g_p(g_p + 1)}{2} e_\tau - 1 - \frac{g_p(g_p + 1)}{2} e_\tau - 1
\]
\[
= \sum_{i=1}^{g_p} (n_i(P) - n_i).
\]

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

Now suppose that \( P \) is a cusp of \( X_0(\mathfrak{p}) \), and we write \( \tau = 0 \) or \( \tau = \infty \). By Proposition 4.9, for \( k = 0, \ldots, g_p - 1 \), we have that
\[
\text{ord}_\tau(D_k(f_i)) \geq (q - 1)j_i(P) + q + 1
\]
for convenience.
with equality if and only if $\text{ord}_\tau(f_i) \not\equiv 0 \pmod{p}$. (Here $\text{ord}_\tau(f_i) \geq 2$.) Again, when computing the determinant $W(f_0, \ldots, f_{g_p-1})$, we will be adding terms all of whose order of vanishing at $\tau$ is $\geq \sum_{i=0}^{g_p-1} ((q-1)j_i(P) + q + 1)$. Thus

$$\text{ord}_\tau W(f_0, \ldots, f_{g_p-1}) \geq \sum_{i=0}^{g_p-1} ((q-1)j_i(P) + q + 1).$$

We have

$$\sum_{i=0}^{g_p-1} ((q-1)j_i(P) + q + 1) = (q-1) \sum_{i=1}^{g_p} (n_i(P) - n_i) + g_p q + \frac{g_p(g_p - 1)}{2} + (q-1) \frac{g_p(g_p - 1)}{2}$$

$$= (q-1) \sum_{i=1}^{g_p} (n_i(P) - n_i) + g_p q + \frac{g_p(g_p - 1)}{2}$$

$$= (q-1) \sum_{i=1}^{g_p} (n_i(P) - n_i) + q \frac{g_p(g_p + 1)}{2}.$$  

And so

$$\text{ord}_P(W(f_0, \ldots, f_{g_p-1})(dz)^{g_p(g_p+1)/2}) \geq \sum_{i=1}^{g_p} (n_i(P) - n_i) + \frac{q g_p(g_p + 1)}{2} - \frac{g_p(g_p + 1)}{2} \frac{q}{q-1}$$

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

The significance of the previous theorem is that the divisor

$$[W(z)] + \frac{g_p(g_p + 1)}{2}[dz]$$

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

**Definition 5.6.** The (modular) Weierstrass weight of a point $P$ on $X_0(p)$ is

$$\text{wt}(P) = \text{ord}_P(W(z)(dz)^{g_p(g_p+1)/2}).$$

**Proposition 5.7.** 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 $\{f_1, \ldots, f_{g_p}\}$ be a basis of eigenforms of $W_p$ of the space $M^2_{2,1}(\Gamma_0(p))$, say with $f_i||W_p = \lambda_i f_i$.

We compute

$$W(f_0, \ldots, f_{g_p-1}) \left( \frac{-1}{\pi z} \right) = \begin{vmatrix}
  f_0 \left( \frac{-1}{\pi z} \right) & (D_1 f_0) \left( \frac{-1}{\pi z} \right) & \cdots & (D_{g_p-1} f_0) \left( \frac{-1}{\pi z} \right) \\
  \vdots & \vdots & \ddots & \vdots \\
  f_{g_p-1} \left( \frac{-1}{\pi z} \right) & (D_1 f_{g_p-1}) \left( \frac{-1}{\pi z} \right) & \cdots & (D_{g_p-1} f_{g_p-1}) \left( \frac{-1}{\pi z} \right) \\
  \lambda_0 \pi z^2 f_0(z) & (D_1 f_0) \left( \frac{-1}{\pi z} \right) & \cdots & (D_{g_p-1} f_0) \left( \frac{-1}{\pi z} \right) \\
  \vdots & \vdots & \ddots & \vdots \\
  \lambda_{g_p-1} \pi z^2 f_{g_p-1}(z) & (D_1 f_{g_p-1}) \left( \frac{-1}{\pi z} \right) & \cdots & (D_{g_p-1} f_{g_p-1}) \left( \frac{-1}{\pi z} \right)
\end{vmatrix}.$$
By Proposition 4.3 we have for each $i$ and $n$:

$$D_n \left( f_i \left( \frac{-1}{\pi z} \right) \right) = z^{-n} \sum_{j=1}^{n} (-1)^j \left( \pi z \right)^{j} \left( \frac{1}{n-j} \right) \left( \frac{1}{(-\pi)^n} \right) (D_j f_i) \left( \frac{-1}{\pi z} \right).$$

