Bull. Austral. Math. Soc. 11G09, 11G15, 11R58
Vol. 52 (1995) [85–90]

RANK ONE DRINFELD MODULES ON HYPERELLIPTIC CURVES

Sunghan Bae and Pyung-Lyun Kang

We extend the recent work of Dummit and Hayes on rank one Drinfeld modules on elliptic curves and hyperelliptic curves in the case that the infinite place is ramified to the case that the infinite place is inert.

0. Introduction

Recently Dummit and Hayes [2] proved Dorman's conjecture [1] that the norms of j-invariants of rank two Drinfeld modules on $\mathbb{F}_q[x]$ with complex multiplication are monic polynomials in $\mathbb{F}_q[x]$, when the infinite place is ramified, that is, the degree of the infinite place is one. They also gave some formulae for the degrees of the norm and trace of the j-invariants of Drinfeld modules on elliptic curves when the degree of the infinite place is one. In this note we follow their method to prove similar results when the infinite place is inert, that is, the degree of the infinite place is two. The main ingredient of the proof is to estimate $v_\infty(\xi(\mathfrak{a}))$ for some fractional ideals $\mathfrak{a}$ of A. To do so, Dummit and Hayes used a formula in [4] which is valid only in the case when the degree of the infinite place is 1. Here we use a formula in [3] valid for any case.

1. Notation and the Proof of Dorman's conjecture

We shall use mostly the same notation as in [2]. Let $f(x) \in \mathbb{F}_q[x]$ be a polynomial of even degree $n \geqslant 4$. If q is odd, we assume that the leading coefficient α is not in $\mathbb{F}_q^2$, and let $k/\mathbb{F}_q(x)$ be the hyperelliptic extension obtained by

$$y^2 = f(x). \tag{1.1}$$

If q is even, let $k/\mathbb{F}_q(x)$ be the hyperelliptic extension obtained by

$$y^2 + h(x)y = f(x), \tag{1.2}$$

with $\deg h(x) = n/2$. We assume that $f(x)$ is square free if q is odd. If q is even, we choose $h(x)$ and $f(x)$ so that the curve defined by (1.2) is nonsingular and $Y^2 + \mu Y - \alpha$

Received 15th September, 1994.
The first author is supported in part by Non Directed Research Fund, Korea Research Foundation 1993 and the second author by BSRI-94-1427, Ministry of Education.

https://doi.org/10.1017/S0004972700014465 Published online by Cambridge University Press

is irreducible over $\mathbb{F}_q$ where μ is the leading coefficient of $h(x)$. Then the infinite place of $\mathbb{F}_q(x)$ is inert in k. The genus g of this curve is $((n/2)-1)$. Let ∞ denote the unique extension to k of the infinite place of $\mathbb{F}_q(x)$, and let k_∞ be the comletion of k at ∞. Then x^{-1} is a uniformiser in k_∞, and determines a sign function

$$\operatorname{sgn} : k_\infty \longrightarrow \mathbb{F}_{q^2}$$

such that $\operatorname{sgn}(x) = 1$. Then $\operatorname{sgn}(y) = \beta$, where $\beta^2 = \alpha$. Let A be the ring of functions in k which are regular away from ∞. Let ϕ be a sgn-normalised rank one Drinfeld module defined over an algebraic closure of k. Then

$$\phi_x = x + aF + F^2 \tag{1.3}$$

$$\phi_y = y + c_1F + \cdots + c_{n-1}F^{n-1} + \beta F^n, \tag{1.4}$$

where F is the Frobenius map $c \mapsto c^q$. The coefficient $a, c_1, \ldots, c_{n-1}$ are the elements of the normalising field $\widetilde{H}$ of (A, sgn) [4]. Let H be the Hilbert class field of A, and h the class number of k. Then it is well known that the ideal class number of A is $2h$. Then $[H:k] = 2h$ and $[\widetilde{H}:H] = (q^2-1)/(q-1) = q+1$. Define the j-invariant $j(\phi) = a^{q+1}$. Then $j(\phi)$ generates H over k. Put

$$J(\phi) = N_{H/k}(j(\phi)),$$

where $N_{H/k}$ is the norm map from H to k. From the theory of complex multiplication, $J(\phi)$ actually lies in $\mathbb{F}_q[x]$. Dorman's conjecture says that $J(\phi)$ is monic.

