Supersingular Reduction of Drinfeld Modules

by

Chantal David [1]

Department of Mathematics and Statistics
A thesis submitted in partial fulfillment
of the requirements of the degree of
Doctor of Philosophy at McGill University
July 1993

ISBN 0-315-91748-2

Acknowledgments

I wish to thank my advisor, Professor Ram Murty, who guided me during the research leading to this thesis. It was a great privilege to be his student and to learn from him.

As a Ph.D. student at McGill, I had the chance to work in a stimulating and friendly atmosphere, and I would like to thank everybody who contributed to that. This includes the professors, staff members and other graduate students of the department, and the organizers and participants of the Québec-Vermont number theory seminars. I also thank David Dorman for helpful discussions related to this work, and Masato Kuwata for his efficient help with the computers.

Most of all, I wish to thank my friend, Benoit Larose, who was at my side during all my graduate studies, enthusiastic when things were going well, and caring when they were not going so well. I am particularly grateful that he always found time to discuss my mathematical problems, even when it meant putting his aside.

Abstract

Let ϕ be a rank 2 Drinfeld A-module over the ring A of polynomials over some finite field $\mathbb{F}_q$. We give a bound on the norm of those primes p of A which are factors of $P_d(j_\phi)$ for two distinct polynomials $d \in A$. We then show that the number of supersingular primes of ϕ with norm smaller than x is $\gg \log\log x$. We investigate the endomorphism rings of supersingular Drinfeld A-modules over finite fields. Under a mild hypothesis, this leads to an upper bound of $x^{3/4}\log^2 x$ for the number of supersingular primes of ϕ, with even degree, and norm smaller than x. Finally, we present the problem of the average distribution of supersingular primes of Drinfeld modules.

Résumé

Soit ϕ un A-module de Drinfeld de rang 2 sur l'anneau A des polynômes sur un corps fini $\mathbb{F}_q$. Nous bornons les premiers p de A qui apparaissent dans la décomposition en facteurs premiers de $P_d(j_\phi)$ pour deux polynômes distincts $d \in A$. Nous montrons alors que le nombre de premiers supersinguliers de ϕ, de norme inférieure à x, est $\gg \log\log x$. Nous étudions les anneaux des endomorphismes des modules supersinguliers sur des corps finis. Sous une hypothèse additionnelle, on obtient alors une borne supérieure de $x^{3/4}\log^2 x$ pour le nombre de premiers supersinguliers de ϕ, de degré pair et de norme inférieure à x. Finalement, nous présentons le problème de la distribution en moyenne des premiers supersinguliers d'un module de Drinfeld ϕ.

Contents

Introduction

We investigate in this thesis the distribution of supersingular primes of rank 2 Drinfeld modules, or elliptic modules. The theory of Drinfeld modules over function fields shows strong analogies with the theory of elliptic curves. To see this in our particular context, we first review the problem of the distribution of supersingular primes of elliptic curves.

Let E be an elliptic curve over $\mathbb{Q}$. The structure of its endomorphism ring $\text{End}(E)$ is well known. It contains the multiplication-by-m maps $[m]$, and then $\mathbb{Z} \subseteq \text{End}(E)$. If $\text{End}(E)$ is strictly larger than $\mathbb{Z}$, it has to be an order $\mathcal{O}$ in a quadratic imaginary extension of $\mathbb{Q}$. The curve E is then said to be a complex multiplication curve, or to have complex multiplication (by $\mathcal{O}$).

If E is an elliptic curve defined over a finite field $\mathbb{F}_p$, the ring $\text{End}(E)$ is always larger than $\mathbb{Z}$, since it also contains the Frobenius automorphism of $\mathbb{F}_p$. The possible endomorphism rings of elliptic curves over finite fields were studied by Deuring, who proved that $\text{End}(E)$ is either an order in a quadratic imaginary extension (and the curve is said to be ordinary), or an order in a definite quaternion algebra (and the curve is said to be supersingular).

If E is an elliptic curve defined over $\mathbb{Q}$, the reduction of E over the finite field $\mathbb{F}_p$

is an elliptic curve over this field, for all but finitely many primes p. We denote this elliptic curve by E_p. It is then natural to ask how often supersingularity happens. If E is a complex multiplication curve, the question was answered by Deuring [3]. Let

$$\pi_E(x) = \#\{p \leq x : E_p \text{ is supersingular}\}.$$

Then Deuring showed that

$$\pi_E(x) \sim \frac{1}{2}\frac{x}{\log x},$$

i.e. supersingularity happens for half of the primes. In general, Deuring also gave a criterion to detect supersingular primes of a curve E. Let $P_d(x)$ be the monic polynomial whose roots are exactly the j-invariants of the elliptic curves over $\overline{\mathbb{Q}}$ with complex multiplication by the order

$$\mathcal{O}_d = \mathbb{Z}\left[\frac{d+\sqrt{-d}}{2}\right].$$

Theorem (Deuring's Criterion) *Let E be an elliptic curve defined over $\mathbb{Q}$. Then p is a supersingular prime of E if and only if there exists a positive integer d such that*

$$P_d(j_E) \equiv 0 \ mod\, p$$

and p does not split in the quadratic extension $\mathbb{Q}(\sqrt{d})/\mathbb{Q}$.

Until recently, it was not known if, given an elliptic curve $E/\mathbb{Q}$ without complex multiplication, there are infinitely many primes p such that the reduction of E at p is supersingular. Elkies answered this question [7], and it was shown by Elkies [8] and Murty [21] that

$$\pi_E(x) \gg \log\log x$$

under the generalised Riemann Hypothesis. Recently, some unconditional estimates were obtained by Fouvry and Murty [10]. Murty also noted that an upper bound of $O(x^{3/4})$ follows from the work of Kaneko [19]. For elliptic curves over $\mathbb{Q}$ without complex multiplication curves, we have:

Conjecture (Lang-Trotter Conjecture)

$$\pi_E(x) \sim C_E \frac{\sqrt{x}}{\log x}.$$

Recently, Fouvry and R. Murty [10] showed that the Lang-Trotter conjecture is true on average.

Let L be a field over A, i.e. an $\mathbb{F}_q$-algebra morphism $\gamma : A \to L$, where L is an overfield of $\mathbb{F}_q$. Let $A = \mathbb{F}_q[T]$ be the ring of polynomials in one indeterminate over finite fields, and $\mathbb{G}_a$ be the additive group scheme over L. A rank 2 Drinfeld A-module ϕ over a field L is a ring homomorphism

$$\begin{aligned} \phi : A &\longrightarrow \operatorname{End}_L(\mathbb{G}_a) \\ a &\longmapsto \phi_a \end{aligned}$$

with some additional properties (see Chapter 1 for more details). Then the multiplication-by-a maps ϕ_a form a subring of $\operatorname{End}(\phi)$ isomorphic to A. Over $L = \mathbb{F}_q(T)$, the quotient field of A, either $\operatorname{End}(\phi) = A$, or $\operatorname{End}(\phi)$ contains an order of a quadratic imaginary field extension of $\mathbb{F}_q(T)$. Over $L = A/\mathfrak{p}$, $\operatorname{End}(\phi)$ is either a commutative ring or an order in a quaternion algebra over $\mathbb{F}_q(T)$. In the latter case, we say that ϕ is supersingular. Then, given a rank 2 Drinfeld A-module defined over A, and $\mathfrak{p}$ a regular prime, let $\phi_{\mathfrak{p}}$ be the reduction of ϕ on $L = A/\mathfrak{p}$, and

$$\pi_\phi(x) = \#\left\{\mathfrak{p} \in \text{Spec } A : |\mathfrak{p}| \le x \text{ and } \phi_{\mathfrak{p}} \text{ is supersingular}\right\}.$$

Brown [2] showed that the theory developed by Deuring for elliptic curves over finite fields transfers to the case of Drinfeld modules, and then showed that

$$\pi_\phi(x) \gg \log\log\log x.$$

Following the same ideas, but with sharper estimates, we improve this lower bound to $\sqrt{\log\log x}$ (Theorem 3.2). This can be further improved if we know an analog to the result of Gross and Zagier [14] on singular moduli. More precisely, let $P_d(x)$ be the polynomial whose roots are exactly the j-invariants of the rank 2 Drinfeld A-modules with complex multiplication by $A[\sqrt{d}]$. We show that if p divides $P_{d_1}(j_\phi)$ and $P_{d_2}(j_\phi)$, then $\deg p \leq \deg d_1 d_2$ (Theorem 2.1). This generalize a result of Dorman [5], and we use it to get a bound of $\log\log x$ (Theorem 3.3). All those estimates hold unconditionally, since the Riemann hypothesis is proved in the case of function fields.

We then turn to the problem of finding upper bounds to $\pi_\phi(x)$. In the classical case of an elliptic curve E, these can be obtained via the l-adic representations

$$\rho_{E,l} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{GL}_2(\mathbb{Z}_l).$$

By Serre's Theorem, $\overline{\rho}_{E,l}$, the reduction mod l of the representation $\rho_{E,l}$, is a surjective map on $\mathrm{GL}_2(\mathbb{F}_l)$ for all but finitely many l. Upper bounds then follow applying the Čebotarev's Density Theorem and the generalized Riemann Hypothesis to the finite Galois extensions $K_l/\mathbb{Q}$, where K_l is the fixed field of $\ker \overline{\rho}_l$. In the case of Drinfeld modules, there are similar representations over the $\mathfrak{q}$-adic Tate modules of ϕ (see for example [13]), but the analog of Serre's Theorem is not known. This would be an interesting question for future research.

Another way to approach the problem is to find elements of small norm in $\mathrm{End}(\phi)$. Then, the supersingular primes of ϕ with $|\phi| \leq x$ will be found as factors of $P_d(j_\phi)$, where d is of small norm, and $\pi_\phi(x)$ can be bounded above. This is the subject of Chapter 4. We first find 2 families of maximal orders which are candidates for the endomorphism rings of supersingular Drinfeld A-modules over the finite fields $A/\mathfrak{p}$, when $\deg \mathfrak{p}$ is even. In each of those maximal orders, we find elements of small norm. It is still to be shown that these 2 families cover the isomorphism classes of the endomorphism rings of supersingular Drinfeld modules over $A/\mathfrak{p}$. We would then have

$$\pi_\phi^{even}(x) \ll x^{3/4}\log^2 x$$

where

$$\pi_\phi^{even}(x) = \#\{\mathfrak{p} \in \text{Spec } A : \deg \mathfrak{p} \text{ is even, } |\mathfrak{p}| \le x \text{ and } \phi_\mathfrak{p} \text{ is supersingular}\}$$

(Theorem 4.10).

Finally, we present in Appendix 1 some questions for further research. By Deuring's criterion for Drinfeld modules (Theorem 1.15),

$$\pi_\phi(x) \sim \frac{1}{2}\frac{x}{\log_q x}$$

when ϕ has complex multiplication. In general, we compute the average

$$\frac{1}{K_a K_b}\sum_{\substack{|a|\le K_a \\ |b|\le K_b}} \pi_{\phi(a,b)}(x)$$

where $\phi(a,b)$ is the Drinfeld A-module given by

$$\gamma(T) + a\mathcal{F} + b\mathcal{F}^2, \quad a, b \in A, b \neq 0.$$

As in Fouvry and Murty [10], we expect to obtain an average distribution of $\frac{\sqrt{x}}{\log x}$, i.e. the Lang-Trotter conjecture would hold on average for Drinfeld modules.

Chapter 1

Function Fields and Drinfeld Modules

1.1 Function Fields

We define here function fields, and review some of their properties, namely the Riemann Hypothesis, the Čebotarev Theorem and the Riemann-Hurwitz Formula. See [9] for more details.

Throughout this thesis, let $\mathbb{F}_q$ be the finite field with q elements, $q = p^s$ with $p \neq 2$.

1.1.1 Definitions

Definition 1.1 *A function field (of 1 variable) over $\mathbb{F}_q$ is an extension $K/\mathbb{F}_q$ such that*

(i) the transcendence degree of $K/\mathbb{F}_q$ is 1;

(ii) K is finitely generated over $\mathbb{F}_q$;

(iii) $\mathbb{F}_q$ is algebraically closed in K.