Furthermore using the product rule we have

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

Combining Equations (5.1) and (5.2) and using induction on $n$, we obtain that

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

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

$$W(f_0, \ldots, f_{g_p-1}) \left( \frac{-1}{\pi z} \right) = \left| \lambda_i \pi^{n+1} z^{2n+2} (D_n f_i)(z) \right|,$$

where $0 \leq i \leq g_p - 1$ indexes the rows and $0 \leq n \leq g_p - 1$ indexes the columns of the matrix.

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

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

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

6. PROOFS OF THEOREMS 1.1 AND THEOREM 1.2

We are now in a position to show Theorems 1.1 and 1.2.

For simplicity throughout this section we will write

$$W = \widetilde{N}(W) = \pi^{q^d k/2} \prod_{\gamma \in \Gamma_0(p) \setminus GL_2(\mathbb{A})} W|_{k,l},$$

which is the form which appears in the statement of Theorem 3.8 and

$$F_p(x) \overset{\text{def}}{=} \prod_{P \in \Gamma_0(p)} (x - j(P))^{\text{wt}(P)}.$$

We note that this is a polynomial since only finitely many points $P$ have $\text{wt}(P) \neq 0$, 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 Theorems 1.1 and 1.2 is to relate the companion polynomial of $W(z)$ to the polynomial $F_p(x)$. Then applying Theorems 3.7 and 3.8 to $W(z)$, we show that $W$ has lower filtration than weight, and conclude that its divisor is supported on all of the supersingular locus.
Theorem 6.1. Let $W(z)$ be as in equation (6.1). Let $P(W, x)$ be the companion polynomial of the form $W(z)$ defined in equation (3.6). Then

$$P(W, x) = x^{\epsilon(d)}F_p(x).$$

for

$$\epsilon(d) = \begin{cases} \frac{q^d}{q+1}(g_p^2 + g_p + \gamma((q^d + 1)g_p(g_p + 1), g_p(g_p + 1))) & \text{if } d \text{ is even}, \\ \frac{q^d}{q+1}\gamma((q^d + 1)g_p(g_p + 1), g_p(g_p + 1)) & \text{if } d \text{ is odd}. \end{cases}$$

Proof. Let $\tau$ be any element of the Drinfeld upper half-plane $\Omega$, and let $P_\tau$ be the point on $Y_0(p)$ corresponding to $\tau$. Further let $e_\tau$ be the order of the stabilizer of $\tau$ in $\tilde{\Gamma}_0(p)$. Then we have

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

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

$$\text{ord}_\tau W(z) = \text{wt}(P_\tau),$$

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

$$\text{ord}_\tau W(z) = (q + 1) \text{wt}(P_\tau) + q \frac{g_\tau(g_\tau + 1)}{2}.$$

Let now $\tau_0$ be a point in the Drinfeld upper-half space $\Omega$ that is not in the equivalence class of the elliptic point of $X_0(1)$. Since $W$ is a multiple of

$$\prod_{\gamma \in \Gamma_0(p) \setminus \text{GL}_2(A)} W_{k,l}[\gamma];$$

and the map $X_0(p) \to X_0(1)$ is unramified above $\tau_0$, we have

$$\text{ord}_{\tau_0} W(z) = \sum_{P_\tau \in Y_0(p), \ \tau \sim \tau_0} \text{wt}(P_\tau),$$

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

The case of $d$ even If the degree $d$ of the prime polynomial generating $p$ is even, then $X_0(p)$ has two elliptic points, and the fiber above the elliptic point of $X_0(1)$ in $X_0(p)$ contains in addition $\frac{q^d}{q^{d+1}}$ non-elliptic points [9]. Thus if $\tau_0 \in \Omega$ is in the $\text{GL}_2(A)$-equivalence class of the elliptic point on $X_0(1)$, we have

