Cyclicity and Titchmarsh divisor problem for Drinfeld modules

Cristian Virdol

Abstract Let $A=\mathbb{F}_q[T]$, where $\mathbb{F}_q$ is a finite field, let $Q=\mathbb{F}_q(T)$, and let F be a finite extension of Q. Consider ϕ a Drinfeld A-module over F of rank r. We write $r=hed$, where E is the center of $D:=\mathrm{End}_{\overline{F}}(\phi)\otimes Q$, $e=[E:Q]$, and $d=[D:E]^{\frac{1}{2}}$. If $\wp$ is a prime of F, we denote by $\mathbb{F}_\wp$ the residue field at $\wp$. If ϕ has good reduction at $\wp$, let $\bar{\phi}$ denote the reduction of ϕ at $\wp$. In this article, in particular, when $r\neq d$, we obtain an asymptotic formula for the number of primes $\wp$ of F of degree x for which $\bar{\phi}(\mathbb{F}_\wp)$ has at most $(r-1)$ cyclic components. This result answers an old question of Serre on the cyclicity of general Drinfeld A-modules. We also prove an analogue of the Titchmarsh divisor problem for Drinfeld modules.

1. Introduction

Let $\mathbb{F}_q$ be a finite field, let $A=\mathbb{F}_q[T]$, let $Q=\mathbb{F}_q(T)$, let F be a finite extension of Q, let $\mathbb{F}_F$ be the constant field of F, and let $\overline{\mathbb{F}}_F$ be the algebraic closure of $\mathbb{F}_F$. For $\wp$ a prime of F, we denote by $\mathbb{F}_\wp$ the residue field at $\wp$ and by $\overline{\mathbb{F}}_\wp$ the algebraic closure of $\mathbb{F}_\wp$. Let ϕ be a Drinfeld A-module over F of rank r. For all but finitely many primes $\wp$ of F, ϕ has good reduction at $\wp$, and we denote by $\mathcal{P}_\phi$ the set of primes $\wp$ of F of good reduction for ϕ. For $\wp\in\mathcal{P}_\phi$, let $\bar{\phi}$ be the reduction of ϕ at $\wp$.

We have that $\bar{\phi}(\mathbb{F}_\wp)\subseteq\bar{\phi}[m](\overline{\mathbb{F}}_\wp)\subseteq(A/mA)^r$, for some $m\in A$ with $m\neq 0$, where $\bar{\phi}[m](\overline{\mathbb{F}}_\wp)$ is the set of m-division points of $\bar{\phi}$ in $\overline{\mathbb{F}}_\wp$. Hence,

$$\bar{\phi}(\mathbb{F}_\wp)\simeq A/w_1A\times A/w_2A\times\cdots\times A/w_sA, \tag{1.1}$$

where $s\leq r$, $w_i\in A\setminus\mathbb{F}_q$, and $w_i\mid w_{i+1}$ for $1\leq i\leq s-1$. Each A/w_iA is called a *cyclic component* of $\bar{\phi}(\mathbb{F}_\wp)$. (Thus, when $r=1$, $\bar{\phi}(\mathbb{F}_\wp)$ is always cyclic.) If $s<r$, we say that $\bar{\phi}(\mathbb{F}_\wp)$ has at most $(r-1)$ cyclic components.

For $x\in\mathbb{N}$, define

$$f_{\phi,F}(x)=\big|\{\wp\in\mathcal{P}_\phi\mid \deg_F\wp=x,\bar{\phi}(\mathbb{F}_\wp)\text{ has at most }(r-1)\text{ cyclic components}\}\big|,$$

Kyoto Journal of Mathematics, Vol. 57, No. 3 (2017), 505–518
First published online 14, April 2017.
DOI 10.1215/21562261-2017-0004,
Received June 1, 2015. Revised February 17, 2016. Accepted April 20, 2016.
2010 Mathematics Subject Classification: Primary 11G09; Secondary 11G15.
The author's work supported by the Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (2015R1D1A1A01056643).

where $\deg_F \wp = [\mathbb{F}_\wp : \mathbb{F}_F]$. Let $F(\phi[m])$ be the field obtained by adjoining to F the m-division points $\phi[m]$ of ϕ.

For $x \in \mathbb{N}$ we define (throughout this article $m \in A$ is a monic polynomial and $p \in A$ is the prime below $\wp$)

$$f'_{\phi,F}(x) := \sum_{\substack{\wp \in \mathcal{P}_\phi \\ \deg_F \wp = x}} \left|\left\{m \in A \mid (m,p) = 1, \wp \text{ splits completely in } F\big(A[m]\big)\right\}\right|. \tag{1.2}$$

Let $r_m := [F(\phi[m]) \cap \overline{\mathbb{F}}_F : \mathbb{F}_F]$, let $d_F := [\mathbb{F}_F : \mathbb{F}_q]$, and let $\pi_F(x)$ be the number of primes of F of degree x. Let E be the center of $D := \mathrm{End}_{\overline{F}}(\phi) \otimes Q$. By the theory of central simple algebras, there exist positive integers e, d, h such that $[E : Q] = e$, $[D : E] = d^2$, and $r = hed$.

In this article we prove the following results.

