ACADEMIC PRESS

Available at WWW.MATHEMATICSWEB.ORG POWERED BY SCIENCE DIRECT®

Journal of Number Theory 102 (2003) 107–117

JOURNAL OF Number Theory

http://www.elsevier.com/locate/jnt

# "Weak" congruences for coefficients of the Eisenstein series for $\mathbb{F}_q[T]$ of weight $q^k - 1$

José Gallardo and Bartolomé López*,[1]

*Departamento de Matemáticas, Universidad de Cádiz, Polígono Río San Pedro s/n, ES-11510 Puerto Real (Cádiz), Spain*

Received 13 August 2002; revised 6 November 2002

Communicated by D. Goss

**Abstract**

We study the expansion of the Eisenstein series for $\mathbb{F}_q[T]$ of weight $q^k - 1$, $k \in \mathbb{N}$, and using the fact that they are eigenfunctions for the Hecke operators, we prove congruences for some of their coefficients.


*MSC:* 11G09; 11F52

*Keywords:* Drinfeld modular forms; Hecke operators

## Introduction

In two previous works (cf. [3,5]), the existence of congruences for the coefficients of two distinguished Drinfeld modular forms, the discriminant function $\Delta$ and its $(q-1)$th root $h$, was proven. In both cases, the result was obtained using the fact that those modular forms are eigenfunctions for the action of the Hecke operators; the congruences allowed to prove empirical rules (obtained from examples) for some coefficients of both modular forms. In the present work, using the same basic argument, we prove that there exist (weaker) similar congruences for the Eisenstein

*Corresponding author. Fax: +34-956-016288.

*E-mail address:* bartolome.lopez@uca.es (B. López).

[1] The second author thanks the Ministerio de Ciencia y Tecnología of Spain (project BFM2001-1488-C02-C01) for financial support.

0022-314X/03/$ - see front matter 
doi:10.1016/S0022-314X(03)00063-5

series of weight $q^k-1$, $k\in\mathbb{N}$ (compare Theorem 2 with Theorem 2.4 of [3] and Theorem 1 of [5]). Using these "weak" congruences, the coefficients $a_{q^{d+k}+q^{k-1}+\cdots+1}$ of the Eisenstein series of weight $q^k-1$, for $d\in\mathbb{N}$, are determined up to a factor of degree $q^k-q$ (see Corollary 7).

The proof of the main result of this work, the congruences of Theorem 2, follows the same scheme as the proof of the congruences in [5]. Nevertheless, there are three differences, which are essential ingredients of the present proof. First, due to the fact that there exist no "strong" congruences in this case (see Remark 6), Hecke operators $T_{\mathfrak{p}^m}$ associated to $m$th powers of an irreducible polynomial $\mathfrak{p}$ have to be used instead of simple operators $T_{\mathfrak{p}}$. Secondly, the known property $a_n\neq 0\Rightarrow n\equiv 0,1 \bmod q$, satisfied by the Eisenstein series of weight $q^k-1$ (cf. [2, Proposition 6.10, p. 684]), has to be replaced by the property stated in Proposition 1. Third, in order to arrive to our conclusion, a more detailed study of the multinomial coefficients $\frac{(i_0+\cdots+i_{md})!}{i_0!\cdots i_{md}!} \bmod p$, where $p$ is the characteristic of $\mathbb{F}_q$, has to be done (see Lemma 4).

Here, the case of the coefficients $a_{q^{d+k}+q^{k-1}+\cdots+1}$ of the Eisenstein series of weight $q^k-1$ has been dealt with. There are two directions in which this work may be continued. The first one is to extend our result to the Eisenstein series of weight $r(q-1)$, $r\in\mathbb{N}$. The second, to study other coefficients of the Eisenstein series; for example, it seems that there exist (empirical) rules for the coefficients $a_{q^{d+k}}$ and $a_{q^{d+k}+q^{k-1}+\cdots+q^l}$, $l=0,1,\ldots,k-1$, of the Eisenstein series of weight $q^k-1$; a first problem would be to prove these rules. We think that, in both cases, new arguments should be brought up in order to extend our result. The reason being, the Goss polynomials (the basic tool used here) are inefficient in some examples and furthermore, handling these polynomials becomes much more complicated in the general situation than in the case dealt with in this work.

## 1. Preliminaries

Let $A:=\mathbb{F}_q[T]$ be the ring of polynomials over the finite field $\mathbb{F}_q$ and let $K:=\mathbb{F}_q(T)$ be its quotient field. We consider the completion $K_\infty:=\mathbb{F}_q((1/T))$ of $K$ at the place $\infty$, and the completed algebraic closure of $K_\infty$, $C:=\hat{\bar{K}}_\infty$.

Let $C\{\tau\}$ be the ring of non-commutative polynomials over $C$, where $\tau$ is the Frobenius endomorphism; the product in $C\{\tau\}$ satisfies the rule $\tau\alpha=\alpha^q\tau$, $\alpha\in C$. The ring $C\{\tau\}$ can be identified with the ring of $q$-additive polynomials $\sum_{i=0}^{l} c_iX^{q^i}$, where the product is given by substitution.