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

On the other hand, by equation (3.6), we have

$$\text{ord}_{\tau_0} W(z) = \gamma((q^d + 1)g_\tau(g_\tau + 1), g_\tau(g_\tau + 1)) + (q + 1)M,$$

where $M$ is the order of vanishing of $P(W, x)$ at $j(\tau_0) = 0.$
Combining these two equations we obtain
\begin{equation}
\gamma((q^d + 1)g_p(g_p + 1), g_p(g_p + 1)) + M = \frac{q}{q + 1} (g_p^2 + g_p + \gamma((q^d + 1)g_p(g_p + 1), g_p(g_p + 1))) + \sum_{\tau \in Y_0(p), \tau \sim \tau_0} \text{wt}(P_\tau).
\end{equation}

For \( d \) even, let \( \epsilon(d) = \frac{q}{q + 1} (g_p^2 + g_p + \gamma((q^d + 1)g_p(g_p + 1), g_p(g_p + 1))) \).

Equations (6.3) and (6.4) imply the equality of polynomials
\[ P(W, x) = x^{\epsilon(d)} F_p(x). \]

The case of \( d \) odd If the degree \( d \) of the prime polynomial generating \( p \) is odd, then \( X_0(p) \) has no elliptic points, and the fiber above the elliptic point of \( X_0(1) \) in \( X_0(p) \) contains \( \frac{q^d + 1}{q+1} \) non-elliptic points. Thus if \( \tau_0 \) is in the \( \text{GL}_2(A) \)-equivalence class of the elliptic point on \( X_0(1) \), we have
\[ \text{ord}_{\tau_0} W(z) = (q + 1) \sum_{\tau \in Y_0(p), \tau \sim \tau_0} \text{wt}(P_\tau). \]

On the other hand, by equation (3.6), we have
\[ \text{ord}_{\tau_0} W(z) = \gamma((q^d + 1)g_p(g_p + 1), g_p(g_p + 1)) + (q + 1)M, \]
where \( M \) is the order of vanishing of \( P(W, x) \) at \( j(\tau_0) = 0 \).

Combining these two equations we obtain that
\begin{equation}
\gamma((q^d + 1)g_p(g_p + 1), g_p(g_p + 1)) + M = \frac{q}{q + 1} \gamma((q^d + 1)g_p(g_p + 1), g_p(g_p + 1)) + \sum_{\tau \in Y_0(p), \tau \sim \tau_0} \text{wt}(P_\tau).
\end{equation}

For \( d \) odd, let \( \epsilon(d) = \frac{q}{q + 1} \gamma((q^d + 1)g_p(g_p + 1), g_p(g_p + 1)) \).

Equations (6.3) and (6.5) imply
\[ P(W, x) = x^{\epsilon(d)} F_p(x), \]
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 \( \text{GL}_2(A) \) that is congruent to \( W(z) \) modulo \( p \).

**Theorem 6.2.** Let \( q \geq 3 \), then there exists a Drinfeld modular form \( F \) of weight \( g_p(g_p + q^d) \) and type \( \frac{2g_p(g_p + 1)}{2} \) for \( \text{GL}_2(A) \) such that
\[ W(z) \equiv F(z) \pmod{p}. \]

**Proof.** We choose a basis \( \{ f_0, \ldots, f_{g_p - 1} \} \) for the space \( M^2_{2,1}(\Gamma_0(p)) \) such that
\[ W(z) = W(f_0, \ldots, f_{g_p - 1}), \]
and such that for each \( i \) \( f_i \) has rational, \( p \)-integral \( u \)-series coefficients at \( \infty \).

By Theorem 3.7 there is a basis \( \{ F_0, \ldots, F_{g_p - 1} \} \) for the space \( M^2_{q^d+1,1}(\text{GL}_2(A)) \), all of whose elements have rational, \( p \)-integral \( u \)-series coefficients and such that \( f_i \equiv F_i \pmod{p} \).
As we remarked in the proof of Proposition 3.4, when computing the forms \( W(f_0, \ldots, f_{g_p - 1}) \) and \( W(F_0, \ldots, F_{g_p - 1}) \), one needs to compute \( D_n \) for \( n < q^d \). Thus in all of the cases we will consider, we have that \( f_i \equiv F_i \pmod{p} \) implies that \( D_n(f_i) \equiv D_n(F_i) \pmod{p} \) by Corollary 4.7.