THEOREM 1.1

Let ϕ be a Drinfeld A-module over F of rank $r \geq 2$. We write $r = hed$, where E is the center of $D := \mathrm{End}_{\overline{F}}(\phi) \otimes Q$, $e = [E : Q]$, and $d = [D : E]^{\frac{1}{2}}$. Assume that $r \neq d$. Then, for $x \in \mathbb{N}$, we have

$$f_{\phi,F}(x) = c_{\phi,F}(x)\pi_F(x) + O\big((q^{d_F x})^{\Delta_{r,h,e}}\big),$$

where

$$\Delta_{r,h,e} = \begin{cases} \frac{r+3}{2r+2} & \text{if } h^2 e \geq \frac{r+1}{2}, \\ \frac{h^2 e+1}{2h^2 e} & \text{otherwise,} \end{cases}$$

and

$$c_{\phi,F}(x) = \sum_{\substack{m \in A \\ m \text{ is monic}}} \frac{\mu_q(m) r_m(x)}{[F(\phi[m]) : F]},$$

where $\mu_q(\cdot)$ is the Möbius function of A and

$$r_m(x) = \begin{cases} 3r_m & \text{if } r_m \mid x, \\ 0 & \text{otherwise.} \end{cases}$$

Moreover, assume that $F = Q$, $D = A$, and all division fields of ϕ are geometric. (Thus, $r_m(x) = r_m = 1$, and $c_{\phi,F} := c_{\phi,F}(x)$ is independent of x.) Then, from [11, Theorem 3], we know that $c_{\phi,F}$ is positive if and only if $Q(\phi[a]) \neq Q$ for all $a \in A$ of degree 1.

THEOREM 1.2

Under the same conditions and assumptions as in Theorem 1.1, for $x \in \mathbb{N}$, we have

$$f'_{\phi,F}(x) = c'_{\phi,F}(x)\pi_F(x) + O\big((q^{d_F x})^{\Delta_{r,h,e}}\big),$$

where

$$\Delta_{r,h,e} = \begin{cases} \frac{r+3}{2r+2} & \text{if } h^2 e \geq \frac{r+1}{2}, \\ \frac{h^2 e+1}{2h^2 e} & \text{otherwise,} \end{cases}$$

and

$$c'_{\phi,F}(x) = \sum_{\substack{m \in A \\ m \text{ is monic}}} \frac{r_m(x)}{[F(\phi[m]) : F]},$$

where

$$r_m(x) = \begin{cases} r_m & \text{if } r_m \mid x, \\ 0 & \text{otherwise.} \end{cases}$$

Theorem 1.1 is a generalization of [11, Theorem 1], where only the case $\mathrm{End}_{\overline{F}}(\phi) = A$ was considered (i.e., with our notation $r = hed$, with $h = r$ and $e = d = 1$), but the error term in the asymptotic formula in [11, Theorem 1] even in this particular case is weaker than ours. (The error terms in Theorem 1.1 above and [11, Theorem 1] coincide only when $r = 2$, $h = 2$, and $e = d = 1$.) To improve and generalize the asymptotic formula in [11, Theorem 1], we make use of the Chebotarev density theorem, the open image theorem for l-adic representations associated to general Drinfeld A-modules (i.e., [13, Theorem 0.1]), Lemma 3.3, which the authors of [11], [2], and [3] could prove only for $k = 1$ and $k = r$ (in the case of both Drinfeld modules and abelian varieties), Lemmas 3.4 and 3.5, the sets $S_c(m)$ defined in Section 5, and the splitting from formula (5.1).

In the very particular case $r = 2$, $h = 1$, $e = 2$, $d = 1$, Theorems 1.1 and 1.2 are also a generalization and improvement of Cojocaru and Shulman [3, (9)] and of the main theorem of [3], that is, [3, Theorem 1.1]. (In [3] an additional condition is imposed: ϕ has complex multiplication (CM) by the full ring of integers of an imaginary quadratic field.)

Here is a brief history of the cyclicity question we consider in this article. Let E be an elliptic curve defined over $\mathbb{Q}$ of conductor N. For p a rational prime we denote by $\mathbb{F}_p$ the finite field of cardinality p and by $\overline{\mathbb{F}}_p$ the algebraic closure of $\mathbb{F}_p$. Let $\mathcal{P}_E$ be the set of rational primes p of good reduction for E (i.e., $(p, N) = 1$). For $p \in \mathcal{P}_E$, we denote by $\bar{E}$ the reduction of E at p. We have that $\bar{E}(\mathbb{F}_p) \subseteq \bar{E}[m](\overline{\mathbb{F}}_p) \subseteq (\mathbb{Z}/m\mathbb{Z})^2$ for any positive integer m satisfying $|\bar{E}(\mathbb{F}_p)| \mid m$. Hence,

$$\bar{E}(\mathbb{F}_p) \simeq \mathbb{Z}/m_1\mathbb{Z} \times \mathbb{Z}/m_2\mathbb{Z}, \tag{1.3}$$

where $m_i \in \mathbb{Z}_{\geq 1}$ and $m_1 \mid m_2$. Each $\mathbb{Z}/m_i\mathbb{Z}$ is called a cyclic component of $\bar{E}(\mathbb{F}_p)$. If $m_1 = 1$, we say that $\bar{E}(\mathbb{F}_p)$ is *cyclic*.

For $x \in \mathbb{R}$, define

$$f_{E,\mathbb{Q}}(x) = \left|\left\{p \in \mathcal{P}_E \mid p \leq x, \bar{E}(\mathbb{F}_p) \text{ is cyclic}\right\}\right|.$$

In 1976, Serre proved (see [15] and also [12, Theorem 2]), under generalized Riemann hypothesis (GRH), that if E is a non-CM elliptic curve, then

$$f_{E,\mathbb{Q}}(x) = c_E \operatorname{li} x + o\Big(\frac{x}{\log x}\Big),$$

where $\operatorname{li} x := \int_2^x \frac{1}{\log t}\, dt$ and

$$c_E = \sum_{m=1}^{\infty} \frac{\mu(m)}{[\mathbb{Q}(E[m]) : \mathbb{Q}]},$$

where $\mu(\cdot)$ is the Möbius function. Moreover, Serre proved that $c_E > 0$ if and only if $\mathbb{Q}(E[2]) \neq \mathbb{Q}$. In 2004, the error term in Serre's estimate was improved by Cojocaru and Murty [2, Theorem 1.1], where they obtained the formula

$$f_{E,\mathbb{Q}}(x) = c_E \operatorname{li} x + O\big(x^{5/6}(\log x)^{2/3}\big).$$

This corresponds to the case $r = 2$, $h = 2$, $e = 1$, and $d = 1$ in Theorem 1.1 above, and we obtain

$$f_{\phi,F}(x) = c_{\phi,F}(x)\pi_F(x) + O\big((q^{d_F x})^{5/6}\big),$$

which is the same formula as in [11, Theorem 1.1].