A *Drinfeld module* of rank $r$ over $C$ is a ring $\mathbb{F}_q$-homomorphism $\phi:A\to C\{\tau\}$ determined by

$$\phi_T=T\tau^0+\sum_{i=1}^{r} c_i\tau^i,$$

where $c_i\in C$, $c_r\neq 0$. Two modules $\phi$, $\phi'$ are *isomorphic* if there exists an element $u\in C^*$ such that $u\cdot\phi_a=\phi'_a\cdot u$ for any $a\in A$.

An *A-lattice* in $C$ of rank $r$ is a discrete free $A$-module $\Lambda \subset C$ of rank $r$. The exponential function

$$e_\Lambda(z) = z \prod_{\lambda \in \Lambda - \{0\}} (1 - z/\lambda)$$

can be associated to $\Lambda$. Through this function, a Drinfeld module of rank $r$ can be constructed. This construction establishes a bijection between the set of lattices of rank $r$ in $C$ and the set of Drinfeld modules of rank $r$ over $C$.

The *Carlitz module* is the rank one module determined by

$$\rho_T = T\tau^0 + \tau = TX + X^q.$$

Let $L = \bar{\pi}A$ be the lattice in $C$ corresponding to $\rho$ (the element $\bar{\pi} \in C$ is determined up to a unit of $A$). From the exponential function $e_L$ associated to $L$, we define the functions

$$t(z) = e_L(\bar{\pi}z)^{-1} \quad \text{and} \quad s(z) = t(z)^{q-1}.$$

These functions will be used along the work as parameters of the expansion of the Eisenstein series of weight $q^k - 1$.

Let $a \in A$. We consider the polynomial $\rho_a = \sum_{i=0}^{\deg a} l_i X^{q^i}$. Then $l_0 = a$ and the leading coefficient of $\rho_a$ is the leading coefficient of $a$; the rest of the coefficients of $\rho_a$ satisfy the recursion

$$l_i = \frac{l_{i-1}^q - l_{i-1}}{[i]}, \tag{1}$$

where $[i] = T^{q^i} - T = \prod_{\substack{\mathfrak{p} \text{ monic, prime} \\ \deg \mathfrak{p} | i}} \mathfrak{p}$.

The $A$-lattices of rank two in $C$ are of the form $u(zA + A)$, where $u \in C^*$, $z \in \Omega := C - K_\infty$. Homothetic lattices correspond to isomorphic Drinfeld modules; hence, any Drinfeld module of rank two is isomorphic to one in the form

$$\phi_T = T\tau^0 + g(z)\tau + \Delta(z)\tau^2, \tag{2}$$

where $z \in \Omega$. The functions $g(z)$ and $\Delta(z)$ (on $\Omega$) are *modular forms* for the group $\Gamma(1) := GL(2, A)$ of weights $q - 1$ and $q^2 - 1$, respectively. A function $h$ on $\Omega$ is called a *modular form of weight k* for the group $\Gamma(1)$ if it is holomorphic on $\Omega$ (in the rigid analytic sense), it has an expansion of the form $h = \sum_{n \geqslant 0} c_n s(z)^n$ and it satisfies

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

for every $\left(\begin{smallmatrix} a & c \\ b & d \end{smallmatrix}\right) \in \Gamma(1)$. The $C$-vector space of modular forms of weight $k$ is denoted by $M_k$; it follows from the definition of modular form that $M_k$ is trivial for $k \not\equiv 0 \bmod q - 1$. Distinguished modular forms are the *Eisenstein series* of weight $k$,

which are defined as

$$E_k(z) = \sum_{\substack{c,d\in A\\(c,d)\neq(0,0)}} \frac{1}{(cz+d)^k}. \tag{3}$$

The functions $g$ and $\Delta$ considered above can be expressed in terms of Eisenstein series: $g = (T^q - T)E_{q-1}$ and $\Delta = (T^{q^2} - T)E_{q^2-1} + (T^q - T)^q (E_{q-1})^{q+1}$ (cf. [2, Proposition 6.9, p. 684], or [4, Theorem 2.1.1, p. 27]).

In the sequel, the symbols $\mathfrak{a}, \mathfrak{p}$ will denote *monic* polynomials in $A$. Let $\mathfrak{p}$ be an irreducible (and monic) polynomial with $\deg \mathfrak{p} = d$. Let $m \in \mathbb{N}$; the *Hecke operators* $T_{\mathfrak{p}^m}$ act on the spaces $M_k$ and this action can be explicitly given on $t$-expansions of modular forms: if $h = \sum_{n\geqslant 0} c_n t^n \in M_k$, then

$$T_{\mathfrak{p}^m}\left(\sum_{n\geqslant 0} c_n t^n\right) = \sum_{i=0}^{m} \mathfrak{p}^{(m-i)\,k} \sum_{n\geqslant 0} c_n G_{n,\mathfrak{p}^i}(\mathfrak{p}^i t_{\mathfrak{p}^{m-i}}), \tag{4}$$