Let Λ_x be the A-module of x-torsion points of ϕ. Let $K_x = \widetilde{H}(\Lambda_x)$ and K_x^+ be the fixed field of the inertia group G_∞ at ∞. Fix an embedding $\mathrm{e} : K_x^+ \longrightarrow k_\infty$. Let C be the completion of the algebraic closure of k_∞. Then e extends to an embedding, also called e, of K_x into C. The image $\mathrm{e}(xA)$ of xA is a lattice in C. Therefore there is an invariant $\xi(xA) \in C$ such that the Drinfeld module ϕ^Γ determined by the lattice $\Gamma = \xi(xA)\cdot xA$ is sgn-normalised. Since K_x is independent of the choice of sgn-normalised Drinfeld modules, we may replace ϕ by this ϕ^Γ. A generator λ of Λ_x may be constructed by

$$\lambda = \xi(xA) \prod_{\gamma \in xA - 0} \left(1 - \frac{1}{\gamma}\right). \tag{1.5}$$

If a fractional ideal $\mathfrak{a}$ of A is prime to x, then

$$\lambda^{\sigma_\mathfrak{a}} = \xi(x\mathfrak{a}^{-1}) \prod_{\gamma \in x\mathfrak{a}^{-1} - 0} \left(1 - \frac{1}{\gamma}\right), \tag{1.6}$$

where $\sigma_{\mathfrak{a}}$ is the Artin isomorphism of $K_{\mathfrak{x}}/k$ associated with $\mathfrak{a}$. If v_∞ is the normalised valuation on $K_{\mathfrak{x}}^{+}$ induced by the embedding e, then we write $\deg z = -2v_\infty(z)$ for every $z \in K_{\mathfrak{x}}^{+}$. Let $z = -\lambda^{q-1}$ and $Z = -\lambda^{q^2-1} = -z^{q+1}$. We shall calculate the degrees of z and Z.

Let $\mathcal{Z}_{\mathfrak{a}}(S)$ be the partial zeta function $\mathcal{Z}_{0,\mathfrak{a}}(S)$ defined in [**3**, III, (1.10)]. It is shown in [**3**, IV, (4.10)] that

$$\deg \xi(\mathfrak{a}) = \mathcal{Z}'_{\mathfrak{a}}(1), \tag{1.7}$$

for any fractional ideal $\mathfrak{a}$ of A. Let

$$L_i(\mathfrak{a}) = L\left(\mathfrak{a}^{-1}\infty^{i+[(\deg \mathfrak{a})/2]}\right) = \{\gamma \in \mathfrak{a}; \deg \gamma \leqslant 2i + 2\left[\frac{\deg \mathfrak{a}}{2}\right]\}.$$

Let $u_i = dim_{\mathbb{F}_q} L_i(\mathfrak{a})$. Then from the Riemann-Roch theorem,

$$u_g = \begin{cases} g, & \text{if } \deg \mathfrak{a} \text{ is odd} \\ g+1, & \text{if } \deg \mathfrak{a} \text{ is even.} \end{cases}$$

Using the equation [**3**, III, (2.5)], we can easily get

PROPOSITION 1. *Let $\mathfrak{a}$ be a fractional ideal of A. Then*

$$\mathcal{Z}'_{\mathfrak{a}}(1) = \begin{cases} -\deg \mathfrak{a} + 1 + \dfrac{2q^g}{q^2-1} - 2\sum\limits_{i=0}^{g-1} q^{u_i}, & \textit{if } \deg \mathfrak{a} \textit{ is odd} \\ -\deg \mathfrak{a} + \dfrac{2q^{1+g}}{q^2-1} - 2\sum\limits_{i=0}^{g-1} q^{u_i}, & \textit{if } \deg \mathfrak{a} \textit{ is even.} \end{cases} \tag{1.8}$$