Therefore we have

\[
W(f_0, \ldots, f_{g_p - 1}) \equiv W(F_0, \ldots, F_{g_p - 1}) \pmod{p}.
\]

The form \( W(F_0, \ldots, F_{g_p - 1}) \) is modular for \( \text{GL}_2(A) \) of weight \( g_p(q^d + 1) \) and type \( g_p(g_p + 1) \), and we denote it \( F \) for simplicity.

We can now prove Theorem 1.1:

**Proof of Theorems 1.1 and 1.2** Since \( W \) has rational, \( p \)-integral \( u \)-series coefficients at \( \infty \) and is an eigenform of the Fricke involution, Theorem 3.8 states that

\[
\mathcal{W} = N(W) \equiv W^2 \pmod{p},
\]

Since it is a multiple of \( N(W) \), \( \mathcal{W} \) is a form of weight \((q^d + 1)g_p(g_p + 1)\) and type \( g_p(g_p + 1) \) for \( \text{GL}_2(A) \).

By Theorem 6.2, we have

\[
(6.6) \quad \mathcal{W} \equiv F^2 \pmod{p}.
\]

The form \( F^2 \) is of weight \( 2g_p(q^d + 1) \) and type \( g_p(g_p + 1) \).

We note now that the proof of Proposition 3.5 can be adapted say the following: Let \( f \) and \( f' \) be two Drinfeld modular forms for \( \text{GL}_2(A) \) of weights \( k > k' \) and of types \( l \) and \( l' \), respectively, both with rational \( p \)-integral \( u \)-series coefficients and not \( \equiv 0 \pmod{p} \). Then for \( \alpha = \frac{k - k'}{q - 1} \) and \( a = \left\lfloor \frac{\gamma(q - 1,0)q + \gamma(k',l)}{q + 1} \right\rfloor \). Then the polynomial \( x^aP(f,x) \) is divisible by \( S_p(x)^\alpha \) in \( \mathbb{F}_p[x] \).

Applying this to equation (6.6), we have \( \alpha = g_p(g_p - 1) \). Then in \( \mathbb{F}_p[x] \) we have that

\[
S_p(x)^{g_p(g_p - 1)} \mid x^aP(\mathcal{W},x) = x^{a + e(d)}F_p(x).
\]

**The case of \( d \) even** In this case \( j = 0 \) is not supersingular, so \( x \) does not divide \( S_p(x) \), and we conclude that

\[
S_p(x)^{g_p(g_p - 1)} \mid F_p(x).
\]

Thus each supersingular \( j \)-invariant is the reduction modulo \( p \) of a root of \( F_p(x) \).

By Theorem 5.5

\[
\text{wt}(P) = \text{ord}_p(W(z)(dz)^{g_p(g_p + 1)/2}) \geq \sum_{i=1}^{g_p} (n_i(P) - n_i),
\]

where the inequality is strict only at cusps, elliptic points and Weierstrass points. Recall also that a Weierstrass point is a point such that

\[
\sum_{i=1}^{g_p} (n_i(P) - n_i) > 0.
\]

By definition (equation (6.2)) the polynomial \( F_p(x) \) has zeros at the Weierstrass points, and possibly also at the elliptic points of \( X_0(p) \), which have \( j = 0 \). Since \( j = 0 \) is not
supersingular when \(d\) is even, then each supersingular \(j\)-invariant is the reduction modulo \(p\) of the \(j\)-invariant of a Weierstrass point.

**The case of \(d\) odd** The zeroes of \(F_p\) are either Weierstrass points or elliptic points, and it is impossible to say if \(j = 0\) appears as a root of \(F_p\) because it is a Weierstrass point or because it is elliptic. Therefore we cannot conclude that one of the points with \(j = 0\) is a Weierstrass point of \(X_0(p)\), and the supersingular point \(j = 0\) might not be the reduction modulo \(p\) of a Weierstrass point.

