PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 148, Number 9, September 2020, Pages 3733–3747
https://doi.org/10.1090/proc/15002
Article electronically published on April 28, 2020

A PRIME ANALOGUE ERDŐS-POMERANCE RESULT FOR DRINFELD MODULES WITH ARBITRARY ENDOMORPHISM RINGS

WENTANG KUO AND DAVID TWEEDLE

(Communicated by Matthew Papanikolas)

ABSTRACT. Let $\mathbf{k}$ be a global function field, and let $\mathbf{A}$ be the elements of $\mathbf{k}$ regular outside a fixed place ∞.

Let $\phi : \mathbf{A} \to K\{\tau\}$ be a Drinfeld module of generic characteristic and rank n. For a prime $\wp$ of K of good reduction, let $\mathbb{F}_\wp$ be the residue field at $\wp$, and let $\chi_{\mathbf{A}}\big(\phi(\mathbb{F}_\wp)\big)$ be the Euler-Poincaré characteristic of $\mathbb{F}_\wp$ viewed as an $\mathbf{A}$-module.

We determine the normal order of the number of distinct prime ideals of $\mathbf{A}$ dividing $\chi_{\mathbf{A}}\big(\phi(\mathbb{F}_\wp)\big)$, denoted by $\omega_{\mathbf{A}}\Big(\chi_{\mathbf{A}}\big(\phi(\mathbb{F}_\wp)\big)\Big)$, as $\wp$ runs over primes of K of degree x with a specified splitting behaviour.

Furthermore, let $a \in K$ be non-torsion for ϕ, and let $f_a(\wp)$ be the Euler-Poincaré characteristic of the submodule of $\phi(\mathbb{F}_\wp)$ generated by a modulo $\wp$. We also consider the problem of determining the distribution of $\omega_{\mathbf{A}}\big(f_a(\wp)\big)$ as $\wp$ runs over primes of K of degree x with a specified splitting behaviour.

Note that we do not make restrictions on $\mathbf{A}$, ϕ, or its endomorphism ring $\mathrm{End}_{K^{\mathrm{sep}}}(\phi)$.

1. INTRODUCTION

Consider $\omega(n)$, the number of distinct prime divisors of a positive integer n. In 1934, Turán [30] proved that

$$\sum_{n\le x}(\omega(n)-\log\log x)^2 \ll x\log\log x$$

as $x\to\infty$.

This implies the earlier result of Hardy and Ramanujan [13] that for all $\epsilon>0$

$$\#\{n\le x \mid \ |\omega(n)-\log\log(n)|>\epsilon\log\log n\}=\mathrm{o}(x)$$

as $x\to\infty$, where $\#S$ means the number of elements of the set S.

Now, let

$$G(u)=\frac{1}{\sqrt{2\pi}}\int_{-\infty}^{u} e^{-t^2/2}\ \mathrm{d}t$$

be the cumulative distribution function of the normal distribution with mean 0 and standard deviation 1.

Received by the editors August 28, 2019, and, in revised form, January 9, 2020.
2010 *Mathematics Subject Classification.* Primary 11G09; Secondary 11R45, 11N36.
The research of the first author was supported by an NSERC discovery grant RGPIN-2015-03709.

This probabilistic study of arithmetical functions led Erdős and Kac [8] to prove that $\omega(n)$ satisfies

$$\lim_{x\to\infty}\frac{1}{x}\#\left\{n\le x \;\middle|\; \frac{\omega(n)-\log\log n}{\sqrt{\log\log n}}\le u\right\}=G(u).$$

The study of arithmetical functions using probabilistic ideas, called probabilistic number theory, eventually yielded a generalised Erdős-Kac theorem, which was discovered independently by Kubilius [17] and Shapiro [28]. The interested reader can review Elliott's monograph [4, 5].

Returning to Turán's result, Erdős [7] proved that

$$\sum_{p\le x}(\omega(p-1)-\log\log x)^2\ll\pi(x)\log\log x$$

as $x\to\infty$. This is a prime analogue of Turán's result. Naturally, one then tries to determine the distribution of $\omega(p-1)$.

Halberstam in [12] proved that

$$\lim_{x\to\infty}\frac{1}{\pi(x)}\#\left\{p\le x \;\middle|\; \frac{\omega(p-1)-\log\log x}{\sqrt{\log\log x}}\le u\right\}=G(u),$$

by considering the moments of $\omega(p-1)$.

Informally, the number of distinct prime factors of $p-1$ for $p\le x$ follows a normal distribution with mean $\log\log x$ and standard deviation $\sqrt{\log\log x}$.

If we write $p-1=\#\mathbb{F}_p^*$, then we see that Erdős and Halberstam are studying the distribution of $\omega(\#\mathbb{F}_p^*)$ as p varies. This may be generalised in several different ways. One consideration is to replace $p-1$ with $\varphi(n)$. Note that the framework of Kubilius and Shapiro does not apply here. But nonetheless, Erdős and Pomerance in [6] showed that

$$\lim_{x\to\infty}\frac{1}{x}\#\left\{n\le x \;\middle|\; \frac{\omega\big(\varphi(n)\big)-(1/2)(\log\log x)^2}{(1/\sqrt{3})(\log\log x)^{3/2}}\le u\right\}=G(u).$$

But there are other fruitful investigations. In particular, think of $\mathbb{F}_p^*$ as the $\mathbb{F}_p$ points of the multiplicative group. Then replace the multiplicative group with another algebraic group (see especially [15] for a helpful framework). To motivate our study, let $E/\mathbb{Q}$ be an elliptic curve defined over the rationals. Then we may try to determine the normal order of $N_p=\#E(\mathbb{F}_p)$ for primes $p\le x$. On the generalized Riemann hypothesis (GRH) and assuming E has no complex multiplication, Miri and Murty [24] established that

$$\sum_{p\le x}(\omega(N_p)-\log\log x)^2\ll\pi(x)\log\log x.$$

Then if E has complex multiplication, Liu [22] proved (unconditionally) that

$$\sum_{p\le x}(\omega(N_p)-\log\log x)^2\ll\pi(x)\log\log x$$

and then further established the Erdős-Kac type result [23] (on the GRH if E does not have complex multiplication)

$$\lim_{x\to\infty}\frac{1}{\pi(x)}\#\left\{p\le x \;\middle|\; \frac{\omega(N_p)-\log\log x}{\sqrt{\log\log x}}\le u\right\}=G(u).$$

The goal of this paper is to prove a Drinfeld module analogue to the above result in the case of non-trivial endomorphism ring. This is an analogue to the above theorem for elliptic curves with complex multiplication established by Liu. Once this is done, we will also prove an Erdős-Pomerance type result. This is a generalization of the work of the first author with Kuan and Yao [16].

We will now introduce the notation that we need for our main theorems.

2. Notation

Let r be a prime power, and let $\mathbb{F}_r$ be the finite field with r elements. Let X be a smooth, projective curve over $\mathbb{F}_r$ with a closed point ∞, and let $\mathbf{A}$ be the ring of functions on X regular everywhere, except perhaps ∞. Let K be an $\mathbf{A}$-field of generic characteristic, and denote the corresponding copy of $\mathbf{A}$ inside K by A.

The fraction field of A will be k, and so K/k is a field extension. Assume that K/k is a finite extension, in particular, K is a global function field. Fix a separable closure K^{sep} of K. Let $\phi : \mathbf{A} \to K\{\tau\}$ be a Drinfeld module of rank n. Let $\mathbf{B} = \text{End}_{K^{\text{sep}}}(\phi)$ be the endomorphism ring of ϕ. There exists a finite extension K'/K such that $\mathbf{B} \subseteq K'\{\tau\}$, and let $\psi : \mathbf{B} \to K'\{\tau\}$ be the Drinfeld module of rank n' given by inclusion, where $n = n'v$. In fact, strictly speaking ψ is not necessarily a Drinfeld module as $\mathbf{B}$ may not be the ring of integers of $\mathbf{A}$ in $\mathbf{B} \otimes_{\mathbf{A}} \mathbf{k}$. See [11, Proposition 4.7.19].

For a place $\wp$ of K, either $\wp$ lies over the place ∞ of k (in which case we say that $\wp$ is an infinite place) or else it lies over a finite place of k, which then corresponds to a prime ideal $\mathfrak{p}$ of $\mathbf{A}$. Let $O_\wp$ be the local ring corresponding to $\wp$ with $m_\wp$ its maximal ideal and $\mathbb{F}_\wp$ the residue field. If there exists $u \in K$ so that for all $a \in \mathbf{A}$, ρ_a has all coefficients in $O_\wp$ and leading coefficient in $O_\wp - m_\wp$ where $\rho = u\phi u^{-1}$, then we say that ϕ has good reduction at $\wp$. Clearly, ϕ has good reduction at all but finitely many places $\wp$, and only finitely many of those require $u \neq 1$.