Let K be a function field over $\mathbb{F}_q$. A prime divisor of K is an equivalence class of places of K which are trivial on $\mathbb{F}_q$. Let $\mathcal{P}(K)$ be the set of prime divisors of K. For $\mathfrak{p} \in \mathcal{P}(K)$, the completion of K at $\mathfrak{p}$ is denoted by $K_\mathfrak{p}$. It is a local field, with valuation ring $O_\mathfrak{p}$ and maximal ideal $m_\mathfrak{p}$. The finite field $O_\mathfrak{p}/m_\mathfrak{p}$ is called the residue field at $\mathfrak{p}$, and denoted $\mathbb{K}_\mathfrak{p}$. For any $\mathfrak{p} \in \mathcal{P}(K)$, we define the norm $|\mathfrak{p}|$ and the degree $\deg \mathfrak{p}$ by

$$\#(O_\mathfrak{p}/m_\mathfrak{p}) = |\mathfrak{p}| = q^{\deg \mathfrak{p}}.$$

Let $\mathcal{D}(K)$ be the free abelian group generated by the elements of $\mathcal{P}(K)$. It is called the group of divisors of K. Each divisor of $\mathcal{D}(K)$ can be written as

$$\mathfrak{a} = \sum_\mathfrak{p} \alpha_\mathfrak{p}\, \mathfrak{p}$$

where $\mathfrak{p}$ runs over the prime divisors, the $\alpha_\mathfrak{p}$ are integers and all but finitely many of them are zero. We say that the divisor $\mathfrak{a}$ is positive, or that $\mathfrak{a} \geq 0$, when $\alpha_\mathfrak{p} \geq 0$ for every pime divisor $\mathfrak{p}$. Finally, for any $\mathfrak{a} \in \mathcal{D}(K)$, we define

$$|\mathfrak{a}| = \prod_\mathfrak{p} |\mathfrak{p}|^{\alpha_\mathfrak{p}},$$

which also gives

$$\deg \mathfrak{a} = \sum_\mathfrak{p} \alpha_\mathfrak{p} \deg \mathfrak{p}.$$

Let $A = \mathbb{F}_q[T]$ and $F = \mathbb{F}_q(T)$ denote respectively the ring of polynomials and the field of rational functions in an indeterminate T. Then F is a function field over $\mathbb{F}_q$ (with genus 0). The prime divisors of F consist of the prime ideals $\mathfrak{p} = (p)$ of A, and ∞, the place at infinity, which is also called the prime at ∞. For $a \in A^*$, we define $|a|$ and $\deg a$ by

$$|a| = q^{\deg a} = |\mathfrak{a}|,$$

where $\mathfrak{a} = (a)$. Then, for $f = \frac{\mathfrak{a}}{\mathfrak{b}} \in F^*$, we define $|f|$ and $\deg f$ by

$$|f| = q^{\deg f} = q^{\deg a - \deg b}.$$

The completion F_∞ of F at the infinite prime is $\mathbb{F}_q((T^{-1}))$, the field of formal Laurent series in T^{-1}. The (unique) extension of $|\ |$ to F_∞ is also denoted by $|\ |$. Let $\overline{F}_\infty$ be the algebraic closure of F_∞, and $\mathfrak{C}$ the completicn of the algebraic closure $\overline{F}_\infty$. Let $\mathfrak{H} = \mathfrak{C} - F_\infty$ be the Drinfeld "upper half-plane".

1.1.2 Riemann Hypothesis

Let K be a function field of 1 variable over $\mathbb{F}_q$, and denote its genus by g_K. Define the ζ-function of the function field $K/\mathbb{F}_q$ to be the Dirichlet series

$$\zeta_K(s) = \prod_{\mathfrak{p} \in \mathcal{P}(K)} (1 - |\mathfrak{p}|^{-s})^{-1} = \sum_{\substack{\mathfrak{a} \in \mathcal{D}(K) \\ \mathfrak{a} \geq 0}} |\mathfrak{a}|^{-s}.$$

We also define

$$Z_K(t) = \sum_{\substack{\mathfrak{a} \in \mathcal{D}(K) \\ \mathfrak{a} \geq 0}} t^{\deg \mathfrak{a}}$$

such that $\zeta_K(s) = Z_K(q^{-s})$. Then

(1) The Dirichlet series $\zeta_K(s)$ converges in the right-half plane $\mathrm{Re}(s) > 1$; $\zeta_K(s)$ is an analytic and non-zero function in this region.

(2) $\zeta_K(s)$ has a meromorphic continuation to the whole complex plane, with only poles being simple poles at $s = 0$ and $s = 1$. We also denote this analytic continuation by $\zeta_K(s)$.

(3) The function $Z_K(t)$ satisfies the functional equation:

$$(\sqrt{q}t)^{1-g_K}\, Z_K(t) = (\sqrt{q}t)^{g_K - 1}\, Z_K\left(\frac{1}{qt}\right).$$

(4) The function $\zeta_K(t)$ satisfies the functional equation:

$$q^{s(g_K-1)}\zeta_K(s) = q^{(1-s)(g_K-1)}\zeta_K(1-s).$$

One can also show that

$$Z_K(t) = \frac{L_K(t)}{(1-t)(1-qt)} \tag{1.1}$$

with $L_K(t) = a_0 + a_1 t + \ldots + a_{2g_K}t^{2g_K}$ is a polynomial with rational coefficients, which can be written as

$$L_K(t) = \prod_{i=1}^{g_K}(1-\omega_i t)(1-\omega_i' t)$$

with

$$\omega_i\omega_i' = q \quad \text{for } 1 \leq i \leq g_K$$

We can then state the Riemann Hypothesis for function fields:

Theorem 1.2 (Riemann Hypothesis)

(a) The zeros of $\zeta_K(s)$ lie on the line $Re(s) = \frac{1}{2}$;

(b) The zeros of $Z_K(t)$ lie on $|t| = q^{-1/2}$;

(c) $|\omega_i| = |\omega_i'| = \sqrt{q}$ for $i = 1, \ldots, g_K$.

1.1.3 Čebotarev's Theorem

We state here an explicit version of the Čebotarev density theorem for function fields. We specialise to the case of extensions E/F, where $F = \mathbb{F}_q(T)$, but one could develop the theorem for any Galois extension E/K of function fields, as in [9]. Let G be the Galois group $G = \mathrm{Gal}(E/F)$. For $\mathfrak{p}$ an unramified prime ideal of A, let

$$\left(\frac{E/F}{\mathfrak{p}}\right)$$

be the Artin symbol of $\mathfrak{p}$ relative to the extension E/F. We denote by L the algebraic closure of $\mathbb{F}_q$ in E, and let

$$N = [L : \mathbb{F}_q];$$
$$M = [E : LF].$$

Let C be a conjugacy class in G, and denote

$$\begin{aligned} P_{unr}(E/F) &= \{\mathfrak{p} \in \text{Spec } A \;:\; \mathfrak{p} \text{ is unramified in } E/F\} \\ P_k(E/F) &= \{\mathfrak{p} \in P_{unr}(E/F) \;:\; \deg \mathfrak{p} = k\} \\ C_k(E/F;C) &= \left\{\mathfrak{p} \in P_k(E/F) \;:\; \left(\frac{E/F}{\mathfrak{p}}\right) = C\right\} \end{aligned}$$

Then, using the Riemann Hypothesis, one can show that

Theorem 1.3 (Čebotarev's Density Theorem) *([9, Proposition 5.16]) Let ϕ be the Frobenius element of $\mathbb{F}_q$, i.e.*

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

Let a be a positive integer such that

$$res_L\, \tau = res_L\, \phi^a \text{ for any } \tau \in C.$$

Then, for $k \not\equiv a \bmod N$,

$$|C_k(E/F;C)| = 0$$

and for $k \equiv a \bmod N$

$$\left| |C_k(E/F;C)| - \frac{|C|}{M}\frac{q^k}{k} \right| \ll |C| q^{k/2} \left(1 + \frac{g_E}{kM}\right),$$

where the O-constant is absolute.

(This is in fact strnnger than what is given in the statement of Proposition 5.16 of [9], since we are in the particular case of Galois extensions over $\mathbb{F}_q(T)$.)

Let

$$\pi_{\mathcal{C}}(E/F;x) = \#\left\{\mathfrak{p} \in P_{unr}(E/F) \ : \ |\mathfrak{p}| \leq x, \text{ and } \left(\frac{E/F}{\mathfrak{p}}\right) = \mathcal{C}\right\}.$$

Then

$$\begin{aligned} \pi_{\mathcal{C}}(E/F;x) &= \sum_{q^k \leq x} |C_k(E/F;\mathcal{C})| \\ &= \sum_{\substack{q^k \leq x \\ k \equiv a(N)}} |C_k(E/F;\mathcal{C})|. \end{aligned}$$

1.1.4 Riemann-Hurwitz Formula

Let E be a finite separable extension of a function field K over $\mathbb{F}_q$. We define the different $\mathfrak{D}_{E/K}$ to be the divisor of $\mathcal{D}(E)$

$$\mathfrak{D}_{E/K} = \sum m(\mathfrak{P})\mathfrak{P}$$

where $\mathfrak{P}$ runs over the prime divisors of $E/\mathbb{F}_q$ (see [9, p. 24] for a more precise definition). One can compute that

$$m(\mathfrak{P}) = \begin{cases} 0 & \text{if } \mathfrak{P} \text{ is unramified} \\ (e(\mathfrak{P}|\mathfrak{p}) - 1) & \text{if } \mathfrak{P} \text{ is tamely ramified.} \end{cases}$$

The case of wild ramification is much more subtle, but will not be needed in this work.

Theorem 1.4 (Riemann Hurwitz Formula) *([9, p. 24]) Let E/K as defined above. Then*

$$2g_E - 2 = [E:K](2g_K - 2) + \deg \mathfrak{D}_{E/K}.$$

1.1.5 Quadratic Reciprocity

Finally, we state here the quadratic reciprocity over function fields. The details can be found in [22].

Let O_∞ and m_∞ be respectively the valuation ring and the maximal ideal of the completion $F_\infty = \mathbb{F}_q((T^{-1}))$ of $F = \mathbb{F}_q(T)$ at the infinite place. Any $f \in F^*$ can be written uniquely as $\alpha\, u\, T^{\deg f}$, where

$$\begin{aligned} \alpha &\in \mathbb{F}_q^* \\ u &\in O_\infty^1 = \{f \in O_\infty^* : f \equiv 1 \bmod m_\infty\}. \end{aligned}$$

We then define

$$\begin{aligned} \omega(f) &= \alpha \\ \mathrm{sgn}\ f &= \omega(f)^{(q-1)/2} = \begin{cases} 1 & \text{if } \omega(f) \in (\mathbb{F}_q^*)^2 \\ -1 & \text{if } \omega(f) \notin (\mathbb{F}_q^*)^2 \end{cases} \end{aligned}$$

Theorem 1.5 (Quadratic Reciprocity) *Suppose $a, b \in A^*$ are non-zero coprime polynomials. Then*

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

where $(a,b)_\infty$ is the quadratic Hilbert symbol at ∞.

We explicitly compute $(a,b)_\infty$ as

$$(a,b)_\infty = \omega\left((-1)^{\deg a \deg b}\frac{a^{\deg b}}{b^{\deg a}}\right)^{(q-1)/2} \tag{1.2}$$

for any $a, b \in F^*$. If $a, b \in A^*$, we can rewrite the last expression as

$$(a,b)_\infty = (-1)^{\frac{q-1}{2}\deg a \deg b}(\mathrm{sgn}\ a)^{\deg b}(\mathrm{sgn}\ b)^{\deg a}. \tag{1.3}$$

1.2 Drinfeld Modules

We review here the basic facts about Drinfeld modules, which were first defined in [6]. The material of this section can also be found in [11], [13] or [15] for example.

1.2.1 Definitions

Let L be a field over $\mathbb{F}_q$ with an $\mathbb{F}_q$-algebra morphism

$$\gamma : A \to L.$$

We will always have that γ is an injection, or the reduction map mod $\mathfrak{p}$, for $\mathfrak{p}$ a prime ideal of A. Let $L\{\mathcal{F}\}$ be the ring generated by L and $\mathcal{F}$ under the relations

$$\mathcal{F}\, c = c^q\, \mathcal{F} \quad \text{for any } c \in L.$$

If we identify $\mathcal{F}$ with the Frobenius automorphism $x \mapsto x^q$ of $\mathbb{F}_q$, $L\{\mathcal{F}\}$ is naturally a subring of $\mathrm{End}_L(\mathbb{G}_a)$, where $\mathbb{G}_a$ is the additive group scheme of L. Each element of $\mathrm{End}_L(\mathbb{G}_a)$ can be written uniquely as a left polynomial

$$\sum c_i \mathcal{F}^i, \quad c_i \in L.$$

These polynomials are multiplied by substitution, corresponding to composition of endomorphisms in the ring $\mathrm{End}_L(\mathbb{G}_a)$. For $u \in L\{\mathcal{F}\}$, let $\deg u$ be the degree in $\mathcal{F}$ of the left polynomial u.

Definition 1.6 *A Drinfeld A-module ϕ of rank $r > 0$ over L is a ring homomorphism*

$$\begin{aligned} \phi : A &\longrightarrow L\{\mathcal{F}\} \\ a &\longmapsto \phi_a \end{aligned}$$

such that

(i) $\forall a \in A,\ \deg \phi_a = r \deg a$;

(ii) ϕ_a *has constant term* $\gamma(a)$.

If the map $\gamma : A \longrightarrow L$ *is injective, then* ϕ *is said to have generic characteristic; if not, its characteristic is Ker* γ.

Let ϕ be a Drinfeld A-module of rank r over F. Then ϕ is completely determined by ϕ_T, the value of ϕ at T. We then write it as

$$\phi_T = \gamma(T) + a_1\mathcal{F} + \ldots + a_r\mathcal{F}^r,\ \ a_i \in L,\ 1 \leq i \leq r,\ \ a_r \neq 0.$$

We consider here rank 2 Drinfeld A-modules, or elliptic modules. Such a Drinfeld A-module can be written as

$$\phi_T = \gamma(T) + a\mathcal{F} + b\mathcal{F}^2,\ \ a, b \in L,\ \ b \neq 0.$$

We also denote it by $\phi(a, b)$. The j-invariant j_ϕ of $\phi(a, b)$ is

$$j_\phi = \frac{a^{q+1}}{b}.$$

Definition 1.7 *A morphism, or isogeny, between 2 Drinfeld A-modules* ϕ *and* ψ *over L is an element* $c \in L\{\mathcal{F}\}$ *such that* $c \circ \phi_a = \psi_a \circ c$ *for all* $a \in A$. *If* $c \in L^*$ *and* $\psi_a = c \circ \phi_a \circ c^{-1}$, *then* ψ *and* ϕ *are isomorphic. Non-trivial isogenies exist only between modules of the same rank. For* ϕ *a rank 2 Drinfeld A-module defined over L, the set of L-isogenies* $\phi \longrightarrow \phi$ *is denoted by* $End_L(\phi)$, *and is a ring under the usual operations. We denote by* $End(\phi)$ *the ring* $End_{\overline{L}}(\phi)$.