For all other points, the proof proceeds as in the case of \(d\) even.

\[\square\]

6.1. **A refinement of the statement.** Since \(W\) is of weight \((q^d + 1)g_p(g_p + 1)\) and type \(g_p(g_p + 1)\), \(F^2\) is of weight \(2g_p(g_p + q^d)\) and type \(g_p(g_p + 1)\), and
\[
W \equiv F^2 \pmod{p},
\]
we have that \(W\) and \(F^2 g_p^{(g_p - 1)}\) are two forms of the same weight and type that are congruent modulo \(p\), and therefore their companion polynomials are congruent modulo \(p\):
\[
P(W, x) \equiv P(F^2, x)P(g_d, x)^{(g_p - 1)} \pmod{p}.
\]

**The case of \(d\) even** Applying Proposition 3.6 part 1 \(g_p(g_p - 1)\) times, we have
\[
P(W, x) \equiv P(F^2, x)P(g_d, x)^{(g_p - 1)} \pmod{p}.
\]
Since \(P(W, x) = x^{\epsilon(d)}F_p(x)\) and \(P(g_d, x) = S_p(x)\), we have
\[
x^{\epsilon(d)}F_p(x) \equiv P(F^2, x)S_p(x)^{(g_p - 1)} \pmod{p}.
\]
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 \(X_0(p)\) – for example with which multiplicity is each supersingular \(j\)-invariant the reduction modulo \(p\) of the \(j\)-invariant of a Weierstrass point – and the failure of \(W(z)\) to capture the quantity \(\sum_{i=1}^{g_p} (n_i(P) - n_i)\).

**The case of \(d\) odd** Applying Proposition 3.6 part 2 \(g_p(g_p - 1)\) times, we have
\[
P(W, x) \equiv x^bP(F^2, x)P(g_d, x)^{(g_p - 1)} \pmod{p},
\]
where \(b = \left\lfloor \frac{g_p(g_p - 1) + \gamma(k, l)}{q + 1} \right\rfloor\).

Then we have
\[
F_p(x) \equiv x^{b - \epsilon(d)}P(F^2, x)P(g_d, x)^{(g_p - 1)} \pmod{p}.
\]

7. **A special case**

Because of its significance, it would be of great interest to compute the reduction modulo \(p\) of the form \(F\) explicitly, or even just its divisor modulo \(p\). This task, however, seems extremely difficult. However, under some rather restrictive conditions we are in position to prove Theorem 1.3 which provides an explicit form which is congruent to \(F\) modulo \(p\), and gives us an analogue of the main theorem of [25]. This in turns allows us to prove Theorem 1.4 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

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

We note that \( W_\delta(f_1, \ldots, f_n) = W(f_1, \ldots, f_n) \).

Recall from the proof of Theorem 6.2 that there exists a basis \( \{ F_0, \ldots, F_{g_p-1} \} \) for the space \( M^2_{g^2+1,1}(GL_2(A)) \), all of whose elements have rational, \( p \)-integral \( u \)-series coefficients and such that

\[
\text{(7.1)} \quad W(z) \equiv W_\delta(F_0, \ldots, F_{g_p-1}) \pmod{p}.
\]

Furthermore, \( W_\delta(F_0, \ldots, F_{g_p-1}) \) was the form which we denoted by \( F \).

Let \( \partial_n^{(d)} \) be the Serre operator from Section 4.5, 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 \( M_\delta \) for the matrix appearing in the definition of \( W_\delta(F_0, \ldots, F_{g_p-1}) \), and \( M_\theta \) for the matrix appearing in the definition of \( W_\theta(F_0, \ldots, F_{g_p-1}) \). Then we have that the \( (n+1) \)st column of \( M_\delta \) 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

\[
\text{(7.2)} \quad W_\delta(F_0, \ldots, F_{g_p-1}) = W_\theta(F_0, \ldots, F_{g_p-1}).
\]

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

Since the algebra of Drinfeld modular forms for \( GL_2(A) \) is generated by \( g \) and \( h \), we have that

\[
g^{n(q+1)}h^{q^2-2q+2-n(q-1)}, \quad 0 \leq n \leq q - 1
\]

is a basis of Drinfeld modular forms with integral \( u \)-series coefficients for the space \( M^2_{q^2+1,1}(GL_2(A)) \).

