AVERAGE DISTRIBUTION OF SUPERSINGULAR DRINFELD MODULES

CHANTAL DAVID

ABSTRACT. Let ϕ be a rank 2 Drinfeld module defined over $\mathbb{F}_q(T)$. For each monic prime polynomial $p \in \mathbb{F}_q[T]$ which is a prime of good reduction of ϕ, the reduction of ϕ at p is a rank 2 Drinfeld module ϕ_p over the finite field $\mathbb{F}_q[T]/(p)$; depending on the structure of the ring $\text{End}(\phi_p)$, the prime p is either a supersingular or an ordinary prime of ϕ. We prove in this paper that, *on average*, supersingular primes are distributed according to the Lang-Trotter conjecture (for Drinfeld modules). We first show this result averaging over Drinfeld modules, and then over isomorphism classes of Drinfeld modules.

1. INTRODUCTION.

Let $\mathbb{F}_q$ be the finite field with q elements, for q some power of an odd prime different from 3. Let $R = \mathbb{F}_q[T]$ be the ring of polynomials in one variable over $\mathbb{F}_q$, and $F = \mathbb{F}_q(T)$ be the field of rational functions in one variable over $\mathbb{F}_q$.

Let $\phi(a, b)$ denote the Drinfeld R-module of rank 2 and generic characteristic with equation

$$\phi(T) = \gamma(T) + af + bf^2, \quad a, b \in R, \ b \neq 0, \tag{1.1}$$

where f denotes the Frobenius automorphism of $\mathbb{F}_q$.

Given a Drinfeld module $\phi(a, b)$ as defined by (1.1), we investigate in this paper the distribution of the supersingular primes of ϕ. This is the analogous, over function fields, to the distribution of supersingular primes of elliptic curves. Brown [2] was the first to examine this new situation, and to notice that most of the theory extends from elliptic curves to Drinfeld modules. Then, similarly to the classical case of elliptic curves (see [6] and [14]), he obtained lower bounds for the number of supersingular primes of a Drinfeld module ϕ over $\mathbb{F}_q(T)$; these bounds are improved in [3].

Let $P(k)$ be the set of monic prime polynomials of degree k of $\mathbb{F}_q[T]$. Let

$$\pi_{\phi(a,b)}(k)$$

Partially supported by CICMA.

denote the number of p in $P(k)$ such that $\phi(a,b)$ has good reduction at p and $\phi_p(a,b)$ is supersingular.

If $\phi(a,b)$ has complex multiplication by an order of a quadratic imaginary extension K/F, by Deuring's criterion ([5] for elliptic curves, [2] for Drinfeld modules),

$$\pi_{\phi(a,b)}(k) = \#\left\{p \in P(k) : p \text{ does not split in } K\right\}.$$

Let L be the algebraic closure of $\mathbb{F}_q$ in K; then using the Čebotarev Density Theorem for function fields [7, Proposition 5.16]

(i) when $L = \mathbb{F}_q$,

$$\pi_{\phi(a,b)}(k) \sim \frac{1}{2}\frac{q^k}{k};$$

(ii) when $L = \mathbb{F}_{q^2}$,

$$\pi_{\phi(a,b)}(k) \sim \frac{q^k}{k} \text{ for } k \text{ odd},$$

and

$$\pi_{\phi(a,b)}(k) = 0 \text{ for } k \text{ even}.$$

If $\phi(a,b)$ does not have complex multiplication, the Lang-Trotter conjecture for Drinfeld modules is

Conjecture 1.1. *Let ϕ be a Drinfeld module defined over $\mathbb{F}_q(T)$. Then there is a constant C_ϕ such that when $k \to \infty$*

$$\pi_\phi(k) \sim C_\phi \, \frac{q^{k/2}}{k}.$$

We prove in this paper that this conjecture holds on average. More precisely, we prove the following

Theorem 1.2. *Let A, B be positive integers satisfying*

$$A, B \geq k.$$

Then, when $k \to \infty$

$$\frac{1}{q^{A+1}q^{B+1}} \sum_{\substack{\deg a \leq A \\ \deg b \leq B}} \pi_{\phi(a,b)}(k) \sim C(k,q)\, \frac{q^{k/2}}{k},$$

where $C(k,q)$ depends on q and on the parity of k. More precisely,

$$C(k,q) = \begin{cases} \dfrac{q}{(q+1)(q-1)} & \text{when } k \text{ is even} \\[2ex] \dfrac{q^{1/2}}{(q-1)} & \text{when } k \text{ is odd.} \end{cases} \tag{1.2}$$