The following Theorem then justifies the definition of the quantity j_ϕ:

Theorem 1.8 *(Gekeler [11, Lemma 4.1]) Let L be algebraically closed. Then two elliptic A-modules* $\phi(a, b)$, *and* $\psi(a', b')$ *are isomorphic if and only if* $j_\phi = j_\psi$.

There is an analytic description of rank 2 Drinfeld modules over $\mathfrak{C}$, in terms of A-lattices. In fact, the category of such modules is equivalent to the category of A-lattices of rank 2 in $\mathfrak{C}$. Hence, by Theorem 1.8, $GL_2(A)\backslash\mathfrak{H}$ parametrises the set of isomorphism classes of rank 2 Drinfeld A-modules over $\mathfrak{C}$ by the analytic map

$$\begin{aligned} j : GL_2(A)\backslash\mathfrak{H} &\xrightarrow{\sim} \mathfrak{C} \\ A \oplus Az &\longmapsto j(z). \end{aligned}$$

This j-function is the analog of the Dedekind j-function, and enjoys many of the same properties, as will be seen in the next sections.

1.2.2 Complex Multiplication

Theorem 1.9 *Let ϕ be a rank r Drinfeld A-module defined over L. Then*

(i) End(ϕ) is a projective A-module of rank $\leq r^2$.

(ii) If ϕ is of generic characteristic, then End(ϕ) is a commutative A-module of rank $\leq r$.

Let ϕ be a rank 2 Drinfeld A-module defined over L. It is clear that $A \subseteq \mathrm{End}(\phi)$, and ϕ is called singular when $\mathrm{End}(\phi) \neq A$. In order to describe singular modules, we need

Definition 1.10 *A quadratic imaginary extension K/F is a field extension of dimension 2 over F such that ∞ does not split in K.*

The following Lemma characterises those extensions:

Lemma 1.11 *Let $K = F(\sqrt{a})$, with $a \in A^*$. Then*

(i) if $\deg a$ is even, and sgn $a = 1$, ∞ splits in K/F;

(ii) if $\deg a$ is even and sgn $a = -1$, then ∞ is inert in K/F;

(iii) if $\deg a$ is odd, then ∞ ramifies in K/F.

Let O_K be the integral closure of A in K. An order $\mathcal{O}$ of K is an A-subalgebra of O_K whose field of fractions is K.

Definition 1.12 *Let $\mathcal{O}$ be an order in a quadratic imaginary extension K/F. A singular rank 2 Drinfeld A-module ϕ is said to have complex multiplication by $\mathcal{O}$ if there is an embedding $\mathcal{O} \subseteq End\,(\phi)$.*

Let $P_{\mathcal{O}}(x)$ be the monic polynomial whose roots are exactly the j-invariants of all the singular rank 2 Drinfeld A-modules defined over $\mathfrak{C}$ with complex multiplication by $\mathcal{O}$. We consider the special case $K = F(\sqrt{d})$ for some $d \in A$, where d is a fundamental discriminant, or equivalently square-free, and $\mathcal{O} = O_K = A[\sqrt{d}]$. Then denote $P_{\mathcal{O}}(x)$ by $P_d(x)$. The roots of $P_d(x)$ are called the singular moduli associated to d. By the analytic parametrisation, we can write

$$\begin{aligned} P_d(x) &= \prod_{\mathcal{O}\subseteq End(\phi)} (x - j(\mathcal{O})) \\ &= \prod_{\substack{[\tau] \\ disc(\tau)=d}} (x - j(\tau)), \end{aligned} \tag{1.4}$$

where the product is over the equivalences classes $[\tau]$ of quadratic imaginary elements of discriminant d over A. Let $h(d)$ be the class number of O_K.

Theorem 1.13 *Let $d \in A$ be a fundamental discriminant, and let $P_d(x)$ be as in (1.4). Let τ be such that $j(\tau)$ is a singular moduli associated to d. Then* *(i) $j(\tau)$ is integral of degree $h(d)$ over A;*

(ii) The $h(d)$ Galois conjugates of $j(\tau)$ over O_K are the values $j(\tau')$, where τ' runs through the equivalence classes $[\tau']$ of imaginary quadratic elements of discriminant d over A;

(iii) $P_d(x)$ is a polynomial of degree $h(d)$ over A.

Proof: See [11] and [16].

1.2.3 Supersingular modules and supersingular reduction

Let $\mathfrak{p} = (p)$ be a prime ideal of A. Then $\mathbb{F}_\mathfrak{p} = A/\mathfrak{p} \simeq \mathbb{F}_{q^{\deg p}}$. Let ϕ be a rank 2 Drinfeld A-module of characteristic $\mathfrak{p}$ over $L = \mathbb{F}_\mathfrak{p}$, i.e.

$$\gamma : A \longrightarrow L$$

is the reduction map mod $\mathfrak{p}$ sending a to a mod $\mathfrak{p}$. Let τ be the Frobenius automorphism of $\mathbb{F}_q$

$$\tau : x \mapsto x^{q^{\deg p}}.$$

Then $\tau \in \mathrm{End}(\phi)$, since

$$\tau \circ \phi_a = \phi_a \circ \tau$$

for all $a \in A$, ϕ being defined over $\mathbb{F}_q$.

Definition 1.14 *The Drinfeld module ϕ described above is supersingular if the following equivalent conditions hold:*

(1) ϕ_p is purely inseparable, i.e. $\phi_p = \mathcal{F}^h$ for some integer h;

(2) There is no p-torsion points, i.e. $Ker(\phi_p) = 0$;

(3) $End_{\overline{L}}(\phi)$ is a non-commutative ring;

(4) $End_{\overline{L}}(\phi)$ is a maximal order in the unique quaternion algebra over F which is ramified at $\mathfrak{p}$ and ∞, and unramified elsewhere.

The equivalence of those properties is proved in [11, Thm 5.3] and [13, Proposition 4.1]. A Drinfeld module which is not supersingular is said to be ordinary.

Let $\phi = \phi(a,b)$ be a rank 2 Drinfeld A-module of generic characteristic over F defined by

$$\phi_T = \gamma + a\mathcal{F} + b\mathcal{F}^2, \quad a, b \in A, \ b \neq 0. \tag{1.5}$$

Let $\mathfrak{p} = (p)$ be a prime ideal of A. For $u = \sum c_i \mathcal{F}^i \in \phi(A)$, let

$$u \bmod \mathfrak{p} = \sum (c_i \bmod \mathfrak{p}) \mathcal{F}^i.$$

The reduction of ϕ at $\mathfrak{p}$ (or at p) is then the A-module $\phi_\mathfrak{p}$ defined by

$$\begin{aligned} \phi_\mathfrak{p} : A &\longrightarrow \mathbb{F}_\mathfrak{p}\{\mathcal{F}\} \\ a &\longmapsto \phi_a \bmod \mathfrak{p}. \end{aligned}$$

$\phi_\mathfrak{p}$ is a rank 2 Drinfeld A-module over the residue field $\mathbb{F}_\mathfrak{p}$ for all $\mathfrak{p} = (p)$ such that $p \nmid b$. These are called the regular primes of ϕ. For those primes, we say that $\mathfrak{p}$ (or p) is a supersingular prime for ϕ, or that ϕ has supersingular reduction at $\mathfrak{p}$ (or p), if $\phi_\mathfrak{p}$ is a supersingular A-module. If not, we say that $\mathfrak{p}$ (or p) is an ordinary prime for ϕ, or that ϕ has ordinary reduction at $\mathfrak{p}$ (or p).

The following theorem is the statement of the criterion of Deuring, which allows the detection of supersingular primes of elliptic curves, in the context of Drinfeld modules.

Theorem 1.15 (Deuring's Criterion) *[2, Lemma 2.9.3] Let $\phi(a,b)$ be the rank 2 Drinfeld module as defined by (1.5). Let $\mathfrak{p} = (p)$ be a regular prime of ϕ. Then ϕ has* *supersingular reduction at* $\mathfrak{p}$ *if and only if there exists an order* $\mathcal{O}$ *of an imaginary quadratic field extension* K *of* F *such that*

(1) $P_{\mathcal{O}}(j_\phi) \equiv 0 \ mod \, p$*;*

(2) p *is inert or ramified in* K.

Chapter 2

A bound for the prime divisors of the resultant

2.1 Introduction

Let ϕ be the rank 2 Drinfeld A-module defined over F

$$\phi_T = \gamma(T) + a\mathcal{F} + b\mathcal{F}^2, \quad a, b \in F,\ b \neq 0, \tag{2.1}$$

with j-invariant

$$j_\phi = \frac{a^{q+1}}{b} \in F^*.$$

We prove in this chapter the following Theorem:

Theorem 2.1 *Let d_1, $d_2 \in A$ be two distinct fundamental discriminants, and let p be a prime element of A such that*

$$p \mid P_{d_1}(j_\phi) \text{ and } p \mid P_{d_2}(j_\phi).$$

Then $\deg p \leq \deg d_1 d_2$.

For at least one of d_1 or d_2 of even degree, the result was proved by Dorman (see [4] and [5]), as a corollary of the explicit factorization of

$$J(d_1, d_2) = \prod_{\substack{[\tau], [\tau'] \\ disc(\tau)=d_1 \\ disc(\tau')=d_2}} (j(\tau) - j(\tau'))^{\left(q^2-1/\omega\omega'\right)},$$

where ω and ω' are the number of roots of unity in the quadratic orders of discriminant d and d' respectively.

It should be noted that we cannot apply Dorman's result in our work, since in the next chapter, we are going to apply Theorem 2.1 with d_1 and d_2 odd degree polynomials in order to get lower bounds on $\pi_\phi(x)$.

We prove Theorem 2.1 following the ideas of Kaneko [19] which proves a similar result for elliptic curves. His proof depends on the arithmetic of quaternion algebras over $\mathbb{Q}$. We can transfer the proof to the case of Drinfeld modules, since the structure of quaternion algebras is similar over any global field.

2.2 Quaternion algebras

We review here the basic facts about quaternion algebras. All the material of this section is from [24]. Let K be a global field, either a function field over a finite field or a number field.

Definition 2.2 *A quaternion algebra H/K is a K-algebra of basis 1, i, j, ij,*

$$H = K + Ki + Kj + Kij,$$

where $i^2 = a$, $j^2 = b$, $ij = -ji$ for some $a, b \in K^*$. We denote $H = \{a,b\}$.

Then, any element h in H/K is quadratic over K with minimal polynomial

$$x^2 - \mathrm{tr}(h)\, x + \mathrm{n}(h),$$

where the (reduced) trace tr and the (reduced) norm n of

$$h = x + yi + zj + tij$$

are defined by

$$\begin{aligned} \mathrm{tr}(h) &= 2x; \\ \mathrm{n}(h) &= x^2 - ay^2 - bz^2 + abt^2. \end{aligned}$$

The trace and the norm enjoy the following properties:

(i) $\mathrm{n}(hk) = \mathrm{n}(h)\,\mathrm{n}(k)$;

(ii) $\mathrm{tr}(ah + bk) = a\,\mathrm{tr}(h) + b\,\mathrm{tr}(k)$;

(iii) $\mathrm{tr}(hk) = \mathrm{tr}(kh)$;

when $h, k \in H$, $a, b \in K$.

Definition 2.3 *Let v be a prime divisor of K. Then v is said to ramify in H if $H_v = H \otimes_K K_v$ is a field.*

Writing $H = \{a, b\}$, one can show

$$v \text{ ramifies in } H \iff (a, b)_v = -1$$

where $(a, b)_v$ is the local quadratic Hilbert symbol. Also, for any H/K, the number of ramified places is finite. We denote this set by $\mathrm{Ram}(H)$.

Theorem 2.4 (Classification Theorem) *$|Ram(H)|$ is even, and for any finite set S of prime divisors of K with $|S|$ even, there is, up to isomorphism, a unique quaternion algebra H/K such that $Ram(H) = S$.*

Example: We are interested in the quaternion algebras H over $F = \mathbb{F}_q(T)$ such that $\mathrm{Ram}(H) = \{\mathfrak{p}, \infty\}$, $\mathfrak{p}$ a prime ideal of A. These contain, as maximal orders, the rings $\mathrm{End}(\phi)$, for ϕ a supersingular Drinfeld A-module in characteristic $\mathfrak{p}$ (see Definition 1.14). Let $H = F_{\mathfrak{p},\infty}$ denote the unique, up to isomorphism, quaternion algebra ramifying exactly $\mathfrak{p}$ and ∞. We give here an explicit description of H as

$$H = F + F\alpha + F\beta + F\alpha\beta \qquad (2.2)$$

where

$$\alpha^2 = a,\ \beta^2 = b,\ \alpha\beta = -\beta\alpha.$$

First note that since

$$(a, b)_\infty = (-1)^{\frac{q-1}{2}\deg a \deg b}(\mathrm{sgn}\ a)^{\deg b}(\mathrm{sgn}\ b)^{\deg a},$$

neither a or b can be a polynomial of even degree and positive sign, i.e. a and b have to be quadratic imaginary in the sense of Lemma 1.11. Let $a = up$ where p is the unique monic prime of A such that $\mathfrak{p} = (p)$, and $u \in \mathbb{F}_q^*$. If $\deg p$ is even, we choose u to be a non-square in $\mathbb{F}_q^*$. Let $p' \neq p$ be a monic prime of A, and denote $\mathfrak{p}' = (p')$. By Cebotarev's Density Theorem, one can choose p' such that

$$\left(\frac{u}{p'}\right) = (-1)^{1+\deg p} \qquad (2.3)$$

$$\left(\frac{p}{p'}\right) = (-1)^{1+\deg p}. \qquad (2.4)$$

Let $b = vp'$, $v \in \mathbb{F}_q^*$. If $\deg p'$ is even, we choose v to be a non-square in $\mathbb{F}_q^*$. We compute (see [22], Chapiter III, Theorems 5.4 and 5.5)

$$(a, b)_{\mathfrak{q}} = (up, vp')_{\mathfrak{q}} = 1 \text{ for all } \mathfrak{q} \neq \mathfrak{p}, \mathfrak{p}'$$

and by (2.3) and (2.4)

$$\begin{aligned}(a,b)_\infty = (up, vp')_\infty &= -1\\ (a,b)_{\mathfrak{p}'} = (up, vp')_{\mathfrak{p}'} &= \left(\frac{up}{p'}\right) = 1.\end{aligned}$$

Finally, $(a,b)_\mathfrak{p} = (up, vp')_\mathfrak{p} = -1$ follows from the product formula

$$\prod_{\mathfrak{p}\in\mathcal{P}(F)} (a,b)_\mathfrak{p} = 1.$$

(In this case, this is also the quadratic reciprocity). This shows that H can be written as (2.2), where

$$a = up \text{ and } b = vp'$$

with the restrictions given above.