The $\mathbf{A}$-characteristic of $\mathbb{F}_\wp$ will be denoted by $\mathfrak{p}$. For an $\mathbf{A}$-module N of finite length, let $\chi_{\mathbf{A}}(N)$ denote the Euler-Poincaré characteristic of N. Recall that $\chi_{\mathbf{A}}(\cdot)$ is determined by the two properties that $\chi_{\mathbf{A}}(\mathbf{A}/I) = I$ for all ideals $I \subseteq \mathbf{A}$, and $\chi_{\mathbf{A}}(M) = \chi_{\mathbf{A}}(N)\chi_{\mathbf{A}}(N')$ if there is an exact sequence of $\mathbf{A}$-modules

$$0 \to N \to M \to N' \to 0.$$

Notice that if we consider $\chi = \chi_{\mathbb{Z}}$, then $\chi\big(E(\mathbb{F}_p)\big) = \big(N_p\big)$, where $\big(N_p\big)$ is the principal ideal of $\mathbb{Z}$ generated by $N_p = \#E(\mathbb{F}_p)$. So, $\chi_{\mathbf{A}}\big(\phi(\mathbb{F}_\wp)\big)$ is a natural Drinfeld module analogue to $N_p = \#E(\mathbb{F}_p)$.

To demonstrate the analogy further, recall Taelman's seminal work [29], in which he proves a class number formula for Drinfeld modules. For an $\mathbf{A}$-module M, let $|M|$ be a monic generator of $\chi_{\mathbf{A}}(M)$. Then define $L(\phi/\mathbf{A}) = \prod_{\mathfrak{p}} \frac{|\mathbf{A}/\mathfrak{p}|}{|\phi(\mathbf{A}/\mathfrak{p})|}$. Taelman then proves a formula for $L(\phi/\mathbf{A})$ in terms of a certain regulator and a class module. Of course, there have since been many developments. For example, see [1].

We now turn our attention back to Erdős-Kac type results.

For an ideal $\mathfrak{a}$ of $\mathbf{A}$, denote by $\omega_{\mathbf{A}}(\mathfrak{a})$ the number of distinct prime ideals dividing $\mathfrak{a}$. In this paper, we consider the distribution of $\omega_{\mathbf{A}}\Big(\chi_{\mathbf{A}}\big(\phi(\mathbb{F}_\wp)\big)\Big)$ as $\wp$ runs over primes of K of degree x (where x becomes large).

Assume that $\mathbf{A} = \mathbb{F}_q[T]$, let $K = \mathbb{F}_q(T)$, and assume that $\text{End}_{K^{\text{sep}}}(\phi) = \mathbf{A}$. The following theorem was proved by Liu and the first author [19] in the case that ϕ is

the Carlitz module, and generalised to the case that the rank of ϕ is arbitrary by Liu and the first author [20] and independently by Cojocaru [2].

Theorem 2.1. *Assume that* $\mathbf{A} = \mathbb{F}_q[T]$, $\mathbf{B} = \mathbf{A}$, *and* $K = \mathbb{F}_q(T)$. *Then*

$$\sum_{\deg \wp \leq x} \left(\omega_{\mathbf{A}}\left(\chi_{\mathbf{A}}\left(\phi(\mathbb{F}_\wp)\right)\right) - \log x\right)^2 \ll \pi_K(x) \log x.$$

So the first goal of this paper is to remove the restriction that $\mathbf{A} = \mathbb{F}_q[T]$, and remove the restriction that $\mathrm{End}(\phi) = \mathbf{A}$. In fact, it is the latter condition which is non-trivial.

We will now state the first main result of our paper. Let $c \subseteq \mathrm{Gal}(K'/K)$ be a fixed conjugacy class. Fix $g \in c$, and let $E \subseteq K'$ be such that $\mathrm{Gal}(K'/E) = \langle g \rangle$. Let $j(K)$, $j(E)$, and $j(K')$ denote the degrees of the constant fields of K, E, and K' over $\mathbb{F}_q$. Define

$$\mathcal{P}(K, c, x) = \{\wp \text{ a place of } K \mid \deg \wp = x, (\wp, K'/K) = c\}.$$

Theorem 2.2. *As* $x \equiv j(E) \bmod j(K')$ *and* $x \to \infty$,

$$\lim_{x\to\infty} \frac{1}{\#\mathcal{P}(K,c,x)} \left\{ \wp \in \mathcal{P}(K,c,x) \;\middle|\; \frac{\omega_{\mathbf{A}}\left(\chi_{\mathbf{A}}\left(\phi(\mathbb{F}_\wp)\right)\right) - \log x}{\sqrt{\log x}} \leq u \right\} = G(u).$$

Remark 2.3. A brief word on the integers $j(E)$ and $j(K')$. They represent the possibility that part of the extension K'/K may be a constant field extension. In previous works [2, 16, 19, 20], it was assumed that $K' = K$ and so this possibility could not occur.

Now, fix $a \in K$ any non-torsion point for ϕ, and let $f_a(\wp)$ denote the Euler-Poincaré characteristic of the submodule of $\phi(\mathbb{F}_\wp)$ generated by a. The following is a generalization of part of the work of the first author and Kuan and Yao in [16].

Theorem 2.4. *As* $x \equiv j(E) \bmod j(K')$ *and* $x \to \infty$,

$$\lim_{x\to\infty} \frac{1}{\#\mathcal{P}(K,c,x)} \left\{ \wp \in \mathcal{P}(K,c,x) \;\middle|\; \frac{\omega_{\mathbf{A}}\left(f_a(\wp)\right) - \log x}{\sqrt{\log x}} \leq u \right\} = G(u).$$

We first show in Section 3 that if $\mathbf{k}$ is the fraction field of $\mathbf{A}$, $\mathrm{End}_K(\phi) = \mathbf{A}'$ with $\mathbf{k}'$ the fraction field of $\mathbf{A}'$, and $\mathbf{l}$ the fraction field of $\mathbf{B}$, then $\mathrm{Gal}(K'/K) \cong \mathrm{Gal}(\mathbf{l}/\mathbf{k}')$. Of course, $\mathbf{k} \subseteq \mathbf{k}'$ can be almost arbitrary (in particular, it may be completely inseparable, and it may not be a normal extension).

First, we choose $g \in c$, and let E be the fixed field of $\langle g \rangle \subseteq \mathrm{Gal}(K'/K)$. Let $\mathbf{E} \subseteq \ell$ be the subfield such that $\mathrm{Gal}(\ell/\mathbf{E}) = \langle g \rangle$. Let $\mathbf{A}' = \mathbf{E} \cap \mathbf{B}$, and let $\phi' : \mathbf{A}' \to E\{\tau\}$ be the corresponding Drinfeld module. Let $\mathfrak{q}$ be a prime of $\mathbf{A}'$, and let $\mathcal{C}_\mathfrak{q} \subseteq \mathrm{Gal}(K'(\phi'[\mathfrak{q}])/E)$ comprise those σ such that $\sigma|_{K'} = g$ and $\sigma\lambda = \lambda$ for some $0 \neq \lambda \in \phi'[\mathfrak{q}]$. We are able to compute the size of $\mathcal{C}_\mathfrak{q}$ relative to $[K'(\phi'[\mathfrak{q}]) : E]$.

In Section 4, we are able to estimate the number of primes $\wp'$ of E such that $(\wp', K'/E) = g$, and such that $\mathfrak{q}$ divides the Euler-Poincaré characteristic of $\phi'(\mathbb{F}_{\wp'})$ using the Chebotarev density theorem.

Then we are able to show that the main contribution to the average value of $\omega_{\mathbf{A}}\left(\chi_{\mathbf{A}}\left(\phi(\mathbb{F}_\wp)\right)\right)$ as $(\wp, K'/K) = c$ comes from primes of $\mathbf{A}'$. We may compare this to the work of Liu in [23]. In Liu's work, all primes contribute equally to the

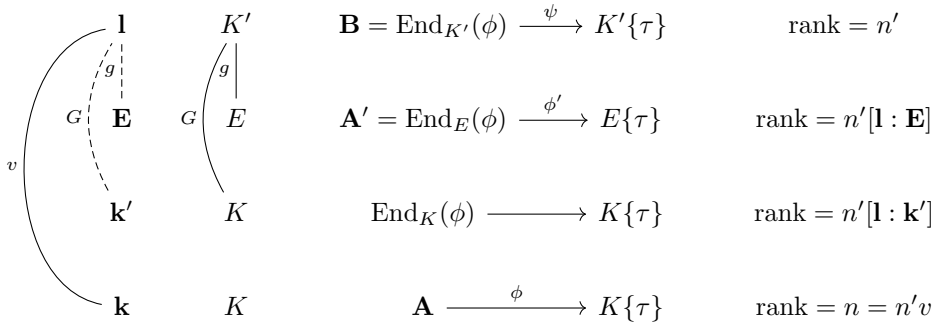
average value of $\omega\big(\#E(\mathbb{F}_p)\big)$ as p ranges over primes of supersingular reduction. This is comparable to the case when $E = K$. In [23], only primes which are split contribute to $\omega\big(\#E(\mathbb{F}_p)\big)$ as p ranges over primes which have ordinary reduction. This is analogous to the case where $E = K'$ for our situation. Furthermore, for Drinfeld modules, only the case that $K' = K$ has been done before (see [20] and [2]). In our work, there are many "in between" situations which are not covered by the two extreme cases of completely inert and completely split. Yet we are able to dispose of all the different situations at once.