In the average of the previous theorem, the same Drinfeld module may be counted more than once, since the summation runs over Drinfeld modules, and not over isomorphism classes of Drinfeld modules. This restriction to classes of Drinfeld modules would only change the constant by a factor of a zeta function. More precisely, let $a, b \in \mathbb{F}_q[T]$. Then for any $c \in \mathbb{F}_q[T]$, the Drinfeld modules

$$\phi(a,b) \text{ and } \phi'(c^{q-1}a, c^{q^2-1}b)$$

are isomorphic over $\mathbb{F}_q(T)$. Let

$$M = \left\{(a,b) \in \mathbb{F}_q[T]^2 : c^{q-1} \mid a \Longrightarrow c^{q^2-1} \not| \, b, \text{ for any monic } c \in \mathbb{F}_q[T]\right\}. \tag{1.3}$$

Then two Drinfeld modules $\phi(a,b)$ and $\phi'(a',b')$, with (a,b) and $(a',b') \in M$ are never isomorphic over $\mathbb{F}_q(T)$. We then obtain

Theorem 1.3. *Let $\epsilon > 0$, and A, B be positive integers satisfying*

$$C = \min\left(\frac{A}{q-1}, \frac{B}{q^2-1}\right) < k$$

and

$$A, B \geq k(1+\epsilon) \quad , \quad A + B \geq C + k(2+\epsilon).$$

Then, when $k \to \infty$

$$\frac{1}{q^{A+1}q^{B+1}} \sum_{\substack{\deg a \leq A \ \deg b \leq B \\ (a,b) \in M}} \pi_{\phi(a,b)}(k) \sim C'(k,q)\, \frac{q^{k/2}}{k},$$

where $C'(k,q)$ depends on q and on the parity of k. More precisely,

$$C'(k,q) = \zeta^{-1}(q^2+q-2)\; C(k,q).$$

We also have to insure that complex multiplication Drinfeld modules do not contribute significantly to these averages. If a Drinfeld module ϕ has complex multiplication by an order in the quadratic imaginary field $K/\mathbb{F}_q(T)$, then $K(j_\phi)$ is the Hilbert class field of K. As ϕ is defined over $\mathbb{F}_q(T)$, its j-invariant $j_\phi \in \mathbb{F}_q(T)$, and then K must have class number one. But there are only a finite number of class number one quadratic imaginary extensions of $\mathbb{F}_q(T)$, existing only in characteristic 2 or 3 (see [13]). We then assume that q is a power of an odd prime different from 3, such that there is no complex multiplication Drinfeld module defined over $\mathbb{F}_q(T)$.

Finally, we mention that the Lang-Trotter conjecture was also proved to be true on average for elliptic curves by Fouvry and Murty [8].

2. Drinfeld modules.

Since the subject of Drinfeld modules is less known than the classical case of elliptic curves, we review here some basic facts. The material of this section can be found in [4], or [9].

Let L be a field over $\mathbb{F}_q[T]$, i.e. an extension of $\mathbb{F}_q$ with an $\mathbb{F}_q$-algebra morphism

$$\gamma : \mathbb{F}_q[T] \to L.$$

Let $\mathbb{G}_a$ be the additive group scheme of L. The ring $\mathrm{End}(\mathbb{G}_a)$ contains the translations by elements of L and the Frobenius automorphism of $\mathbb{F}_q$

$$f : x \longrightarrow x^q.$$

The following then holds in $\mathrm{End}(\mathbb{G}_a)$

$$f \circ c = c^q \circ f \quad \text{for any } c \in L. \tag{2.1}$$

Let $L\{f\}$ be the left twisted polynomial ring generated by L anf f, i.e.

$$L\{f\} = \left\{ \sum_{i=0}^{n} c_i f^i : c_i \in L \right\},$$

where multiplication is given by (2.1). For any $u \in L\{f\}$, let $\deg u$ be the degree in f of the left polynomial u.

Definition 2.1. *A Drinfeld $\mathbb{F}_q[T]$-module ϕ of rank $r > 0$ over L is a ring homomorphism*

$$\begin{array}{rcl} \phi : \mathbb{F}_q[T] & \longrightarrow & L\{f\} \subseteq \mathrm{End}\ (\mathbb{G}_a) \\ a & \longmapsto & \phi(a) \end{array}$$

such that

- *(i) for all $a \in \mathbb{F}_q[T]$, $\deg \phi(a) = r \deg a$;*
- *(ii) $\phi(a)$ has constant term $\gamma(a)$.*

If the map $\gamma : \mathbb{F}_q[T] \to L$ is injective, then ϕ is said to have generic characteristic; if not, its characteristic is Ker γ.