We now specialize H to be a quaternion algebra over $F = \mathbb{F}_q(T)$, the quotient field of $A = \mathbb{F}_q[T]$.

2.2.1 Orders in H/F

Definition 2.5 *An ideal I of H/F is a finitely generated A-submodule of H such that $F \otimes_A I \simeq H$.*

Definition 2.6 *An element $h \in H$ is an integer (over A) if $A[h]$ is a finitely generated A-module. Equivalently, $h \in H$ is an integer if its trace $tr(h)$ and its norm $n(h)$ are in A.*

Definition 2.7 *Let H/F be a quaternion algebra. The following are equivalent, and define an order $\mathcal{O}$ of H/F.*

(1) An ideal $\mathcal{O}$ which is also a subring of H.

(2) A ring of integers $\mathcal{O}$ containing A and such that $F\mathcal{O} = H$.

A maximal order is an order which is not contained in any order different from itself.

Let $\mathcal{O}$ be an order in H. Then its reduced discriminant $d(\mathcal{O})$ is defined to be $\mathrm{n}\left((\mathcal{O}^{*})^{-1}\right)$, where $\mathcal{O}^{*} = \{x \in H : \mathrm{tr}(x\mathcal{O}) \in \mathcal{O}\}$. For

$$\mathcal{O} = A\mu_1 + A\mu_2 + A\mu_3 + A\mu_4,$$

let

$$D(\mu_1, \mu_2, \mu_3, \mu_4) = \det\left(\mathrm{tr}(\mu_1\mu_2)\right).$$

Then we compute

$$d(\mathcal{O})^2 = \left(D(\mu_1, \mu_2, \mu_3, \mu_4)\right). \tag{2.5}$$

Lemma 2.8

(i) Let $\mathcal{O}$ and $\mathcal{O}'$ be orders in H. If $\mathcal{O} \subseteq \mathcal{O}'$, then $d(\mathcal{O}) \subseteq d(\mathcal{O}')$.

(ii) $\mathcal{O}$ is a maximal order

$$\Longleftrightarrow d(\mathcal{O}) = \prod_{\substack{\mathfrak{p} \in Ram(H) \\ \mathfrak{p} \neq \infty}} \mathfrak{p}.$$

2.2.2 Quadratic subfields of H/F

Given H/F a quaternion algebra over $F = \mathbb{F}_q(T)$, we are looking for a criterion to determine when a quadratic extension L/F is embedded in H/F.

Example: Let $H = F_{\mathfrak{p},\infty}$, the quaternion algebra described in the above example. Then, it is not difficult to see that every element of H/F is quadratic imaginary over F, i.e. a quadratic extension L/K embedded in H/K has to be quadratic imaginary.

In general, one can prove:

Theorem 2.9 *[24, Theorem 3.8] Let L/F be a quadratic field extension and H/F a quaternion algebra. Then $L \subset H$ if and only if $L_v = L \otimes_F F_v$ is a field for all $v \in Ram(H)$.*

If v is a prime ideal $\mathfrak{p} = (p)$ of A, then

$$\begin{aligned} p \text{ splits in } L &\iff L_{\mathfrak{p}} \text{ is not a field;} \\ p \text{ is inert in } L &\iff L_{\mathfrak{p}}/K_{\mathfrak{p}} \text{ is a non-ramified field extension;} \\ p \text{ ramifies in } L &\iff L_{\mathfrak{p}}/K_{\mathfrak{p}} \text{ is a ramified field extension.} \end{aligned}$$

Then for the quadratic extension $L = F(\sqrt{d})$ of F, d a fundamental discriminant, we get

$$L \subset H \iff \left(\frac{d}{p}\right) \neq 1. \tag{2.6}$$

Let L/F be a quadratic extension, B an A-order in L and $\mathcal{O}$ a maximal order in H. Then

$$i : B \hookrightarrow \mathcal{O}$$

is an optimal embedding of B in $\mathcal{O}$ when $i(L) \cap \mathcal{O} = B$.

2.3 Proof of the Theorem

Let $d_1, d_2 \in A$, be two distinct fundamental discriminants of A. Let p be a regular prime of ϕ such that

$$p \mid P_{d_1}(j_\phi) \quad \text{and} \quad p \mid P_{d_2}(j_\phi).$$

Then

$$\mathcal{O}_1 = A\left[\sqrt{d_1}\right]$$

and

$$\mathcal{O}_2 = A\left[\sqrt{d_2}\right]$$

are optimally embedded in $\mathrm{End}(\phi)$, which is a maximal order in $F_{\mathrm{p},\infty}$. Write R for this maximal order. Let α_i be the image of $\sqrt{d_i}$ in R, $i = 1, 2$, and consider the A-submodule of R

$$L = A + A\alpha_1 + A\alpha_2 + A\alpha_1\alpha_2.$$

Let $s = \mathrm{tr}(\alpha_1\alpha_2)$. Then one computes

$$D(1, \alpha_1, \alpha_2, \alpha_1\alpha_2) = \left(4d_1d_2 - s^2\right)^2.$$

We also have

$$\mathrm{n}(\alpha_1\alpha_2) = \mathrm{n}(\alpha_1)\mathrm{n}(\alpha_2) = d_1d_2,$$

and since $\alpha_1\alpha_2 \notin F$,

$$\Delta = \mathrm{tr}^2(\alpha_1\alpha_2) - 4\mathrm{n}(\alpha_1\alpha_2) = s^2 - 4d_1d_2 \neq 0.$$

This implies that $D(1, \alpha_1, \alpha_2, \alpha_1\alpha_2) \neq 0$, and then L has rank 4 over A. Since L is also a ring, it is an order in $F_{\mathrm{p},\infty}$. Then by (2.5) and Lemma 2.8,

$$\begin{aligned} & p^2 \mid D(1, \alpha_1, \alpha_2, \alpha_1\alpha_2) = \left(4d_1d_2 - s^2\right)^2 \\ \Longrightarrow \quad & p \mid 4d_1d_2 - s^2. \end{aligned}$$

Then,

$$|p| \leq \max\left(|d_1d_2|, |s^2|\right).$$

Suppose that

$$|s^2| > |d_1d_2|.$$

Then $f = \mathrm{tr}^2(\alpha_1\alpha_2) - 4\mathrm{n}(\alpha_1\alpha_2)$ is a polynomial of even degree with leading coefficient in $(\mathbb{F}_q^*)^2$, which is impossible since f is quadratic imaginary. Then,

$$|s^2| \leq |d_1d_2|$$

and finally

$$|p| \leq |d_1 d_2|,$$

which we can write as

$$\deg p \leq \deg d_1 d_2.$$

Chapter 3

Lower Bounds

3.1 Introduction

Through all this chapter, let ϕ be a rank 2 Drinfeld A-module over A, defined by

$$\phi_T = \gamma(T) + a\mathcal{F} + b\mathcal{F}^2, \quad a, b \in A, \ b \neq 0, \tag{3.1}$$

with j-invariant

$$j_\phi = \frac{a^{q+1}}{b} \in F^*.$$

Let

$$\pi_\phi(x) = \#\left\{\mathfrak{p} \in \text{ Spec } A : |\mathfrak{p}| \leq x, \text{ and } \phi_\mathfrak{p} \text{ is supersingular}\right\}.$$

We give in this chapter lower bounds for $\pi_\phi(x)$. This is done by extending the ideas of Elkies [7] and Fouvry and Murty [10], who found lower bounds for the number of supersingular primes of elliptic curves, to the context of Drinfeld modules. In [2], Brown used a similar method to get that

$$\pi_\phi(x) \gg \log\log\log x. \tag{3.2}$$

Following the same lines, but with sharper estimates, we first improve (3.2) to

$$\pi_\phi(x) \gg \sqrt{\log\log x}$$

(see Theorem 3.2). Using the result of Chapter 2, we can improve the last bound to

$$\pi_\phi(x) \gg \log\log x$$

(see Corollary 3.4).

Our proof applies only to non-exceptional Drinfeld modules ϕ. Following [2], exceptional ϕ are defined by

Definition 3.1 *A rank 2 Drinfeld A-module ϕ over F is called exceptional if the following conditions hold:*

(i) $q \equiv 1$ mod 4;

(ii) j_ϕ is a square in F_∞;

(iii) the prime factors of even positive degree of the numerator of j_ϕ have even multiplicities.

Applying base change (see [2]), we only have to consider the 3 cases:

(C1) $q \equiv 3(4)$ and $j_\phi T$ is not a square in F_∞;

(C2) $q \equiv 1(4)$ and j_ϕ is not a square in F_∞;

(C3) $q \equiv 1(4)$, j_ϕ is a square in F_∞, and there is a prime element p_0 of A with even degree, and p_0 divides the numerator of j_ϕ to an odd power.

We then show the following theorems concerning lower bounds for $\pi_\phi(x)$.

Theorem 3.2 *Let ϕ a non-exceptional Drinfeld A-module over F, as given by (3.1). Then,*

$$\pi_\phi(x) \gg \sqrt{\log\log x}.$$

Theorem 3.3 *Let ϕ a non-exceptional Drinfeld A-module over F, as given by (3.1). Then, there exists an infinite sequence $x_1, x_2, \ldots$ with $x_m \to \infty$ and a positive constant K such that*

$$\pi_\phi(x_m) \geq K \log x_m.$$

Furthermore, $\log x_{m+1} \ll x_m^{1/4} \log^2 x_m$.

Theorem 3.3 implies the following corollary:

Corollary 3.4

$$\begin{aligned} \pi_\phi(x) &= \Omega(\log x) \\ &\textit{and} \\ \pi_\phi(x) &\gg \log\log x. \end{aligned}$$

3.2 A New Supersingular Prime for ϕ

Let $P = \{p_1, p_2, \ldots, p_n\}$ be a set of distinct monic primes of A, containing all the non-regular primes of ϕ, all the primes dividing the numerator of j_ϕ, and where the only other primes are supersingular primes of ϕ. We are looking for a new supersingular prime for ϕ.

3.2.1 Computation of Legendre symbols

Let $f \in F^{*}$. Then we can write

$$f = \frac{a}{b}, \quad a, b \in A, \quad \gcd(a,b) = 1, \quad b \text{ monic}$$

in a unique way. Let π be a prime element of A. Let N_π be the numerator of $P_\pi(f)$, i.e.

$$N_\pi = P_\pi(f) b^{h(\pi)}. \tag{3.3}$$

Lemma 3.5 *[2, lemma 4.1.10] Let S be the finite set of prime ideals of A which divide the numerator of f to an odd power. If $\deg \pi$ is odd and sufficiently large, then*

$$\left(\frac{\pi}{N_\pi}\right) = (-\omega(\pi))^{\left(\deg f + \frac{q-1}{2}\right)\frac{q-1}{2}} \omega(f)^{\frac{q-1}{2}} \prod_{p \in S} \left(\frac{\pi}{p}\right).$$

Proof: The complete proof can be found in [2]. It is necessary to have $\deg \pi$ odd to insure that

$$P_\pi(x) \equiv x\, R^2(x) \bmod \pi$$

for $R(x)$ a polynomial in $A[x]$ satisfying $(x, R(x)) = 1$. Then one computes

$$\begin{aligned} \left(\frac{\pi}{N_\pi}\right) &= \left(\frac{N_\pi}{\pi}\right)(\pi, N_\pi)_\infty \\ &= \left(\frac{a}{\pi}\right)(\pi, N_\pi)_\infty \\ &= (\pi, a)_\infty (\pi, N_\pi)_\infty \prod_{p \in S} \left(\frac{\pi}{p}\right), \end{aligned}$$

and for $\deg \pi$ odd and big enough, one can show

$$(\pi, a)_\infty (\pi, N_\pi)_\infty = (-\omega(\pi))^{\left(\deg f + \frac{q-1}{2}\right)\frac{q-1}{2}} \omega(f)^{\frac{q-1}{2}}.$$

Remark: This criterion will allow the detection of an infinite number of supersingular primes associated to ϕ only if ϕ is a non-exeptional Drinfeld module. See [2, 4.1.14] for more details.

