# Deligne's congruence and supersingular reduction of Drinfeld modules

*by* Gunther Cornelissen

It appears to be Deligne who has first observed that the Hasse-invariant for a prime number $p$ is congruent modulo $p$ to the Eisenstein of weight $p-1$ on $SL(2,\mathbf{Z})$ ([11],(2.1)). Said otherwise, the polynomial

$$P_p(X) = \prod_{E_{p-1}(z)=0} (X - j(z))$$

lift the supersingular polynomial to characteristic zero. This observation brings to mind the following idea: if a rational elliptic curve has supersingular reduction at a prime $p$, then the Eisenstein series $E_{p-1}$ acquires a zero modulo $p$ at the complex point $z$ whose $j$-invariant $j = j(z)$ is that of the elliptic curve. This means that *if* the value $P_p(j)$ is integral, then either

$$(*) \qquad |P_p(j)| \geq p,$$

or $z$ is a zero of $E_{p-1}$. If one can exclude the latter possibility (namely, that zeros of Eisenstein series have rational $j$-invariants), then $(*)$ provides a relation between $j$ and $p$ such that $j$ is a supersingular invariant modulo $p$.

Unfortunately, I have not yet been able to make this idea produce meaningful information about elliptic curves. But, as was pointed out by E.-U. Gekeler ([6]), the Hasse invariant modulo a prime polynomial $\mathfrak{p}$ for rank-two Drinfeld modules over the polynomial ring $A = \mathbf{F}_q[T]$ is equally congruent to an appropriate Eisenstein series for $GL(2,A)$. In this paper, I want to exploit the above idea to gain information on the arithmetic of function fields. It turns out to bound the number of primes of supersingular reduction of a fixed degree for a given Drinfeld module over $A$ with "sufficiently small" $j$-invariant (what this means exactly will be stated below).

Let $\phi : A \to \mathrm{End}(\mathbf{G}_a(\mathbf{F}_q(T))$ be a ring morphism such that

$$\phi(T) = TX + gX^q + \Delta X^{q^2}, \text{ where } g \in A, \Delta \in A - \{0\},$$

and we have identified the endomorphisms of the additive group scheme with additive polynomials in the variable $X$. Such $\phi$ is called a (rank-two) Drinfeld module (defined over $A$), and for any prime $\mathfrak{p} \in A$, it makes sense to consider the reduction of $\phi$ modulo $\mathfrak{p}$, obtained by reducing the coefficients $g$ and $\Delta$ of $\phi$. A prime $\mathfrak{p}$ not dividing $\Delta$ is called supersingular if the coefficient of $X^{q^{\deg(\mathfrak{p})}}$ in $\phi(\mathfrak{p})$ is divisible by $\mathfrak{p}$. Let

$$j = \frac{g^{q+1}}{\Delta} \text{ and } m(k) = \frac{q^k - q^{\chi(k)}}{q^2 - 1}.$$

Let $s_i(g, \Delta)$ be the number of monic primes of degree $i$ which do not divide $\Delta$ and which are supersingular for $\phi$.

**Theorem A.** *If $j \neq 0$ and $j \neq T^q - T$, then*

$$\sum_{i=1}^{k} i s_i(g, \Delta) \leq (m(k) + \chi(k)) \cdot \max\{q + \deg(\Delta), (q+1)\deg(g)\} + \chi(k)\deg(g),$$

*where $\chi$ is the characteristic function of the odd integers, i.e. $\chi(2\mathbf{Z}+1) = 1$ and $\chi(2\mathbf{Z}) = 0$. Furthermore,*

1. *If $j = 0$, then an ordinary prime of $A$ is supersingular if and only if it has odd degree.*
2. *If $j = T^q - T$, then the formula holds for $k > 2$, but should be replaced by $2s_2(g, \Delta) \leq q^2 - q$ for $k = 2$.*

*Remark.* The Drinfeld module $\phi$ can also have good supersingular reduction at a prime dividing $\Delta$, in the correct (technical) sense to be defined below. But theorem A applies in particular to a global minimal model of $\phi$, for which the divisors of $\Delta$ are the precisely the primes of bad reduction (*cf. infra*). So for a minimal model, $s_i(g, \Delta)$ is really the number of supersingular primes of degree $i$ for $\phi$.

For Drinfeld modules with integral $j$-invariants ($j \in A$), there is a second version of this theorem. A typical example of such a Drinfeld module is given by $\phi(T) = TX + jX^q + j^q X^{q^2}$.