We consider here only rank 2 Drinfeld $\mathbb{F}_q[T]$-modules, and simply refer to them as Drinfeld modules.

Let ϕ be a Drinfeld module over L. Then ϕ is completely determined by $\phi(T)$. We then write such a Drinfeld module as

$$\phi(T) = \gamma(T) + af + bf^2, \quad a, b \in L, \quad b \neq 0,$$

and denote it $\phi(a, b)$.

Definition 2.2. *A L-morphism, or L-isogeny, between 2 Drinfeld modules ϕ and ψ defined over L is an element $c \in L\{f\}$ such that*

$$c \circ \phi(a) = \psi(a) \circ c \quad \text{for all } a \in \mathbb{F}_q[T].$$

The set of L-isogenies $\phi \longrightarrow \phi$ is denoted by $\mathrm{End}_L(\phi)$, and is a ring under the usual operations. The ring of $\overline{L}$-isogenies is denoted $\mathrm{End}(\phi)$.

Let ϕ be a Drinfeld module over $\mathbb{F}_q(T)$. It is clear from the definition of ϕ that $\mathbb{F}_q[T] \subseteq \mathrm{End}(\phi)$. If $\mathrm{End}(\phi)$ is strictly larger than $\mathbb{F}_q[T]$, it has to be an order $\mathcal{O}$ in some quadratic imaginary extension over $\mathbb{F}_q(T)$. The Drinfeld module ϕ is then said to have complex multiplication (by $\mathcal{O}$).

Let $p \in P(k)$, and let ϕ be a Drinfeld module of characteristic $\mathfrak{p} = (p)$ over $\mathbb{F}_{\mathfrak{p}} = \mathbb{F}_q[T]/(p)$. The Frobenius automorphism of $\mathbb{F}_{\mathfrak{p}}$

$$x \longrightarrow x^{q^{\deg p}}$$

commutes with ϕ, and is then a $\mathbb{F}_{\mathfrak{p}}$-isogeny of ϕ. There are two possible situations for the ring $\mathrm{End}(\phi)$:

(i) $\mathrm{End}(\phi)$ is an order in a quadratic imaginary extension over $\mathbb{F}_q(T)$; ϕ is then said to be ordinary.
(ii) $\mathrm{End}(\phi)$ is a maximal order in the unique quaternion algebra over $\mathbb{F}_q(T)$ ramifying exactly at p and ∞; ϕ is then said to be supersingular.

Now let $\phi(a, b)$ be a Drinfeld module defined over $\mathbb{F}_q(T)$, with $a, b \in \mathbb{F}_q[T]$. If $p \in P(k)$ and $p \not| b$, then p is a prime of good reduction for $\phi(a, b)$. In this case, let $\phi_p(a, b)$ denote the reduction of $\phi(a, b)$ mod p. This is a Drinfeld module of characteristic $\mathfrak{p} = (\mathfrak{p})$, defined over $\mathbb{F}_{\mathfrak{p}}$. We then say that p is a supersingular (respectively ordinary) prime of $\phi(a, b)$ if $\phi_p(a, b)$ is a supersingular (respectively ordinary) Drinfeld module over $\mathbb{F}_{\mathfrak{p}}$.

3. Drinfeld modules over finite fields.

We now compute the average distribution of supersingular primes. We first express the sum of Theorem 1.2 as a sum involving Drinfeld modules over the finite fields $\mathbb{F}_{\mathfrak{p}}$. Inverting the summations, we write

$$\begin{aligned} &\sum_{\substack{\deg a \leq A \\ \deg b \leq B}} \pi_{\phi(a,b)}(k) \\ &= \sum_{p \in P(k)} \# \Big\{ (a, b) \in \mathbb{F}_q[T]^2 : \deg a \leq A, \ \deg b \leq B, \\ &\qquad\qquad \text{and } \phi(a, b) \text{ has good supersingular reduction at } p \Big\}. \end{aligned}$$

Lemma 3.1. *Let $p \in P(k)$, and A, B positive integers.*

(i) Then, for any α, β of $\mathbb{F}_q[T]/(p)$,

$$\# \left\{ (a,b) \in \mathbb{F}_q[T]^2 : \deg a \leq A,\ \deg b \leq B,\ a \equiv \alpha\,(p),\ b \equiv \beta\,(p) \right\} = \left(\frac{q^{A+1}}{q^k} + O(1) \right) \left(\frac{q^{B+1}}{q^k} + O(1) \right).$$

(ii) If A, B are sufficiently large to have $A, B \geq k$, then for any α, β of $\mathbb{F}_q[T]/(p)$,

$$\# \left\{ (a,b) \in \mathbb{F}_q[T]^2 : \deg a \leq A,\ \deg b \leq B,\ a \equiv \alpha\,(p),\ b \equiv \beta\,(p) \right\} = \frac{q^{A+1} q^{B+1}}{q^{2k}}.$$

