C. R. Acad. Sci. Paris, t. 330, Série I, p. 1053–1058, 2000
Théorie des nombres/*Number Theory*

A congruence for the coefficients of the Drinfeld discriminant function

Bartolomé LÓPEZ

Departamento de Matemáticas, Universidad de Cádiz, 11510 Puerto Real, Cádiz, Spain

(Reçu le 13 février 2000, accepté après révision le 25 avril 2000)

Abstract. We prove a congruence for some coefficients of the expansion of the Drinfeld discriminant function and from it we determine the coefficients with subscript q^d+1. © 2000 Académie des sciences/Éditions scientifiques et médicales Elsevier SAS

Une congruence pour les coefficients de la fonction discriminant de Drinfeld

Résumé. *Nous démontrons une congruence pour certains coefficients du développement de la fonction discriminant de Drinfeld. En se fondant sur cette congruence nous déterminons les coefficients d'indice* q^d+1. © 2000 Académie des sciences/Éditions scientifiques et médicales Elsevier SAS

Version française abrégée

Soient $A=\mathbb{F}_q[T]$ l'anneau des polynômes à coefficients dans $\mathbb{F}_q$, $K=\mathbb{F}_q(T)$, $K_\infty=\mathbb{F}_q((1/T))$ et soit C le complété de la clôture algébrique de K_∞.

Soit $C\{\tau\}$ l'anneau non commutatif des polynômes à coefficients dans C, où τ est la substitution de Frobenius. Un *module de Drinfeld* de rang r sur C est un homomorphisme de $\mathbb{F}_q$-algèbres, $\phi : A\to C\{\tau\}$ qui applique T sur $\phi_T=T\tau^0+\sum_{i=1}^r c_i\tau^i$, où $c_i\in C$ et $c_r\neq 0$.

Un A-réseau dans C de rang r est un A-module $\Lambda\subset C$ discret, de type fini et tel que $\dim_K K\Lambda=r$. Au moyen de la fonction exponentielle

$$e_\Lambda(z)=z\prod_{\lambda\in\Lambda-\{0\}}\left(1-\frac{z}{\lambda}\right),$$

on établit une bijection entre les réseaux de rang r dans C et les modules de Drinfeld de rang r sur C.

Dans le cas du rang 1, on a le module de *Carlitz* ρ qui applique T sur $\rho_T=T\tau^0+\tau$. Soit $L=\overline{\pi}A$ le réseau correspondant ($\overline{\pi}$ est déterminé à une unité de A près). Soit e_L la fonction exponentielle associée

---

Note présentée par Jean-Pierre SERRE.

S0764-4442(00)00500-0/FLA

à L ; on considère les fonctions

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

La fonction $s(z)$ correspond à la fonction classique $e^{2\pi i z}$.

Les réseaux de rang 2 dans C sont de la forme $u(zA + A)$, où $u \in C^*$, $z \in \Omega = C - K_\infty$. Ainsi, un module de Drinfeld de rang 2 est isomorphe à un module de la forme $\phi_T = T\tau^0 + g(z)\tau + \Delta(z)\tau^2$, où $z \in \Omega$. Les fonctions $g(z)$ et $\Delta(z)$ sont des *formes modulaires* pour le groupe $\Gamma(1) := \mathrm{GL}(2, A)$, de poids $q - 1$ et $q^2 - 1$, respectivement.

Énonçons le résultat principal. Rappelons que la fonction discriminant $\Delta(z)$ a un développement de la forme :

$$\overline{\pi}^{1-q^2} \Delta(z) = \sum_{n \geqslant 0} a_n s^n,$$

où $a_n \in A$ et $\deg a_{n+1} \leqslant n$. Les coefficients a_n sont tels que $a_n \neq 0 \Rightarrow n \equiv 0, 1 \bmod q$.

THÉOREME 1. – *Soient $\mathfrak{p} = (p) \subset A$ un idéal premier, p unitaire et $\deg p = d$. Alors, pour chaque $k \in \mathbb{N}$, on a*

$$a_{kq^{d+1}+1} \equiv a_{kq+1} \bmod \left(p^q\right).$$

La congruence du théorème 1 et la condition $\deg a_{n+1} \leqslant n$ déterminent les coefficients d'indice $q^d + 1$:

COROLLAIRE 2. – *On a*

$$a_{q^{d+1}+1} = a_{q+1} + [d]^q.$$

Pour $q = 2$, $a_{q+1} = 1 + [1]$ et pour $q > 2$, $a_{q+1} = -[1]$ (cf. *corollaire* 10.3 *de* [1], *p.* 691).