**Theorem B.** *If $j \in A$ and $j \notin \{0, T^q - T\}$, then*

$$\sum_{i=1}^{k} i(s_i(g, \Delta) - \varepsilon_i(g)) \leq m(k) \cdot \max\{q, \deg j\},$$

*where $\varepsilon_i(g)$ is the number of monic primes of degree $i$ not dividing $\Delta$ but dividing $g$ if $i$ is odd, and zero otherwise.*

This formula is trivial if $\deg(j)$ is large (say, larger then $q^3$, since $is_i(g, \Delta) < q^i$ and $m(k) \approx q^{k-2}$), and produces only very weak asymptotics as $k$ grows (of type: the fraction of primes of degree $k$ which is supersingular remains bounded). It is known in general that the set of supersingular primes $\{\mathfrak{p}\}$ of a

Drinfeld module without complex multiplication has density zero, but is infinite of asymptotic order $\gg \log\log x$ for $q^{\deg(\mathfrak{p})} < x$, at least for the infinite class of so-called non-exceptional Drinfeld modules. (Brown [1], David [2]). On the other hand, Poonen has constructed Drinfeld modules without supersingular primes, and at the same time corrected the notion of exceptional module, as a miscalculation occurred in the work of Brown ([12]).

The statements in theorem A and B are of a *non-asymptotic* sort. They typically produce corollaries of the following type:

**Example A.** *If a Drinfeld module has supersingular reduction at no primes of degree one and at all primes of degree two, then either*

1. $\deg j \leq q$ *and* $j = T^q - T$ *or* $\deg \Delta \geq q^2 - 2q$, *or*
2. $\deg j > q$ *and* $\deg(g) \geq (q^2 - q)/(q+1)$.

**Example B.** *For an integral $j$-invariant of degree $\deg j < q$, the number of supersingular primes of degree 2 is less then $q/2$, and if this bound is attained, the number of supersingular primes of degree 3 not dividing $g$ is less then or equal to $q^2/3$.*

To any Drinfeld module $\phi$ over $A$ one can associate a two-dimensional $\mathfrak{p}$-adic Galois representation of the separable Galois group of $K$ given by its action on the Tate module

$$\varprojlim_{n} \{x \in C : \phi(\mathfrak{p}^n)(x) = 0\}$$

of $\mathfrak{p}^\infty$-division points of $\phi$. The above theorems impose restrictions on the local structure (the image of the decomposition group) at $\mathfrak{p}$ of such representations, *e.g.*: for Drinfeld modules with integral $j$-invariants of degree less then $q$, the $\mathfrak{p}$-adic representation is not ordinary at $\mathfrak{p}$ for at most $\approx 1/q$ primes $\mathfrak{p}$ of any fixed degree.

It is remarkable to see that such non-asymptotic formulae follow from considering supersingular moduli as moduli of zeros of Eisenstein series modulo $\mathfrak{p}$, whereas the asymptotic results of Brown *et. al.* follow from considering them as singular moduli modulo $\mathfrak{p}$. Actually, more lifts of the supersingular polynomial for elliptic curves are known (by hypergeometric polynomials, or Atkin-polynomials; *see* [10]), and perhaps one can deduce useful information by applying our idea to one of those lifts.

The plan of this paper is as follows: after a short introduction on supersingular Drinfeld modules and modular forms for function fields, we recall Deligne's congruence for Drinfeld modules, and establish further congruences for Eisenstein series. Then we study integrality, boundedness and rationality of $j$-invariants of zeros of Eisenstein series. Finally, we apply our idea to obtain the theorem.

That the elliptic point $j = 0$ occurs separately in the theorem comes as no surprise, but the invariant $j = T^q - T$ seems to be more mysterious. In the last section, we take a closer look at it.

## 1. Drinfeld modules and modular forms

(1.1) *Function Fields.* Let $A = \mathbf{F}_q[T]$ be the polynomial ring over the finite field $\mathbf{F}_q$ of $q(>2)$ elements, $K$ its quotient field, and $K_\infty$ and $C$ respectively its completion w.r.t. the valuation $-\deg$, and the completion of an algebraic closure of $K_\infty$.

We will denote $T^{q^i} - T$ by the symbol $\langle i \rangle$. It equals the product of all irreducibles in $A$ of degree dividing $i$ ([9]).