3.2.2 Choice of the new supersingular prime

Choose $\beta \in \mathbb{F}_q^*$ such that

$$(-\beta)^{(q-1)/2} = -w(j_\phi)^{(q-1)/2}, \tag{3.4}$$

i.e.

$$\text{sgn } (-\beta) = -\text{ sgn } (j_\phi).$$

Let $S = \{s_1, \ldots, s_n\}$ be the set of signs

$$s_i = \begin{cases} -1 & \text{if } p_i = p_0 \text{ in case (C3);} \\ 1 & \text{otherwise.} \end{cases}$$

Let π be a prime polynomial of A such that

(i) $\omega(\pi) = \beta$;

(ii) $\deg(\pi)$ is odd;

(iii) $\left(\frac{\pi}{p_i}\right) = s_i, \; 1 \leq i \leq n.$

We then say that π is an *admissible prime associated to* P, S *and* β. By Čebotarev's Density Theorem, there is an infinite number of such primes.

Let $N_\pi = N_\pi(j_\phi)$ be the numerator of $P_\pi(j_\phi)$, as in (3.3). Then, for $\deg \pi$ sufficiently large, we have (Lemma 3.5)

$$\left(\frac{\pi}{N_\pi}\right) = (-\omega(\pi))^{\left(\deg j_\phi + \frac{q-1}{2}\right)\frac{q-1}{2}} \, \omega(j_\phi)^{\frac{q-1}{2}} \prod_{p \in S} \left(\frac{\pi}{p}\right).$$

Using (3.4), this is

$$\left(\frac{\pi}{N_\pi}\right) = (-1)^{\deg j_\phi}(-1)^{\frac{q-1}{2}} \, (\text{sgn } j_\phi)^{\deg j_\phi + \frac{q-1}{2} + 1} \tag{3.5}$$

in cases (C1) and (C2), and

$$\left(\frac{\pi}{N_\pi}\right) = (-1)^{\deg j_\phi}(\operatorname{sgn}\, j_\phi)^{1+\deg j_\phi}(-1) \tag{3.6}$$

in case (C3).

Lemma 3.6 *$f \in F^*$ is a square in F_∞ if and only if*

(i) $\deg f$ *is even;*

(ii) $\omega(f) \in (\mathbb{F}_q^*)^2$.

We then compute that

$$\left(\frac{\pi}{N_\pi}\right) = -1$$

in cases (C1), (C2) and (C3). Then there is a prime $p(\pi) \in A$ dividing N_π, and such that

$$\left(\frac{\pi}{p(\pi)}\right) = -1.$$

By Deuring's criterion (Theorem 1.15), $p(\pi)$ is a supersingular prime for ϕ. Also, $p(\pi)$ cannot be one of the p_i's. This is clear in cases (C1) and (C2), since then π is a quadratic residue mod p_i, $1 \leq i \leq n$. In case (C3), one can show that the exceptional prime p_0 is a prime of ordinary reduction (see [2]). Then we also have $p(\pi) \neq p_0$. This shows that there exists an infinite number of supersingular primes for ϕ. In the next sections, we give asymptotic estimates for the number of such primes.

Finally, it is clear that

$$|p(\pi)| \leq |N_\pi|. \tag{3.7}$$

3.3 Number of admissible primes

Let $P = \{p_1, \ldots, p_n\}$ be a set of prime elements of A, $S = \{s_1, \ldots, s_n\}$ be a set of signs $s_i = \pm 1$ for $1 \leq i \leq n$, and $\beta \in \mathbb{F}_q^*$. Let $\pi_{P,S,\beta}(x)$ be the number of primes π of A such that

(i) π is unramified in the Galois extension $F\left(\sqrt{p_1}, \ldots, \sqrt{p_n}\right)/F$;

(ii) π is an admissible prime associated to P, S, and β;

(iii) $|\pi| \leq x$.

We show in this section the two Propositions:

Proposition 3.7 *There is an admissible prime $\pi(P, S, \beta)$ associated to P, S and β such that*

$$|\pi(P, S, \beta)| \leq C\, 4^n \left(\sum_{i=1}^{n} \log |p_i|\right)^2,$$

for some sufficiently large constant C, which depends only on q.

Proposition 3.8

$$\pi_{P,S,\beta}(x) \gg \frac{1}{2^n} \frac{x}{\log x},$$

when

$$x \geq C\, 4^n \left(\sum_{i=1}^{n} \log |p_i|\right)^2,$$

for some sufficiently large constant C, where C and the O-constant depend only on q.

To prove Propositions 3.7 and 3.8, we apply the Čebotarev's density Theorem to the Galois extension K_n/F, where

$$K_n = F\left(\sqrt{\alpha}, \sqrt{p_1}, \ldots, \sqrt{p_n}\right),$$

and α is a non-square of $\mathbb{F}_q^*$. L, the algebraic closure of $\mathbb{F}_q$ in K_n, is given by

$$L = \mathbb{F}_{q^2}$$

and

$$\begin{aligned} N &= [L : \mathbb{F}_q] = 2 \\ M &= [K_n : LF] = [K_n : \mathbb{F}_{q^2}(T)] = 2^n. \end{aligned}$$

We also compute

$$\mathrm{Gal}(K_n/F) \simeq (\mathbb{Z}/2\mathbb{Z})^{n+1}.$$

Lemma 3.9 *There exists a unique $g(P,S,\beta) \in Gal\,(K_n/F)$ such that for a prime $\pi \in A$, unramified in K_n, the followings are equivalent:*

(1) $\deg \pi$ is odd, and for $1 \le i \le n$, $\left(\frac{\pi}{p_i}\right) = s_i$ and $\omega(\pi) = \beta$;

(2) $\left(\frac{K_n/F}{\pi}\right) = g(P,S,\beta)$ and $\omega(\pi) = \beta$.

Proof: Any $g \in$ Gal (K_n/F) can be written as $g = g_\alpha \times g_1 \times \ldots \times g_n$ with $g_\alpha \in$ Gal $F(\sqrt{\alpha})/F$, and $g_i \in$ Gal $F(\sqrt{p_i})/F$. Let π be an unramified prime element of A. Then

(1) $\left(\frac{\alpha}{\pi}\right) = 1 \iff \deg \pi$ is even;

(2) By quadratic reciprocity (Theorem 1.5)

$$\left(\frac{p_i}{\pi}\right)\left(\frac{\pi}{p_i}\right) = (-1)^{\frac{q-1}{2}\deg p_i \deg \pi}(\mathrm{sgn}\ \pi)^{\deg p_i}(\mathrm{sgn}\ p_i)^{\deg \pi}.$$

The Lemma follows from there.

Since $\mathrm{Gal}(K_n/F)$ is abelian, the conjugacy class of $g(P,S,\beta)$ is

$$\mathcal{C} = \{g(P,S,\beta)\},$$

and by last Lemma,

$$\pi_{P,S,\beta}(x) = \pi_{\mathcal{C}}(K_n/F; x). \tag{3.8}$$

Using the Čebotarev Density Theorem (Theorem 1.3), we get

$$\pi_{\mathcal{C}}(K_n/F; x) = \sum_{\substack{q^k \leq x \\ \deg k \text{ odd}}} |C_k(K_n/F; \mathcal{C})|,$$

where, for $\deg k$ odd,

$$|C_k(K_n/F; \mathcal{C})| = \frac{1}{2^n}\frac{q^k}{k} + O\left(q^{k/2}\left(1 + \frac{g_{K_n}}{k2^n}\right)\right).$$

Lemma 3.10

$$g_{K_n} \ll 2^n \sum_{i=1}^{n} \log|p_i|$$

Proof: Consider the Galois extension K_n'/F, where

$$K_n' = F\left(\sqrt{p_1}, \ldots, \sqrt{p_n}\right).$$

K_n' is a function field over $\mathbb{F}_q$, and the extension K_n over $\mathbb{F}_q^2$ is a constant field extension of K_n' over $\mathbb{F}_q$, which gives $g_{K_n} = g_{K_n'}$. Applying Riemann-Hurwitz Formula (Theorem 1.4) to the extension K_n'/F, we get

$$g_{K_n'} \ll 2^n + \deg \mathfrak{D}_{K_n'/F}, \tag{3.9}$$

and since K_n'/F is Galois, we compute

$$\begin{aligned}\deg \mathfrak{D}_{K_n'/F} &= \sum_{\mathfrak{P} \in \mathcal{P}(K_n')} (e(\mathfrak{P}|\mathfrak{p}) - 1) \deg \mathfrak{P} \\ &= \sum_{\mathfrak{p} \in \mathcal{P}(F)} (e(\mathfrak{p}) - 1)\, f(\mathfrak{p})\, g(\mathfrak{p}) \deg \mathfrak{p}.\end{aligned}$$

The only primes ideals of Spec A which ramify in K_n' are the ideals (p_i), $i = 1, \ldots, n$. Then

$$\deg \mathfrak{D}_{K_n'/F} \ll 2^n \sum_{i=1}^{n} \log|p_i|, \tag{3.10}$$

and the Lemma follows from (3.9) and (3.10).

With the previous Lemma, we write

$$|C_k(K_n/F;C)| = \frac{1}{2^n}\frac{q^k}{k} + O\left(\frac{q^{k/2}}{k}\left(k + \sum_{i=1}^{n} \log|p_i|\right)\right). \tag{3.11}$$

for k odd. First consider

$$f(x) = \frac{1}{2^n}\frac{x}{\log_q x} + O\left(\frac{\sqrt{x}}{\log_q x}\left(\log_q x + \sum_{i=1}^{n} \log|p_i|\right)\right) \tag{3.12}$$

for any positive real x. When $x = q^k$, with k odd, this is (3.11). For

$$x \geq C\, 4^n \left(\sum_{i=1}^{n} \log|p_i|\right)^2,$$

for a sufficiently large absolute constant C, the main term in (3.12) is strictly larger than a fraction of the error term, which gives

$$f(x) > 0$$

and

$$f(x) \gg \frac{1}{2^n}\frac{x}{\log_q x}.$$

Let l be the smallest odd integer such that

$$q^l \geq C\, 4^n \left(\sum_{i=1}^{n} \log|p_i|\right)^2.$$

Then

$$q^l \leq C\, q^2\, 4^n \left(\sum_{i=1}^{n} \log|p_i|\right)^2,$$

and

$$|C_l(K_n/F;x)| > 0,$$

which proves Proposition 3.7.

Similarly, for any

$$x \geq q^2\, 4^n \left(\sum_{i=1}^{n} \log|p_i|\right)^2, \tag{3.13}$$

let l be the unique odd integer such that $q^l \leq x < q^{l+2}$. Then

$$\begin{aligned}\pi_{P,S,\beta}(x) &= \sum_{k=1}^{l} |C_k(K_n/F;C)| \\ &\geq |C_l(K_n/F;C)|.\end{aligned}$$

By (3.13),

$$q^l \geq C\,4^n \left(\sum_{i=1}^{n} \log|p_i|\right)^2,$$

and then

$$|C_l(K_n/F;C)| \gg \frac{1}{2^n}\frac{q^l}{l} \geq \frac{\log q}{q^2}\frac{1}{2^n}\frac{x}{\log x},$$

which proves Proposition 3.8.

3.4 Order of $p(\pi)$

We prove in this section the following Theorem:

Theorem 3.11 *Let ϕ, π and $p(\pi)$ be as in Section 3.2.2. Then*

$$p(\pi) \ll \exp\left(C|\pi|^{1/2}\log^2|\pi|\right),$$

where C and the O-constant depend only on ϕ and q.

By (3.7), it suffices to show that

$$N_\pi \ll \exp\left(C\,|\pi|^{1/2}\,\log^2|\pi|\right).$$

We prove in this section the more general Theorem:

Theorem 3.12 *Let $d \in A$ be square-free, and let ϕ be a rank 2 Drinfeld A-module as given by (3.1). Let N_d be the numerator Num $P_d(j_\phi)$. Then*

$$N_d \ll \exp\left(C\,|d|^{1/2}\,\log^2|d|\right),$$

where the C and the O-constant depend only on q and ϕ.

Let $j_\phi = \frac{f}{g}$, $f, g \in A^*$. Then

$$N_d = \text{Num } P_d(j_\phi) = g^{h(d)} P_d(j_\phi).$$

As in the classical case, the following Lemma allows us to choose the values z for which $j(z)$ is a singular moduli associated to d.

Lemma 3.13 *Each of the singular moduli associated to d can be written as $j(z)$, where the minimal polynomial of z over A has the form*

$$ax^2 + bx + c, \quad \textit{with } |b| < |a| \leq |c|, \ a \textit{ monic }, \ (a, b, c) = 1.$$

We then write

$$P_d(j_\phi) = \prod_{i=1}^{h(d)} (j_\phi - j(z_i))$$

where

$$z_i = \frac{-b_i \pm \sqrt{b_i^2 - 4a_i c_i}}{2a_i} \tag{3.14}$$

with

$$|b_i| < |a_i| \leq |c_i| \quad \text{and} \quad b_i^2 - 4a_i c_i = d. \tag{3.15}$$

Lemma 3.14 *Let $j(z)$ be a singular modulus associated to d. Then*

$$|j(z)| \ll \exp\left(C_q |z|\right)$$

where C_q depends only on q.

Proof: The result follows using the explicit formulas for $j(z)$ developed in [2, Lemma 2.8.2].

In particular, for $1 \leq i \leq n$,

$$|j(z_i)| \ll \exp\left(C_q |z_i|\right) = \exp\left(C_q \frac{|d|^{1/2}}{|a_i|}\right)$$

since

$$|z_i| = \frac{|-b_i \pm \sqrt{d}|}{|2a_i|} = \frac{|d|^{1/2}}{|a_i|}$$

by (3.15). Choose

$$C \geq \max(C_q,\ \log|j_\phi|).$$

Then

$$\begin{aligned} P_d(j_\phi) &\ll \prod_{i=1}^{h(d)} \left(|j_\phi| + \exp\left(C\frac{|d|^{1/2}}{|a_i|}\right)\right) \\ &\ll 2^{h(d)} \prod_{i=1}^{h(d)} \exp\left(C\frac{|d|^{1/2}}{|a_i|}\right) \\ &= 2^{h(d)} \exp\left(C|d|^{1/2} \sum_{i=1}^{h(d)} \frac{1}{|a_i|}\right), \end{aligned}$$

since $|a_i| \leq |d|^{1/2}$ for $1 \leq i \leq n$. We then have to bound $h(d)$ and $\sum_{i=1}^{h(d)} \frac{1}{|a_i|}$.