La preuve du théorème 1 utilise l'action des *opérateurs de Hecke* $T_\mathfrak{p}$ ($\mathfrak{p} = (p)$ est un idéal premier dans A, p unitaire) sur le développement par rapport à t de la fonction discriminant.

Soit $\overline{\pi}^{1-q^2} \Delta(z) = \sum_{n \geqslant 0} c_n t^n$. Alors, la congruence du théoreme 1 se traduit par

$$c_{(mq+1)(q-1)} \equiv c_{(mq^{d+1}+1)(q-1)} \bmod \left(p^q\right). \tag{1}$$

La fonction $\Delta(z)$ est une fonction propre pour les $T_\mathfrak{p}$ et les valeurs propres correspondantes sont p^{q-1} (*cf.* corollaire 7.5 de [1], p. 685). On a l'équation :

$$p^{q-1}\left(\sum_{n \geqslant 0} c_n t^n\right) = p^{q^2-1} \sum_{n \geqslant 0} c_n t_p^n + \sum_{n \geqslant 0} c_n G_{n,\mathfrak{p}}(pt), \tag{2}$$

où $t_p(z) = t(pz)$ et $G_{n,\mathfrak{p}}$ est le $n^{\text{ème}}$ *polynôme de Goss* par rapport à $\ker \rho_p$ (*cf.* [1], paragraphe 3). Une analyse élémentaire de l'équation (2) réduit la preuve de la congruence de l'équation (1) à celle du lemme suivant.

LEMME 3. – *Soient $\mathfrak{p} = (p)$ un idéal premier, p unitaire et $\deg p = d$. Soit γ le coefficient de $G_{n,\mathfrak{p}}(pt)$ correspondant à $t^{(mq+1)(q-1)}$, où $n = q - 1 \bmod q(q-1)$. Si $n = (mq^{d+1} + 1)(q-1)$, alors $\gamma = p^{q-1}$. Si $n \neq (mq^{d+1} + 1)(q-1)$, alors $\gamma \equiv 0 \bmod (p^{2q-1})$.*

La preuve du lemme 3 utilise une formule explicite pour les polynômes de Goss $G_{n,\mathfrak{p}}$ (*cf.* [1], paragraphe 3).

1. Preliminaries and main result

We introduce several definitions and results on Drinfeld modules. Details of all these facts can be found in [1].

Let $A=\mathbb{F}_q[T]$ be the ring of polynomials over the finite field $\mathbb{F}_q$ in an indeterminate T. Let $K=\mathbb{F}_q(T)$. We consider the field $K_\infty=\mathbb{F}_q((1/T))$, its algebraic closure $\overline{K}_\infty$ and the completion C of $\overline{K}_\infty$.

Let $C\{\tau\}$ be the ring of non-commutative polynomials over C, where τ is the Frobenius endomorphism. We can identify $C\{\tau\}$ with the ring of q-additive polynomials $\sum_{i=0}^{\ell} c_i X^{q^i}$ where the product is given by substitution.

A *Drinfeld module* of rank r over C is a ring $\mathbb{F}_q$-homomorphism $\phi : A \to C\{\tau\}$ given by $\phi_T = T\tau^0+\sum_{i=1}^{r} c_i\tau^i$, where $c_i\in C$ and $c_r\neq 0$.

An A-*lattice* in C of rank r is a discrete, finitely generated A-module $\Lambda\subset C$ such that $\dim_K K\Lambda=r$. Through the exponential function

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

we can establish a bijection between lattices of rank r in C and Drinfeld modules of rank r over C.

Let us first consider the rank one case. The *Carlitz* module is given by

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

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

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

The expansion of the discriminant function will be given with respect to these functions (as parameters).

For a given $a\in A$, we consider $\rho_a=\sum_{0\leqslant i\leqslant \deg a}\ell_i X^{q^i}$. The leading coefficient of ρ_a is the leading coefficient of a and the other coefficients satisfy:

$$\ell_0=a, \quad \ell_i=\frac{\ell_{i-1}^q-\ell_{i-1}}{[i]}, \tag{1}$$

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

Any Drinfeld module of rank two over C is isomorphic to one given by:

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

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

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

for every $\left(\begin{smallmatrix} a & b\\ c & d\end{smallmatrix}\right)\in\Gamma(1)$. The C-vector space of modular forms of weight k is denoted by M_k.