(1.2) *Drinfeld modules* ([3]). Let $L$ be a field with a morphism $i : A \to L$. A (rank-two) Drinfeld ($A$-)module over $L$ is a ring morphism

$$\begin{array}{rcl} \phi : A & \to & \mathrm{End}\ \mathbf{G}_a(L) \\ T & \mapsto & i(T)X + gX^q + \Delta X^{q^2}, \end{array}$$

where $g = g(\phi) \in L, \Delta = \Delta(\phi) \in L^*$, and we have identified the endomorphisms of the additive group scheme with additive polynomials in the variable $X$.

A morphism $u$ of two Drinfeld modules $\phi$ and $\psi$ is an element $u \in \mathrm{End}\ \mathbf{G}_a(L)$ such that $\phi \circ u = u \circ \psi$. Two Drinfeld modules are isomorphic over the algebraic closure $\bar{L}$ if and only if $j(\phi) = j(\psi)$, where $j(\phi) = g^{q+1}/\Delta$ is called the $j$-invariant of $\phi$.

(1.3) *Supersingularity* ([4], [7]). The ring of endomorphisms of a Drinfeld module $\phi$ over $\bar{L}$ is either $A$, an order in an imaginary extension of $K$ (imaginary means that the valuation $-\deg$ is inert), or a maximal order in a quaternion algebra over $K$ which is ramified at a unique finite prime. The latter case can only occur if $i$ is not injective, and then we call $\phi$ *supersingular*. It turns out that

$$\phi(\ker(i)) = lX^{q^{\deg(\ker(i))}} + \text{(higher degree terms)},$$

and $\phi$ is supersingular if and only if $l = 0$.

(1.4) *Reduction of Drinfeld modules.* A Drinfeld module $\phi$ over a complete local field $L$ with maximal ideal $\mathfrak{m}$ is called minimal if its coefficients $g, \Delta$ are integral and the $\mathfrak{m}$-valuation of $\Delta$ is minimal within the $L$-isomorphism class of $\phi$. We denote by $\phi^{\min}$ a minimal Drinfeld module belonging to $\phi$. A Drinfeld module $\phi$ is said to have good reduction over $L$ if $\mathfrak{m}$ does not divide $\Delta(\phi^{\min})$, and it then makes sense to consider the reduction of $\phi^{\min}$ (obtained by reducing the coefficients) as a Drinfeld module over the residue field of $L$, where the map $i$ from (1.2) is the reduction map modulo $\mathfrak{m}$. We say that a Drinfeld module $\phi$ over $L$ has supersingular reduction modulo a prime $\mathfrak{m}$ of good reduction if the reduction of a minimal model $\phi^{\min}$ at $\mathfrak{m}$ is supersingular.

Now suppose that $\phi$ is a Drinfeld module defined over the global field $K$, and assume that $\mathfrak{p}$ is a prime of $A$. The $\phi$ is said to have good (resp. supersingular) reduction modulo $\mathfrak{p}$ if it has good (resp. supersingular) reduction when considered over the completion $K_\mathfrak{p}$ of $K$ at $\mathfrak{p}$.

**(1.4.1) Lemma** *For any Drinfeld module $\phi$ defined over $A$, there exists a minimal model $\phi'$ over $A$ within the $K$-isomorphism class of $\phi$, in the sense that*

$$ord_\mathfrak{m}(\Delta(\phi')) = ord_\mathfrak{m}(\Delta(\phi^{\min}/K_\mathfrak{m}))$$

*for all* $\mathfrak{m}$ *in* $A$.

*Proof.* Assume that $u_\mathfrak{m}$ is the isomorphism of $\phi/K_\mathfrak{m}$ with its minimal model $\phi^{\min}/K_\mathfrak{m}$. Then

$$\Delta(\phi) = u_\mathfrak{m}^{q^2-1}\Delta(\phi^{\min}/K_\mathfrak{m}),$$

and $u_\mathfrak{m}$ is non-zero for only finitely many $\mathfrak{m}$. If we set

$$u = \prod_\mathfrak{m} \mathfrak{m}^{\mathrm{ord}_\mathfrak{m}(u_\mathfrak{m})},$$

then $\phi' = u^{-1} \circ \phi \circ u$ is the desired global minimal model. □

Observe that a minimal Drinfeld module $\phi$ has good reduction at a prime $\mathfrak{p}$ if and only if $\mathfrak{p}$ does not divide the discriminant $\Delta$ of $\phi$. This means that for a minimal Drinfeld module, $s_i(g, \Delta)$ is the total number of supersingular primes of degree $i$.