$\square$

Choose A, B such that $A, B \geq k$. Then, by Lemma 3.1(ii),

$$\sum_{\substack{\deg a \leq A \\ \deg b \leq B}} \pi_{\phi(a,b)}(k) = \sum_{p \in P(k)} \frac{q^{A+1} q^{B+1}}{q^{2k}} \# \{ \text{ supersingular modules defined over } \mathbb{F}_{\mathfrak{p}} \ \}.$$

By the work of Gekeler [10], the number of supersingular Drinfeld modules defined over $\mathbb{F}_{\mathfrak{p}}$ is related to properties of D, the unique quaternion algebra over $\mathbb{F}_q(T)$ which ramifies exactly at p and ∞. More precisely, let $I(\mathfrak{p})$ be the set of isomorphism classes of supersingular modules of characteristic $\mathfrak{p}$, i.e. defined over $\overline{\mathbb{F}_{\mathfrak{p}}}$, and let $I'(\mathfrak{p})$ be the set of isomorphism classes of supersingular Drinfeld modules defined over $\mathbb{F}_{\mathfrak{p}}$.

Lemma 3.2. *Let $h(D)$ and $t(D)$ be respectively the class number and the type number of D. Then*

$$\# I'(\mathfrak{p}) = 2\,t(D) - h(D).$$

If $\mathfrak{p} = (p)$ with $p \in P(k)$, and u is a non-square in $\mathbb{F}_q^*$, then

$$\# I'(\mathfrak{p}) = \begin{cases} \frac{1}{2} h(\sqrt{up}) & \text{when } \deg p \text{ is even} \\ \frac{1}{2} \left(h(\sqrt{up}) + h(\sqrt{p}) \right) & \text{when } \deg p \text{ is odd} \end{cases} \tag{3.1}$$

where $h(\sqrt{up})$ and $h(\sqrt{p})$ are the class numbers of the quadratic imaginary extensions $F(\sqrt{up})$ and $F(\sqrt{p})$ respectively.

Proof: This is just a restatement of the work of Gekeler in [10]. We are looking at the case $r = 2$. By [10, Thm 4.3], $\# I(\mathfrak{p}) = h(D)$, and by [10, Prop 4.6], the number of orbits of $I(\mathfrak{p})$ under the action of $\mathrm{Gal}(\overline{\mathbb{F}_{\mathfrak{p}}}/\mathbb{F}_{\mathfrak{p}})$ is equal to $t(D)$. But every supersingular Drinfeld module of characteristic $\mathfrak{p}$ is isomorphic to one defined over L, where $[L:\mathbb{F}_{\mathfrak{p}}]=2$. We then consider the action of $\mathrm{Gal}(L/\mathbb{F}_{\mathfrak{p}})=\{1,\sigma\}$ on $I(\mathfrak{p})$. Let ϕ be a Drinfeld module of characteristic $\mathfrak{p}$. Since

$$\phi \simeq \phi^{\sigma} \iff j_{\phi}=j_{\phi^{\sigma}} \iff {j_{\phi}}^{\sigma}=j_{\phi} \iff j_{\phi}\in\mathbb{F}_{\mathfrak{p}},$$

we get

$$t(D)=\#I'(\mathfrak{p})+\frac{\#I(\mathfrak{p})-\#I'(\mathfrak{p})}{2} \iff \#I'(\mathfrak{p})=2\,t(D)-h(D)$$

counting the orbits of $I(\mathfrak{p})$ under the action of $\mathrm{Gal}(L/\mathbb{F}_{\mathfrak{p}})$. Finally, since

$$h(D)=\begin{cases}\dfrac{q^{\deg p}-1}{q^2-1} & \text{when } \deg p \text{ is even}\\[2ex] \dfrac{q^{\deg p}-q}{q^2-1}+1 & \text{when } \deg p \text{ is odd}\end{cases}$$

and

$$t(D)=\begin{cases}\dfrac{1}{2}\left(\dfrac{q^{\deg p}-1}{q^2-1}+\dfrac{1}{2}h(\sqrt{up})\right) & \text{when } \deg p \text{ is even}\\[2ex] \dfrac{1}{2}\left(\dfrac{q^{\deg p}-q}{q^2-1}+1+\dfrac{1}{2}\left(h(\sqrt{up})+h(\sqrt{p})\right)\right) & \text{when } \deg p \text{ is odd,}\end{cases}$$

we get the second part of the lemma. □

Let $\phi(a,b)$ and $\phi'(a',b')$ be two supersingular Drinfeld modules of characteristic $\mathfrak{p}$. Then

$$\phi(a,b)\simeq\phi'(a',b') \iff \exists c\in\overline{\mathbb{F}_{\mathfrak{p}}}^{*} \text{ such that } a'=c^{q-1}a \text{ and } b'=c^{q^2-1}b.$$