Lemma 3.15

$$h(d) \ll |d|^{1/2} \log|d|$$

where the O-constant depends only on q.

Proof: Let

$$\chi_d(a) = \left(\frac{d}{a}\right)$$

for $a \in A$. In general, χ_d is not a character mod d, since by quadratic reciprocity (Theorem 1.5)

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

but in particular cases, as $\deg d$ even and $\operatorname{sgn} d = 1$, χ_d is a character mod d. In any case,

$$a \equiv b \bmod d, \text{ and } \deg a \equiv \deg b \bmod 2 \Longrightarrow \chi_d(a) = \chi_d(b).$$

Lemma 3.16 *For $k \geq \deg |d|$,*

$$\sum_{\deg a = k} \chi_d(a) = 0.$$

Proof: The q^k monic polynomials of A of exact degree k are evenly distributed mod d. Then, using quadratic reciprocity,

$$\sum_{\deg a=k} \left(\frac{d}{a}\right) = q^{k-\deg d} \sum_{a \bmod d} \left(\frac{d}{a}\right) = (-1)^{\frac{q-1}{2} k \deg d} (\mathrm{sgn}\ d)^k \sum_{a \bmod d} \left(\frac{a}{d}\right) = 0.$$

Let

$$L(s, \chi_d) = \sum_a \chi_d(a) \, |a|^{-s},$$

where the sum is taken over monic polynomials $a \in A$. Then $L(s, \chi_d)$ is the finite sum

$$L(s, \chi_d) = \sum_{\deg a < \deg d} \left(\frac{d}{a}\right) |a|^{-s}.$$

Artin showed in his thesis [1] that there is a class number formula over function fields. More precisely,

Theorem 3.17

(i) If $\deg d$ *is odd,* $L(1, \chi_d) = \frac{\sqrt{q}}{\sqrt{|d|}}\ h(d)$*;*

(ii) If $\deg d$ *is even, and sgn* $d = -1$, $L(1, \chi_d) = \frac{q+1}{\sqrt{2|d|}}\ h(d)$*;*

(iii) If $\deg d$ *is even, and sgn* $d = 1$, $L(1, \chi_d) = \frac{q-1}{\sqrt{|d|}}\ h(d)\ \log |\epsilon_d|$, *where*

$$A[\sqrt{d}]^* = \mathbb{F}_q^* \times < \epsilon_d > .$$

(This precise form of Artin's result is from [17].)

Since

$$L(1,\chi_d) = \sum_{\deg a < \deg d} \left(\frac{d}{a}\right) |a|^{-1} \ll \log |d|,$$

this completes the proof of Lemma 3.15.

Lemma 3.18

$$\sum_{i=1}^{h(d)} \frac{1}{|a_i|} \ll \log^2 |d|$$

where the O-constant depends only on q.

Proof: The number of z_i with $a_i = a$, where a is some fixed value, is smaller then the number of solutions to $x^2 \equiv d \bmod a$. Also, for any $1 \leq i \leq h(d)$, $|a_i| \leq |d|^{1/2}$ by (3.15). Then

$$\sum_{i=1}^{h(d)} \frac{1}{|a_i|} \leq \sum_{1 \leq |a| \leq |d|^{1/2}} \frac{2^{\omega(a)}}{|a|},$$

where the sum runs over monic polynomials $a \in A$, and $\omega(a)$ is the number of monic prime divisors of a. Now consider the product

$$\prod_p \left(1 + \frac{2}{|p|-1}\right)$$

taken over monic primes $p \in A$. It can be rewritten as

$$\prod_p \left(1 + \frac{1}{|p|}\right)\left(1 + \frac{1}{|p|} + \frac{1}{|p|^2} + \ldots\right) = 1 + \sum_a \frac{2^{\omega(a)}}{|a|}.$$

Then

$$\sum_{1 \leq |a| \leq |d|^{1/2}} \frac{2^{\omega(a)}}{|a|} \leq \prod_{|p| \leq |d|^{1/2}} \left(1 + \frac{2}{|p|-1}\right) \ll \log^2 |d|,$$

which gives the Lemma 3.18.

In conclusion,

$$\begin{aligned} N_d &\ll 2^{h(d)} |g|^{h(d)} \exp\left(C|d|^{1/2} \sum_{i=1}^{h(d)} \frac{1}{|a_i|}\right) \\ &\ll \exp\left(C'|d|^{1/2} \log^2 |d|\right). \end{aligned}$$

Remark: This improves the bound given in [2], which is $N_\pi \ll \exp(|\pi|^4)$.

3.5 Proof of First Theorem

Let $p_1, \ldots, p_n$ be given, and as in Section 3.2.2, choose π an admissible prime, and $p(\pi) \mid N_\pi$ a new supersingular prime. By Proposition 3.7, it is possible to choose π with

$$|\pi| \ll 4^n \left(\sum_{i=1}^{n} \log |p_i| \right)^2 ,$$

and by Theorem 3.11

$$|p(\pi)| \ll \exp \left(C |\pi|^{1/2} \log^2 |\pi| \right).$$

Then

$$\log |p(\pi)| \ll 2^n \left(\sum_{i=1}^{n} \log |p_i| \right) \left(n + \log \left(\sum_{i=1}^{n} \log |p_i| \right) \right)^2 .$$

Without lost of generality, we suppose that $|p_i| \leq |p_n|$ for $1 \leq i \leq n$. Then, writing p_{n+1} for $p(\pi)$, we have

$$\log |p_{n+1}| \ll 2^n \, n \, (\log |p_n|) \, (n + \log n + \log\log |p_n|)^2 .$$

and by induction on n, we get that

$$\log |p_n| \ll \exp (n^2),$$

from which Theorem 3.2 follows.

3.6 Proof of Second Theorem

We now show Theorem 3.3, which improves the previous Theorem. The proof works as follows. Given $p_1, \ldots, p_n$, we choose admissible primes π associated to $p_1, \ldots, p_n$, as in Section 3.2.2. For each of these admissible π, we get a new supersingular prime $p(\pi)$. By construction, any of the $p(\pi)$ is different from the primes $p_1, \ldots, p_n$. If we can also insure that they are all distinct, we can use Proposition 3.8, which counts the number of admissible π, to count the supersingular primes $p(\pi)$ associated to those admissible primes. Theorem 2.1 gives the criterion which insures that the primes $p(\pi)$ are distinct.

To prove Theorem 3.3, it suffices to show that for x large enough with

$$\pi_\phi(x) < K \log x,$$

there exists $x' > x$ with $\pi_\phi(x') \geq K \log x'$, and $\log x' \ll x^{1/4} \log^2 x$. Here K is any positive value such that

$$K \;<\; \frac{1}{4}\,\frac{1}{\log 2}. \tag{3.16}$$

Then, choose x with

$$n = \pi_\phi(x) < K \log x,$$

and let $p_1, \ldots, p_n$ be the n supersingular primes of ϕ with $|p| \leq x$. By Proposition 3.8, for x big enough such that

$$\sqrt{x} \geq C 4^n n^2 \log^2 \sqrt{x}, \tag{3.17}$$

the number of admissible primes π associated with $\{p_1, \ldots, p_n\}$, and such that $|\pi| \leq \sqrt{x}$, is

$$\gg \frac{1}{2^n} \frac{\sqrt{x}}{\log \sqrt{x}}.$$

We do have to insure that it is possible to choose both x and n in this way, and such that (3.17) holds. But since $n < K \log x$, we have

$$4^n n^2 \log^2 \sqrt{x} < \frac{K^2}{4} x^{K \log 4} \log^4 x,$$

and then for x big enough and any K such that (3.16) holds

$$\sqrt{x} \geq C 4^n n^2 \log^2 \sqrt{x}.$$

As seen in Section 3.2.2, for each of those admissible π, we obtain a prime of supersingular reduction $p(\pi)$, which is not one of the p_i. Furthermore, as seen in Section 3.4,

$$|p(\pi)| \ll \exp\left(C\,|\pi|^{1/2}\log^2|\pi|\right)$$

for each of the $p(\pi)$, which gives

$$|p(\pi)| \ll \exp\left(C\,x^{1/4}\log^2 x\right)$$

by choice of the π's. Suppose that $p(\pi_1) = p(\pi_2) = p$ for some $\pi_1 \neq \pi_2$. Then, by Theorem 2.1, we conclude that $|p| \leq x$, i.e. p is among $p_1, \ldots, p_n$, which is impossible. Then, each of the admissible π in the range under consideration gives a different supersingular prime $p(\pi)$. Let $x' = \max|p(\pi)|$. Then

$$\log x' \ll x^{1/4}\log^2 x.$$

Also, since $n < K\log x$,

$$\pi_\phi(x') \gg \frac{1}{2^n}\frac{\sqrt{x}}{\log\sqrt{x}} > \frac{x^{\frac{1}{2}-K\log 2}}{\log\sqrt{x}}.$$

Then for x large enough, and for any K such that (3.16) holds, we get

$$\pi_\phi(x') > K\log x'.$$

This completes the proof of the Theorem.

Corollary 3.4 follows applying Theorem 3.3 to find $x_m \leq x \leq x_{m+1}$. Then

$$\pi_\phi(x) \geq K\log x_m \gg (\log\log x_{m+1}) \geq (\log\log x).$$

Chapter 4

Upper Bounds

4.1 Introduction

Let ϕ be a rank 2 supersingular A-module defined over A, i.e.

$$\phi_T = \gamma(T) + a\mathcal{F} + b\mathcal{F}^2, \quad a, b \in A, \ b \neq 0. \tag{4.1}$$

For all regular primes $\mathfrak{p} = (p)$ of ϕ, let $\phi_\mathfrak{p}$ be the reduction of ϕ in characteristic $\mathfrak{p}$. We now look at upper bounds of

$$\pi_\phi(x) = \#\{\mathfrak{p} \in \text{Spec } A : |\mathfrak{p}| \leq x \text{ and } \phi_\mathfrak{p} \text{ is supersingular}\}.$$

The following argument was pointed out by R. Murty for the case of elliptic curves. To each supersingular prime $\mathfrak{p} = (p)$, let $d(p)$ be a positive constant such that there exists a monic prime $p \in A$ with

$$p \mid P_d(j_\phi)$$

and $|d| \leq d(p)$. For any square free $d \in A$, the number of prime factors of $P_d(j_\phi)$ is bounded by

$$\log N_d(j_\phi) \ll |d|^{1/2} \log^2 |d|$$

by the results of Section 3.4. Then

$$\pi_\phi(x) \ll \sum_{|d| \leq D} |d|^{1/2} \log^2 |d|, \tag{4.2}$$

where

$$D = \max_{|p| \leq x} d(p).$$

Let $\mathfrak{p}$ be a supersingular prime, and let $\phi_\mathfrak{p}$ be its reduction of ϕ mod $\mathfrak{p}$, Then $\mathrm{End}(\phi_\mathfrak{p})$ is an order in $F_{\mathfrak{p},\infty}$. By Deuring's lifting lemma for Drinfeld modules, if

$$A[\sqrt{d}] \subseteq \mathrm{End}(\phi_\mathfrak{p}),$$

then

$$p \mid P_d(j_\phi).$$

We then address in this chapter the task of finding quadratic orders $A[\sqrt{d}]$ in $\mathrm{End}(\phi_p)$, where $|d|$ is small enough to give a non-trivial bound in (4.2). By the choice of ϕ, $\phi_\mathfrak{p}$ is defined over $\mathbb{F}_\mathfrak{p}$. This gives certain restrictions on the endomorphism ring $\mathrm{End}(\phi_\mathfrak{p})$, and there are $\frac{1}{2}h(\sqrt{up})$ isomorphism classes of such rings, where u is a non-square in $\mathbb{F}_q^*$ (see next section). We first look for explicit representatives $\mathcal{O}$ for those isomorphism classes, and for each such $\mathcal{O}$, we look for elements $h \in \mathcal{O}$ satisfying

$$h^2 - d = 0$$

with $|d|$ small. The work of this chapter is strongly influenced by papers of Ibukiyama [18] and Kaneko [19], who solve equivalent problems in the case of elliptic curves.

4.2 Number of supersingular modules over finite fields

Let $\mathfrak{p} = (p)$ be a prime ideal of A, p a monic prime polynomial. Let ϕ be a rank 2 Drinfeld A-module in characteristic $\mathfrak{p}$, i.e.

$$\phi_T = \gamma(T) + a\mathcal{F} + b\mathcal{F}^2,$$

with

$$a, b \in \overline{\mathbb{F}}_{\mathfrak{p}},$$

and let $\Sigma(\mathfrak{p})$ be the set of isomorphism classes of such modules. Let D be the unique (up to isomorphism) quaternion algebra over $F = \mathbb{F}_q(T)$ with

$$\mathrm{Ram}(D) = \{\mathfrak{p}, \infty\}.$$

Fix any maximal order $\mathcal{O}$ in D. Then the number of left ideal classes of $\mathcal{O}$ do not depend on the choice of the maximal order $\mathcal{O}$, and is the class number of D, denoted $h(D)$. Two maximal orders $\mathcal{O}$ and $\mathcal{O}'$ are isomorphic when there is an A-algebra isomorphism $\psi : \mathcal{O} \longrightarrow \mathcal{O}'$. The type number $t(D)$ of D is the number of types, or isomorphism classes, of maximal orders in D. Since any maximal order appears, up to isomorphism, as the order associated to one of the left ideal classes of $\mathcal{O}$, we always have $t(D) \leq h(D)$.