where $t_{\mathfrak{a}}(z) = t(\mathfrak{a}z) = t^{q^{\deg \mathfrak{a}}}/f_{\mathfrak{a}}(t)$, $f_{\mathfrak{a}}(X) = \rho_{\mathfrak{a}}(X^{-1})X^{q^{\deg \mathfrak{a}}}$, and $G_{n,\mathfrak{p}^i}$ is the $n$th *Goss polynomial* with respect to $\ker \rho_{\mathfrak{p}^i}$. The Goss polynomials can be defined by the following recursion formula (cf. [2, p. 323]): let $\rho_{\mathfrak{a}}(X) = l_0 X + l_1 X^q + \cdots + l_{\deg \mathfrak{a}} X^{q^{\deg \mathfrak{a}}}$ and $\alpha_i = l_i/\mathfrak{a}$; then $G_{n,\mathfrak{a}} = 0$ for $n \leqslant 0$, $G_{1,\mathfrak{a}} = X$ and

$$G_{n,\mathfrak{a}}(X) = X(G_{n-1,\mathfrak{a}} + \alpha_1 G_{n-q,\mathfrak{a}} + \alpha_2 G_{n-q^2,\mathfrak{a}} + \cdots) \text{ for } n > 1.$$

There also exists an explicit formula for the polynomials $G_{n,\mathfrak{a}}$ that will be used in Section 2.

## 2. Coefficients of the Eisenstein series $E_{q^k-1}$

Let us now consider the Eisenstein series of weight $q^k - 1$, $E_{q^k-1}$ (see Eq. (3)). It follows that

$$\tilde{\pi}^{1-q^k} E_{q^k-1}(z) = (-1)^{k+1} L_k^{-1} - \sum_{\mathfrak{a}\text{ monic}} G_{q^k-1}(t_{\mathfrak{a}}), \tag{5}$$

where $L_0 = 1$ and $L_k = [k][k-1]\cdots[1]$, and $G_{q^k-1}$ is the Goss polynomial associated to the lattice $L = \tilde{\pi}A$ (cf. [2, Eq. (6.3), p. 682]). An explicit formula for $G_{q^k-1}$ is given by

$$G_{q^k-1} = \sum_{i<k} (-1)^i L_i^{-1} X^{q^k - q^i};$$

this formula is deduced from Proposition (3.10) and Eq. (4.3) of [2]. We conclude that

$$\bar{\pi}^{1-q^k} E_{q^k-1}(z) = (-1)^{k+1} L_k^{-1} - \left( \sum_{i<k} (-1)^i L_i^{-1} \sum_{\mathfrak{a} \text{ monic}} t_{\mathfrak{a}}^{q^k - q^i} \right). \tag{6}$$

From Eq. (6), it is seen that the expansion of $E_{q^k-1}$ as power series in $s(z)$ satisfies that $\bar{\pi}^{1-q^k} E_{q^k-1}(z) = \sum_{n \geqslant 0} a_n s^n$, with $a_n \in K(= \mathbb{F}_q(T))$.

**Proposition 1.** *Let $\sum_{n \geqslant 0} a_n s^n$ be the expansion of $E_{q^k-1}$. Then $a_n \neq 0$ implies that $n \equiv 0,\ q^{k-1},\ q^{k-1} + q^{k-2}, \ldots, q^{k-1} + \cdots + q + 1 \bmod q^k$.*

**Proof.** Let $\mathfrak{a} \in A$ be a monic polynomial. For $i \in \mathbb{N}$, we consider

$$t_{\mathfrak{a}}^{q^i - 1} = \frac{s^{q^{\deg \mathfrak{a} + i - 1} + \cdots + q^{\deg \mathfrak{a}}} f_{\mathfrak{a}}}{f_{\mathfrak{a}}^{q^i}}. \tag{7}$$

It is seen that $f_{\mathfrak{a}}(s) = 1 + b_1 s^{q^{\deg \mathfrak{a} - 1}} + \cdots + b_{\deg \mathfrak{a}} s^{q^{\deg \mathfrak{a} - 1} + \cdots + q + 1}$, where $b_i \in A$. Hence, if we write $s^{q^{\deg \mathfrak{a} + i - 1} + \cdots + q^{\deg \mathfrak{a}}} f_{\mathfrak{a}} = \sum_{n \geqslant 0} c_n s^n$, then $c_n \neq 0$ implies

$$n \equiv 0, q^{i-1},\ q^{i-1} + q^{i-2}, \ldots, q^{i-1} + \cdots + q + 1 \bmod q^i,$$

and $t_{\mathfrak{a}}^{q^i - 1}$ satisfies the same congruence property. Therefore, from the expression for $E_{q^k-1}$ given in Eq. (6), the result is easily derived. □

Congruences for some coefficients of the series $\bar{\pi}^{1-q^k} E_{q^k-1}$ are now proven. Observe that, from the formula for $E_{q^k-1}$ given in Eq. (6), it follows that the coefficients considered in Theorem 2 belong to $A$.