Let $\phi(a,b)$ be defined over $\mathbb{F}_{\mathfrak{p}}$. The number of $\phi'(a',b')$ also defined over $\mathbb{F}_{\mathfrak{p}}$ and in the isomorphism class of $\phi(a,b)$ is then $q^{\deg p}-1$. With this observation, when $A,B\geq k$, we get

$$\begin{aligned}\sum_{\substack{\deg a\leq A\\ \deg b\leq B}}\pi_{\phi(a,b)}(k) &= \sum_{p\in P(k)}\frac{q^{A+1}q^{B+1}}{q^{2k}}\left(q^k-1\right)\#I'(\mathfrak{p})\\ &= q^{A+1}q^{B+1}\left(q^{-k}-q^{-2k}\right)\sum_{p\in P(k)}\#I'(\mathfrak{p}), \qquad (3.2)\end{aligned}$$

where $\sum_{p\in P(k)}\#I'(\mathfrak{p})$ is a summation of class numbers by Lemma 3.1.

4. Class Number Formula.

The quadratic reciprocity over $\mathbb{F}_q[T]$ reads as

Lemma 4.1. *Let $a, b \in \mathbb{F}_q[T]$, with positive degrees. For any*

$$a = \sum_{i=0}^{k} a_i T^i, \quad a_i \in \mathbb{F}_q, \quad a_k \neq 0$$

in $\mathbb{F}_q[T]$, let

$$\operatorname{sgn} a = \begin{cases} 1 & \text{if } a_k \text{ is a square in } \mathbb{F}_q^* \\ -1 & \text{if } a_k \text{ is not a square in } \mathbb{F}_q^*. \end{cases}$$

Then

$$\left(\frac{a}{b}\right)\left(\frac{b}{a}\right) = (-1)^{\frac{q-1}{2} \deg a \deg b} (\operatorname{sgn} a)^{\deg b} (\operatorname{sgn} b)^{\deg a}.$$

Proof: From the Hilbert reciprocity law

$$\left(\frac{a}{b}\right)\left(\frac{b}{a}\right) = (a, b)_\infty,$$

and the lemma follows from the computation of the Hilbert symbol $(a, b)_\infty$. See, for example, [15, Chapter III, Section 5]. $\square$

Let $d \in \mathbb{F}_q[T]$ a polynomial of positive degree, $d = \alpha\, d'$ with $\alpha \in \mathbb{F}_q^*$ and d' a non-square in $\mathbb{F}_q[T]$. Let

$$\chi_d(n) = \left(\frac{d}{n}\right), \quad n \in \mathbb{F}_q[T].$$

As usual, we define

$$L(s, \chi_d) = \sum_n \chi_d(n)\, |n|^{-s}$$

where

$$|n| = q^{\deg n},$$

and the sum $\sum_n$ runs over monic polynomials in $\mathbb{F}_q[T]$. By the choice of d, when $k \geq \deg d$, it follows from quadratic reciprocity that

$$\sum_{\deg n = k} \chi_d(n) = 0, \tag{4.1}$$

where the sum $\sum_{\deg n = k}$ runs over monic polynomials of degree k of $\mathbb{F}_q[T]$. The L-series $L(s, \chi_d)$ is then the finite sum

$$L(s, \chi_d) = \sum_{\deg n < \deg d} \chi_d(n)\, |n|^{-s}.$$

We now state the case of the class number formula that we need to evaluate (3.2).

Lemma 4.2.

(i) Let p be a prime polynomial of odd degree k in $\mathbb{F}_q[T]$ (not necessarily monic). Then

$$h\left(\sqrt{p}\right) = \frac{q^{k/2}}{q^{1/2}}\, L(1, \chi_p).$$

(ii) Let p be a monic prime polynomial of even degree k in $\mathbb{F}_q[T]$. Let u be a non-square in $\mathbb{F}_q^*$. Then

$$h\left(\sqrt{up}\right) = \frac{2q^{k/2}}{q+1}\, L(1, \chi_{up}).$$

Proof: This is proved in Artin's thesis [1]. □

Then, we can rewrite the inner sum of (3.2) as

$$\sum_{p \in P(k)} \# I'(\mathfrak{p}) = \begin{cases} \dfrac{q^{k/2}}{q+1} \displaystyle\sum_{p \in P(k)} L(1, \chi_{up}) & \text{when } k \text{ is even} \\[2ex] \dfrac{q^{k/2}}{2q^{1/2}} \displaystyle\sum_{p \in P(k)} L(1, \chi_p) + L(1, \chi_{up}) & \text{when } k \text{ is odd.} \end{cases} \tag{4.2}$$