In Section 5, we are able to determine the distribution of $\omega_{\mathbf{A}}\Big(\chi_{\mathbf{A}}\big(\phi(\mathbb{F}_\wp)\big)\Big)$ as $\deg \wp = x$ and $(\wp, K'/K) = c$. In Section 6, we generalise the work of [16] using the considerations of the previous sections as well as work contained mostly in [18].

3. Galois theory considerations

Let us fix $g \in \mathrm{Gal}(K'/K)$, and let E be the subfield of K' so that $\mathrm{Gal}(K'/E)$ is generated by g. Corresponding to each field K', E, K are the endomorphism rings $\mathbf{B} = \mathrm{End}_{K'}(\phi)$, $\mathbf{A}' = \mathrm{End}_E(\phi)$, $\mathrm{End}_K(\phi) \supseteq \mathbf{A}$. Corresponding to each endomorphism ring are the fields $\mathbf{l} = \mathbf{B}\otimes_{\mathbf{A}}\mathbf{k}$, $\mathbf{E} = \mathbf{A}'\otimes_{\mathbf{A}}\mathbf{k}$, and $\mathbf{k}' = \mathrm{End}_K(\phi)\otimes_{\mathbf{A}}\mathbf{k}$.

The following diagram shows the relationship between the different endomorphism rings, their fraction fields (in bold face), and their fields of definition. The dotted lines represent the computation of Galois groups which will be tackled in Proposition 3.1.



Proposition 3.1. *Let $\phi : \mathbf{A} \to K\{\tau\}$ be a Drinfeld module. Let $\mathbf{k}$ be the fraction field of $\mathbf{A}$. Let $\mathrm{End}_K(\phi)$ be the ring of endomorphisms defined over K, and let $\mathbf{k}' = \mathrm{End}_K(\phi)\otimes_{\mathbf{A}}\mathbf{k}$. Similarly, let $\mathrm{End}_{K^{\mathrm{sep}}}(\phi) = \mathbf{B}$, and let $\mathbf{l} = \mathbf{B}\otimes_{\mathbf{A}}\mathbf{k}$.*

Then $\mathbf{k}' \subseteq \mathbf{l}$ is a Galois extension. Furthermore, there exists a field K' such that $\mathrm{Gal}(\mathbf{l}/\mathbf{k}') \cong \mathrm{Gal}(K'/K)$ and $\mathbf{B} = \mathrm{End}_{K'}(\phi)$.

Proof. First, check that $\mathrm{Gal}(K^{\mathrm{sep}}/K)$ acts on $\mathbf{B} \subseteq K^{\mathrm{sep}}\{\tau\}$ (by acting on the coefficients) while fixing $\mathrm{End}_K(\phi)$. Then check that this defines a homomorphism $\rho : \mathrm{Gal}(K^{\mathrm{sep}}/K) \to \mathrm{Aut}(\mathbf{l}/\mathbf{k}')$. The image of this homomorphism must be of the form $\mathrm{Gal}(\mathbf{l}/F)$. Then notice that elements of $F \cap \mathbf{B}$ are fixed by all $\sigma \in \mathrm{Gal}(K^{\mathrm{sep}}/K)$, and hence $F \cap \mathbf{B} \subseteq K\{\tau\}$, which implies that $F = \mathbf{k}'$, as required. Then find K' such that $\rho : \mathrm{Gal}(K'/K) \to \mathrm{Gal}(\mathbf{l}/\mathbf{k}')$ is an isomorphism. Necessarily, $\mathbf{B} = \mathrm{End}_{K'}(\phi)$. □

Remark 3.2. We have three Drinfeld modules appearing, $\phi : \mathbf{A} \to K\{\tau\}$, $\phi' : \mathbf{A}' \to E\{\tau\}$, and $\psi : \mathbf{B} \to K'\{\tau\}$. The Drinfeld module ψ is the "full CM" Drinfeld module. If we want to apply the open image theorem of Pink and Rütsche [26], we can only apply it to ψ. The Drinfeld module ϕ' is a bridge between ϕ and ψ. What will happen is that $\wp$ will be a prime of K such that $(\wp, K'/K) = c$, $\wp'$ will be a prime of E such that $(\wp', K'/E) = g$, and so the structure of $\phi(\mathbb{F}_\wp)$ as an $\mathbf{A}$-module will just be the restriction of the $\mathbf{A}'$-module structure of $\phi'(\mathbb{F}_{\wp'})$, since $\mathbb{F}_\wp \cong \mathbb{F}_{\wp'}$ as fields. Then we will be in the very specialised situation of $\mathrm{Gal}(K'/E)$ being generated by g and in this situation we are able to bridge the gap between ϕ' and ψ using semilinear algebra considerations.

Let us proceed with the technical details.

Let $\mathfrak{q}$ be a prime of $\mathbf{A}'$. Let $K_\mathfrak{q} = K'(\phi'[\mathfrak{q}])$. We must construct a certain conjugacy class $\mathcal{C}_\mathfrak{q}$ and estimate its size relative to $[K_\mathfrak{q} : E]$.

Recall that $\mathrm{Gal}(K'/E)$ is a cyclic group generated by g. Let f be the order of g. Let $j(K')$ denote the degree of the constant field of K' over $\mathbb{F}_r$, and similarly for $j(E)$ and $j(K)$.

Factorise $\mathfrak{q}\mathbf{B}$ as $\mathfrak{q}\mathbf{B} = \mathcal{Q}_1 \cdots \mathcal{Q}_s$. Let u be the inertial degree $u = [\mathbf{B}/\mathcal{Q}_1 : \mathbf{A}'/\mathfrak{q}]$ and note that $su = f$. Furthermore, we may reorder $\mathcal{Q}_1, \ldots, \mathcal{Q}_s$ such that $g(\mathcal{Q}_1) = \mathcal{Q}_2$, $g(\mathcal{Q}_2) = \mathcal{Q}_3$, …, $g(\mathcal{Q}_{s-1}) = \mathcal{Q}_s$ since g generates the Galois group $\mathrm{Gal}(\mathbf{l}/\mathbf{k}')$ and this Galois group must permute the primes lying above $\mathfrak{q}$ transitively. Now, we also see that we may identify

$$\mathbf{B}/\mathcal{Q}_1 \overset{g}{\cong} \mathbf{B}/\mathcal{Q}_2 \overset{g}{\cong} \cdots \overset{g}{\cong} \mathbf{B}/\mathcal{Q}_s$$

as

$$x + \mathcal{Q}_i \mapsto g(x) + g(\mathcal{Q}_i) = g(x) + \mathcal{Q}_{i+1}.$$

Finally, if we suppose that we extend g to an element $g' \in \mathrm{Gal}(K^{\mathrm{sep}}/E)$ whose restriction to K' is g, then we may also use g' to identify

$$\psi[\mathcal{Q}_1] \overset{g'}{\cong} \psi[\mathcal{Q}_2] \overset{g'}{\cong} \cdots \overset{g'}{\cong} \psi[\mathcal{Q}_s]$$

as $\mathbf{B}/\mathcal{Q}_i$-modules in a way that agrees with the above identification. This identification is achieved by noting that

$$g'\big(\psi_b(\lambda)\big) = \psi_{g(b)}\big(g'(\lambda)\big)$$

for all $b \in \mathbf{B}$.

Recall the following consequence of the open image theorem of Pink and Rütsche.

Theorem 3.3 ([26, Theorem 0.1])**.** *There exists an element $M \in \mathbf{A}'$ such that if $\mathfrak{a}$ is an ideal of $\mathbf{A}'$ and $\gcd(\mathfrak{a}, M) = 1$, then*

$$\mathrm{Gal}(K_\mathfrak{a}/K') \cong \mathrm{GL}_{n'}(\mathbf{B}/\mathfrak{a}\mathbf{B})$$

and $K_\mathfrak{a}/K'$ is a geometric extension (i.e., the field of constants of $K_\mathfrak{a}$ is equal to the field of constants of K').

Remark 3.4. Recall that n' is the rank of $\psi : \mathbf{B} \to K'\{\tau\}$, so that $\psi[\mathfrak{a}\mathbf{B}] \cong (\mathbf{B}/\mathfrak{a}\mathbf{B})^{n'}$ as $\mathbf{B}$-modules.