In particular, if $\mathfrak{a}$ is principal,

$$\mathcal{Z}'_{\mathfrak{a}}(1) = \begin{cases} -\deg \mathfrak{a} + 1 + 2\left(\dfrac{q^g}{q^2-1} - \dfrac{q^g-1}{q-1}\right) & \textit{if } \deg \mathfrak{a} \textit{ is odd} \\ -\deg \mathfrak{a} + 2\left(\dfrac{q^{1+g}}{q^2-1} - \dfrac{q^{1+g}-q}{q-1}\right) & \textit{if } \deg \mathfrak{a} \textit{ is even} \end{cases} \tag{1.9}$$

and if $g = 1$ and $\mathfrak{a}$ is not principal,

$$\mathcal{Z}'_{\mathfrak{a}}(1) = \begin{cases} -(1 + \deg \mathfrak{a}) + \dfrac{2q}{q^2-1}, & \textit{if } \deg \mathfrak{a} \textit{ is odd} \\ -(2 + \deg \mathfrak{a}) + \dfrac{2q^2}{q^2-1}, & \textit{if } \deg \mathfrak{a} \textit{ is even.} \end{cases} \tag{1.10}$$

PROOF: We get (1.8) by differentiating the equation [**3**, III, (2.5)]. If $\mathfrak{a} = (a)$ is principal and $\deg a$ is odd (respectively even), then $u_i = i$ (respectively $i + 1$),

https://doi.org/10.1017/S0004972700014465 Published online by Cambridge University Press

since $ax^{i-1} \in L_i(\mathfrak{a}) - L_{i-1}(\mathfrak{a})$ for $i > 0$ (respectively $ax^i \in L_i(\mathfrak{a}) - L_{i-1}(\mathfrak{a})$ for $i \geqslant 0$) and $u_g = g$ (respectively $g+1$). Hence $\sum_{i=0}^{g-1} q^{u_i} = (q^g - 1)/(q-1)$ (respectively $(q^{1+g} - q)/(q-1)$). Thus (1.9) follows from (1.8). (1.10) follows from (1.8) since $u_0 = 0$.

Now assume that $g > 1$, and $\mathfrak{a}$ is nonprincipal. To estimate $\mathcal{Z}_{\mathfrak{a}}(1)$ we have to estimate $\sum_{i=0}^{g-1} q^{u_i}$. Since $0 \leqslant u_i - u_{i-1} \leqslant 2$, we have

$$\sum_{i=0}^{g-1} q^{u_i} \geqslant q^{u_g-2} + q^{u_g-4} + \cdots + q^{u_g-2[(u_g)/2]} + 1 + \cdots + 1$$

$$= \frac{q^{u_g} - q^{u_g-2[u_g/2]}}{q^2-1} + g - \left[\frac{u_g}{2}\right].$$

Since $u_g - 2[u_g/2] \leqslant 1$, if deg $\mathfrak{a}$ is odd,

$$\mathcal{Z}'_{\mathfrak{a}}(1) \leqslant -\deg \mathfrak{a} + 1 - 2g + 2\left[\frac{g}{2}\right] + \frac{2q}{q^2-1}, \tag{1.11}$$

and if deg $\mathfrak{a}$ is even,

$$\mathcal{Z}'_{\mathfrak{a}}(1) \leqslant -\deg \mathfrak{a} - 2g + 2\left[\frac{g+1}{2}\right] + \frac{2q}{q^2-1}. \tag{1.12}$$

We can find a set $\mathcal{P}$ consisting of A, $h-1$ nonprincipal fractional ideals of degree 0, and h fractional ideals of degree 1 representing the ideal class group of A. Furthermore, we take the ideals to be prime to x. Then from (1.5) and (1.6) we have deg λ = deg $\xi(xA)$ and deg $\lambda^{\sigma_{\mathfrak{a}}}$ = deg $\xi\left(x\mathfrak{a}^{-1}\right)$, for $\mathfrak{a} \in \mathcal{P}$.