**Theorem 2.** *Let $\bar{\pi}^{1-q^k} E_{q^k-1}(z) = \sum_{n \geqslant 0} a_n s^n$ be the expansion of $E_{q^k-1}$ with respect to $s(z)$. Let $\mathfrak{p} \in A$ be irreducible and monic with $\deg \mathfrak{p} = d$. If $d = 1$, then, for each $m \in \mathbb{N}$, we have that*

$$a_{q^{m+k} + q^{k-1} + \cdots + 1} \equiv a_{q^k + \cdots + q + 1} \bmod \mathfrak{p}.$$

*If $d > 1$, then, for each $m \in \mathbb{N}$, we have that*

$$a_{q^{md+k} + q^{k-1} + \cdots + 1} \equiv a_{q^k + \cdots + q + 1} \bmod \mathfrak{p}^{q^k}.$$

**Proof.** Let $\bar{\pi}^{1-q^k} E_{q^k-1}(z) = \sum_{n \geqslant 0} c_n t^n$ be the expansion of $E_{q^k-1}$ with respect to $t(z)$. For each $m \in \mathbb{N}$, we will prove that, if $\deg \mathfrak{p} = 1$, then

$$c_{(q^k + \cdots + q + 1)(q-1)} \equiv c_{(q^{m+k} + q^{k-1} + \cdots + 1)(q-1)} \bmod \mathfrak{p}, \tag{8}$$

and if $\deg \mathfrak{p} > 1$, then

$$c_{(q^k+\cdots+q+1)(q-1)} \equiv c_{(q^{md+k}+q^{k-1}+\cdots+1)(q-1)} \bmod \mathfrak{p}^{q^k}. \tag{9}$$

The series $E_{q^k-1}$ is an eigenfunction for all the operators $T_{\mathfrak{a}}$ with $\mathfrak{a} \in A$ monic, and the corresponding eigenvalues are $\mathfrak{a}^{q^k-1}$ (cf. Proposition 1.4 of [1, p. 95]). Eq. (4) gives the effect of $T_{\mathfrak{p}^m}$ on $t$-expansions of modular forms; for the series $E_{q^k-1}$ we get:

$$\begin{aligned}\mathfrak{p}^{m(q^k-1)}\left(\sum_{n\geqslant 0} c_n t^n\right) &= \mathfrak{p}^{m(q^k-1)} \sum_{n\geqslant 0} c_n t_{\mathfrak{p}^m}^n + \cdots + \mathfrak{p}^{q^k-1} \sum_{n\geqslant 0} c_n G_{n,\mathfrak{p}^{m-1}}(\mathfrak{p}^{m-1} t_{\mathfrak{p}}) \\ &\quad + \sum_{n\geqslant 0} c_n G_{n,\mathfrak{p}^m}(\mathfrak{p}^m t).\end{aligned} \tag{10}$$

In order to prove the congruences of Eqs. (8) and (9), we determine the $t^{q^{k+1}-1}$-coefficient of the right-hand side in Eq. (10). For $\deg \mathfrak{p} = 1$, this term may only appear in $\mathfrak{p}^{q^k-1} \sum_{n\geqslant 0} c_n G_{n,\mathfrak{p}^{m-1}}(\mathfrak{p}^{m-1} t_{\mathfrak{p}})$ or $\sum_{n\geqslant 0} c_n G_{n,\mathfrak{p}^m}(\mathfrak{p}^m t)$, and for $\deg \mathfrak{p} > 1$, it may only appear in $\sum_{n\geqslant 0} c_n G_{n,\mathfrak{p}^m}(\mathfrak{p}^m t)$; this claim is proven in Lemma 5.

The $t^{q^{k+1}-1}$-coefficient of $\mathfrak{p}^{q^k-1} \sum_{n\geqslant 0} c_n G_{n,\mathfrak{p}^{m-1}}(\mathfrak{p}^{m-1} t_{\mathfrak{p}})$ (for any polynomial $\mathfrak{p}$ with $\deg \mathfrak{p} = 1$) is also studied in Lemma 5; we prove that it belongs to $A$ and it is determined mod $\mathfrak{p}^{m(q^k-1)+1}$. In Lemma 4, we prove that the $t^{q^{k+1}-1}$-coefficient of $\sum_{n\geqslant 0} c_n G_{n,\mathfrak{p}^m}(\mathfrak{p}^m t)$ (for any irreducible polynomial $\mathfrak{p}$) belongs to $A$, and it is determined mod $\mathfrak{p}^{m(q^k-1)+q^k}$. From both lemmas, the congruences of Eqs. (8) and (9) are easily derived. □

The following remark will be used in the proof of Lemmas 4 and 5; it is an immediate consequence of the Lucas formula.

**Remark 3.** Let $p \in \mathbb{N}$ be a prime and $v_p$ the $p$-adic valuation on $\mathbb{Q}$. Let $m, n \in \mathbb{N}$ be such that $n < m$ and $v_p(n) < v_p(m)$; then $\binom{m}{n} \equiv 0 \bmod p$.