Remark 3.5. If $M \in \mathbf{A}'$ satisfies the statement of Theorem 3.3, then so does any M' such that $M | M'$. Therefore, we may replace M with M' if necessary. We will be thinking of M as an element whose divisors are all the "bad" primes of $\mathbf{A}'$. If

we ever need to exclude a prime $\mathfrak{q}$ from consideration, we can simply replace M by xM, where $0 \neq x \in \mathfrak{q}$.

Proposition 3.6. *Recall that g is a generator of $\mathrm{Gal}(K'/E)$ and let $\lambda_1, \ldots, \lambda_{n'}$ be a basis of $\phi'[\mathfrak{q}]$ as a $\mathbf{B}/\mathfrak{q}\mathbf{B}$-module. Suppose that $\gcd(\mathfrak{q}, M) = 1$. Then we can choose an extension of g, say $g' \in \mathrm{Gal}(K^{\mathrm{sep}}/E)$, so that $g'(\lambda_i) = \lambda_i$.*

Proof. Let $h \in \mathrm{Gal}(K^{\mathrm{sep}}/E)$ be such that $h|_{K'} = g$. In general if $g'|_{K'}$ equals g, then $T = g'h^{-1}$ is a $\mathbf{B}/\mathfrak{q}\mathbf{B}$-linear operator on $\phi'[\mathfrak{q}]$. It is clear that $\{h(\lambda_i)\}$ is a basis of $\phi'[\mathfrak{q}]$ if $\{\lambda_i\}$ is a basis of $\phi[\mathfrak{q}]$.

By the open image theorem proved by Pink and Rütsche in [26], choose $g' \in \mathrm{Gal}(K^{\mathrm{sep}}/E)$ such that $U = g'h^{-1}$ when restricted to $\phi'[\mathfrak{q}]$ is the change of basis from $\{h(\lambda_i)\}$ to $\{\lambda_i\}$. Now $g'(\lambda_i) = \lambda_i$, as required. □

Remark 3.7. Compare the above proposition to [3] and [21] (in which the field of coefficients is an algebraically closed field). The main difference is that in our situation not all g-semilinear operators may be viewed as Frobenius operators. In fact, the g' we produce has the property that $(g')^k$ is the identity in $\mathrm{Gal}(K_{\mathfrak{q}}/E)$.

Corollary 3.8. *Suppose that $\gcd(\mathfrak{q}, M) = 1$. Then $\mathrm{Gal}(K_{\mathfrak{q}}/K')$ is isomorphic to $\mathrm{GL}_{n'}(\mathbf{B}/\mathfrak{q}\mathbf{B})$. Furthermore,*

$$\mathrm{Gal}(K_{\mathfrak{q}}/E) \cong \mathrm{Gal}(K_{\mathfrak{q}}/K') \rtimes \mathrm{Gal}(K'/E).$$

We now construct the conjugacy class $\mathcal{C}_{\mathfrak{q}}$ and our goal is to find its size relative to $[K_{\mathfrak{q}} : E]$.

Let $\mathcal{C}_{\mathfrak{q}} \subseteq \mathrm{Gal}(K_{\mathfrak{q}}/E)$ consist of those σ such that $\sigma|_{K'} = g$, and such that $\sigma(\lambda) = \lambda$ for some $0 \neq \lambda \in \phi'[\mathfrak{q}]$.

Therefore, for a square-free ideal $\mathfrak{n}$ of $\mathbf{A}'$, let $\mathcal{C}_{\mathfrak{n}} = \prod \mathcal{C}_{\mathfrak{q}} \subseteq (\prod \mathrm{Gal}(K_{\mathfrak{q}}/K')) \rtimes \mathrm{Gal}(K'/E)$. Furthermore, we will assume that $\gcd(\mathfrak{n}, M) = 1$.

Proposition 3.9. *Suppose that $\sigma \in \mathrm{Gal}(K_{\mathfrak{q}}/E)$ and $\sigma|_{K'} = g$. Let $h = g^s$ so that $\sigma^s|_{K'} = h$. Recall that*

$$\phi'[\mathfrak{q}] = \psi[\mathcal{Q}_1] \oplus \cdots \oplus \psi[\mathcal{Q}_s].$$

Then $\sigma(\lambda) = \lambda$ for some $0 \neq \lambda \in \phi'[\mathfrak{q}]$ if and only if $\sigma^s(\lambda_1) = \lambda_1$ for some $0 \neq \lambda_1 \in \psi[\mathcal{Q}_1]$.

Proof. Suppose now $0 \neq \lambda \in \phi'[\mathfrak{q}]$ and $\sigma\lambda = \lambda$. Write $\lambda = \lambda_1 + \lambda_2 + \cdots + \lambda_s$ according to the decomposition $\phi'[\mathfrak{q}] = \psi[\mathcal{Q}_1] \oplus \psi[\mathcal{Q}_2] \oplus \cdots \oplus \psi[\mathcal{Q}_s]$. Notice that $\sigma\lambda_1 = \lambda_2$, $\sigma\lambda_2 = \lambda_3$, …, $\sigma\lambda_s = \lambda_1$. It follows that $\sigma^s\lambda_1 = \lambda_1$ and also if $\sigma^s\lambda_1 = \lambda_1$ for some $0 \neq \lambda_1 \in \psi[\mathcal{Q}_1]$, then $\sigma\lambda = \lambda$, where $\lambda = \lambda_1 + \sigma\lambda_1 + \cdots + \sigma^{s-1}\lambda_1$. □

Notice that h must be the Frobenius automorphism of $\mathbf{B}/\mathcal{Q}_1$ over $\mathbf{A}'/\mathfrak{q}$ and σ^s is an h-semilinear operator on $\psi[\mathcal{Q}_1]$.

Proposition 3.10. *Write $\sigma = Tg$, where $T : \phi'[\mathfrak{q}] \to \phi'[\mathfrak{q}]$ is $\mathbf{B}$-linear, and write $\sigma^s = Uh$, where $U : \psi[\mathcal{Q}_1] \to \psi[\mathcal{Q}_1]$ is $\mathbf{B}$-linear. Then decompose $T = T_1 \oplus \cdots \oplus T_s$ and set $T'_s = gT_sg^{-1}$, $T'_{s-1} = g^2T_{s-1}g^{-2}$, …, $T'_2 = g^{s-1}T_2g^{-s+1}$ (in fact, it is more accurate to write $T'_i = hg^{-(i-1)}T_ig^{i-1}h^{-1}$). Then*

$$U = T_1T'_sT'_{s-1}\cdots T'_2.$$

In particular, if U is fixed, then there are $|\mathrm{GL}_{n'}(\mathbf{B}/\mathcal{Q}_1)|^{s-1}$ elements σ of $\mathrm{Gal}(K_{\mathfrak{q}}/E)$ such that $\sigma|_{K'} = g$ and $\sigma^s = Uh$.

Proof. Notice that $Uh = \sigma^s$ and $T_1 T_s' \cdots T_2' h = \sigma^s$. Furthermore, in the equation

$$U = T_1 T_s' \cdots T_2'$$

any choice of s of the variables determines the last. □

Now it remains to calculate the number of $U \in \mathrm{Gal}(K_{\mathcal{Q}_1}/K')$ such that $Uh\lambda = \lambda$ for some $0 \neq \lambda \in \psi[\mathcal{Q}_1]$.

(1) $\mathbb{F}$ — the field $\mathbf{A}'/\mathfrak{q}$, a finite field with q elements.
(2) $\mathbb{K}$ — the field $\mathbf{B}/\mathcal{Q}_1$, a field extension of $\mathbb{F}$ of degree u.
(3) V — $\psi[\mathcal{Q}_1]$, a $\mathbb{K}$-vector space of dimension n'.
(4) h — the Frobenius of $\mathbb{K}/\mathbb{F}$, extended to V by choosing a basis to be fixed by h. Note that in this situation, V may be identified with a field extension of $\mathbb{K}$, and h a Frobenius operator on V (see [3]).
(5) $G = \mathrm{GL}(V)$ — the $\mathbb{K}$-linear invertible transformations from V to V.
(6) $C \subseteq G$ — the elements $U \in G$, such that $L = Uh$ has $\ker(L-1) \neq 0$.

Proposition 3.11. *We have*

$$|C|/|G| = \sum_{j=1}^{n'} \frac{(-1)^{j-1}}{(q-1)(q^2-1)\cdots(q^j-1)}.$$

Proof. In the above situation, L is an $\mathbb{F}$-linear operator on V. So the space $W = \ker(L-1)$ is an $\mathbb{F}$-subspace of V. But notice that if $\mathbf{v} \in V$ is such that $L(\mathbf{v}) = \mathbf{v}$, and $a \in \mathbb{K}$, we have $L(a\mathbf{v}) = h(a)\mathbf{v}$. In particular, $\mathbb{K} \cdot W \cong \mathbb{K} \otimes_{\mathbb{F}} W$. Furthermore, any linearly independent subset (over $\mathbb{F}$) of W is linearly independent over $\mathbb{K}$.