We now prove Dorman's conjecture. From (1.9), deg $(z) < 0$, so deg $\left(xz^{-1} + z^q\right)$ = deg $\left(xz^{-1}\right)$. Since $x - az + z^{q+1} = 0$, sgn $\left(a^{q+1}\right)$ = sgn $\left(xz^{-1}\right)^{q+1}$ = sgn $\left(-\left(x^{q+1}\right)/Z\right) = -1$, since sgn $(x) = 1$ and $Z = -\lambda^{q^2-1}$ is totally positive [5, Theorem 4.17]. This means that sgn $(j(\phi)) = -1$. If $\mathfrak{a} \in \mathcal{P}$, then by (1.11) and (1.12) deg $z^{\sigma_{\mathfrak{a}}} < 0$. Now a similar process as before would give sgn $\left(j(\phi)^{\sigma_{\mathfrak{a}}}\right)$ = sgn $\left(-\left(x^{q+1}\right)/(Z^{\sigma_{\mathfrak{a}}})\right) = -1$ Then

$$\operatorname{sgn}(J(\phi)) = \prod_{\sigma \in \mathrm{Gal}\left(\widetilde{H}/k\right)} \operatorname{sgn}\left(j(\phi)^{\sigma}\right) = (-1)^{2h} = 1,$$

as desired.

2. Determination of sgn-normalised Drinfeld modules, Trace and Norm for $g = 1$

Exactly the same method would give two polynomials $P(a)$ and $Q(a)$ with coefficients in A that a must satisfy so that (1.3) and (1.4) give a sgn-normalised Drinfeld module. Let $\Upsilon(a)$ be the monic greatest common divisor of $P(a)$ and $Q(a)$. Then a defines a sgn-normalised Drinfeld module if and only if $\Upsilon(a) = 0$. As in [2], we have

Theorem 1.

(a) *The polynomial $\Upsilon(a)$ is integral with respect to A and is separable and irreducible of degree $2(q+1)h$.*

(b) *The coefficients of $\Upsilon(a)$ are elements of $\mathbb{F}_q[x]$, and $\mathbb{F}_q(x,a)$ is an extension of $\mathbb{F}_q(x)$ of degree $2(q+1)h$ if a is a root of $\Upsilon(a) = 0$.*

Proof: The proof of (a) is exactly the same as in the case that $\deg \infty = 1$. For (b), let $\mathrm{Gal}(k/\mathbb{F}_q(x)) = \{1, \tau\}$. Since $\widetilde{H}$ contains $\mathbb{F}_{q^2}(x)$ and $\mathbb{F}_{q^2}(x)$ and k are disjoint over $\mathbb{F}_q(x)$, we can extend τ to an element of $\mathrm{Gal}\left(\widetilde{H}/\mathbb{F}_q(x)\right)$ so that $\tau(\beta) = \beta^q = -\beta$ from our choice of β. Let $\mathcal{D}$ be the set of sgn-normalised Drinfeld A-modules. Then $\tau \circ \mathcal{D} \circ \tau = \mathcal{D}$, since

$$\begin{aligned} \tau \circ \phi \circ \tau(y) &= \tau \circ \phi_{-y} \\ &= \cdots - \tau(\beta) F^n \\ &= \cdots + \beta F^n \end{aligned}$$

is sgn-normalised. Thus $\tau \circ \phi \circ \tau = \sigma\phi$, for some $\sigma \in \mathrm{Gal}\left(\widetilde{H}/k\right)$. Hence $x + \tau(a)F + F^2 = x + \sigma(a)F + F^2$, and $\tau(a) = \sigma(a)$. Also $(\tau \circ \phi \circ \tau)_y = \cdots + \beta F^n$ and $\sigma\phi_y = \cdots + \sigma(\beta)F^n$, so we have $\sigma(\beta) = \beta$. Thus we may replace τ by $\tau\sigma$ to have $\tau(a) = a$. But $0 = (\Upsilon(a))^\tau = \Upsilon^\tau(a^\tau) = \Upsilon^\tau(a)$ and $\Upsilon(a)$ is monic irreducible, so we have $\Upsilon^\tau = \Upsilon$. Hence Υ lies in $\mathbb{F}_q[x][a]$ and $\mathbb{F}_q(x,a)$ is an extension of $\mathbb{F}_q(x)$ of degree $2(q+1)h$.