The following Theorems are analogous to the work of Deuring [3] on the endomorphism rings of supersingular elliptic curves in characteristic p.

Theorem 4.1 *([13, Theorem 4.3]) Let ϕ be a supersingular Drinfeld module in characteristic $\mathfrak{p}$. Then the left ideal classes of End(ϕ) correspond bijectively to the elements of $\Sigma(\mathfrak{p})$.*

Theorem 4.2 *([13, Proposition 4.6]) The isomorphism classes of maximal orders in D correspond bijectively to the orbits of $\Sigma(\mathfrak{p})$ under the action of the Galois group $G = Gal(\overline{\mathbb{F}}_\mathfrak{p}/\mathbb{F}_\mathfrak{p})$.*

Then, $|\Sigma(\mathfrak{p})| = h(D)$ by Theorem 4.1. One computes (see for example [13])

$$h(D) = \begin{cases} \frac{q^d-1}{q^2-1} & \text{when } \deg p \text{ is even} \\ \frac{q^d-q}{q^2-1} + 1 & \text{when } \deg p \text{ is odd,} \end{cases}$$

and

$$t(D) = \begin{cases} \frac{1}{2}\left(\frac{q^d-1}{q^2-1} + \frac{1}{2}h(\sqrt{up})\right) & \text{when } \deg p \text{ is even} \\ \frac{1}{2}\left(\frac{q^d-q}{q^2-1} + 1 + \frac{1}{2}\left(h(\sqrt{up}) + h(\sqrt{p})\right)\right) & \text{when } \deg p \text{ is odd.} \end{cases}$$

Any supersingular Drinfeld module in characteristic $\mathfrak{p}$ can be defined over L, a degree 2 extension of $\mathbb{F}_\mathfrak{p}$. The orbits of $\Sigma(\mathfrak{p})$ under the action of $\mathrm{Gal}(\overline{\mathbb{F}}_\mathfrak{p}/\mathbb{F}_\mathfrak{p})$ are then the orbits of $\Sigma(\mathfrak{p})$ under the action of

$$\mathrm{Gal}(L/\mathbb{F}_\mathfrak{p}) = \{1, \tau\}$$

where

$$\tau : x \longmapsto x^{q^d}, \quad d = \deg p. \tag{4.3}$$

For $\phi \in \Sigma(\mathfrak{p})$, let $[\phi]$ denote the orbit of ϕ. When the supersingular module ϕ is defined over $\mathbb{F}_\mathfrak{p}$, $\tau \in \mathrm{End}(\phi)$ since

$$\tau \circ \phi_a = \phi_a \circ \tau$$

for all $a \in A$. Then

$$[\phi] = \{\phi\}$$

in this case. When ϕ is not defined over $\mathbb{F}_\mathfrak{p}$,

$$[\phi] = \{\phi, \phi^\tau\}$$

where $\phi \not\simeq \phi^\tau$ and ϕ^τ is not defined over $\mathbb{F}_\mathfrak{p}$. The number of classes of supersingular modules over $\mathbb{F}_\mathfrak{p}$ can then be computed as $2t(D) - h(D)$, and is

$$\begin{cases} \frac{1}{2}h(\sqrt{up}) & \text{when } \deg p \text{ is even} \\ \frac{1}{2}\left(h(\sqrt{up}) + h(\sqrt{p})\right) & \text{when } \deg p \text{ is odd.} \end{cases} \tag{4.4}$$

Let ϕ be such a supersingular module. Then, in the maximal order $\mathrm{End}(\phi)$, τ satisfies a polynomial equation

$$\tau^2 - cp = 0$$

for some $c \in \mathbb{F}_q^*$. We then look for maximal orders of D which contain $\sqrt{up}$.

4.3 Maximal orders in even degree characteristic

¿From now on, let $\mathfrak{p}$ be an even degree prime ideal in A, and write $\mathfrak{p} = (p)$ with p monic of even degree.

Let $u, v \in \mathbb{F}_q^*$, with u a non-square in $\mathbb{F}_q^*$, and L be the set of monic primes l satisfying

$$\left(\frac{u}{l}\right) = -1; \tag{4.5}$$

$$\left(\frac{p}{l}\right) = -1. \tag{4.6}$$

(Note that there is an infinite number of such l by the Čebotarev Density Theorem.) Then D can be explicitly written as

$$D_v(l) = F + F\alpha + F\beta_{vl} + F\alpha\beta_{vl}$$

where

$$\alpha^2 = up, \;\; \beta_{vl}^2 = vl, \;\; \alpha\beta_{vl} = -\beta_{vl}\alpha.$$

(This is the construction of Section 2.2 for the special case $\deg p$ even.) Of course, we have $D_v(l) \simeq D_v(l')$ for any $l, l' \in L$. For any $l \in L$, there exists r such that

$$r^2 \equiv up \bmod l \tag{4.7}$$

by (4.5) and (4.6). Consider the A-submodules of D

$$\mathcal{O}_v(l,r) = A + A\beta_{vl} + A\alpha + A\left(\frac{(r+\alpha)\beta_{vl}}{l}\right). \tag{4.8}$$

Lemma 4.3 *For any $l \in L$, $v \in \mathbb{F}_q^*$, and r satisfying (4.7), the A-modules $\mathcal{O}_v(l,r)$ are maximal orders of D.*

Proof: One easily checks that

(i) $1,\ \alpha,\ \beta_{vl},\ \alpha\beta_{vl} \in \mathcal{O}_v(l,r)$;

(ii) $\mathcal{O}_v(l,r)$ is a ring;

(iii) $D(1,\ \alpha,\ \beta_{vl},\ (r\beta_{vl} + \alpha\beta_{vl})/l) = -16u^2v^2p^2$.

Then, by (i) and (ii), $\mathcal{O}_v(l,r)$ is an order of D. By (iii), the reduced discriminant $d(\mathcal{O}_v(l,r))$ is $\mathfrak{p}$, and $\mathcal{O}_v(l,r)$ is a maximal order.

We note that $\alpha = \sqrt{up} \in \mathcal{O}_v(l,r)$ for each $l \in L$. Since

$$\mathcal{O}_v(l,r) \simeq \mathcal{O}_v(l,r')$$

whenever r and r' satisfy (4.7), we write $\mathcal{O}_v(l)$ for $\mathcal{O}_v(l,r)$. Similarly,

Lemma 4.4 *If $v' = w^2v$ for some $w \in \mathbb{F}_q^*$, then*

$$\mathcal{O}_v(l) \simeq \mathcal{O}_{v'}(l).$$

Proof: The F-linear map

$$\psi : \mathcal{O}_{v'}(l) \longrightarrow \mathcal{O}_v(l)$$

induced by

$$\begin{aligned}\psi(\alpha) &= \alpha \\ \psi(\beta_{v'l}) &= w\beta_{vl} \\ \psi(\alpha\beta_{v'l}) &= \psi(\alpha)\psi(\beta_{v'l})\end{aligned}$$

is an isomorphism between $\mathcal{O}_{v'}(l)$ and $\mathcal{O}_v(l)$.

We then consider the 2 families of maximal orders containing $\sqrt{up}$:

(i) $\mathcal{O}_v(l)$, for $l \in L$ and v a square in $\mathbb{F}_q^*$;

(ii) $\mathcal{O}_{v'}(l)$, for $l \in L$ and v' a non-square in $\mathbb{F}_q^*$.

Let $\mathcal{O}$ be a maximal order in D. An element $x \in \mathcal{O}$ is a unit of $\mathcal{O}$ when x^{-1} exists and belongs to $\mathcal{O}$. The group of units of $\mathcal{O}$ is denoted by $\mathcal{O}^*$, and the groups of units of norm 1 by $\mathcal{O}^1$. One easily sees that

$$x \in \mathcal{O}^* \Longleftrightarrow \mathrm{n}(x) \in \mathbb{F}_q^*.$$

Lemma 4.5 *When* $\deg p$ *is even, any maximal order* $\mathcal{O}$ *of* D *has*

$$\begin{aligned}\mathcal{O}^* &= \mathbb{F}_q^* \\ \mathcal{O}^1 &= \{\pm 1\}\end{aligned}$$

Proof: Let $x \in \mathcal{O}$. Then $\mathrm{n}(x), \mathrm{tr}(x) \in A$, and $x \in A[\sqrt{d}]$, $d = \mathrm{tr}(x)^2 - 4\mathrm{n}(x)$. Then the quadratic extension $F(\sqrt{d})$ is embedded in D. Since $\deg p$ is even, $d \notin \mathbb{F}_q^*$ (see (2.6) of Section 2.2.2), and $\deg d \geq 1$. Write $x = a + b\sqrt{d}$, with $a, b \in A$. We have

$$\mathrm{n}(x) = a^2 - db^2,$$

and since d is quadratic imaginary, $\deg a^2 \neq \deg db^2$ or sgn $a^2 \neq$ sgn db^2, which gives

$$\mathrm{n}(x) \in \mathbb{F}_q^* \Longleftrightarrow b = 0 \text{ and } a \in \mathbb{F}_q^*$$

and

$$\mathrm{n}(x) = 1 \Longleftrightarrow b = 0 \text{ and } a = \pm 1.$$

Let $l, l' \in L$, $l \neq l'$. By (4.5) and (4.6), l and l' split in $A[\sqrt{up}]$, and we write

$$\begin{aligned}(l) &= \mathfrak{L}\,\overline{\mathfrak{L}}\\ (l') &= \mathfrak{L}'\,\overline{\mathfrak{L}'}\end{aligned}$$

in $A[\sqrt{up}]$.

Theorem 4.6 *Fix any $v \in \mathbb{F}_q^*$, and let $\mathcal{O}_v(l)$ and $\mathcal{O}_v(l')$ be two maximal orders as given in (4.8). Then, the following are equivalent:*

(i) $\mathcal{O}_v(l) \simeq \mathcal{O}_v(l')$;

(ii) $x^2 - upy^2 = ll'$, for some $x, y \in A$;

(iii) $\mathfrak{L}\,\mathfrak{L}'$ is a principal ideal, for some $\mathfrak{L}$ above l, and some $\mathfrak{L}'$ above l'.

Proof: Taking norms, the equivalence between (ii) and (iii) is clear. We show the equivalence between (i) and (ii).

First suppose that there is an isomorphism

$$\psi : \mathcal{O}_v(l') \longrightarrow \mathcal{O}_v(l).$$

Since $\mathcal{O}^1 = \{\pm 1\}$, $\pm\alpha$ are the only elements of $\mathcal{O}_v(l)$ of norm $-up$, and $\psi(\alpha) = \pm\alpha$. Let

$$\begin{aligned}\psi(\beta_{vl'}) &= a + b\beta_{vl} + c\alpha + d\left(\frac{(r+\alpha)\beta_{vl}}{l}\right) \\ &= a + c\alpha + \left(\frac{bl+dr}{l}\right)\beta_{vl} + \frac{d}{l}\alpha\beta_{vl}.\end{aligned}$$

Since $\mathrm{tr}(\psi(\beta_{vl'})) = 0$ and $\psi(\alpha)\psi(\beta_{vl'}) = -\psi(\beta_{vl'})\psi(\alpha)$, we must have $a = c = 0$. Then

$$\begin{aligned}-vl' = \mathrm{n}(\psi(\beta_{vl'})) &= -\frac{(bl+dr)^2}{l^2}vl + \frac{d^2}{l^2}uvpl \\ \Longleftrightarrow ll' &= (bl+dr)^2 - upd^2,\end{aligned}$$

which proves (ii).