Define $\mathcal{X}$ to be a partially ordered set where each element W of $\mathcal{X}$ is an $\mathbb{F}$-vector subspace of V, such that $\mathbb{K}W \cong \mathbb{K} \otimes_{\mathbb{F}} W$. If $W \in \mathcal{X}$, then any subspace of W is also an element of $\mathcal{X}$, and $W \leq W'$ if and only if $W \subseteq W'$.

Define $\mu(W, W')$ to be the Möbius function on the partially ordered set defined above (see [27]). In fact, it is clear that if $W \leq W'$, then there exists W'' such that $W' = W \oplus W''$ and so $\mu(W, W') = \mu(0, W'')$.

In particlar, if $\dim(W'') = j$, the following is due to Hall (see [27, Example 2, p. 351]):

$$\mu(0, W'') = (-1)^j q^{\binom{j}{2}}.$$

So, we have established that $\mu(W, W') = (-1)^j q^{\binom{j}{2}}$, where $j = \dim(W') - \dim(W)$.

Now, define $N(0)$ to be $\#\{U \in G \mid \ker(Uh - 1) = 0\}$. The ratio we are to investigate is then given by

$$\frac{|C|}{|G|} = 1 - \frac{N(0)}{|G|}$$

and $N(0)$ is given by Möbius inversion ([27, Proposition 2]),

$$\frac{N(0)}{|G|} = \sum_W \mu(0, W) \frac{M(W)}{|G|},$$

where $M(W) = \#\{U \in G \mid W \subseteq \ker(Uh - 1)\}$.

If $j = \dim(W)$, then

$$M(W) = (Q^{n'} - Q^j)(Q^{n'} - Q^{n'-j+1}) \cdots (Q^{n'} - Q^{n'-1}),$$

where $Q = q^u$ and $n' = \dim(V)$.

The number of subspaces $W \in \mathcal{X}$ with $\dim(W) = j$ is $(Q^{n'} - 1)(Q^{n'} - Q) \cdots (Q^{n'} - Q^{j-1}) \cdot (q^j - 1)^{-1}(q^j - q)^{-1} \cdots (q^j - q^{j-1})^{-1}$.

Now the sum occurring in $N(0)/|G|$ over W with $\dim(W) = j$ is

$$(-1)^j \frac{(Q^{n'} - 1) \cdots (Q^{n'} - Q^{j-1})}{(q^j - 1) \cdots (q^j - q^{j-1})} \cdot (Q^{n'} - Q^j) \cdots (Q^{n'} - Q^{n'-1}) q^{\binom{j}{2}} \cdot \frac{1}{(Q^{n'} - 1) \cdots (Q^{n'} - Q^{n'-1})},$$

which simplifies to

$$(-1)^j \frac{1}{(q^j - 1)(q^{j-1} - 1) \cdots (q - 1)}. \qquad \square$$

Proposition 3.12. *For square-free ideals $\mathfrak{N}$ of $\mathbf{A}'$, define $\lambda(\mathfrak{N})$ so that*

$$\frac{|\mathcal{C}_{\mathfrak{N}}|}{|\operatorname{Gal}(K_{\mathfrak{N}}/E)|} = \lambda(\mathfrak{N}) \frac{1}{[K' : E]}.$$

Suppose $\mathfrak{N}$ is prime to M; then $\lambda(\mathfrak{N}) = \prod_{\mathfrak{q}|\mathfrak{N}} \lambda(\mathfrak{q})$. Furthermore, if $\mathfrak{q}$ is a prime ideal not dividing M, then

$$\frac{1}{r^{\deg \mathfrak{q}} - 1} - \frac{1}{(r^{\deg \mathfrak{q}} - 1)(r^{2 \deg \mathfrak{q}} - 1)} \leq \lambda(\mathfrak{q}) \leq \frac{1}{r^{\deg \mathfrak{q}} - 1}.$$

Proof. Apply Proposition 3.11. $\square$

4. Application of the Chebotarev density theorem

Let $\mathcal{P}(E, g, x)$ be the set of places of E of degree x such that $(\wp', K'/E) = g$ (this makes sense as $\operatorname{Gal}(K'/E)$ is a cyclic group).

Let $F = \{X \mapsto X^{r^{\deg \wp}}\}$ be the Frobenius map corresponding to $\mathbb{F}_\wp$. Let $f_\wp(X) \in \mathbf{A}[X]$ be the characteristic polynomial of F, and let $g_{\wp'}(X) \in \mathbf{A}'[X]$ be the characteristic polynomial of F (as an endomorphism of ϕ'). Given that $(\wp', K'/E) = g$, let $\wp''$ be the prime of K' lying above $\wp'$, let F^s be the Frobenius map corresponding to $\wp''$, and let $h_{\wp''}(X) \in \mathbf{B}[X]$ be its characteristic polynomial.

Now for an ideal $\mathfrak{N}$ of $\mathbf{A}'$ define

$$\pi(E, \mathfrak{N}, g, x) = \#\{\wp' \in \mathcal{P}(E, g, x) \ : \ \mathfrak{N} | g_{\wp'}(1)\mathbf{A}'\}.$$

Let $\pi_E(x)$ denote the number of places $\wp'$ of E of degree x.

Then working through [9, Lemma 6.4.8] (see also [14]), we are able to estimate $\pi(E, \mathfrak{N}, g, x)$ in terms of $\pi_E(x)$.

Proposition 4.1. *For a square-free ideal $\mathfrak{N}$ of $\mathbf{A}'$, we have*

$$\pi(E, \mathfrak{N}, g, x) = \frac{|\mathcal{C}_{\mathfrak{N}}|}{[K_{\mathfrak{N}} : E]} \pi_E(x) + \mathrm{O}(|\mathcal{C}_{\mathfrak{N}}| \deg \mathfrak{N} r^{x/2})$$

as $x \to \infty$ and $x \equiv j(E) \bmod j(K')$ and $\pi(E, \mathfrak{N}, g, x) = 0$ if $x \not\equiv j(E) \bmod j(K')$.

Proof. Note that the degree of the different divisor of $K_{\mathfrak{N}}/E$ is bounded by a constant times $\deg \mathfrak{N}[K_{\mathfrak{N}} : E]$ (see [10]). Then apply the Chebotarev density theorem [9, Lemma 6.4.8] to obtain the result as given. $\square$

Proposition 4.2. *Let $\mathfrak{N}$ be a square-free ideal of $\mathbf{A}'$. Then*

$$\pi(E,\mathfrak{N},g,x)=\frac{1}{[K':E]}\lambda(\mathfrak{N})\frac{r^x}{x}+\mathrm{O}(r^{x/2}r^{(n\cdot n'-1)\deg\mathfrak{N}}\deg\mathfrak{N})$$

as $x\equiv j(E) \bmod j(K')$ and $x\to\infty$.

Proof. Apply Propositions 4.1 and 3.12. □

In fact, $h_{\wp''}(X^s)=g_{\wp'}(X)$, and for all $a\in\mathbf{A}$, $N_{\mathbf{E}/\mathbf{k}}\big(g_{\wp'}(a)\big)=f_\wp(a)$. In particular, $N_{\mathbf{E}/\mathbf{k}}\big(g_{\wp'}(1)\big)=f_\wp(1)$.

For an $\mathbf{A}$-module N, let $\chi_{\mathbf{A}}(N)$ be the Euler-Poincaré characteristic of N. We have that (see [11, Proposition 4.12.21])

$$\chi_{\mathbf{A}}\big(\phi(\mathbb{F}_\wp)\big)=f_\wp(1)\mathbf{A}.$$

Let $\mathcal{P}(K,c,x)$ be the set of places $\wp$ of K of degree x such that $(\wp,K'/K)=c$. Now for an ideal N of $\mathbf{A}$ define

$$\pi(K,N,c,x)=\#\{\wp\in\mathcal{P}(K,c,x)\ :\ N|f_\wp(1)\mathbf{A}\}.$$

Proposition 4.3. *Let Q be a prime of $\mathbf{A}$, and let $\mathfrak{q}_1,\dots,\mathfrak{q}_\ell$ be the primes of $\mathbf{A}'$ such that $N_{\mathbf{E}/\mathbf{k}}(\mathfrak{q}_i)=Q$. Then*

$$[C_G(g):\langle g\rangle]\pi(K,Q,c,x)=\sum_{i=1}^{\ell}\pi(E,\mathfrak{q}_i,g,x)+\mathrm{O}(r^{x/2})+\mathrm{O}(r^{x-2\deg Q})$$

as $x\to\infty$. If $\ell=0$, that is, every prime of $\mathbf{A}'$ lying above Q has inertial degree greater than 1, then take the right-hand side to be $\mathrm{O}(r^{x/2})+\mathrm{O}(r^{x-2\deg Q})$ instead.