Therefore there is a constant \( a \in K \) such that

\[
W_\delta(F_0, \ldots, F_{g_p-1}) = W_\delta(F_0, \ldots, F_{g_p-1})
\]

\[
\quad = aW_\theta(h^{q^2-q+1}, \ldots, g^{q^2-1}h^q),
\]

where the first equality is equation (7.2) and so

\[
\text{(7.3)} \quad W(z) \equiv aW_\theta(h^{q^2-q+1}, \ldots, g^{q^2-1}h^q) \pmod{p}
\]

by equation (7.1).

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 \( \partial^n f = n!\partial_1^{(k)} f \), where as before the exponent of \( n \) on \( \partial \) denotes the \( n \)-fold iteration. Therefore when \( q = p \), the computation of \( W_\theta(h^{p^2-p+1}, \ldots, g^{p^2-1}h^p) \) can be performed using the fact that \( \partial(g) = -h \) and \( \partial(h) = 0 \), and we get

\[
W_\theta(h^{p^2-p+1}, \ldots, g^{p^2-1}h^p) = g^{p^2(p-1)/2} h^{p^2(p+1)/2}.
\]
Thus equation (7.3) becomes

\[ W(z) \equiv ag \frac{p^2(p-1)}{2} h \frac{p^2(p+1)}{2} \pmod{p} \]

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 \( \infty \). Then the order of vanishing of \( W(z)(dz)^{\frac{p(p+1)}{2}} \) at \( \infty \) is

\[ \frac{n_0}{p-1} = \frac{p}{p-1} \left( \frac{p(p+1)}{2} \right) . \]

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

Equation (7.4) then forces \( n_0 = \frac{p^2(p+1)}{2} \). Since the leading coefficient of \( W(z) \) is a power of \( \pi \) by definition and \((-1)^{(p+1)/2}\) is not zero modulo \( p \), this forces the leading coefficient of \( W(z) \) to be \( 1 \) and

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

from which it follows that

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

This proves the following theorem:

**Theorem 1.3.** If \( p \) is odd, \( \pi \in \mathbb{F}_p[T] \) has degree 3, \( p \) is the ideal generated by \( \pi \), and the Wronskian on \( X_0(p) \) is denoted by \( W(z) \), then \( W(z) \) has leading coefficient 1 and rational, \( p \)-integral \( u \)-series coefficients at \( \infty \) and furthermore we have

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

Thanks to this congruence we may now prove:

**Theorem 1.4.** If \( p \) is odd, \( \pi \in \mathbb{F}_p[T] \) has degree 3, \( p \) is the ideal generated by \( \pi \), then we have

\[ \prod_{P \in Y_0(p)} (x - j(P))^\text{wt}(P) \equiv \prod_{\phi \in \mathcal{F}_p, \phi \text{ supersingular}} (x - j(\phi))^\mu(\phi^{-p-1}) \pmod{p}, \]

where \( g_p \) is the genus of the curve \( X_0(p) \).

**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 $\epsilon(d) = \frac{p}{p+1} \gamma((p^3 + 1)p(p + 1), 2) = 0$. This is because in this case we can take $\mu((p^3 + 1)p(p + 1), 2) = (p^3 + 1)p \equiv 2 \pmod{p - 1}$, which is the type of the form.

We will apply Proposition 3.6 part 2, $g_p(g_p - 1) = p(p - 1)$ 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