5. Sums of L-series.

We compute here the sums of L-series given above. This is similar to the computations done in [12], where the average of the class numbers is computed over all discriminants, while our average involves only prime discriminants. We will compute

$$\sum_{p \in P(k)} L(1, \chi_p) \tag{5.1}$$

for k odd. The two other sums of L-series are computed in a completely similar way.

Since the function field analogue of the Riemann Hypothesis holds, we get an effective version of the Čebotarev Density Theorem. More precisely, we consider the following particular case of [7, Proposition 5.16]

Proposition 5.1. *Let E be a Galois extension of $F = \mathbb{F}_q[T]$ such that the algebraic closure of $\mathbb{F}_q$ in E stays $\mathbb{F}_q$. Let $G = \mathrm{Gal}(E/F)$ of order n, and let $\mathfrak{c}$ be a conjugacy class in G. Let*

$$C_k(E/F; \mathfrak{c}) = \left\{ p \in P(k),\ \textit{unramified in } E/F,\ \textit{and such that } \left(\frac{E/F}{p}\right) \in \mathfrak{c} \right\}.$$

Then

$$\left| \#C_k(E/F;\mathfrak{c}) - \frac{|\mathfrak{c}|}{n}\frac{q^k}{k} \right| < 8|\mathfrak{c}| q^{k/2}\left(1+\frac{g_E}{kn}\right). \quad \square$$

We need 2 simple cases of this proposition, namely:

(i) $E = F$.

Then, Proposition 5.1 gives

$$\left| \#P(k) - \frac{q^k}{k} \right| < 8q^{k/2}. \tag{5.2}$$

(ii) $E = F(\sqrt{n}), n \in \mathbb{F}_q[T]$ a monic non-square of degree $N \geq 1$. Write $n = f^2 m$, m square free of degree $M \geq 1$. Then

$$g_E = \begin{cases} \dfrac{M}{2} - 1 & \text{if } M \text{ is even} \\ \\ \dfrac{M-1}{2} & \text{if } M \text{ is odd .} \end{cases}$$

Using $\mathfrak{c} = \{1\}$ in $\mathrm{Gal}(E/F) = \{\pm 1\}$, Proposition 5.1 gives

$$\left| \#C_k(E/F;\mathfrak{c}) - \frac{1}{2}\frac{q^k}{k} \right| < 8\frac{q^{k/2}}{k}\left(k+N\right). \tag{5.3}$$

Then, since

$$\#C_k(E/F;\mathfrak{c}) = \frac{1}{2}\sum_{p\in P_{unr}(k)} 1 + \left(\frac{n}{p}\right),$$

where $P_{unr}(k)$ is the set of primes $p \in P(k)$ which do not ramify in $F(\sqrt{n})/F$, we get the estimate

$$\sum_{p\in P(k)} \left(\frac{p}{n}\right) = O\left(\frac{q^{k/2}}{k}(k+N)\right),$$

using (5.2), (5.3) and quadratic reciprocity.

We now use these results to evaluate (5.1). Inverting the summations,

$$\sum_{p\in P(k)} L(1,\chi_p) = \sum_{N=0}^{k-1} q^{-N} \sum_{\deg n = N}\sum_{p\in P(k)} \left(\frac{p}{n}\right). \tag{5.4}$$

When n is a square in $\mathbb{F}_q[T]$, say $n = m^2$, we have that $\left(\frac{p}{n}\right) = \left(\frac{p}{m}\right)^2 = 1$ for $(p,n) = 1$. But, since $0 \leq \deg n < \deg p$, the condition

$(p,n)=1$ is always true. Then,

$$\begin{aligned}\sum_{\substack{\deg n=N\\ n \text{ square}}}\sum_{p\in P(k)}\left(\frac{p}{n}\right) &= \sum_{\substack{\deg n=N\\ n \text{ square}}} \#P(k)\\ &= \left(\frac{q^k}{k}+O(q^{k/2})\right)\sum_{\substack{\deg n=N\\ n \text{ square}}} 1 \end{aligned}\tag{5.5}$$

by (i). The number of monic polynomials $n\in\mathbb{F}_q[T]$ such that $\deg n = N$ and n is a square is $q^{N/2}$ when N is even, and 0 when N is odd.