Proof. The number of primes $\wp'$ of E lying above $\wp$ with $(\wp',K'/E)=g$ is exactly equal to $[C_G(g):\langle g\rangle]$. Furthermore, $\mathfrak{q}_i$ divides $g_{\wp'}(1)\mathbf{A}'$ if and only if $Q=N_{\mathbf{E}/\mathbf{k}}(\mathfrak{q}_i)$ divides $f_\wp(1)\mathbf{A}$. This holds for each $\mathfrak{q}_i$ lying above Q.

The difference of $[C_G(g):\langle g\rangle]\pi(K,Q,c,x)-\sum_{i=1}^{\ell}\pi(E,\mathfrak{q}_i,g,x)$ is bounded by the sum of the number of primes $\wp'$ of E such that $\deg\wp=x$, but with inertia degree ≥ 2, plus the number of primes $\wp'$ counted by $\pi(E,\mathfrak{q}_i\mathfrak{q}_j,g,x)$ plus the number of primes $\wp'$ counted by $\pi(E,\mathfrak{Q},g,x)$, where $\mathfrak{Q}$ has inertial degree greater than 1 over Q. It is elementary that the first of these sums is $\mathrm{O}(r^{x/2})$, while Proposition 4.2 bounds the latter two errors by $\mathrm{O}(r^{x-2\deg Q})$. □

5. Erdős-Kac type results

In this section we extend the results of [2] and [20] to the case when $\mathbf{A}\neq\mathbb{F}_r[T]$, and we also include the possibility that the endomorphism ring is non-trivial.

Let $\mathcal{Q}(\mathbf{A}',g,y)$ be the set of all primes $\mathfrak{q}$ of $\mathbf{A}'$ such that $\mathrm{Norm}_{\mathbf{E}/\mathbf{k}}(\mathfrak{q})=Q$ is a prime of $\mathbf{A}$, $\gcd(\mathfrak{q},M)=1$, and such that $\deg\mathfrak{q}\leq y$. Let $\mathbb{F}_{r^J}$ be the constant field of $\mathbf{A}'$.

For each ideal $I\subseteq\mathbf{A}$, define $\omega_{y,1,g}(I)$ to be the number of divisors of I which are norms of elements of $\mathcal{Q}(\mathbf{A}',g,y)$ weighted as follows:

$$\omega_{y,1,g}(I)=\frac{1}{[C_G(g):\langle g\rangle]}\#\{\mathfrak{q}\in\mathcal{Q}(\mathbf{A},g,y)\mid \mathrm{Norm}_{\mathbf{E}/\mathbf{k}}(\mathfrak{q})|I\}.$$

If $f:\mathcal{P}(K,c,x)\to\mathbb{C}$, define $E_{K,c,x}(f)=\frac{1}{\#\mathcal{P}(K,c,x)}\sum_{\wp\in\mathcal{P}(K,c,x)}f(\wp)$.

Proposition 5.1. *Let $y = x/\log x$. Then*

$$E_{K,c,x}\left(\left|\frac{\omega_{\mathbf{A}}\left(\chi_{\mathbf{A}}\left(\phi(\mathbb{F}_\wp)\right)\right) - \omega_{y,1,g}\left(\chi_{\mathbf{A}}\left(\phi(\mathbf{F}_\wp)\right)\right)}{\sqrt{\log x}}\right|\right) \to 0$$

as $x \to \infty$.

Proof. For each prime Q of $\mathbf{A}$, define S_Q to be the number of $\wp \in \mathcal{P}(K,c,x)$ such that $Q | \chi_{\mathbf{A}}\left(\phi(\mathbb{F}_\wp)\right)$. Now choose β such that $0 < \beta \leq \frac{1}{2n\cdot n'}$. Let $\Sigma = \sum_{\deg Q > \beta x} S_Q$, $\Sigma' = \sum_{y < \deg Q \leq \beta x} S_Q$, and we are to bound

$$\sum_{\wp \in \mathcal{P}(K,c,x)} \left(\omega_{\mathbf{A}}\left(\chi_{\mathbf{A}}\left(\phi(\mathbb{F}_\wp)\right)\right) - \omega_{y,1,g}\left(\chi_{\mathbf{A}}\left(\phi(\mathbb{F}_\wp)\right)\right)\right) \leq \Sigma + \Sigma'.$$

First, let us bound Σ. It is elementary that

$$\Sigma \ll \#\mathcal{P}(K,c,x).$$

Now split $\Sigma' = S_1 + S_2$, where S_1 is the sum of S_Q where $y < \deg Q \leq \beta x$ and there exists a prime $\mathfrak{Q}$ of $\mathbf{A}'$ such that $Q = \mathrm{Norm}_{\mathbf{E}/\mathbf{k}}(\mathfrak{Q})$, and S_2 is the sum of S_Q where $\deg Q \leq \beta x$ and Q^2 divides $\mathrm{Norm}_{\mathbf{E}/\mathbf{K}}(\mathfrak{Q})$ for all $\mathfrak{Q}$ lying above Q.

Applying Proposition 4.2 in the case that $\ell = 0$,

$$\begin{aligned} S_2 &\ll \textstyle\sum_{\deg Q \leq \beta x} r^{x - 2\deg Q}/x \\ &\leq (r^x/x)\textstyle\sum_{m < \beta x} r^{-2m} r^m \ll r^x/x \end{aligned}$$

which is $\ll \#\mathcal{P}(K,c,x)$ as $x \to \infty$.

For S_1 we use Proposition 4.2 to obtain

$$S_1 \ll \sum_{y < m \leq \beta x} (r^{x-m}/x)(r^m/m) \ll (r^x/x)\log\log x.$$

The result follows. □

Once we have reduced ourselves to the consideration of $\omega_{y,1,g}$, the remainder of the section is routine application of the theory in [23].

For $\mathfrak{q} \in \mathcal{Q}(\mathbf{A}', g, y)$, define a random variable $V_{\mathfrak{q}}$ to be 1 with probability $\lambda(\mathfrak{q})$ and 0 with probability $1 - \lambda(\mathfrak{q})$. Define $S_y = \sum_{\mathfrak{q} \in \mathcal{Q}(\mathbf{A}', g, y)} V_{\mathfrak{q}}$.

Proposition 5.2.

$$\begin{aligned} \mathrm{E}[S_y] &= \log x + \mathrm{O}(\log\log x), \\ \mathrm{Var}[S_y] &= \log x + \mathrm{O}(\log\log x). \end{aligned}$$

Proof. Let $\mathbb{F}_{q^J}$ be the constant field of $\mathbf{E}$, the number of $\mathfrak{q} \in \mathcal{Q}(\mathbf{A}', g, y)$ with $\deg \mathfrak{q} = j$ is Jr^j/j if $J | j$. Therefore,

$$\begin{aligned} \mathrm{E}[S_y] &= \sum_{\substack{j \equiv 0 \bmod J \\ j < y}} J(r^j/j)(r^j - 1)^{-1} + \mathrm{O}(r^{-j/2}) \\ &= \log(y) + \mathrm{O}(1), \end{aligned}$$

using the bound that $|\lambda_Q - (r^{\deg Q} - 1)^{-1}| \leq (r^{\deg Q} - 1)^{-2}$.

Similarly,

$$\begin{aligned}\operatorname{Var}[S_y] &= \sum_{\substack{j\equiv 0 \bmod J\\ j<y}} J(r^j/j)\big((r^j-1)^{-1}-(r^j-1)^{-2}\big)+\mathrm{O}(r^{-j/2})\\ &= \log y+\mathrm{O}(1).\end{aligned}$$

Now, write $\log y = \log x - \log\log x$ to complete the proof. □

Proposition 5.3. *For $s\in\mathbb{N}$, we have $\sup_x \left|\mathrm{E}\left[\left(\frac{S_y-\mathrm{E}[S_y]}{\sqrt{\operatorname{Var}[S_y]}}\right)^s\right]\right| < \infty$. Therefore, S_y is normally distributed with mean $\mathrm{E}[S_y]$ and standard deviation $\sqrt{\operatorname{Var}[S_y]}$.*

Proof. The proof is contained in [22, Lemma 7]. □

Proposition 5.4. *For all $s\in\mathbb{N}$,*

$$\lim_{x\to\infty}\left|\mathrm{E}\left[\left(\frac{S_y-\mathrm{E}[S_y]}{\sqrt{\operatorname{Var}[S_y]}}\right)^s\right]-\mathrm{E}_{K,c,x}\left[\left(\frac{\omega_{y,1,g}\Big(\chi_{\mathbf{A}}\big(\phi(\mathbb{F}_\wp)\big)\Big)-\mathrm{E}[S_y]}{\sqrt{\operatorname{Var}[S_y]}}\right)^s\right]\right|=0.$$

Proof. The proof boils down to showing that for primes $\mathfrak{q}_1,\mathfrak{q}_2,\dots,\mathfrak{q}_\ell\in\mathcal{Q}(\mathbf{A}',g,y)$ and for $\mathfrak{N}=\mathfrak{q}_1\cdots\mathfrak{q}_\ell$, we have that

$$\mathrm{E}[V_{\mathfrak{q}_1}V_{\mathfrak{q}_2}\cdots V_{\mathfrak{q}_\ell}]-\pi(E,\mathfrak{N},g,x)=\mathrm{O}(r^{(\deg\mathfrak{N})(n\cdot n'-1)}\deg N r^{-x/2}),$$

which follows from Proposition 4.2. □

Now, we can prove that the number of prime divisors of the Euler-Poincaré characteristic of $\phi(\mathbb{F}_\wp)$ is normally distributed. Recall that

$$G(u)=\frac{1}{\sqrt{2\pi}}\int_{-\infty}^{u} e^{-t^2/2}\,\mathrm{d}t$$

is the cumulative distribution function of the normal distribution with mean 0 and standard deviation 1.