$$F_p(x) \equiv P(W, x) \pmod{p}$$

$$\equiv x^{p-1}P(G, x)P(g_3, x)^{p(p-1)} \pmod{p}$$

$$\equiv x^{p(p-1)}P(g_3, x)^{p(p-1)} \pmod{p}$$

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

This conclude the proof since $g_p = p$ in this case. \qed

References

[1] S. Ahlgren and K. Ono, Weierstrass points on $X_0(p)$ and supersingular $j$-invariants, Math. Ann. 325 (2003), 355–368.
[2] C. Armana, Torsion rationelle des modules de Drinfeld, Ph.D. thesis, Université Paris Diderot - Paris 7, 2008.
[3] M. Baker, Specialization of linear systems from curves to graph. With an appendix by Brian Conrad, Algebra Number Theory 2 (2008), no. 6, 613–653.
[4] V. Bosser and F. Pellarin, Hyperdifferential properties of Drinfeld quasi-modular forms, Int. Math. Res. Not. IMRN (2008).
[5] On certain families of Drinfeld quasi-modular forms, J. Number Theory (2009), 2952–2990.
[6] D. Dobi, N. Wage, and L. Wang, Supersingular rank two Drinfel’d modules and analogs of Atkin’s orthogonal polynomials, International Journal of Number Theory 5 (2009), 885–895.
[7] V.G. Drinfel’d, Elliptic modules (Russian), Mat. Sb. (N. S.) 94 (1974), 594–627.
[8] J. Fresnel and M. van der Put, Géométrie analytique rigide et applications, Progress in Mathematics, vol. 18, Birkhäuser, 1981.
[9] E.-U. Gekeler, Drinfeld-Moduln und modulare Formen über rationalen Funktionenkörpern, Bonner Math. Schriften, vol. 119, 1980.
[10] Drinfeld Modular Curves, Lecture Notes in Mathematics, vol. 1231, Springer-Verlag, 1986.
[11] Über Drinfeld’sche Modulkurven vom Hecke-Typ, Compositio Mathematica 57 (1986), 219 – 236.
[12] On the coefficients of Drinfeld modular forms, Invent. Math. 93 (1988), 667–700.
[13] E.-U. Gekeler and U. Nonnengardt, Fundamental domains of some arithmetic groups over function fields, Int. J. Math. 6 (1995), 689–708.
[14] E.-U. Gekeler and M. Reversat, Jacobians of Drinfeld modular curves, Journal für die reine und angewandte Mathematik 476 (1996), 27 – 93.
[15] L. Gerritzen and M. van der Put, Schottky groups and Mumford curves, Lecture Notes in Mathematics, vol. 817, Springer-Verlag, 1980.
[16] D.M. Goldschmidt, Algebraic Functions and Projective Curves, Graduate Texts in Mathematics, vol. 215, Springer, 2003.
[17] D. Goss, $\pi$-adic Eisenstein series for function fields, Compositio Math. 41 (1980), 3–38.
[18] H. Hasse and H.L. Schmidt, Über die Ausnahmeklassen bei abstrakten hyperelliptischen Funktio-

nenkörpern, Journal für die reine und angewandte Mathematik 176, 184.
[19] M. Kaneko and M. Koike, On extremal quasimodular forms, Kyushu Journal of Mathematics 60 (2006), 457–470.
[20] R. Kiehl, Der Endlichkeitssatz für eigentliche Abbildungen in der nichtarchimedischen Funktionen- theorie, Invent. Math. 2 (1967), 191–214.
[21] Theorem A und Theorem B in der nichtarchimedischen Funktionentheorie, Invent. Math. 2 (1967), 256–273.
[22] L. Carlitz, On certain functions connected with polynomials in a Galois field, Duke Math. J. 1 (1935), 137–168.
[23] A.P. Ogg, On the Weierstrass points of $X_0(n)$, Illinois Journal of Mathematics 22 (1978), no. 1, 31–35.
[24] D.E. Rohrlich, Some remarks on Weierstrass points, Progress in Mathematics, vol. 26, pp. 71–78, Birkhäuser, 1982.
[25] Weierstrass points and modular forms, Illinois Journal of Mathematics 29 (1985), no. 1, 134–141.
[26] F.K. Schmidt, Zur arithmetischen Theorie der algebraischen Funktionen. II. Allgemeine Theorie der Weierstraßpunkte, Mathematische Zeitschrift 45 (1939), no. 1, 75–96.
[27] K.-O. Stöhr and J.F. Voloch, Weierstrass points and curves over finite fields, Proc. London Math. Soc. (3) 52 (1986), 1–19.
[28] Y. Uchino and T. Satoh, Function field modular forms and higher derivations, Math. Ann. 311 (1998), 439–466.
[29] C. Vincent, Drinfeld modular forms modulo $p$ and Weierstrass points on Drinfeld modular curves, Ph.D. thesis, University of Wisconsin – Madison, 2012.
[30] On the trace and norm map from $\Gamma_0(p)$ to $GL_2(A)$, Journal of Number Theory 142 (2014), 18–43.

Department of Mathematics, Stanford University, California 94305
E-mail address: cvincent@stanford.edu