When the elliptic curve E has CM by the full ring of integers of an imaginary quadratic field, Cojocaru and Murty in Theorem 1.2 of [CM] obtained a better asymptotic formula:

$$f_{E,\mathbb{Q}}(x) = c_E \operatorname{li} x + O\big(x^{3/4}(\log x)^{1/2}\big).$$

This corresponds (with the condition "full ring of integers" removed) to the case $r = 2$, $h = 1$, $e = 2$, and $d = 1$ in Theorem 1.1 above, and we obtain

$$f_{\phi,F}(x) = c_{\phi,F}(x)\pi_F(x) + O\big((q^{d_F x})^{3/4}\big),$$

which is better than [3, (9)] or [3, the formula in Theorem 1.1]. (These two last results were obtained also under the restriction: "ϕ has CM by the full ring of integers of an imaginary quadratic field.")

Finally, the results regarding Serre's cyclicity question from [15], [2], and [11] were extended to arbitrary abelian varieties defined over number fields in [18] and to arbitrary generic Drinfeld A-modules in this article. We remark that Theorem 1.2 is an analogue of the Titchmarsh divisor problem for Drinfeld modules of rank $r \geq 2$ (see [1], [17] for details). We remark that the methods of this article could be used to generalize [1] and [5], where the authors were able to prove their results only for the very particular case when the abelian variety A from [1] is defined over $\mathbb{Q}$ and contains an abelian subvariety E of dimension 1 also defined over $\mathbb{Q}$ (see [1, Theorem 1.2 and Remark 4.1] and also [5, the last sentence of Section 1.1], where the authors say that they can prove their results only for "abelian varieties defined over $\mathbb{Q}$ which have a 1-dimensional subvariety which is also defined over $\mathbb{Q}$").

2. Known results

For F a finite extension of Q, we define $G_F := \mathrm{Gal}(F^{\mathrm{sep}}/F)$, where F^{sep} is the separable closure of F inside a fixed algebraic closure $\overline{F}$ of F. Let ϕ be a Drinfeld A-module over F of rank r. For $m \in A$ with $m \neq 0$, we denote by $\phi[m]$ the m-division points of ϕ in $\overline{F}$. Then

$$\phi[m] \simeq (A/mA)^r.$$

If $F(\phi[m])$ is the field obtained by adjoining to F the elements of $\phi[m]$, then we have a natural injection

$$\Phi_m : \mathrm{Gal}\big(F\big(\phi[m]\big)/F\big) \hookrightarrow \mathrm{Aut}\big(\phi[m]\big) \simeq \mathrm{GL}_r(A/mA).$$

We denote $G_m := \mathrm{Im}\,\Phi_m(\mathrm{Gal}(F(\phi[m])/F))$. Define

$$n(m) := |G_m| = \big[F\big(\phi[m]\big) : F\big].$$

For a rational prime l, let

$$T_l(\phi) = \varprojlim \phi[l^n]$$

and $V_l(\phi) = T_l(\phi) \otimes Q$. The Galois group G_F acts on

$$T_l(\phi) \simeq A_l^r,$$

where A_l is the l-adic completion of A at l, and also on $V_l(\phi) \simeq Q_l^r$, and we obtain a continuous representation

$$\rho_{\phi,l} : G_F \to \mathrm{Aut}\big(T_l(\phi)\big) \simeq \mathrm{GL}_r(A_l) \subset \mathrm{Aut}\big(V_l(\phi)\big) \simeq \mathrm{GL}_r(Q_l).$$

Hence, we get a representation

$$\rho_\phi := G_F \to \prod_l \mathrm{GL}_r(A_l).$$

If $\wp \in \mathcal{P}_\phi$, let $\mathfrak{p} = \wp \cap A$, let $p \in A$ be the prime such that $pA = \mathfrak{p}$, and let $l \in A$ be a prime satisfying $(l,p) = 1$. Then $F(\phi[l^\infty])/F$ is unramified at $\wp$, and let $\sigma_\wp$ be the Artin symbol of $\wp$ in $\mathrm{Gal}(F(\phi[l^\infty])/F)$. We denote by $P_{\phi,\wp}(X) = X^r + a_{1,\phi}(\wp)X^{r-1} + \cdots + a_{r-1,\phi}(\wp)X + u_\wp p^{m_\wp} \in A[X]$, where $u_\wp \in \mathbb{F}_q^*$ and $m_\wp = [\mathbb{F}_\wp : A/\mathfrak{p}]$, the characteristic polynomial of $\sigma_\wp$ on $T_l(\phi)$. Then $P_{\phi,\wp}(X)$ is independent of l. One can identify $T_l(\phi)$ with $T_l(\bar\phi)$, where $\bar\phi$ is the reduction of ϕ at $\wp$, and the action of $\sigma_\wp$ on $T_l(\phi)$ is the same as the action of the Frobenius $\pi_\wp$ of $\bar\phi$ on $T_l(\bar\phi)$. Define $Q_{\phi,\wp}(X) = X^r + c_{1,\phi}(\wp)X^{r-1} + \cdots + c_{r-1,\phi}(\wp)X + c_{r,\phi}(\wp) \in A[X]$ by $Q_{\phi,\wp}(X) := P_{\phi,\wp}(X+1)$.