When n is not a square in $\mathbb{F}_q[T]$, the character $\left(\frac{\cdot}{n}\right)$ is not the trivial character. Then,

$$\sum_{\substack{\deg n=N\\ n \text{ non-square}}}\sum_{p\in P(k)}\left(\frac{p}{n}\right) = \sum_{\substack{\deg n=N\\ n \text{ non-square}}} O\left(\frac{q^{k/2}}{k}(k+N)\right)\tag{5.6}$$

by (ii).

Then, using (5.5) and (5.6), we get

$$\begin{aligned}\sum_{p\in P(k)} L(1,\chi_p) &= \sum_{N=0}^{k-1} q^{-N}\, O\left(q^N\,\frac{q^{k/2}}{k}\,(k+N)\right)\\ &\quad+\sum_{\substack{N=0\\ N\text{even}}}^{k-1} q^{-N}\, q^{N/2}\,\left(\frac{q^k}{k}+O\left(q^{k/2}\right)\right)\\ &= \frac{1}{1-q^{-1}}\,\frac{q^k}{k}+O\left(kq^{k/2}\right).\end{aligned}$$

In a completely similar way, we compute that $\sum_{p\in P(k)} L(1,\chi_{up})$ is also

$$\frac{1}{1-q^{-1}}\,\frac{q^k}{k}+O\left(kq^{k/2}\right)$$

for any positive integer k (odd or even).

Finally, using these results in (4.2), we get

$$\sum_{p\in P(k)}\#I'(\mathfrak{p}) = \begin{cases}\dfrac{q}{(q+1)(q-1)}\,\left(\dfrac{q^{3k/2}}{k}\right)+O\left(kq^k\right) & \text{when } k \text{ is even}\\[2ex] \dfrac{q}{\sqrt{q}(q+1)}\left(\dfrac{q^{3k/2}}{k}\right)+O\left(kq^k\right) & \text{when } k \text{ is odd,}\end{cases}\tag{5.7}$$

and using that in (3.2), we get Theorem 1.2.

6. Averaging over isomorphism classes.

We now prove Theorem 1.3. We then want to compute the average

$$\sum_{\substack{\deg a \le A,\ \deg b \le B \\ (a,b) \in M}} \pi_{\phi(a,b)}(k), \tag{6.1}$$

where M is defined by (1.3).

The characteristic function

$$\chi_M(a,b) = \begin{cases} 1 & (a,b) \in M \\ 0 & (a,b) \notin M \end{cases}$$

can be written as

$$\chi_M(a,b) = \sum_{\substack{c^{q-1} | a \\ c^{q^2-1} | b}} \mu(c),$$

where μ is the Mobius function, and the sum runs over monic $c \in \mathbb{F}_q[T]$. Then, we write (6.1) as

$$\sum_{\substack{\deg a \le A \\ \deg b \le B}} \sum_{\substack{c^{q-1} | a \\ c^{q^2-1} | b}} \mu(c) \sum_{p \in P(k)} \chi(a,b;p)$$

where $\chi(a,b;p) = 1$ when the reduction $\phi_p(a,b)$ of $\phi(a,b)$ over $\mathbb{F}_\mathfrak{p}$ is supersingular, and $\chi(a,b;p) = 0$ otherwise. Inverting the summations, we get

$$\sum_{p \in P(k)} \sum_{c} \mu(c) \sum_{\substack{a = c^{q-1} a' \\ \deg a \le A}} \sum_{\substack{b = c^{q^2-1} b' \\ \deg b \le B}} \chi(c^{q-1}a', c^{q^2-1}b'; p), \tag{6.2}$$

where the summation $\sum_c \mu(c)$ is restricted to monic c in $\mathbb{F}_q[T]$ such that

$$\deg c \le C = \min\left(\frac{A}{q-1}, \frac{B}{q^2-1}\right).$$

When $(p,c) = 1$,

$$\phi_p(c^{q-1}a', c^{q^2-1}b') \simeq \phi_p(a', b'),$$

which gives

$$\chi(a,b;p) = \chi(a',b';p).$$

To insure $(p,c) = 1$, we choose A, B such that

$$C = \min\left(\frac{A}{q-1}, \frac{B}{q^2-1}\right) < k. \tag{6.3}$$

We then rewrite (6.2) as

$$\sum_{p\in P(k)} \sum_{\deg c\leq C} \mu(c) \sum_{\substack{\deg a'\leq A' \\ \deg b'\leq B'}} \chi(a', b'; p) \tag{6.4}$$

where

$$A' = A - (q-1)\deg c \quad \text{and} \quad B' = B - (q^2-1)\deg c.$$

Using Lemma 3.1(i) and following the steps of Section 3, we rewrite (6.4) as

$$\sum_{p\in P(k)} \sum_{\deg c\leq C} \mu(c) \left(\frac{q^{A'+1}}{q^k} + O(1)\right) \left(\frac{q^{B'+1}}{q^k} + O(1)\right) \left(q^k - 1\right) \#I'(\mathfrak{p}). \tag{6.5}$$