Remark. $\Upsilon(a)$ is a polynomial of a^{q+1}, since $\widetilde{H} = k(a)$, $H = k\left(a^{q+1}\right)$ and $[\widetilde{H} : H] = q+1$.

By the remark above $\mathrm{Tr}_{\widetilde{H}/k}(a) = 0$ and $N_{\widetilde{H}/k}(a) = N_{H/k}\left(a^{q+1}\right)$. We shall compute the degrees of $\mathrm{Tr}_{H/k}\left(a^{q+1}\right)$ and $N_{H/k}\left(a^{q+1}\right)$ in the case $g = 1$. Let $\mathcal{P}$ be the set of representatives of the ideal classes as in the previous section. Then $\mathcal{P}$ is decomposed as $\{A\} \cup \mathcal{P}_0 \cup \mathcal{P}_1$, where ideals in $\mathcal{P}_i$ have degree i. By (1.9) and (1.10), we have

$$\begin{aligned} \deg Z &= -2\left(q^3 - q - 1\right) \\ \deg Z^{\sigma_\mathfrak{a}} &= -2\left(q^2 - 2\right) \quad \text{if} \quad \deg \mathfrak{a} = 0 \\ \deg Z^{\sigma_\mathfrak{a}} &= -2\left(q^2 - q - 1\right) \quad \text{if} \quad \deg \mathfrak{a} = 1. \end{aligned}$$

https://doi.org/10.1017/S0004972700014465 Published online by Cambridge University Press

Hence

$$\deg a^{q+1} = \deg \left(x^{q+1}Z^{-1}\right) = 2q^3$$

$$\deg \left(a^{q+1}\right)^{\sigma_{\mathfrak{a}}} = 2\left(q^2+q-1\right) \quad \text{if} \quad \deg \mathfrak{a} = 0,$$

and

$$\deg \left(a^{q+1}\right)^{\sigma_{\mathfrak{a}}} = 2q^2 \quad \text{if} \quad \deg \mathfrak{a} = 1.$$

Therefore we have proved

Theorem 2. deg $N_{H/k}(j(\phi)) = 2\left(q^3 + (2h-1)q^2 + (h-1)q - h + 1\right)$

and

$$\deg \operatorname{Tr}_{H/k}(j(\phi)) = 2q^3.$$

Thus as polynomials in $\mathbb{F}_q[x]$*,*

$$\deg N_{H/k}(j(\phi)) = q^3 + (2h-1)q^2 + (h-1)q - h + 1$$

and

$$\deg \operatorname{Tr}_{H/k}(j(\phi)) = q^3.$$

References

[1] D. Dorman, 'On singular moduli for rank 2 Drinfeld modules', *Compositio Math.* **80** (1991), 235–256.

[2] D. Dummit and D. Hayes, 'Rank-one Drinfeld modules on elliptic curves', *Math. Comp.* **62** (1994), 875–883.

[3] E.U. Gekeler, *Drinfeld modular curves*, Lecture Notes in Mathematics **1231** (Springer-Verlag, Berlin, Heidelberg, New York, 1986).

[4] D. Hayes, 'Analytic class number formulas in global function fields', *Invent. Math.* **65** (1981), 49–69.

[5] D. Hayes, 'Stickelberger elements in function fields', *Compositio Math.* **55** (1985), 209–239.

Department of Mathematics
KAIST
Taejon
305-701 Korea

Department of Mathematics
Choong Nam National University
Taejon
302-764 Korea