We know the following (see [11, Proposition 11]).

LEMMA 2.1

Let F/Q be a finite extension, and let ϕ be a Drinfeld A-module over F of rank $r \geq 2$. If $\wp \in \mathcal{P}_\phi$, let $\mathfrak{p} = \wp \cap A$, and let $p \in A$ be the prime satisfying $pA = \mathfrak{p}$.

(i) *For $m \in A$ with $(m,p) = 1$, the finite A-module $\bar\phi(\mathbb{F}_\wp)$ contains an $(A/mA)^r$-type submodule if and only if $\wp$ splits completely in $F(\phi[m])$.*

(ii) *The module* $\bar{\phi}(\mathbb{F}_\wp)$ *contains at most* $(r-1)$ *cyclic components if and only if* $\wp$ *does not split completely in* $F(\phi[l])$ *for all primes* $l \in A$ *with* $l \neq p$.

3. Drinfeld modules

Let ϕ be a Drinfeld module of rank r, defined over a finite extension F/Q, such that $\mathrm{End}_F\,\phi = \mathrm{End}_{\overline{F}}\,\phi$. (In the proofs of Theorems 1.1 and 1.2 one does not have to assume that $\mathrm{End}_F\,\phi = \mathrm{End}_{\overline{F}}\,\phi$: the reason is that the inequality on the left in Lemma 3.2 below holds true even without the assumption $\mathrm{End}_F\,\phi = \mathrm{End}_{\overline{F}}\,\phi$ as is noted just after the proof of Lemma 3.2.) Let E be the center of $D := \mathrm{End}_{\overline{F}}(\phi) \otimes Q$. By the theory of central simple algebras (see [14, the section after Theorem 0.1]), there exist positive integers e, d, h such that $[E:Q] = e$, $[D:E] = d^2$, and $r = hed$. Let O_E be the "ring of integers" of E.

Let l be a rational prime. Since the actions of $D = \mathrm{End}_F\,\phi \otimes Q$ and G_F on $V_l(\phi)$ commute, we obtain a continuous h-dimensional representation

$$\rho_l : G_F \to \mathrm{Aut}_{D_l} V_l(\phi) \cong \mathrm{GL}_h(E_l),$$

where $D_l := \mathrm{End}_F\,\phi \otimes Q_l$ and $E_l := E \otimes Q_l$. Hence, we get a representation

$$\rho : G_F \to \prod_l \mathrm{GL}_h(O_E \otimes A_l).$$

(Actually throughout this article we should have written, as in [13, Theorem 0.2], $\mathrm{Cent}_{\mathrm{GL}_r(A_l)}(\mathrm{End}_{\overline{F}}(\phi))$ instead of $\mathrm{GL}_h(O_E \otimes A_l)$, but to simplify the notation, because for almost all l these two groups are isomorphic, and also because this identification does not affect our arguments, we leave it in this form.)

We know the following (see [13, Theorem 0.2]).

LEMMA 3.1

The image of the homomorphism

$$\rho : G_F \to \prod_l \mathrm{GL}_h(O_E \otimes A_l)$$

is open.

Hence, we obtain the following (see also [19]).

LEMMA 3.2

Let ϕ *be a Drinfeld* A*-module over* F *of rank* r*. Assume that* $\mathrm{End}_{\overline{F}}(\phi) = \mathrm{End}_F(\phi)$*. We write* $r = hed$*, where* E *is the center of* $D := \mathrm{End}_{\overline{F}}(\phi) \otimes Q$*,* $e = [E:Q]$*, and* $d = [D:E]^{1/2}$*. Then, for* $m \in A$ *a monic polynomial, we have*

$$\left|(O_E/mO_E)^*\right| q^{e(h^2-1)\deg m} \ll |G_m| \leq \left|(O_E/mO_E)^*\right| q^{e(h^2-1)\deg m} < q^{eh^2 \deg m}.$$

Proof

From the injection

$$\phi_m : \mathrm{Gal}\big(F\big(\phi[m]\big)/F\big) \hookrightarrow \mathrm{GL}_h(O_E/mO_E),$$

one obtains trivially the inequality

$$|G_m| \leq \left|(O_E/mO_E)^*\right| q^{e(h^2-1)\deg m} < q^{eh^2 \deg m}.$$

From [16, Théorème 1] (see also [7], [13]), after eventually replacing F by a finite extension, we obtain that the function

$$l^d \mapsto \left[F\left(\phi[l^d]\right) : F\right]$$

is multiplicative in l, where l runs over the rational primes (and d stands for arbitrary powers of l). Hence, from the open image theorem for Drinfeld A-modules, that is, Lemma 3.1 above, we get that

$$\begin{aligned} |G_m| &\gg \left|\mathrm{GL}_h(O_E/mO_E)\right| \\ &= q^{e(h^2-1)\deg m} \prod_{l|m} \left(1 - \frac{1}{q^{\deg l}}\right)\left(1 - \frac{1}{q^{2\deg l}}\right) \cdots \left(1 - \frac{1}{q^{r\deg l}}\right) \\ &= \left|(O_E/mO_E)^*\right| q^{e(h^2-1)\deg m} \prod_{l|m} \left(1 - \frac{1}{q^{2\deg l}}\right) \cdots \left(1 - \frac{1}{q^{r\deg l}}\right), \end{aligned}$$

where the product is over distinct primes $l \mid m$. Because

$$\prod_{l|m} \left(1 - \frac{1}{q^{2\deg l}}\right) \cdots \left(1 - \frac{1}{q^{r\deg l}}\right) \gg \prod_{l} \left(1 - \frac{1}{q^{2\deg l}}\right) \cdots \left(1 - \frac{1}{q^{r\deg l}}\right) \gg 1,$$

where the last product is over all primes l, we are done with the proof of Lemma 3.2. $\square$

We remark that in Lemma 3.2, even if we do not assume that $\mathrm{End}_F\,\phi = \mathrm{End}_{\overline{F}}\,\phi$, we have

$$\left|(O_E/mO_E)^*\right| q^{e(h^2-1)\deg m} \ll |G_m|,$$

because $\mathrm{End}_{F'}\,\phi = \mathrm{End}_{\overline{F}}\,\phi$ for some finite extension F'/F.