For a Drinfeld module which is not necessarily minimal, a prime $\mathfrak{p}$ which doesn't divide $\Delta$ is a prime of good reduction. For such $\mathfrak{p}$

$$\phi(\mathfrak{p}) = l_\mathfrak{p} X^{q^{\deg(\mathfrak{p})}} + \text{ (higher degree terms) mod } \mathfrak{p},$$

and hence $\mathfrak{p}$ is a prime of supersingular reduction if and only if $l_\mathfrak{p} = 0 \bmod \mathfrak{p}$.

(1.5) *Eisenstein series* ([3], [8], [5]). The space $\Omega = C - K_\infty$ can be given the structure of a rigid analytic space, and w.r.t. it the function

$$E_l(z) : \Omega \to C \ : \sum_{(0,0)\neq(a,b)\in A} (\frac{1}{az+b})^l$$

is a holomorphic modular form for the action of $GL(2, A)$ on $\Omega$ given by fractional transformations (with the appropriate notion of analyticity at the the cusp $\infty$). It is non-zero if $l$ is divisible by $q - 1$.

There is a correspondence between Drinfeld modules over $C$ and rank-two $A$-lattices $\Lambda = Az \oplus A$ in $C$ $(z \in \Omega)$ given by $\phi \mapsto z$ if for all $a \in A$ and all $\omega \in \Omega$, $\phi(a)(e_\Lambda(\omega)) = e_\Lambda(a\omega)$, where

$$e_\Lambda(\omega) = \omega \prod_{\lambda\in\Lambda-\{(0,0)\}} (1 - \frac{\omega}{\lambda})).$$

Via this correspondence, the coefficients $g$ and $\Delta$ of the Drinfeld module become modular forms of the variable $z$, if we let $z$ vary in $\Omega$. As a matter of fact, the ring of modular forms for $GL(2, A)$ is the free $C$-algebra spanned by $g$ and $\Delta$, hence $E_l$ is a polynomial in $g$ and $\Delta$.

## 2. Deligne's congruence

As above, let $\phi$ be a Drinfeld module defined over $A$ and $\mathfrak{p}$ a prime of degree $k$ which does not divide $\Delta$. Let $l_\mathfrak{p}(g, \Delta)$ be the coefficient of $X^{q^k}$ in $\phi(\mathfrak{p})$.

Let $A_k(X, Y)$ denote the two-variable polynomial such that

$$\forall z \in \Omega : \ (-1)^{k+1}(\prod_{i\leq k}\langle i\rangle)E_{q^k-1}(z) = A_k(g(z), \Delta(z)).$$

**(2.1) Lemma** *The polynomials $A_k$ satisfy the two term recursion relation*

$$A_k = X^{q^{k-1}} A_{k-1} - \langle k-1 \rangle Y^{q^{k-2}} A_{k-2}$$

*with starting values $A_{-1} = 0, A_0 = 1$. Hence they are defined over $A$.*

*Sketch of Proof.* ([6], (12.2)) It follows from the corresponding identity for Eisenstein series, which in its turn follows from the fact that the Eisenstein series are coefficients in the expansion of the lattice function $e_{Az\oplus A}$ at infinity (like Eisenstein series for $SL(2, \mathbf{Z})$ are coefficients in the expansion of the Weierstraß $\wp$-function). $\square$

**(2.2) Lemma** ("Deligne's congruence") *The congruence*

$$l_{\mathfrak{p}}(g, \Delta) = A_k(g, \Delta) \ mod \ \mathfrak{p}$$

*holds for any $\mathfrak{p}$ of degree $k$ in $A$.*

*Sketch of Proof.* ([6], (12.3)) It follows because both sides as modular forms modulo $\mathfrak{p}$ reduce to 1, and because $A_k(X, Y) - 1$ is the only relation in the ring of modular forms modulo $\mathfrak{p}$. $\square$

This congruence is remarkable in so far that, whereas the "Hasse-invariant" $l_{\mathfrak{p}}$ depends on $\mathfrak{p}$, its lift via Deligne's congruence depends only on the degree $k$ of $\mathfrak{p}$.