Writing

$$q^{A'+1} = \frac{q^{A+1}}{|c|^{q-1}} \quad \text{and} \quad q^{B'+1} = \frac{q^{B+1}}{|c|^{q^2-1}},$$

and using (5.7), we can rewrite (6.5) as

$$C(k,q)\, q^{A+1}\, q^{B+1} \left(\sum_{\deg c\leq C} \frac{\mu(c)}{|c|^{q^2+q-2}}\right) \left(\frac{q^{k/2}}{k} + O(k)\right)$$
$$+ O\left(q^A \frac{q^{3k/2}}{k}\right) + O\left(q^B \frac{q^{3k/2}}{k}\right) + O\left(q^C \frac{q^{5k/2}}{k}\right),$$

where $C(k,q)$ is the constant of (1.2), and the O-constants depend only on q.

Let $\epsilon > 0$, and choose A, B big enough to have

$$A, B \geq k(1+\epsilon) \quad \text{and} \quad A + B \geq C + k(2+\epsilon). \tag{6.6}$$

One easily checks that (6.3) and (6.6) are compatible for small values of ϵ. With this condition, we finally get

$$\sum_{\substack{\deg a\leq A,\ \deg b\leq B \\ (a,b)\in M}} \pi_{\phi(a,b)}(k) =$$
$$C(k,q)\, q^{A+1}\, q^{B+1} \left(\sum_{\deg c\leq C} \frac{\mu(c)}{|c|^{q^2+q-2}}\right) \left(\frac{q^{k/2}}{k}\right) + \underline{o}\left(q^A q^B \frac{q^{k/2}}{k}\right).$$

This proves Theorem 1.3.

Acknowledgements. I would like to thank Ram Murty who suggested me this problem, and David Dorman for helpful discussions related to this work.

References

[1] E. Artin, Quadratische Körper im Gebiel der höheren Kongruenzen I, II (thesis), *in* Collected Papers, ed. S. Lang and J. Tate, Addison-Wesley, 1965.

[2] M.L. Brown, Singular moduli and supersingular moduli of Drinfeld modules, *Invent. Math.* **110** (1992), 419-439.

[3] C. David, Supersingular reduction of Drinfeld modules, *Duke Math. J.* **78** (1995), 399-412.

[4] P. Deligne and D. Husemoller, Survey of Drinfeld modules, *Contemp. Math.* **67** (1987), 25-91.

[5] M. Deuring, Die Typen der Multiplikatorenringe elliptischer Funktionenkörper, *Abh. Math. Sem. Hansischen Univ.* **14** (1941), 197-272.

[6] N. D. Elkies, The existence of infinitely many supersingular primes for every elliptic curve over $\mathbb{Q}$, *Invent. Math.* **89** (1987), 561-567.

[7] M. D. Fried and M. Jarden, "Field arithmetic", Springer-Verlag, Berlin, 1986.

[8] E. Fouvry and M. R. Murty, On the distribution of supersingular primes, *preprint.*

[9] E.-U. Gekeler, Zur Arithmetic von Drinfeld-Moduln, *Math. Ann.* **262** (1983), 167-182.

[10] E.-U. Gekeler, On finite Drinfeld modules, *Journal of Algebra* **141** (1991), 187-203.

[11] D. R. Hayes, A brief introduction to Drinfeld modules, *in* "The Arithmetic of Finite Fields", Ohio State University Mathematical Research Institute Publications **2**, ed. D. Goss, D. Hayes and M. Rosen, Walter de Gruyter, 1992.

[12] J. Hoffstein and M. Rosen, Average values of L-series in function fields, *J. reine angew. Math.* **426** (1992), 117-150.

[13] R. E. MacRae, On unique factorization in certain rings of algebraic functions, *J. Algebra* **17** (1971), 243-261.

[14] M. R. Murty, Recent developments in elliptic curves, *Proceedings of the Ramanujan Centennial International Conference* (1987), 45-54.

[15] J. Neukirch, *Class Field Theory*, Springer-Verlag, 1986.

CICMA, Department of Mathematics and Statistics, Concordia University, 1455 de Maisonneuve Boulevard West, Montréal, Québec, H3G 1M8, CANADA

E-mail address: chantal@abacus.concordia.ca