LEMMA 3.3

Using the same notation as above, let $\wp \in \mathcal{P}_\phi$, and let p be the rational prime below $\wp$. Let $m \in A$ be a monic polynomial such that $(m,p) = 1$. If $\wp$ splits completely in $F(\phi[m])$, then

$$m^k \mid c_{k,\phi}(\wp),$$

for any $k = 1, \ldots, r$.

Proof

Let $l \mid m$ be a rational prime, and let $m(l)$ be the largest natural number such that $l^{m(l)} \mid m$. Let

$$\pi_\wp : \bar{\phi}(\overline{\mathbb{F}}_\wp) \to \bar{\phi}(\overline{\mathbb{F}}_\wp)$$

be the Frobenius endomorphism. Assume that $\wp$ splits completely in $F(\phi[m])$. Then $\bar{\phi}(\overline{\mathbb{F}}_\wp)[l^{m(l)}] \subset \mathrm{Ker}(\pi_\wp - 1)$ and we get that $\rho_{\phi,l}(\sigma_\wp) = I_r + l^{m(l)}B$, where

$B \in M_r(A_l)$. Thus, $X^r + c_{1,\phi}(\wp)X^{r-1} + \cdots + c_{r-1,\phi}(\wp)X + c_{r,\phi}(\wp) = Q_{\phi,\wp}(X) = P_{\phi,\wp}(X+1) = \det((X+1)I_r - \rho_{\phi,l}(\sigma_\wp)) = \det(XI_r - l^{m(l)}B)$, and we obtain that $l^{m(l)k} \mid c_{k,\phi}(\wp)$ for any $k = 1, \ldots, r$. □

LEMMA 3.4

We have

$$\left|c_{k,\phi}(\wp)\right| \le q^{(k/r)d_F \deg_F \wp},$$

for any $k = 1, \ldots, r$.

Proof

We know (Riemann hypothesis; see [9, Theorem 5.1]) that

$$P_{\phi,\wp}(X) = (X - x_{1,\wp}) \cdots (X - x_{r,\wp}),$$

where $|x_{i,\wp}| \le q^{(1/r)d_F \deg_F \wp}$. Hence, $X^r + c_{1,\phi}(\wp)X^{r-1} + \cdots + c_{r-1,\phi}(\wp)X + c_{r,\phi}(\wp) = Q_{\phi,\wp}(X) = P_{\phi,\wp}(X+1) = (X - (x_{1,\wp} - 1)) \cdots (X - (x_{r,\wp} - 1))$, from which we deduce that $|c_{k,\phi}(\wp)| \le q^{(k/r)d_F \deg_F \wp}$, for any $k = 1, \ldots, r$. □

LEMMA 3.5

We have

$$c_{r,\phi}(\wp) = u_\wp p^{m_\wp} + d_1 c_{1,\phi}(\wp) + d_2 c_{2,\phi}(\wp) + \cdots + d_{r-1} c_{r-1,\phi}(\wp) + d_r,$$

where $d_1, \ldots, d_r$ *are integers which depend only on* r.

Proof

From $Q_{\phi,\wp}(X) := P_{\phi,\wp}(X+1)$, we get

$$c_{1,\phi}(\wp) = a_{1,\phi}(\wp) + \binom{r}{1},$$

$$c_{2,\phi}(\wp) = a_{2,\phi}(\wp) + a_{1,\phi}(\wp)\binom{r-1}{1} + \binom{r}{2},$$

$$\vdots$$

$$c_{r,\phi}(\wp) = u_\wp p^{m_\wp} + a_{r-1,\phi}(\wp)\binom{1}{1} + \cdots + \binom{r}{r},$$

and by writing $a_{1,\phi}(\wp)$ in terms of $c_{1,\phi}(\wp)$, then $a_{2,\phi}(\wp)$ in terms of $c_{2,\phi}(\wp)$ and $c_{1,\phi}(\wp), \ldots,$ and $u_\wp p^{m_\wp}$ in terms of $c_{1,\phi}(\wp), \ldots, c_{r,\phi}(\wp)$, we are done with the proof of Lemma 3.5. □

4. Chebotarev density theorem

Let L/F be a Galois extension, let G be the Galois group of L/F, let C be a union of conjugacy classes of G, let $r_L := [L \cap \overline{\mathbb{F}}_F : \mathbb{F}_F]$, and let $\mathbb{F}_L$ be the constant field of L. For $x \in \mathbb{N}$, define

$$\pi_C(x, L/F) = \big|\{\wp \mid \deg_F \wp = x, \wp \text{ is a prime unramified in } L/F, \text{ and } \sigma_\wp \subseteq C\}\big|,$$

where $\sigma_\wp$ is the Artin symbol of $\wp$ in $\mathrm{Gal}(L/F)$.

We know the following result (see [6, Theorem 6.4.8]).