**(2.3) Lemma** *The congruences*

$$A_n = A_{n-k}^{q^k} A_k \ mod \ \mathfrak{p}$$

*hold for any prime $\mathfrak{p}$ of degree $k$.*

*Proof.* Using the fact that

$$\langle n-1 \rangle = \langle n-k-1 \rangle^{q^k} \mod \mathfrak{p},$$

it follows inductively from the recursion (2.1). $\square$

## 3. $j$-invariants of zeros of Eisenstein series

Define the polynomial $P_k$ by the formula

$$A_k(X, Y) = P_k(\frac{X^{q+1}}{Y}) Y^{m(k)} X^{\chi(k)}.$$

Denote the coefficients of $P_k$ by $c_i^{(k)}$, *i.e.*

$$P_k(Z) = \sum_{i=0}^{m(k)} c_i^{(k)} Z^{m(k)-i},$$

where $m(k)$ is as in the introduction.

**(3.1) Lemma** *The coefficients $c_i^{(k)}$ are integral (i.e., in $A$), $c_0^{(k)} \neq 0$ and $c_{m(k)}^{(k)} = 1$ for all $k > 0$. If a coefficient $c_i^{(k)}$ is non-zero, then it is of exact degree $qi$. All roots of $P_k$ have degree $q$.*

*Proof.* The recursion (2.1) translates into

$$P_k(Z) = Z^{d(k)}P_{k-1}(Z) - \langle k-1\rangle P_{k-2}(Z) \text{ where } d(k) = \frac{q^{k-1} + (-1)^k}{q+1}. \tag{3.1.1}$$

From this, the statement about the leading and constant term follows inductively. It is easy to prove that $d(k) > m(k-2)$, and hence the following recursion holds for the coefficients:

$$c_i^{(k)} = \begin{cases} c_i^{(k-1)} & \text{if } i < m(k-2) \\ -\langle k-1\rangle c_{m(k-2)-m(k)+i}^{(k-2)} & \text{otherwise} \end{cases}.$$

From this, it follows by induction that a non-zero $c_i^{(k)}$ has degree $qi$, since $m(k-2) - m(k) = -q^{k-2}$.

The Newton polygon for the valuation $-\deg$ is then a straight line of slope $q$, and hence the statement about the roots of $P_k$ holds. □

(3.2) *Remark.* The polynomial $P_k$ is such that

$$(-1)^{k+1}(\prod_{i\leq k}\langle i\rangle)E_{q^k-1}(z) = g(z)^{\chi(k)}\Delta(z)^{m(k)}P_k(j(z))$$

for all $z \in \Omega$. Since $\Delta$ is non-zero on $\Omega$, this means that the zeros of $P_k$ are exactly the $j$-invariants of non-elliptic zeros of the Eisenstein series $E_{q^k-1}$ (by an elliptic zero $z$ we mean one for which $j(z) = 0$; for such points, which all belong to a single $GL(2,A)$-orbit in $\Omega$, the stabilizer for the action of that group via fractional transformation is larger then the trivial one consisting of the scalar matrices).

**(3.3) Lemma** *If $P_k$ has a rational zero (i.e., $P_k(a) = 0$ for some $a \in K$), then $k = 2$ and $a = \langle 1\rangle$.*

*Proof.* Assume that $P_k(a) = 0$ for some $a \in K$. Since $P_k$ is an integral equation over $A$, we have $a \in A$. Also, since all coefficients $c_i^{(k)}$ for $i \neq m(k)$ are divisible by $\langle 1\rangle$, $a$ has to be divisible by $\langle 1\rangle$. But $a$ has degree $q$ by (3.1), it has to be of the form $a = \alpha \cdot \langle 1\rangle$ for some $\alpha \in \mathbf{F}_q^*$ (note that $a \neq 0$ since $c_0^{(k)} \neq 0$).

By considering the recursion (3.1.1) for $P_k$ modulo primes of degree $k-1$, it follows that all such primes divide $(\alpha\langle 1\rangle)^{d(k)}P_{k-1}(\alpha\langle 1\rangle)$. Hence if $k > 2$

$$\prod_{\deg(\mathfrak{p})=k-1} \mathfrak{p} \text{ divides } P_{k-1}(\alpha\langle 1\rangle).$$

If $N$ denotes the number of such primes $\mathfrak{p}$, then the left hand side has degree $(k-1)N$, whereas if $P_{k-1}(a) \neq 0$, the degree of the right hand side is bounded from above by $qm(k-1)$, since we know the degree of the coefficients $c_i^{(k-1)}$ by the previous lemma. But

$$\begin{aligned}(k-1)N &= q^{k-1} + \text{ (lower terms in } q \text{ with coefficients } \pm 1) \\ &> qm(k-1) = q^{k-2} + \text{ (lower terms in } q \text{ with coefficients } 1)\end{aligned}$$

(consider the two numbers as written down in their $q$-adic expansion, $q > 2$).