Theorem 5.5.

$$\lim_{x\to\infty}\frac{1}{\#\mathcal{P}(K,c,x)}\#\left\{\wp\in\mathcal{P}(K,c,x)\;\middle|\;\frac{\omega_{\mathbf{A}}\Big(\chi_{\mathbf{A}}\big(\phi(\mathbb{F}_\wp)\big)\Big)-\log x}{\sqrt{\log x}}\le u\right\}=G(u).$$

Proof. Notice that

$$\begin{aligned}&\frac{\omega_{y,1,g}\Big(\chi_{\mathbf{A}}\big(\phi(\mathbb{F}_\wp)\big)\Big)-\mathrm{E}[S_y]}{\sqrt{\operatorname{Var}[S_y]}}\\ &\qquad=\frac{\omega_{y,1,g}\Big(\chi_{\mathbf{A}}\big(\phi(\mathbb{F}_\wp)\big)\Big)-\log x}{\sqrt{\log x}}\cdot\frac{\log x}{\sqrt{\operatorname{Var}[S_y]}}+\frac{\log x-\mathrm{E}[S_y]}{\sqrt{\operatorname{Var}[S_y]}}\end{aligned}$$

and $\sqrt{\log x}/\sqrt{\operatorname{Var}[S_y]}\to 1$ and $(\log x-\mathrm{E}[S_y])/\sqrt{\operatorname{Var}[S_y]}\to 0$ as $x\to\infty$.

Then apply Propositions 5.2, 5.3, 5.4. □

6. A prime analogue of the Erdős-Pomerance conjecture for Drinfeld modules

Now, let $0 \neq a \in K$. Let $\mathcal{P}(K, a, c, x)$ be the places $\wp$ of K of good reduction, of degree x, such that $(\wp, K'/K) = c$ and a is a unit modulo $\wp$. Notice that for x large enough $\mathcal{P}(K, a, c, x) = \mathcal{P}(K, c, x)$. As we are interested in the behaviour of $\wp$ as $\deg \wp$ tends to infinity, we may safely omit a and consider $\mathcal{P}(K, c, x)$. For $\wp \in \mathcal{P}(K, c, x)$, let W be the submodule of $\phi(\mathbb{F}_\wp)$ generated by a. Let N be the Euler-Poincaré characteristic of W, and define $f_a(\wp)$ to be the number of distinct primes of $\mathbf{A}$ dividing N. Define $E_a(\wp)$ to be the number of primes Q of $\mathbf{A}$ such that Q divides the Euler-Poincaré characteristic of $\phi(\mathbb{F}_\wp)$ but Q doesn't divide the Euler-Poincaré characteristic of W, the submodule generated by a.

We aim to show that $f_a(\wp)$ follows the same distribution as $\omega_{\mathbf{A}}\Big(\chi_{\mathbf{A}}\big(\phi(\mathbb{F}_\wp)\big)\Big)$. In order to do this we must give an upper bound for the sum of $\big(E_a(\wp)\big)^2$ over $\wp$ with $(\wp, K'/K) = c$. To do this, we will combine the ideas of [16] and [18].

Proposition 6.1.

$$\omega_{\mathbf{A}}\big(f_a(\wp)\big) + E_a(\wp) = \omega_{\mathbf{A}}\Big(\chi_{\mathbf{A}}\big(\phi(\mathbb{F}_\wp)\big)\Big).$$

Proof. This is the definition of $E_a(\wp)$. □

Following previous sections, let $c \subseteq \mathrm{Gal}(K'/K)$ be a fixed conjugacy class, let $g \in c$, let $E \subseteq K'$ be the fixed field of $\langle g \rangle$, let $\phi' : \mathbf{A}' \to E\{\tau\}$ be the Drinfeld module corresponding to the endomorphisms with coefficients in E, and let us consider primes $\wp$ of K such that there is a prime $\wp''$ of K' such that $(\wp'', K'/K) = g$ and the prime lying below $\wp''$ and above $\wp$, called $\wp'$, satisfies $\mathbb{F}_{\wp'} \cong \mathbb{F}_\wp$.

Now, let $E'_a(\wp')$ be the number of primes $\mathfrak{q}$ of $\mathbf{A}'$ such that $\phi'[\mathfrak{q}] \cap \phi'(\mathbb{F}_{\wp'}) \neq 0$ but $\phi'[\mathfrak{q}] \cap W' = 0$, where W' is the $\mathbf{A}'$-submodule of $\phi'(\mathbb{F}_{\wp'})$ generated by a. Then if Q contributes to $E_a(\wp)$, then $W' \cap \phi'[\mathfrak{q}] = 0$ for all $\mathfrak{q}$ dividing Q, and $\phi'[\mathfrak{q}] \cap \phi'(\mathbb{F}_{\wp'}) \neq 0$ for some $\mathfrak{q}$ dividing Q. In particular,

$$E_a(\wp) \leq E'_a(\wp').$$

As in Section 4, we have now reduced ourselves to the case that $\phi' : \mathbf{A}' \to E\{\tau\}$ is a Drinfeld module and $\mathrm{Gal}(K'/E) = \langle g \rangle$ and $\mathrm{Gal}(\mathbf{l}/\mathbf{k}') \cong \mathrm{Gal}(K'/E)$.

Definition 6.2. Let $\mathfrak{a}$ be a square-free ideal of $\mathbf{A}'$. Let

$$\mathfrak{a}^{-1}W' = \{\alpha \in K^{\mathrm{sep}} \mid \phi'_a(\alpha) \in W' \text{ for all } a \in \mathfrak{a}\}.$$

Let $W'' = \{\psi_b(a) \mid b \in \mathbf{B}\} \subseteq K'$. If $\mathfrak{b}$ is an ideal of $\mathbf{B}$, let

$$\mathfrak{b}^{-1}W'' = \{\alpha \in K^{\mathrm{sep}} \mid \psi_b(\alpha) \in W'' \text{ for all } b \in \mathfrak{b}\}.$$

Proposition 6.3. *We have that* $K'(\mathfrak{a}^{-1}W') = K'(\mathfrak{a}^{-1}W'')$.

Define $L^a_\mathfrak{a} = K'(\mathfrak{a}^{-1}W')$. *Fix a basis* $\lambda_1, \ldots, \lambda_{n'}, \alpha$ *for* $\mathfrak{a}^{-1}W''/W''$. *There exists a lift of* $g \in \mathrm{Gal}(K'/E)$ *to* $\mathrm{Gal}(L^a_\mathfrak{a}/E)$ *(which we also call* g*) such that* $g(\lambda_i) = \lambda_i$ *and* $g(\alpha) = \alpha$.

Then for each $\sigma \in \mathrm{Gal}(L^a_\mathfrak{a}/E)$, *we may write* $\sigma = Ug$, *where* $U \in \mathrm{Gal}(L^a_\mathfrak{a}/K')$.

Theorem 6.4 ([25, Theorem 1.6])**.** *There exists an element* $M \in \mathbf{A}'$ *such that if* $\mathfrak{a}$ *is an ideal of* $\mathbf{A}'$ *and* $\gcd(\mathfrak{a}, M) = 1$, *then*

$$\mathrm{Gal}(L^a_\mathfrak{a}/K') \cong (\mathbf{B}/\mathfrak{a}\mathbf{B})^{n'} \rtimes \mathrm{GL}_{n'}(\mathbf{B}/\mathfrak{a}\mathbf{B})$$

and $L^a_\mathfrak{a}/K'$ *is a geometric extension.*

Definition 6.5. Fix a prime $\mathfrak{q}$ of $\mathbf{A}'$. Choose $\alpha \in \mathfrak{q}^{-1}W'/W'$ which gets mapped to a generator of $\mathfrak{q}^{-1}/\mathbf{A}'$ in the exact sequence

$$0 \to \phi'[\mathfrak{q}] \to \mathfrak{q}^{-1}W'/W' \to \mathfrak{q}^{-1}/\mathbf{A}' \to 0.$$

Let $\mathcal{C}_{\mathfrak{q}}^a$ consist of those $\sigma \in \mathrm{Gal}(L_{\mathfrak{a}}^a/K')$ such that $\sigma|_{K'(\phi'[\mathfrak{q}])} \in \mathcal{C}_{\mathfrak{q}}$ and such that $\sigma(\alpha) = \alpha + (\sigma - 1)(\lambda)$ for some $\lambda \in \phi'[\mathfrak{q}]$.