THEOREM 4.1 (CHEBOTAREV DENSITY THEOREM)

Let L/F be a finite Galois extension with Galois group G, and let $C \subseteq G$ be a conjugacy class whose restriction to $\mathbb{F}_L$ is the ath power of the Frobenius automorphism of $\mathbb{F}_F$. If $x \in \mathbb{N}$ and $x \not\equiv a \pmod{r_L}$, then

$$\pi_C(x, L/F) = 0.$$

If $x \equiv a \pmod{r_L}$ and g_L and g_F are the genera of L and F, respectively, then

$$\Big|\pi_C(x, L/F) - r_L \frac{|C|}{|G|}\frac{q^{d_F x}}{x}\Big|$$
$$\leq \frac{2|C|}{x|G|}\big((|G| + g_L r_L)q^{d_F x/2} + |G|(2g_F+1)q^{d_F x/4} + g_L r_L + |G|\Delta_F/d_F\big),$$

where $\Delta_F := [F:Q]$ and $d_F := [\mathbb{F}_F : \mathbb{F}_q]$.

Let $\pi_F(x)$ be the number of primes of F of degree x. Then from Theorem 4.1 with $L = F$, we get

$$\pi_F(x) = \frac{q^{d_F x}}{x} + O\Big(\frac{q^{d_F x/2}}{x}\Big).$$

Also from Theorem 4.1, for C equal to the trivial element of $\mathrm{Gal}(L/F)$, we obtain the following result.

THEOREM 4.2

Let L/F be a finite Galois extension with Galois group G, and let

$$\pi_1(x, L/F) = \big|\{\wp \mid \deg_F \wp = x, \wp \text{ splits completely in } L\}\big|.$$

If $x \in \mathbb{N}$ and $r_L \nmid x$, then

$$\pi_1(x, L/F) = 0.$$

If $r_L \mid x$, then

$$\Big|\pi_1(x, L/F) - \frac{r_L}{|G|}\pi_F(x)\Big| \ll \Big(\frac{g_L r_L}{|G|} + 1\Big)\frac{q^{d_F x/2}}{x},$$

where the implicit constant depends only on F.

We know the following result (see [8, Corollaire 7]).

LEMMA 4.3

For each $m \in A \setminus \mathbb{F}_q$, we have

$$g(m) := g_{F(\phi[m])} \ll D(\phi) \cdot \big[F\big(\phi[m]\big) : F\big] \cdot \deg m,$$

where the implicit constant depends only on F and the constant $D(\phi)$ depends only on ϕ.

We know the following result (see [4, Lemma 3.2], [10, Remark 7.1.9]).

LEMMA 4.4
If ϕ is a Drinfeld A-module over F, and F_ϕ is the field obtained by adjoining to F all division points of ϕ, then

$$E(\phi) = [F_\phi \cap \overline{\mathbb{F}}_F : \mathbb{F}_F] < \infty.$$

5. The proofs of Theorems 1.1 and 1.2

From Lemma 2.1(ii) we get

$$f_{\phi,F}(x) = \sum_{m \in A} \mu_q(m)\pi_1\big(x, F\big(\phi[m]\big)/F\big),$$

where the sum is over monic square-free polynomials m of A. If $\wp$ splits completely in $F(\phi[m])$, then from Lemma 3.3 we obtain that $m^r \mid P_{\phi,\wp}(1)$. Since $\deg P_{\phi,\wp}(1) \le d_F \deg_F \wp = d_F x$, it is sufficient to consider only square-free polynomials $m \in A$ with $\deg m \le d_F x/r$.

If $y = y(x)$ is a real number with $y \le d_F x/r$ (y will be chosen later), then

$$\begin{aligned} f_{\phi,F}(x) &= \sum_{\deg m \le d_F x/r} \mu_q(m)\pi_1\big(x, F\big(\phi[m]\big)/F\big) \\ &= \sum_{\deg m \le y} \mu_q(m)\pi_1\big(x, F\big(\phi[m]\big)/F\big) \\ &\quad + \sum_{y < \deg m \le d_F x/r} \mu_q(m)\pi_1\big(x, F\big(\phi[m]\big)/F\big) \\ &= \text{main} + \text{error}. \end{aligned} \tag{5.1}$$

From Theorem 4.2, we obtain

$$\text{main} = \sum_{\deg m \le y} \frac{\mu_q(m) r_m(x)}{n(m)}\pi_F(x) + \sum_{\deg m \le y} O\Big(\Big(\frac{g(m) r_m(x)}{n(m)} + 1\Big)\frac{q^{d_F x/2}}{x}\Big),$$

and from Lemmas 4.3 and 4.4, we get

$$\sum_{\deg m \le y} \Big(\frac{g(m) r_m(x)}{n(m)} + 1\Big) \ll \sum_{\deg m \le y} D(\phi)E(\phi)\deg m \ll x q^y,$$

because $\deg m \le y \ll x$ and the number of $m \in A$ with $\deg m \le y$ is much less than q^y. Thus,

$$\text{main} = \pi_F(x)\Big(\sum_{\deg m \le y} \frac{\mu_q(m) r_m(x)}{n(m)}\Big) + O(q^{(d_F x/2)+y}). \tag{5.2}$$

Now we estimate the error. For each $c = (c_1, \dots, c_{r-1}) \in A^{r-1}$, with $|c_k| \le q^{(k/r) d_F \deg_F \wp}$, for any $k = 1, \dots, r-1$, and for each square-free monic polynomial

$m \in A$, we define

$$S_c(m) := \{\wp \in \mathcal{P}_A \mid \deg_F \wp = x, c_{k,\phi}(\wp) = c_k \text{ for } k = 1, \ldots, r-1,$$
$$\wp \text{ splits completely in } F\big(A[m]\big)/F\}.$$

Then, because from Lemma 3.4 we know that $|c_{k,\phi}(\wp)| \le q^{(k/r)d_F \deg_F \wp}$, for any $k = 1, \ldots, r$, we obtain

$$\text{error} \le \sum_{\substack{y < \deg m \le d_F x/r \\ m \text{ square-free}}} \sum_{\substack{c \in A^{r-1} \\ |c_k| \le q^{(k/r)d_F \deg_F \wp},\ \text{for } k=1,\ldots,r-1}} \big|S_c(m)\big|.$$