Let $\mathfrak{p} = (p)$ be a prime ideal in A with p monic and $\deg p = d$. *Hecke operators* $T_{\mathfrak{p}}$ act on the spaces M_k. The effect of $T_{\mathfrak{p}}$ on t-expansions is the following: if $h = \sum_{n\geqslant 0} c_n t^n \in M_k$, then

$$T_{\mathfrak{p}}\left(\sum_{n\geqslant 0} c_n t^n\right) = p^k \sum_{n\geqslant 0} c_n t_p^n + \sum_{n\geqslant 0} c_n G_{n,\mathfrak{p}}(pt), \tag{2}$$

where $t_p(z) = t(pz) = t^{q^d}/f_p(t)$, $f_a(X) = \rho_a(X^{-1})X^{q^{\deg a}}$, and $G_{n,\mathfrak{p}}$ is the n-th *Goss polynomial* with respect to $\ker \rho_p$. Goss polynomials are obtained by means of the following recursion formula (*cf.* [2], p. 323) : let $\rho_p(X) = \ell_0 X + \ell_1 X^q + \cdots + \ell_d X^{q^d}$ and $\alpha_i = \ell_i/p$; then,

$$G_{1,\mathfrak{p}}(X) = X, \quad G_{n,\mathfrak{p}}(X) = X(G_{n-1,\mathfrak{p}} + \alpha_1 G_{n-q,\mathfrak{p}} + \alpha_2 G_{n-q^2,\mathfrak{p}} + \cdots). \tag{3}$$

There exists also an explicit formula for the $G_{n,\mathfrak{p}}$ that we will introduce in Section 2. It is derived from the previous formula.

We now present the result on the coefficients of the discriminant function. We recall that Δ has an expansion of the form

$$\overline{\pi}^{1-q^2}\Delta(z) = \sum_{n\geqslant 0} a_n s^n,$$

where $a_n \in A$, and $\deg a_{n+1} \leqslant n$. The coefficients a_n satisfy also that $a_n \neq 0 \Rightarrow n \equiv 0,\ 1 \bmod q$.

THEOREM 1. – *Let $\mathfrak{p} = (p) \subset A$ be a prime ideal, p monic and $\deg p = d$. Then, for each $k \in \mathbb{N}$, we have*

$$a_{kq^{d+1}+1} \equiv a_{kq+1} \bmod \left(p^q\right).$$

The proof of this congruence is given in Section 2 and it is based on the action of Hecke operators on the expansion of the discriminant function. The basic argument was already used by E.-U. Gekeler (*cf.* [2]) to prove a similar congruence for a modular form $h(z)$ whose t-expansion is

$$h(z) = -t \prod_{a \text{ monic}} f_a(t)^{q^2-1}.$$

The next corollary was stated in [2] (and in [4]) as an empirical rule arising from some computations of the expansion of the discriminant.

COROLLARY 2. – *We have*

$$a_{q^{d+1}+1} = a_{q+1} + [d]^q.$$

For $q = 2$, $a_{q+1} = 1 + [1]$ *and for* $q > 2$, $a_{q+1} = -[1]$ (cf., *Corollary* 10.3, *of* [1], *p.* 691).

Proof. – Let (p) be a prime ideal with $\deg p = d$. By Theorem 1, we have that $a_{kq^{d+1}+1} \equiv a_{kq+1} \bmod (p^q)$. Now, if $d' \mid d$ and (p') is a prime ideal with $\deg p' = d'$, then also $a_{kq^{d+1}+1} \equiv a_{kq+1} \bmod \left((p')^q\right)$. Thus, since $[d] = \prod_{\substack{p \text{ monic, prime} \\ \deg p \mid d}} p$,

$$a_{kq^{d+1}+1} \equiv a_{kq+1} \bmod [d]^q.$$

Hence, $a_{q^{d+1}+1} - a_{q+1} = \zeta[d]^q$ for some $\zeta \in \mathbb{F}_q$. Now, the $T^{q^{d+1}}$-coefficient of $a_{q^{d+1}+1}$ is 1 (*cf.* Theorem 2.1 of [2], p. 317; note that the a_n are defined there in a different way). This implies that $\zeta = 1$. □

2. Proof of Theorem 1

Let us consider the expansion of Δ with respect to $t(z)$, $\overline{\pi}^{1-q^2}\Delta(z) = \sum_{n\geqslant 0} c_n t^n$. Then, $a_n = c_{n(q-1)}$; for each $m \in \mathbb{N}$, we will prove the congruence

$$c_{(mq+1)(q-1)} \equiv c_{(mq^{d+1}+1)(q-1)} \bmod \left(p^q\right), \tag{4}$$

from which Theorem 1 follows.