Proposition 6.6. *Let* $\frac{|\mathcal{C}_{\mathfrak{q}}^a|}{[L_{\mathfrak{q}}^a : E]} = \frac{1}{[K' : E]}\lambda(\mathfrak{q})$. *Then,*

$$\frac{1}{r^{\deg \mathfrak{q}}(r^{\deg \mathfrak{q}} - 1)} - \frac{1}{r^{2\deg \mathfrak{q}}(r^{2\deg \mathfrak{q}} - 1)(r^{\deg \mathfrak{q}} - 1)} \leq \lambda(\mathfrak{q}) \leq \frac{1}{r^{\deg \mathfrak{q}}(r^{\deg \mathfrak{q}} - 1)}.$$

Proposition 6.7.

$$\pi(x, L_{\mathfrak{q}}^a/E, \mathcal{C}_{\mathfrak{q}}^a) \ll \mathrm{O}(r^{x - 2\deg \mathfrak{a}}/x) + \mathrm{O}(r^{x/2} \deg \mathfrak{a} r^{\deg \mathfrak{a}(nn' + n - 2)}).$$

Proposition 6.8. $\sum_{\wp \in \mathcal{P}(K,c,x)} \big(E_a(\wp)\big)^2 \ll \#\mathcal{P}(K, c, x)$.

Theorem 2.4 now follows by combining Theorem 2.2 and the proof of [16, Theorem 2]. Details have been omitted.

Acknowledgment

The authors thank the referee for useful comments which improved the exposition in the paper.

References

[1] Bruno Anglès, Tuan Ngo Dac, and Floric Tavares Ribeiro, *Stark units in positive characteristic*, Proc. Lond. Math. Soc. (3) **115** (2017), no. 4, 763–812, DOI 10.1112/plms.12051. MR3716942

[2] Alina Carmen Cojocaru, *The Erdős and Halberstam theorems for Drinfeld modules of any rank*, Acta Arith. **131** (2008), no. 4, 317–340, DOI 10.4064/aa131-4-2. With an appendix by Hugh Thomas. MR2383689

[3] U. Dempwolff, J. Chris Fisher, and Allen Herman, *Semilinear transformations over finite fields are Frobenius maps*, Glasg. Math. J. **42** (2000), no. 2, 289–295, DOI 10.1017/S0017089500020164. MR1763750

[4] P. D. T. A. Elliott, *Probabilistic number theory. I*: *Mean-value theorems*, Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Science], vol. 239, Springer-Verlag, New York-Berlin, 1979. MR551361

[5] Peter D. T. A. Elliott, *Probabilistic number theory. II*: *Central limit theorems*, Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 240, Springer-Verlag, Berlin-New York, 1980. MR560507

[6] Paul Erdős and Carl Pomerance, *On the normal number of prime factors of $\phi(n)$*, Rocky Mountain J. Math. **15** (1985), no. 2, 343–352, DOI 10.1216/RMJ-1985-15-2-343. Number theory (Winnipeg, Man., 1983). MR823246

[7] P. Erdős, *On the normal number of prime factors of $p - 1$ and some related problems concerning Euler's φ-function.* (English), Q. J. Math., Oxf. Ser. **6** (1935), 205–213.

[8] P. Erdős and M. Kac, *The Gaussian law of errors in the theory of additive number theoretic functions*, Amer. J. Math. **62** (1940), 738–742. MR0002374

[9] Michael D. Fried and Moshe Jarden, *Field arithmetic*, 3rd ed., Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge. A Series of Modern Surveys in Mathematics [Results in Mathematics and Related Areas. 3rd Series. A Series of Modern Surveys in Mathematics], vol. 11, Springer-Verlag, Berlin, 2008. Revised by Jarden. MR2445111

[10] Francis Gardeyn, *Une borne pour l'action de l'inertie sauvage sur la torsion d'un module de Drinfeld* (French, with French summary), Arch. Math. (Basel) **79** (2002), no. 4, 241–251, DOI 10.1007/s00013-002-8310-5. MR1944948

[11] David Goss, *Basic structures of function field arithmetic*, Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)], vol. 35, Springer-Verlag, Berlin, 1996. MR1423131
[12] H. Halberstam, *On the distribution of additive number-theoretic functions. III*, J. London Math. Soc. **31** (1956), 14–27. MR0073627
[13] G. H. Hardy and S. Ramanujan, *The normal number of prime factors of a number n [Quart. J. Math.* **48** *(1917), 76–92]*, Collected papers of Srinivasa Ramanujan, AMS Chelsea Publ., Providence, RI, 2000, pp. 262–275. MR2280878
[14] Michiel Kosters, *A short proof of the Chebotarev density theorem for function fields*, Math. Commun. **22** (2017), no. 2, 227–233. MR3687925
[15] E. Kowalski, *Some local-global applications of Kummer theory*, Manuscripta Math. **111** (2003), no. 1, 105–139, DOI 10.1007/s00229-003-0356-6. MR1981599
[16] Yen-Liang Kuan, Wentang Kuo, and Wei-Chen Yao, *On an Erdős-Pomerance conjecture for rank one Drinfeld modules*, J. Number Theory **157** (2015), 1–36, DOI 10.1016/j.jnt.2015.04.020. MR3373227
[17] J. Kubilius, *Probabilistic methods in the theory of numbers*, Translations of Mathematical Monographs, Vol. 11, American Mathematical Society, Providence, R.I., 1964. MR0160745
[18] W. Kuo and D. Tweedle, *Artin's conjecture for Drinfeld modules*, 2017. Submitted.
[19] Wentang Kuo and Yu-Ru Liu, *A Carlitz module analogue of a conjecture of Erdős and Pomerance*, Trans. Amer. Math. Soc. **361** (2009), no. 9, 4519–4539, DOI 10.1090/S0002-9947-09-04723-0. MR2506417
[20] Wentang Kuo and Yu-Ru Liu, *Gaussian laws on Drinfeld modules*, Int. J. Number Theory **5** (2009), no. 7, 1179–1203, DOI 10.1142/S1793042109002638. MR2584268
[21] Serge Lang, *Algebraic groups over finite fields*, Amer. J. Math. **78** (1956), 555–563. MR86367
[22] Yu-Ru Liu, *A generalization of the Erdös-Kac theorem and its applications*, Canad. Math. Bull. **47** (2004), no. 4, 589–606. MR2099756
[23] Yu-Ru Liu, *Prime divisors of the number of rational points on elliptic curves with complex multiplication*, Bull. London Math. Soc. **37** (2005), no. 5, 658–664, DOI 10.1112/S0024609305004558. MR2164827
[24] S. Ali Miri and V. Kumar Murty, *An application of sieve methods to elliptic curves*, Progress in cryptology—INDOCRYPT 2001 (Chennai), Lecture Notes in Comput. Sci., vol. 2247, Springer, Berlin, 2001, pp. 91–98, DOI 10.1007/3-540-45311-3_9. MR1934487
[25] Richard Pink, *Kummer theory for Drinfeld modules*, Algebra Number Theory **10** (2016), no. 2, 215–234, DOI 10.2140/ant.2016.10.215. MR3477742
[26] Richard Pink and Egon Rütsche, *Adelic openness for Drinfeld modules in generic characteristic*, J. Number Theory **129** (2009), no. 4, 882–907, DOI 10.1016/j.jnt.2008.12.002. MR2499412
[27] Gian-Carlo Rota, *On the foundations of combinatorial theory. I. Theory of Möbius functions*, Z. Wahrscheinlichkeitstheorie und Verw. Gebiete **2** (1964), 340–368 (1964), DOI 10.1007/BF00531932. MR174487
[28] Harold N. Shapiro, *Distribution functions of additive arithmetic functions*, Proc. Nat. Acad. Sci. U.S.A. **42** (1956), 426–430, DOI 10.1073/pnas.42.7.426. MR79609
[29] Lenny Taelman, *Special L-values of Drinfeld modules*, Ann. of Math. (2) **175** (2012), no. 1, 369–391, DOI 10.4007/annals.2012.175.1.10. MR2874646
[30] Paul Turán, *On a Theorem of Hardy and Ramanujan*, J. London Math. Soc. **9** (1934), no. 4, 274–276, DOI 10.1112/jlms/s1-9.4.274. MR1574877

Department of Pure Mathematics, Faculty of Mathematics, University of Waterloo, Waterloo, Ontario, N2L 3G1 Canada
Email address: wtkuo@uwaterloo.ca

Department of Mathematics and Statistics, Faculty of Science and Technology, University of The West Indies, St. Augustine, Trinidad and Tobago, West Indies
Email address: david.tweedle@sta.uwi.edu