**Lemma 4.** *Let $\mathfrak{p} \in A$ be irreducible and monic with $\deg \mathfrak{p} = d$. Let $\gamma$ be the $t^{q^{k+1}-1}$-coefficient of $c_n G_{n,\mathfrak{p}^m}(\mathfrak{p}^m t)$; then $\gamma \in A$. Furthermore, if $n = (q^{md+k} + q^{k-1} + \cdots + 1)(q-1)$, then $\gamma = c_n \mathfrak{p}^{m(q^k-1)}$, and if $n \neq (q^{md+k} + q^{k-1} + \cdots + 1)(q-1)$, then $\gamma \equiv 0 \bmod \mathfrak{p}^{m(q^k-1)+q^k}$.*

**Proof.** We first observe that, from Proposition 1, it follows that $c_n = 0$ for $n \not\equiv 0, q^k - q^{k-1}, q^k - q^{k-2}, \ldots, q^k - 1 \bmod q^k(q-1)$. Now, if $n \equiv 0, q^k - q^{k-1}, q^k - q^{k-2}, \ldots, q^k - q \bmod q^k(q-1)$, then $G_{n,\mathfrak{p}^m}(X)$ is a $q$th power of some polynomial in $K[X]$. In view of property $G_{qn,\mathfrak{p}^m}(X) = (G_{n,\mathfrak{p}^m}(X))^q$ of Goss polynomials, we have to study only $G_{n,\mathfrak{p}^m}(\mathfrak{p}^m t)$ for $n \equiv q^k - 1 \bmod q^k(q-1)$; in this case, $c_n \in A$ (this follows from the formula for $E_{q^k-1}$ given in Eq. (6)).

Let us consider the following explicit formula for $G_{n,\mathfrak{p}^m}$ (cf. [2, Eq. (3.8), p. 676]). Let $\rho_{\mathfrak{p}^m}(X) = \sum_{0\leqslant i\leqslant md} l_i X^{q^i}$, $\alpha_i = l_i/\mathfrak{p}^m$; then

$$G_{r+1,\mathfrak{p}^m}(X) = \sum_{j\leqslant r} \sum_{\underline{i}} \binom{j}{\underline{i}} \alpha^{\underline{i}} X^{j+1}, \tag{11}$$

where $\underline{i} = (i_0, \ldots, i_{md})$ runs over the set of $(md+1)$-tuples satisfying $i_0 + \cdots + i_{md} = j$ and $i_0 + i_1 q + \cdots + i_{md} q^{md} = r$, $\alpha^{\underline{i}} = \alpha_0^{i_0} \cdots \alpha_{md}^{i_{md}}$ and $\binom{j}{\underline{i}} = j!/(i_0! \cdots i_{md}!)$.

Let $\beta$ be the $t^{q^{k+1}-1}$-coefficient of $G_{r+1,\mathfrak{p}^m}(\mathfrak{p}^m t)$. Then

$$\beta = \sum_{\underline{i}} \binom{j}{\underline{i}} \alpha_0^{i_0} \cdots \alpha_{md}^{i_{md}} \mathfrak{p}^{m(q^{k+1}-1)},$$

where $1 + i_0 + \cdots + i_{md} = j + 1 = q^{k+1} - 1$ and $i_0 + i_1 q + \cdots + i_{md} q^{md} = r$. In the sequel, we will assume that $r + 1 \equiv q^k - 1 \bmod q^k(q-1)$, which is the only case that we have to study. From Eq. (1), it follows that $\alpha_0 = 1$, $\alpha_{md} = 1/\mathfrak{p}^m$, and $\mathfrak{p}^{m-1}\alpha_i \in A$, for $i = 1, \ldots, md-1$. Thus, if $\underline{i} = (i_0, \ldots, i_{md})$ satisfies $(m-1)(i_1 + \cdots + i_{md-1}) + m i_{md} \leqslant m q^k (q-1) - q^k$, then $\alpha_0^{i_0} \cdots \alpha_{md}^{i_{md}} \mathfrak{p}^{m(q^{k+1}-1)} \in A$ and

$$\alpha_0^{i_0} \cdots \alpha_{md}^{i_{md}} \mathfrak{p}^{m(q^{k+1}-1)} \equiv 0 \bmod \mathfrak{p}^{m(q^k-1)+q^k}.$$

Assume now that $\underline{i} = (i_0, \ldots, i_{md})$ satisfies

$$(m-1)(i_1 + \cdots + i_{md-1}) + m i_{md} > m q^k (q-1) - q^k. \tag{12}$$

It follows that $i_1 + \cdots + i_{md} > q^k(q-2)$ and so $i_0 \leqslant 2q^k - 3$. We now divide $1 + i_0 + i_1 q + \cdots + i_{md} q^{md}$ by $q^k(q-1)$ considering $q$ as an indeterminate. The remainder of this division is

$$\begin{aligned}(i_{md} + \cdots + i_k) q^k + i_{k-1} q^{k-1} + \cdots + i_1 q + i_0 + 1 \\ = (q^{k+1} - 2 - (i_0 + \cdots + i_{k-1})) q^k + \cdots + i_1 q + i_0 + 1.\end{aligned}$$