It follows that $P_{k-1}(a) = 0$ too, and by applying the recursion (3.1.1) repeatedly in the opposite direction, it would follow that $P_1(a) = 0$, whereas $P_1 = 1$. From this contradiction, we conclude that $k = 2$, and since $P_2(Z) = Z - \langle 1 \rangle$, also that $a = \langle 1 \rangle$. □

## 4. Proofs of theorem A and theorem B

(4.1) *Proof of theorem A.* Assume that the Drinfeld module $\phi$ has supersingular reduction modulo $s_i$ primes of degree $i \leq k$ which do not divide $\Delta$, and denote the set of these primes by $S_i = \{\mathfrak{p}_\alpha^{(i)}\}_{\alpha=1}^{d_i}$. Then for any $\mathfrak{p}$ in $S_i$, we have $l_\mathfrak{p}(g, \Delta) = 0 \bmod \mathfrak{p}$, hence by (2.2), any such prime $\mathfrak{p}$ divides $A_i(g, \Delta)$. From the congruences (2.3), we conclude that

$$\prod_{i=1}^{k} \prod_{\alpha=1}^{s_i} \mathfrak{p}_\alpha^{(i)} \text{ divides } A_k(g, \Delta) = g^{\chi(k)} \sum_{i=0}^{k} c_i^{(k)} g^{(q+1)(m(k)-i)} \Delta^i.$$

The degree of the left hand side equals $\sum_{i=1}^{k} i s_i$. On the other hand, using (3.1), we find that if $A_k(g, \Delta) \neq 0$, the degree of the right hand side is bounded by

$$\max\{[q + \deg(\Delta) - (q+1)\deg(g)]i\} + [(q+1)m(k) + \chi(k)]\deg(g).$$

Since for $i \in \{0, m(k)\}$ the coefficient $c_i^{(k)}$ is non-zero, this maximum is attained for one of these values, and a bit of computation shows that

$$\deg(A_k(g, \Delta)) \leq m(k) \max\{q + \deg(\Delta), (q+1)\deg(g)\} + \chi(k)\deg(g).$$

Hence either the inequality in theorem A holds, or $A_k(g, \Delta) = 0$.

Assume first of all that $g = 0$. Then

$$A_k(0, \Delta) = \begin{cases} 0 & \text{if } k \text{ is odd} \\ \prod_{l=1}^{k/2} \langle 2l - 1 \rangle \Delta^{m(k)} & \text{if } k \text{ is even} \end{cases}.$$

Since primes of even degree do not divide $\langle 2l-1 \rangle$, we see that exactly the primes of odd degree are supersingular for $\phi$.

If $A_k(g, \Delta) = 0$ and $g \neq 0$, it follows that $P_k(j) = 0$ for $j = g^{q+1}/\Delta \in K$. Then from (3.3) we conclude that $j = \langle 1 \rangle$ and $k = 2$. So in that case, the formula has to be replaced by $2s_2 \leq q^2 - q$. This finishes the proof of theorem A. □

(4.2) *Proof of theorem B.* Assume that the primes in $S_i$ are arranged in such a way that if $i$ is odd, the divisors of $g$ are the last $\varepsilon_i = \varepsilon_i(g)$ elements in $S_i$. If $j$ is integral, we find in a similar way (eliminating the divisors of $g$ and $\Delta$) that

$$\prod_{i=1}^{k} \prod_{\alpha=1}^{s_i - \varepsilon_i} \mathfrak{p}_\alpha^{(i)} \text{ divides } P_k(j).$$

Unless it is zero, the right hand side has its degree bounded from above by $m(k) \cdot \max\{q, \deg(j)\}$, and one can proceed as in the proof of theorem A. $\square$

(4.3) *Remark.* It follows from these proofs that one can substitute $s_i$ in theorem A by $s_i - \varepsilon_i$ and delete the term $\chi(k)\deg(g)$ from the right hand side, and conversely, one can change $s_i - \varepsilon_i$ in theorem B to $s_i$ at the cost of adding $\chi(k)\deg(g)$ to the right hand side.