From Lemma 3.3 we know that for each $\wp \in S_c(m)$ we have $m^k \mid c_{k,\phi}(\wp)$ for $k = 1, \ldots, r$, and from Lemma 3.5 we know that $c_{r,\phi}(\wp) = u_\wp p^{m_\wp} + d_1 c_{1,\phi}(\wp) + d_2 c_{2,\phi}(\wp) + \cdots + d_{r-1} c_{r-1,\phi}(\wp) + d_r$. Therefore,

$$\sum_{\substack{y < \deg m \le d_F x/r \\ m \text{ square-free}}} \sum_{\substack{c \in A^{r-1} \\ |c_k| \le q^{(k/r)d_F \deg_F \wp},\text{for } k=1,\ldots,r-1}} \big|S_c(m)\big|$$
$$\le \sum_{\substack{y < \deg m \le d_F x/r \\ m \text{ square-free}}} \sum_{\substack{c \in A^{r-1} \\ |c_k| \le q^{(k/r)d_F \deg_F \wp},\text{for } k=1,\ldots,r-1 \\ m^k | c_k,\text{for } k=1,\ldots,r-1}} \sum_{\substack{\wp \in \mathcal{P}_A \\ \deg_F \wp = x \\ c_{k,\phi}(\wp) = c_k,\text{for } k=1,\ldots,r-1 \\ m^r | c_{r,\phi}(\wp) = u_\wp p^{m_\wp} + d_1 c_{1,\phi}(\wp) + \cdots + d_{r-1} c_{r-1,\phi}(\wp) + d_r}} 1$$

$$\ll \sum_{\substack{y < \deg m \le d_F x/r \\ m \text{ square-free}}} \sum_{\substack{c \in A^{r-1} \\ |c_k| \le q^{(k/r)d_F \deg_F \wp},\text{for } k=1,\ldots,r-1 \\ m^k | c_k,\text{for } k=1,\ldots,r-1}} q^{d_F x - r \deg m} \tag{5.3}$$

$$\ll \sum_{\substack{y < \deg m \le d_F x/r \\ m \text{ square-free}}} q^{d_F x - r \deg m} \prod_{k=1}^{r-1} q^{(k/r)d_F x - k \deg m}$$

$$\ll \sum_{\substack{y < \deg m \le d_F x/r \\ m \text{ square-free}}} q^{d_F x - r \deg m} q^{\frac{r-1}{2} d_F x - \frac{(r-1)r}{2} \deg m}$$

$$\ll q^{\frac{r+1}{2} d_F x - \frac{r(r+1)-2}{2} y}.$$

(We remark that in the above computation we should have considered whether c_k is zero or not for each $k = 1, \ldots, r-1$, but in each of these 2^{r-1} cases the computation is similar and could be dealt with by induction.)

Since $|(O_E/mO_E)^*| \gg q^{e\deg m}/\log\deg m$ (see [11]), from Lemma 3.2 (see the remark after it) and Lemma 4.4 we get (see also [11] for all details)

$$\sum_{\deg m>y} \frac{\mu_q(m)r_m(x)}{n(m)} \ll \sum_{\deg m>y} \frac{\log\deg m}{q^{h^2 e\deg m}} \ll \frac{\log y}{q^{(h^2e-1)y}}. \tag{5.4}$$

From (5.1)–(5.4) we distinguish two cases.

(i) If $h^2e \geq \frac{r+1}{2}$, then we choose y such that $q^{(d_F x/2)+y} = q^{\frac{r+1}{2}d_F x - \frac{r^2+r-2}{2}y}$, that is,

$$y = \frac{1}{r+1}d_F x, \tag{5.5}$$

and from (5.2)–(5.4) we get

$$f_{\phi,F}(x) = c_{\phi,F}(x)\pi_F(x) + O(q^{\frac{r+3}{2r+2}d_F x}). \tag{5.6}$$

(ii) If $h^2e < \frac{r+1}{2}$, then we choose y such that $q^{(d_F x/2)+y} = q^{d_F x-(h^2e-1)y}$, that is,

$$y = \frac{1}{2h^2e}d_F x \tag{5.7}$$

(so the error term in (5.1) disappears), and from (5.2) and (5.4) we get

$$f_{\phi,F}(x) = c_{\phi,F}(x)\pi_F(x) + O(q^{\frac{h^2e+1}{2h^2e}d_F x}). \tag{5.8}$$

Thus, we are done with the proof of Theorem 1.1.

Now we prove Theorem 1.2. (We remark that to prove Theorem 1.2 we have to use Lemma 3.2 above, and not a weaker version of it, that is, [19, Lemma 3.2]: the reason is that in the proof of Theorem 1.2 we have to consider a sum over all monic polynomials m of A, and in the proof of Theorem 1.1 it is sufficient to consider a sum over only square-free monic polynomials m of A.)

From the definition of $f'_{\phi,F}(x)$ we get that

$$f'_{\phi,F}(x) = \sum_{m\in A} \pi_1\big(x, F\big(\phi[m]\big)/F\big),$$

where the sum is over monic polynomials m of A. Again, if $\wp$ splits completely in $F(\phi[m])$, then from Lemma 3.3 we deduce that $m^r \mid P_{\phi,\wp}(1)$. Because $\deg P_{\phi,\wp}(1) \leq d_F \deg_F \wp = d_F x$, it is sufficient to consider only monic polynomials $m \in A$ with $\deg m \leq d_F x/r$.