Since $r + 1 \equiv q^k - 1 \bmod q^k(q-1)$, we get the congruence

$$i_{k-1}(q^k - q^{k-1}) + \cdots + i_1(q^k - q) + (i_0 + 2)(q^k - 1) \equiv 0 \bmod q^k(q-1).$$

From this congruence, the following sequence of congruences is easily derived:

$$\begin{aligned} & i_0 + 2 \equiv 0 \bmod q, \\ & \qquad q i_1 + (i_0 + 2) \equiv 0 \bmod q^2, \\ & \qquad \vdots \\ & \qquad q^{k-1} i_{k-1} + \cdots + q i_1 + (i_0 + 2) \equiv 0 \bmod q^k. \end{aligned} \tag{13}$$

Assume that $\binom{j}{\underline{i}} \neq 0$ as an element in $\mathbb{F}_q$. Then, since $v_p(j - i_0) = v_p(i_0 + 2)$ (recall that $j = q^{k+1} - 2$), applying the claim of Remark 3 and the fact that $v_p(\varepsilon!) \geqslant v_p((\varepsilon - \delta)!) + v_p(\delta!)$ for any $\varepsilon, \delta \in \mathbb{N}$, with $\delta < \varepsilon$, we conclude that

$$v_p(i_1) \geqslant v_p(i_0 + 2), \ldots, v_p(i_{k-1}) \geqslant v_p(i_0 + 2).$$

Thus, $v_p(i_1) \geqslant v_p(i_0 + 2) \geqslant v_p(q)$; but now, the second congruence of Eq. (13) implies that $v_p(i_0 + 2) \geqslant v_p(q^2)$, and so $v_p(i_1) \geqslant v_p(q^2), \ldots, v_p(i_{k-1}) \geqslant v_p(q^2)$. Using the rest of the congruences of Eq. (13), we can repeat this argument recursively and we conclude that $v_p(i_0 + 2) \geqslant v_p(q^k)$. Since $i_0 \leqslant 2q^k - 3$, one gets that $i_0 = q^k - 2$; hence, by Eq. (12), $i_{md} > q^k(q - 2)$. Now, applying Remark 3 again and the fact that $v_p(\varepsilon!) \geqslant v_p((\varepsilon - \delta)!) + v_p(\delta!)$, it holds that $i_{md} = q^k(q - 1)$.

In summary, we have that if $(i_0, \ldots, i_{md})$ satisfies the condition of Eq. (12), then

$$\binom{j}{\underline{i}} \alpha_0^{i_0} \cdots \alpha_{md}^{i_{md}} \mathfrak{p}^{m(q^{k+1}-1)} = \begin{cases} \mathfrak{p}^{m(q^k-1)} & \text{if } i_0 = q^k - 2 \text{ and } i_{md} = q^{k+1} - q^k, \\ 0 & \text{if } i_0 \neq q^k - 2 \text{ or } i_{md} \neq q^{k+1} - q^k. \end{cases}$$

This finishes the proof of the lemma. □

**Lemma 5.** *Let $\mathfrak{p} \in A$ be an irreducible polynomial with $\deg \mathfrak{p} = d$, and let $m, a \in \mathbb{N}$. Let $\gamma$ be the $t^{q^{k+1}-1}$-coefficient of $\mathfrak{p}^{a(q^k-1)} c_n G_{n,\mathfrak{p}^{m-a}}(\mathfrak{p}^{m-a} t_{\mathfrak{p}^a})$ ($c_n$ as in the proof of Theorem 2). If $ad > 1$, then $\gamma = 0$. If $d = 1$ and $a = 1$, then $\gamma \in A$ and $\gamma \equiv 0 \bmod \mathfrak{p}^{m(q^k-1)+1}$.*

**Proof.** As in the proof of Lemma 4, we only have to study the expressions $G_{n,\mathfrak{p}^{m-a}}(\mathfrak{p}^{m-a} t_{\mathfrak{p}^a})$ for $n \equiv q^k - 1 \bmod q^k(q - 1)$.

Let $t_{\mathfrak{p}^a} = t^{q^{ad}} / f_{\mathfrak{p}^a}(t)$. The term $t^{q^{k+1}-1}$ may occur in $t_{\mathfrak{p}^a}^i$ only if $i \leqslant q^{k-ad+1} - 1$. Let $\beta$ be the $X^i$-coefficient of the polynomial $G_{n,\mathfrak{p}^{m-a}}(X)$, $i \leqslant q^{k-ad+1} - 1$, and let $\rho_{\mathfrak{p}^{m-a}}(X) = \sum_{0 \leqslant r \leqslant (m-a)d} l_r X^{q^r}$, $\alpha_r = l_r / \mathfrak{p}^{m-a}$. Using the explicit formula for $G_{n,\mathfrak{p}^{m-a}}(X)$ (see Eq. (11)), we find that

$$\beta = \sum_{\underline{i}} \binom{j}{\underline{i}} \alpha_0^{i_0} \cdots \alpha_{(m-a)d}^{i_{(m-a)d}},$$

where $1+i_0+\cdots+i_{(m-a)d}=j+1=i\leqslant q^{k-ad+1}-1$ and $i_0+i_1q+\cdots+i_{(m-a)d}q^{(m-a)d}=n-1$. Assume that $\binom{j}{i}\neq 0$ as an element in $\mathbb{F}_q$; as in the proof of Lemma 4, the congruences of Eq. (13) imply that $i_0+2\equiv 0 \bmod q^k$, so $i_0\geqslant q^k-2$. Hence, since $i_0+\cdots+i_{(m-a)d}\leqslant q^{k-ad+1}-2$, if $ad>1$, then $\binom{j}{i}=0$ as an element in $\mathbb{F}_q$, and therefore $\beta=0$. This proves the first claim of the lemma.