The function $\Delta(z)$ is an eigenform for the $T_{\mathfrak{p}}$ and the corresponding eigenvalues are p^{q-1} (*cf.* Corollary 7.5 of [1], p. 685); by equation (2),

$$p^{q-1}\left(\sum_{n\geqslant 0} c_n t^n\right) = p^{q^2-1}\sum_{n\geqslant 0} c_n t_p^n + \sum_{n\geqslant 0} c_n G_{n,\mathfrak{p}}(pt). \tag{5}$$

Now, in order to prove the congruence of equation (4) we look at the $t^{(mq+1)(q-1)}$-coefficient of the right-hand side in equation (5). Let us first consider the sum $\sum_{n\geqslant 0} c_n G_{n,\mathfrak{p}}(pt)$. We observe that the terms $c_n G_{n,\mathfrak{p}}(pt)$ are zero for $n \not\equiv 0,\, q-1 \bmod q(q-1)$. On the other hand, if $n \equiv 0 \bmod q(q-1)$, then $n \equiv 0 \bmod q$; this implies that $G_{n,\mathfrak{p}}(X)$ is a q-th power of some polynomial (*cf.* Proposition 3.4 of [1], p. 675), and so, the $t^{(mq+1)(q-1)}$-coefficient of $G_{n,\mathfrak{p}}(pt)$ is zero. Thus, we have to study only the terms $c_n G_{n,\mathfrak{p}}(pt)$ with subscript $n \equiv q-1 \bmod q(q-1)$.

LEMMA 3. – *Let* $\mathfrak{p} = (p)$ *be a prime ideal,* p *monic and* $\deg p = d$. *Let* γ *be the* $t^{(mq+1)(q-1)}$-*coefficient of* $G_{n,\mathfrak{p}}(pt)$, *where* $n \equiv q-1 \bmod q(q-1)$. *If* $n = (mq^{d+1}+1)(q-1)$, *then* $\gamma = p^{q-1}$. *If* $n \neq (mq^{d+1}+1)(q-1)$, *then* $\gamma \equiv 0 \bmod (p^{2q-1})$.

Proof. – The following explicit formula for the $G_{n,\mathfrak{p}}$ follows from the formula of equation (3) (*cf.* [1], Section 3). Let $\rho_p(X) = \sum_{0\leqslant i\leqslant d} \ell_i X^{q^i}$ and $\alpha_i = \ell_i/p$; then,

$$G_{k+1,\mathfrak{p}}(X) = \sum_{j\leqslant k}\sum_{\underline{i}} \binom{j}{\underline{i}} \alpha^{\underline{i}} X^{j+1}, \tag{6}$$

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

By equation (6), the $t^{(mq+1)(q-1)}$-coefficient γ of $G_{k+1,\mathfrak{p}}(pt)$ is

$$\gamma = \sum_{\underline{i}} \binom{j}{\underline{i}} \alpha_0^{i_0}\cdots\alpha_d^{i_d}\, p^{(mq+1)(q-1)},$$

where $i_0+\cdots+i_d+1 = j+1 = (mq+1)(q-1)$ and $i_0+i_1q+\cdots+i_dq^d = k$. In what follows, we assume that $k+1 \equiv q-1 \bmod q(q-1)$. The α_i satisfy $\alpha_0 = 1$, $\alpha_d = 1/p$ and $\alpha_1,\ldots,\alpha_{d-1} \in A$; this follows from the recursion of equation (1). Therefore, if $\underline{i} = (i_0,\ldots,i_d)$ is such that $i_d \leqslant (mq+1)(q-1)-(2q-1)$, then

$$\alpha_0^{i_0}\cdots\alpha_d^{i_d}\, p^{(mq+1)(q-1)} \equiv 0 \bmod (p^{2q-1}). \tag{7}$$