For $y = y(x)$ a real number with $y \leq d_F x/r$, we have

$$\begin{aligned} f'_{\phi,F}(x) &= \sum_{\deg m\leq d_F x/r} \pi_1\big(x, F\big(\phi[m]\big)/F\big) \\ &= \sum_{\deg m\leq y} \pi_1\big(x, F\big(\phi[m]\big)/F\big) + \sum_{y<\deg m\leq d_F x/r} \pi_1\big(x, F\big(\phi[m]\big)/F\big) \qquad (5.9) \\ &= \text{main} + \text{error}. \end{aligned}$$

From Theorem 4.2, we get

$$\text{main} = \sum_{\deg m \le y} \frac{r_m(x)}{n(m)} \pi_F(x) + \sum_{\deg m \le y} O\Big(\Big(\frac{g(m) r_m(x)}{n(m)} + 1\Big) \frac{q^{d_F x/2}}{x}\Big),$$

and from Lemmas 4.3 and 4.4 as above, we deduce that

$$\sum_{\deg m \le y} \Big(\frac{g(m) r_m(x)}{n(m)} + 1\Big) \ll \sum_{\deg m \le y} D(\phi) E(\phi) \deg m \ll x q^y.$$

Hence,

$$\text{main} = \pi_F(x) \Big(\sum_{\deg m \le y} \frac{r_m(x)}{n(m)}\Big) + O(q^{(d_F x/2)+y}). \tag{5.10}$$

Now the error can be estimated as above by doing the computations not only for square-free monic polynomials $m \in A$, but also for all monic polynomials $m \in A$, and we get that

$$\text{error} \ll q^{\frac{r+1}{2} d_F x - \frac{r(r+1)-2}{2} y}. \tag{5.11}$$

As above we have that

$$\sum_{\deg m > y} \frac{r_m(x)}{n(m)} \ll \sum_{\deg m > y} \frac{\log \deg m}{q^{h^2 e \deg m}} \ll \frac{\log y}{q^{(h^2 e - 1) y}}, \tag{5.12}$$

and by considering again the cases (i) and (ii) we get that

$$f'_{\phi,F}(x) = c'_{\phi,F}(x) \pi_F(x) + O(q^{\frac{h^2 e + 1}{2h^2 e} d_F x}). \tag{5.13}$$

Thus, we are done with the proof of Theorem 1.2.

References

[1] A. Akbary and D. Ghioca, *A geometric variant of Titchmarsh divisor problem*, Int. J. Number Theory **8** (2012), 53–69. MR 2887882.

[2] A. C. Cojocaru and M. R. Murty, *Cyclicity of elliptic curves modulo $\wp$ and elliptic curve analogues of Linnik's problem*, Math. Ann. **330** (2004), 601–625. MR 2099195.

[3] A. C. Cojocaru and A. M. Shulman, *An average Chebotarev density theorem for generic rank* 2 *Drinfeld modules with complex multiplication*, J. Number Theory **133** (2013), 897–914. MR 2997774. DOI 10.1016/j.jnt.2012.07.001.

[4] C. David, *Frobenius distributions of Drinfeld modules of any rank*, J. Number Theory **90** (2001) 329–340. MR 1858082. DOI 10.1006/jnth.2000.2664.

[5] A. T. Felix and M. R. Murty, *On the asymptotics for invariants of elliptic curves modulo p*, J. Ramanujan Math. Soc. **28** (2013), 271–298. MR 3113386.

[6] M. Fried and M. Jarden, *Field Arithmetic*, 2nd ed., Ergeb. Math. Grenzgeb. (3) **11**, Springer, Berlin, 2005. MR 2102046.

[7] W. Gajda and S. Petersen, *Independence of ℓ-adic Galois representations over function fields*, Compos. Math. **149** (2013), 1091–1107. MR 3078639.

[8] F. Gardeyn, *Une borne pour l'action de l'inertie sauvage sur la torsion d'un module de Drinfeld*, Arch. Math. (Basel) **79** (2002), 241–251. MR 1944948. DOI 10.1007/s00013-002-8310-5.

[9] E.-U. Gekeler, *On finite Drinfeld modules*, J. Algebra **141** (1991), 187–203. MR 1118323.

[10] D. Goss, *Basic Structures of Function Field Arithmetic*, Ergeb. Math. Grenzgeb. (3) **35**, Springer, Berlin, 1996. MR 1423131. DOI 10.1007/978-3-642-61480-4.

[11] W. Kuo and Y.-R. Liu, *Cyclicity of finite Drinfeld modules*, J. Lond. Math. Soc. (2) **80** (2009), 567–584. MR 2559117. DOI 10.1112/jlms/jdp043.

[12] M. R. Murty, *On Artin's conjecture*, J. Number Theory **16** (1983), 147–168. MR 0698163. DOI 10.1016/0022-314X(83)90039-2.

[13] R. Pink and E. Rütsche, *Adelic openness for Drinfeld modules in generic characteristic*, J. Number Theory **129** (2009), 882–907. MR 2499412.

[14] ———, *Image of the group ring of the Galois representation associated to Drinfeld modules*, J. Number Theory **129** (2009), 866–881. MR 2499411.

[15] J.-P. Serre, *Résumé des cours de l'année scolaire*, Annuaire du Collège de France **78** (1979), 67–70.

[16] ———, *Une critere d'indépendance pour une famille de représentations l-adiques*, Comment. Math. Helv. **88** (2013), 541–554. MR 3093502.

[17] E. C. Titchmarsh, *A divisor problem*, Rend. Palermo **54** (1930), 414–429.

[18] C. Virdol, *Cyclic components of abelian varieties (mod $\wp$)*, J. Number Theory **159** (2016), 426–433. MR 3412731.

[19] ———, *Drinfeld modules and subfields of division fields*, Houston J. Math. **42** (2016), 211–221. MR 3502779.

Department of Mathematics, Yonsei University, Seoul, South Korea;
cristian.virdol@gmail.com