Assume now that $a=1$ and $d=1$. By the previous argument, either $\binom{j}{i}=0$ or $i_0=i-1=q^k-2$. In this last case, we have that $n=q^k-1$ and $\beta=1$. Now, since $t_{\mathfrak{p}}=t^q/(1+\mathfrak{p}t^{q-1})$, we have that

$$(\mathfrak{p}^{m-1}t_{\mathfrak{p}})^{q^k-1}=\mathfrak{p}^{(m-1)(q^k-1)}(t^{q^{k+1}-q}+\mathfrak{p}t^{q^{k+1}-1}+\cdots).$$

Hence, the $t^{q^{k+1}-1}$-coefficient of expression $\mathfrak{p}^{(q^k-1)}c_{q^k-1}G_{q^k-1,\mathfrak{p}^{m-1}}(\mathfrak{p}^{m-1}t_{\mathfrak{p}})$ is $c_{q^k-1}\mathfrak{p}^{m(q^k-1)+1}$. Finally, $c_{q^k-1}\in A$ (this follows from the formula for $E_{q^k-1}$ given in Eq. (6)). □

**Remark 6.** Following [2], we define the form $g_k=(-1)^{k+1}\tilde{\pi}^{1-q^k}L_kE_{q^k-1}$. It follows that the expansion of $g_k$ with respect to $s$ satisfies that $g_k=1+b_1s+\cdots$, and the coefficients of this expansion belong to $A$. The form $g_k$ satisfies the congruences of Theorem 2; the question is whether it also satisfies "strong" congruences like the discriminant function (cf. [5, Theorem 1, p. 1056]); the answer is no. For example, if we take $k=1$, the form $g_1=g$ should satisfy the following: for $\deg\mathfrak{p}=1$ and each $m\in\mathbb{N}$,

$$b_{mq^2+1}\equiv b_{mq+1} \bmod \mathfrak{p},$$

and for $\deg\mathfrak{p}=d>1$ and each $m\in\mathbb{N}$,

$$b_{mq^{d+1}+1}\equiv b_{mq+1} \bmod \mathfrak{p}^q.$$

However, $g$ does not satisfy these congruences in general: for example, the second congruence is not satisfied for $q=3$, $m=4$ and any irreducible polynomial $\mathfrak{p}$ with $\deg\mathfrak{p}=2$.

As a corollary of Theorem 2, we determine, up to a factor of degree $q^k-q$, the difference $a_{q^{d+k}+q^{k-1}+\cdots+1}-a_{q^k+\cdots+q+1}$.

**Corollary 7.** *Let $d\in\mathbb{N}$. We have that*

$$a_{q^{d+k}+q^{k-1}+\cdots+1}=a_{q^k+\cdots+q+1}-\frac{[d]^{q^k}P_d(T)}{[1]^{q^k-1}},$$

*with $P_d$ monic and $\deg P_d=q^k-q$. For $q=2$, $a_{q^k+\cdots+q+1}=1$, and for $q>2$, $a_{q^k+\cdots+q+1}=0$.*

**Proof.** Let $\mathfrak{p}$ be irreducible and monic. Let $d\in\mathbb{N}$; by Theorem 2, if $\deg\mathfrak{p}=1$, then $a_{q^{d+k}+q^{k-1}+\cdots+1}\equiv a_{q^k+\cdots+q+1} \bmod \mathfrak{p}$; if $\deg\mathfrak{p}>1$ and $\deg\mathfrak{p}|d$, then $a_{q^{d+k}+q^{k-1}+\cdots+1}\equiv a_{q^k+\cdots+q+1} \bmod \mathfrak{p}^{q^k}$. Thus, since $[d]=\prod_{\substack{\mathfrak{p}\text{ monic,prime}\\ \deg\mathfrak{p}|d}}\mathfrak{p}$, we have that

$$a_{q^{d+k}+q^{k-1}+\cdots+1}\equiv a_{q^k+\cdots+q+1} \bmod \frac{[d]^{q^k}}{[1]^{q^k-1}}.$$