Let us assume that $\underline{i} = (i_0,\ldots,i_d)$ satisfies $i_d > (mq+1)(q-1)-(2q-1)$. Then, $i_0+i_1+\cdots+i_{d-1} \leqslant 2q-3$; this condition and the congruence $k+1 \equiv q-1 \bmod q(q-1)$ determine the index i_0, as follows. We divide $1+i_0+i_1q+\cdots+i_dq^d$ by $q(q-1)$ considering q as an indeterminate. The remainder of this division is $(i_1+i_2+\cdots+i_d)q + i_0 + 1 = ((mq+1)(q-1)-(i_0+1))q + i_0 + 1$. Hence,

$k+1 \equiv -(i_0+1)(q-1) \bmod q(q-1)$. Since $k+1 \equiv q-1 \bmod q(q-1)$ and $i_0 \leqslant 2q-3$, we conclude that $i_0 = q-2$, and so, $i_1 + i_2 + \cdots + i_{d-1} \leqslant q-1$. We now determine the numbers $\binom{j}{\underline{i}}$ in this case. Let $i_d = (mq+1)(q-1) - (2q-1) + r$, $1 \leqslant r \leqslant q$. Then,

$$\begin{aligned}\binom{j}{\underline{i}} &= \frac{j!}{i_0! \cdots i_d!} = \frac{((mq+1)(q-1)-1)!}{(q-2)!\, i_1! \cdots i_d!} \\ &= \frac{((mq+1)(q-1)-1) \cdots ((mq+1)(q-1)-(q-2))}{(q-2)!} \\ &\quad \times \frac{(mq(q-1)) \cdots (mq(q-1)+r+1-q)}{i_1! \cdots i_{d-1}!}.\end{aligned}$$

The first factor of this last product (considered as an element in $\mathbb{F}_q$) is 1: for each s with $1 \leqslant s \leqslant q-2$, we have

$$\frac{mq(q-1)+s}{s} = 1,$$

as an element in $\mathbb{F}_q$. The second factor is zero (for $r < q$); this can be derived from the fact that

$$\frac{(mq(q-1)) \cdots (mq(q-1)+r+1-q)}{(q-r)!} = 0,$$

as an element in $\mathbb{F}_q$, and $\frac{(q-r)!}{i_1! \cdots i_{d-1}!} \in \mathbb{N}$ (since $i_1 + \cdots + i_{d-1} = q-r$). In summary, we have that if $(i_0, \ldots, i_d)$ satisfies $i_d > (mq+1)(q-1) - (2q-1)$, then $i_0 = q-2$ and

$$\binom{j}{\underline{i}} \alpha_0^{i_0} \cdots \alpha_d^{i_d} p^{(mq+1)(q-1)} = \begin{cases} p^{q-1} & \text{if } i_d = mq(q-1), \\ 0 & \text{if } i_d < mq(q-1). \end{cases} \tag{8}$$

In this equation, we use that $i_d = mq(q-1) \Rightarrow i_1 = \cdots = i_{d-1} = 0$. In this case, $k+1 = 1 + i_0 + i_d q^d = (1+mq^{d+1})(q-1)$.

Now, taking together equation (7), for $i_d \leqslant (mq+1)(q-1) - (2q-1)$, and equation (8), for $i_d > (mq+1)(q-1) - (2q-1)$, we get the result. $\square$

Finally, we observe that the first summand of the right-hand side of equation (5) is congruent to zero $\bmod\ (p^{2q-1})$. This remark and Lemma 3 prove the congruence of equation (4).

Acknowledgements. This work was done when I was visiting the Universität des Saarlandes with a postdoctoral grant of the M.E.C. (Spain); so I thank this institution for this finantial support. I thank also DGICYT (project PB97-0284-C02-C01) for financial support.

References

[1] Gekeler E.-U., On the coefficients of Drinfeld modular forms, Invent. Math. 93 (1988) 667–700.
[2] Gekeler E.-U., Growth order and congruences of coefficients of the Drinfeld discriminant function, J. Number Theory 77 (1999) 314–325.
[3] Goss D., Modular forms for $\mathbb{F}_r[T]$, J. Reine Angew. Math. 317 (1980) 16–39.
[4] Trautwein M., Berechnung einiger arithmetischer Funktionen im Zusammenhang mit Drinfeldschen Modulformen, Diplomarbeit, Universität des Saarlandes, 1998.