## 5. A remark on $T^q - T$ as supersingular invariant

(5.1) In [12], Poonen has constructed Drinfeld modules with $j$-invariants

$$j = T^q \frac{(a^{q-1}+1)^{q+1}}{a^{q(q-1)}}, \text{ for any } a \in A - \{0\} \text{ and odd } q$$

having no primes of supersingular reduction (*e.g.*, $j = 4T^q$). There is an obstruction to supersingularity coming from the representations on torsion points of the Drinfeld module, namely: the action of the $\mathfrak{p}$-Frobenius on the $\mathfrak{l}$-torsion ($\mathfrak{l} \neq \mathfrak{p}$) can be conjugate to its action on a the $\mathfrak{l}$-torsion of a supersingular Drinfeld module for only finitely many $\mathfrak{p}$. He asked whether Drinfeld modules where this obstruction does not occur always have an infinite set of supersingular primes. To his knowledge, for $j = T^q - T$ the obstruction does not occur. However, there is some evidence to expect that

$$?\ \gcd(P_k(\langle 1\rangle), \langle k\rangle) = \langle 2 - \chi(k)\rangle.$$

This would imply that a prime $\mathfrak{p}$ of degree $k$ divides $P_k(\langle 1\rangle)$ only if $k = 2$. In particular, it would provide the first example of a Drinfeld module with a *finite, but non-empty* set of supersingular primes (and perhaps not satisfying Poonen's obstruction).

(5.2) In (3.3), it was shown that $j = \langle 1\rangle$ is the only rational non-zero $j$-invariant of zeros of Eisenstein series of weight $q^k - 1$, and that it only occurs for $k = 2$. As a matter of fact, it turns out that the polynomial $P_k$ is irreducible over $K$, and that very probably for $k > 3$

$$\mathrm{Gal}(K(j(z) : E_{q^k-1}(z) = 0)/K) = S_{m(k)},$$

which can be considered as a statement about the arithmetical distribution of the zeros of such modular forms. I hope to return to this point at some other occasion.


## Acknowledgment

The author is post-doctoral fellow of the Fund for Scientific Research - Flanders (FWO - Vlaanderen). This work was done while visiting the MPIM.


## References


[1] M.L. Brown, *Singular moduli and supersingular moduli of Drinfeld modules*, Invent. Math. **110** (1992), 419–439.

[2] C. David, *Supersingular reduction of Drinfeld modules*, Duke Math. J. **78** (1995), no. 2, 399–412.

[3] V.G. Drinfeld, *Elliptic modules*, Math. Sb. **94(136)** (1974), 594–627.

[4] ———, *Elliptic modules II*, Math. Sb. **102(144)** (1977), 182–194.

[5] E.-U. Gekeler, *Drinfeld modular curves*, Lecture Notes in Math., vol. 1231, Springer, Berlin - Heidelberg - New York, 1986.

[6] ———, *On the coefficients of Drinfeld modular forms*, Invent. Math. **93** (1988), 667–700.

[7] ———, *On finite Drinfeld modules*, J. Algebra **141** (1991), 187–203.

[8] D. Goss, *Modular forms for $F_r[T]$*, J. Reine Angew. Math. **317** (1980), 16–39.

[9] ———, *Basic structures of function field arithmetic*, Ergebn. der Math., vol. 35, Springer, Berlin - Heidelberg - New York, 1996.

[10] M. Kaneko and D. Zagier, *Supersingular $j$-invariants, hypergeometric series and Atkin's orthogonal polynomials*, preprint, 1997.

[11] N. Katz, *$p$-adic properties of modular schemes and modular forms*, Modular forms of one variable III, Lecture Notes in Math., vol. 350, Springer, Berlin - Heidelberg - New York, 1972, pp. 69–190.

[12] B. Poonen, *Drinfeld modules with no supersingular primes*, `www:` Algebraic Number Theory Archives (Urbana) preprint nr. 63, 1997.

Max-Planck-Institut für Mathematik, Gottfried-Claren-Straße 26, D-53225 Bonn *(current)*

University of Gent, Dept. of Pure Mathematics, Galglaan 2, B-9000 Gent

e-mail `gc@cage.rug.ac.be`