We now determine the coefficient $a_{q^k+\cdots+q+1}$ by using the formula for $E_{q^k-1}$ given in Eq. (6). An easy analysis of that formula allows us to conclude that $a_{q^k+\cdots+q+1}$ equals the $s^{q^k+\cdots+q+1}$-coefficient of $-\sum_{\substack{\mathfrak{a}\text{ monic}\\ \deg\mathfrak{a}=1}} t_{\mathfrak{a}}^{q^k-1}$. By Corollary 3.11 of [2, p. 677], we get that

$$-\sum_{\substack{\mathfrak{a}\text{ monic}\\ \deg\mathfrak{a}=1}} t_{\mathfrak{a}}^{q^k-1}=-\sum_{0\leqslant i<k}\frac{s^{q^{k+1}-q^{i+1}+\frac{q^k-1}{q-1}}}{(1-s^{q-1}+[1]s^q)^{q^k-q^i}}. \tag{14}$$

If $q=2$ and $i=k-1$, then $q^{k+1}-q^{i+1}+\frac{q^k-1}{q-1}=q^k+\cdots+q+1$, so $a_{q^k+\cdots+q+1}=1$; if $q>2$, then $q^{k+1}-q^{i+1}+\frac{q^k-1}{q-1}>q^k+\cdots+q+1$, so $a_{q^k+\cdots+q+1}=0$.

Let us now prove that the degree of $a_{q^{d+k}+q^{k-1}+\cdots+1}$ is $q^{d+k}-q^{k+1}+q^k$ and its leading coefficient is $-1$. The polynomial $a_{q^{d+k}+q^{k-1}+\cdots+1}$ is the $s^{q^{d+k}+q^{k-1}+\cdots+1}$-coefficient of $-\sum_{\mathfrak{a}\text{ monic}} t_{\mathfrak{a}}^{q^k-1}$. Let

$$C_r=-\sum_{\substack{\mathfrak{a}\text{ monic}\\ \deg\mathfrak{a}=r}} t_{\mathfrak{a}}^{q^k-1}=-s^{q^{k+r-1}+\cdots+q^r}\sum_{\substack{\mathfrak{a}\text{ monic}\\ \deg\mathfrak{a}=r}} 1/f_{\mathfrak{a}}^{q^k-1}.$$

The $f_{\mathfrak{a}}=1+b_1s+\cdots$, considered as power series in $s$, satisfy $\deg b_j\leqslant j$, and so the sum $\sum_{\mathfrak{a}\text{ monic}} 1/f_{\mathfrak{a}}^{q^k-1}$ also satisfies this condition. Hence, if we denote by $\gamma_d$ the $T^{q^{d+k}-q^{k+1}+q^k}$-coefficient of $a_{q^{d+k}+q^{k-1}+\cdots+1}$, the terms $C_r$ for $r>1$ do not contribute to $\gamma_d$. Thus, in order to determine $\gamma_d$, we only have to study $C_1$ (an expression of it is given in Eq. (14)); in this case, the only term that contributes to $\gamma_d$ is $-\frac{s^{q^{k+1}-q^k+\frac{q^k-1}{q-1}}}{(1-s^{q-1}+[1]s^q)^{q^k-q^{k-1}}}$. Hence, if

$$(1-s^{q-1}+[1]s^q)^{q^{k-1}-q^k}=\sum_{n\geqslant 0}\delta_n s^n, \tag{15}$$

$-\gamma_d$ is the $T^{q^{d+k}-q^{k+1}+q^k}$-coefficient of $\delta_{q^{d+k}-q^{k+1}+q^k}$. Now, since the degree of the $s^{q-1}$-coefficient of $1-s^{q-1}+[1]s^q$ is less than $q-1$, in order to calculate $\gamma_d$, we can omit

the summand $-s^{q-1}$ in the left-hand side of Eq. (15). Thus, if

$$(1+[1]s^q)^{q^{k-1}-q^k} = (1+[1]^{q^{k-1}}s^{q^k})(1-[1]^{q^k}s^{q^{k+1}}+[1]^{2q^k}s^{2q^{k+1}}-\ldots) = \sum_{n\geqslant 0}\varepsilon_n s^n, \tag{16}$$

then $-\gamma_d$ is the $T^{q^{d+k}-q^{k+1}+q^k}$-coefficient of $\varepsilon_{q^{d+k}-q^{k+1}+q^k}$. From Eq. (16), we easily deduce that this last coefficient is equal to 1, and so $\gamma_d=-1$. □

**Remark 8.** Corollary 7 does not give much information on the polynomial $P_d(T)$. In principle, it may depend on $d$; nevertheless, we have computed in some cases the expansion of $E_{q^k-1}$ up to certain bounds, and in all the examples the polynomial $P_d(T)$ equals $[k]/[1]$.

## References

[1] E.U. Gekeler, Drinfeld Modular Curves, in: Lecture Notes in Mathematics, Vol. 1231, Springer, Berlin, 1986.
[2] E.U. Gekeler, On the coefficients of Drinfeld modular forms, Invent. Math. 93 (1988) 667–700.
[3] E.U. Gekeler, Growth order and congruences of coefficients of the Drinfeld discriminant function, J. Number Theory 77 (1999) 314–325.
[4] D. Goss, Modular forms for $\mathbb{F}_r[T]$, J. Reine Angew. Math. 317 (1980) 16–39.
[5] B. López, A congruence for the coefficients of the Drinfeld discriminant function, C. R. Acad. Sci. Paris 330 (2000) 1053–1058.