Conversly, suppose that there is $x, y \in A$ such that

$$x^2 - upy^2 = ll'.$$

Since $r^2 \equiv up \bmod l$, we get

$$(x - ry)(x + ry) \equiv 0 \bmod l,$$

and $x \equiv ry \bmod l$, changing y by $-y$ if necessary. Set

$$\begin{aligned} d &= y, \\ b &= \frac{x - ry}{l},\end{aligned}$$

such that

$$(bl + dr)^2 - upd^2 = ll'. \tag{4.9}$$

Let $\psi : D \longrightarrow D$ be the F-linear map given by

$$\psi(1) = 1$$

$$\begin{aligned} \psi(\alpha) &= \epsilon\alpha \\ \psi(\beta_{vl'}) &= b\beta_{vl} + d\frac{(r+\alpha)\beta_{vl}}{l} \\ \psi(\alpha\beta_{vl'}) &= \psi(\alpha)\psi(\beta_{vl'}) \end{aligned}$$

where ϵ can be ± 1. Then ψ is an F-algebra automorphism of D, and we claim that ψ induces an isomorphism between $\mathcal{O}_v(l')$ and $\mathcal{O}_v(l)$. We just have to show that

$$\psi\left(\mathcal{O}_v(l')\right) \subseteq \mathcal{O}_v(l). \tag{4.10}$$

Let $\omega_1 = 1$, $\omega_2 = \beta_{vl}$, $\omega_3 = \alpha$ and $\omega_4 = (r\beta_{vl} + \alpha\beta_{vl})/l$ be the basis of $\mathcal{O}_v(l)$. Then one computes

$$\begin{aligned} \psi(1) &= 1; \\ \psi(\alpha) &= \epsilon\alpha; \\ \psi(\beta_{vl'}) &= b\omega_2 + d\omega_4; \\ \psi\left(\frac{r'\beta_{vl'} + \alpha\beta_{vl'}}{l'}\right) &= \frac{1}{ll'}\Big(bl(r' - \epsilon r) + d\epsilon(up - r^2)\Big)\,\omega_2 + \frac{1}{l'}\left(r'd + \epsilon bl + \epsilon dr\right)\omega_4. \end{aligned}$$

Then, for (4.10) to be verified, we have to insure that

$$\begin{aligned} \frac{1}{ll'}\Big(bl(r' - \epsilon r) + d\epsilon(up - r^2)\Big) &\in A; & (4.11) \\ \frac{1}{l'}\left(r'd + \epsilon bl + \epsilon dr\right) &\in A. & (4.12) \end{aligned}$$

By the choice of b and d,

$$(bl + dr)^2 - upd^2 = ll',$$

which gives

$$\begin{aligned} & (bl + dr)^2 - r'^2 d^2 \equiv 0 \bmod l' \\ \Longleftrightarrow \quad & bl + dr \equiv r'd \bmod l' \ \text{ or } \ bl + dr \equiv -r'd \bmod l'. \end{aligned}$$

Choose ϵ such that

$$bl + dr + \epsilon r'd \equiv 0 \bmod l'. \tag{4.13}$$

Then (4.12) holds. For (4.11), the numerator is divisible by l since $r^2 \equiv up \bmod l$. It is also divisible by l' since

$$\begin{aligned} & bl(r' - \epsilon r) + d\epsilon(up - r^2) \\ \equiv \quad & bl(r' - \epsilon r) + d\epsilon(r' - \epsilon r)(r' + \epsilon r) \\ \equiv \quad & (r' - \epsilon r)(bl + dr + \epsilon dr') \equiv 0 \bmod l' \end{aligned}$$

by (4.13). This completes the proof of Theorem 4.6.

4.4 Number of orders $\mathcal{O}_v(l)$

We fix any $v \in \mathbb{F}_q^*$, and we consider the family of maximal orders $\mathcal{O}_v(l)$. As in the previous section, let

$$\begin{aligned} L &= \left\{ l \in \text{Spec } A : \left(\frac{u}{l}\right) = \left(\frac{p}{l}\right) = -1 \right\} \\ &= \{ l \in \text{Spec } A : \deg l \text{ is odd and } l \text{ splits in } A[\sqrt{up}] \} . \end{aligned}$$

Let C be the class group of $A[\sqrt{up}]$. Then by Theorem 4.6, the map

$$\begin{aligned} m : L &\longrightarrow \left\{ \sigma, \sigma^{-1} \right\}, \quad \sigma \in C \\ l &\longmapsto m(l) = \left\{ [\mathfrak{L}], [\overline{\mathfrak{L}}] \right\} \end{aligned}$$

is such that

$$m(l) = m(l') \Longleftrightarrow \mathcal{O}_v(l) \simeq \mathcal{O}_v(l').$$

Then the number of isomorphism classes of the maximal orders $\mathcal{O}_v(l)$ is $|\text{Im}(m)|$. We define L' to be the set

$$L' = \{ \mathfrak{L} \in \text{Spec } A[\sqrt{up}] : \deg \mathfrak{L} \text{ is odd} \} .$$

Let $\mathfrak{L} \in \operatorname{Spec} A[\sqrt{up}]$, and $(l) = \mathfrak{L} \cap A$. Then

$$\mathfrak{L} \in L' \iff l \text{ splits in } A[\sqrt{up}] \text{ and } \deg l \text{ is odd},$$

i.e.

$$\mathfrak{L} \in L' \iff l \in L.$$

Lemma 4.7 *Let $S = \{[\mathfrak{L}] : \mathfrak{L} \in L'\}$. Then*

$$|S| = \frac{h(\sqrt{up})}{2}.$$

Proof: Let H be the Hilbert class field of $F(\sqrt{up})$, as defined in [23]. Then, the Artin's map

$$\mathfrak{L} \longmapsto \sigma_{\mathfrak{L}} = \left(\frac{H/F(\sqrt{up})}{\mathfrak{L}}\right)$$

induces an isomorphism between C and $G = \operatorname{Gal}\left(H/F(\sqrt{up})\right)$. Since ∞ is inert from F to $F(\sqrt{up})$, the field of constants in H is $\mathbb{F}_{q^2}$ [23, Theorem 1.3]. Fix $\sigma \in G$. Let τ be the Frobenius automorphism

$$x \longmapsto x^q,$$

and let $a(\sigma) = 0$ or 1 be such that

$$\operatorname{res}_{\mathbb{F}_{q^2}} \sigma = \operatorname{res}_{\mathbb{F}_{q^2}} \tau^{a(\sigma)}.$$

Fix some positive integer k. Then, by Čebotarev Density Theorem (Theorem 1.3), there is some $\mathfrak{L} \in \operatorname{Spec} A[\sqrt{up}]$ with $\sigma_{\mathfrak{L}} = \sigma$ and $\deg \mathfrak{L} = k$ if and only if

$$k \equiv a(\sigma) \bmod 2.$$

Then

$$\sigma = \sigma_{\mathfrak{L}} \text{ for some } \mathfrak{L} \in L' \iff a(\sigma) = 1,$$

and the result follows counting the elements $\sigma \in G$ such that $a(\sigma) = 1$.

We then use this result to count $|\mathrm{Im}(m)|$. Let $l \in L$, and write $(l) = \mathfrak{L}\overline{\mathfrak{L}}$ in Spec $A[\sqrt{up}]$. Then

$$\mathfrak{L} \in L' \Leftrightarrow \overline{\mathfrak{L}} \in L',$$

and

$$[\overline{\mathfrak{L}}] = [\mathfrak{L}]^{-1}.$$

Let

$$S_1 = \left\{[\mathfrak{L}] : \mathfrak{L} \in L' \text{ and } [\mathfrak{L}]^2 = 1\right\}.$$

Then

$$\begin{aligned} |\mathrm{Im}(m)| &= \text{Card } \left\{\{[\mathfrak{L}], [\mathfrak{L}]^{-1}\}, \mathfrak{L} \in L'\right\} \\ &= \frac{|S| + |S_1|}{2} \end{aligned}$$

where

$$|S| = \frac{h(\sqrt{up})}{2}$$

by last Lemma.

4.5 Elements of small norm in $\mathcal{O}_v(l)$

Let $\mathcal{O}_v(l)$ be the maximal orders of D described by (4.8).

Theorem 4.8 *There exists $h \in \mathcal{O}_v(l)$ such that h satisfies the polynomial equation*

$$h^2 - d = 0,$$

where $d \in A$ is a square-free polynomial of positive degree such that

$$|d| \leq \frac{q}{(q^2 - 1)^{1/2}} |p|^{1/2}.$$

Proof: Let $h \in \mathcal{O}(l)$, i.e.

$$\begin{aligned} h &= z + x\beta_{vl} + w\alpha + y\frac{r\beta_{vl} + \alpha\beta_{vl}}{l} \\ &= z + w\alpha + \frac{(xl + yr)}{l}\beta_{vl} + \frac{y}{l}\alpha\beta_{vl} \end{aligned}$$

with $x, y, z, w \in A$. We have the equations

$$\begin{aligned} \mathrm{tr}(h) &= 2z; & (4.14) \\ \mathrm{n}(h) &= z^2 - w^2up - \frac{(xl + yr)^2}{l^2}vl + \frac{y^2}{l^2}uvpl. & (4.15) \end{aligned}$$

¿From (4.14), we get $z = 0$. We also set $w = 0$, and (4.15) becomes

$$Q(x, y) = (-vl)x^2 + 2(-vr)xy + v\left(\frac{up - r^2}{l}\right)y^2 \qquad (4.16)$$

which is a quadratic form with coefficients in A of discriminant $\Delta = -uv^2p$. Completing the square, we write any such quadratic form $ax^2 + 2bxy + cy^2$ as

$$a\left(x + \frac{b}{a}y\right)^2 + \frac{\Delta}{a}y^2, \qquad (4.17)$$

where $\Delta = ac - b^2$ is the discriminant. Using that result, we get that the quadratic form $Q(x, y)$ of (4.16) is 0 if and only if

$$vl\left(x + \frac{r}{l}y\right)^2 = uv\frac{p}{l}y^2.$$

Comparing the leading coefficients on both sides, last equality is satisfied only when both sides are 0, i.e. for $(x, y) = (0, 0)$. We now show that for any quadratic form

$$Q(x, y) = ax^2 + 2bxy + cy^2, \quad a, b, c \in A$$

of discriminant $\Delta = ac - b^2$ such that

$$Q(x, y) \neq 0 \text{ for all } (x, y) \neq (0, 0) \in A^2,$$

there is $(x,y) \neq (0,0) \in A^2$ such that

$$|Q(x,y)| \leq \sqrt{|\Delta|}.$$

Indeed, write $b = af + g$, with $f, g \in A$, $\deg g < \deg a$. Then using $(x,y) = (-f,1)$ in (4.17), we get

$$|Q(-f,1)| = \left| a\left(\frac{g}{a}\right)^2 + \frac{\Delta}{a} \right| \leq \frac{|a|}{q^2} + \frac{|\Delta|}{|a|}.$$

Consider

$$I = \inf_{\substack{(x,y)\in A^2 \\ (x,y)\neq(0,0)}} |Q(x,y)|.$$

Without lost of generality, transforming $Q(x,y)$ in an equivalent quadratic form, we can suppose that $I = |a|$, obtained at $(x,y) = (1,0)$. Then, we have that

$$|a| \leq \frac{|a|}{q^2} + \frac{|\Delta|}{|a|} \Longleftrightarrow |a| \leq \frac{q}{(q^2-1)^{1/2}} |\Delta|^{1/2}.$$

4.6 A partial Result

In Section 4.3, we found 2 families of maximal orders of D containing $\sqrt{up}$. By analogy with the rational case, i.e. maximal orders in $\mathbb{Q}_{p,\infty}$, we make the following hypothesis:

Hypothesis 4.9 *Let ϕ be a rank 2 Drinfeld A-module defined over $\mathbb{F}_{\mathfrak{p}}$. Then there is some $l \in L$ such that*

$$End\,(\phi) \simeq \mathcal{O}_v(l) \;\; or \;\; End\,(\phi) \simeq \mathcal{O}_{v'}(l).$$

Let

$$\pi_\phi^{even}(x) = \#\{\mathfrak{p} \in \text{Spec } A : \deg \mathfrak{p} \text{ is even, } |\mathfrak{p}| \leq x \text{ and } \phi_{\mathfrak{p}} \text{ is supersingular}\}.$$

Then, following Section 4.1, we get

Theorem 4.10 *Assuming Hypothesis 4.9,*

$$\pi_\phi^{even}(x) \ll x^{3/4} \log^2 x,$$

where the O-constant depends only on q.

Proof: By Theorem 4.8, with $C_q = q/(q^2-1)$,

$$\pi_\phi^{even}(x) \ll \sum_{|d| \le C_q \sqrt{x}} |d|^{1/2} \log^2 x \ll_q x^{3/4} \log^2 x.$$

Appendix A

Average Distribution of Supersingular Primes

Let $\phi(a,b)$ denote the Drinfeld A-module given by

$$\phi_T = \gamma(T) + a\mathcal{F} + b\mathcal{F}^2, \quad a, b \in A,\ b \neq 0, \tag{A.1}$$

and for each regular $\mathfrak{p} \in \operatorname{Spec} A$, let

$$\phi(a,b)_{\mathfrak{p}}$$

be the reduction of $\phi(a,b)$ over the finite field $\mathbb{F}_{\mathfrak{p}}$. As usual, we denote

$$\pi_{\phi(a,b)}(x) = \#\{\mathfrak{p} \in \operatorname{Spec} A : |\mathfrak{p}| \leq x \text{ and } \phi(a,b)_{\mathfrak{p}} \text{ is supersingular}\}.$$

We want to evaluate the distribution of the supersingular primes averaging over all the Drinfeld A-modules given by (A.1). We then consider the sum

$$\sum_{\substack{|a| \leq K_a \\ |b| \leq K_b}} \pi_{\phi(a,b)}(x),$$

which we write as

$$\sum_{\substack{\mathfrak{p}\in \operatorname{Spec} A\\ |\mathfrak{p}|\le x}} \#\{\phi(a,b) : |a| \le K_a,\ |b| \le K_b,\ \text{and } \phi(a,b)_{\mathfrak{p}} \text{ is supersingular}\}.$$

Fix $\mathfrak{p} \in \operatorname{Spec} A$, $\mathfrak{p} = (p)$, with p a monic polynomial of degree d. We first count the number of supersingular modules ϕ over $\mathbb{F}_{\mathfrak{p}}$. Let u be a non-square in $\mathbb{F}_q^*$, and let $H(p)$ be the number of isomorphism classes of supersingular modules defined over $\mathbb{F}_{\mathfrak{p}}$. We showed in Chapter 4 that

$$H(p) = \begin{cases} \frac{1}{2}h(\sqrt{up}) & \text{when } d = \deg p \text{ is even;} \\ \frac{1}{2}\left(h(\sqrt{up}) + h(\sqrt{p})\right) & \text{when } d = \deg p \text{ is odd.} \end{cases} \tag{A.2}$$

Lemma A.1 *([11, Lemma 4.1]) Let $\phi(a,b)$ and $\psi(a',b')$ be rank 2 Drinfeld A-modules over L. Write*

$$\begin{aligned} \phi_T &= \gamma(T) + a\mathcal{F} + b\mathcal{F}^2 \\ \psi_T &= \gamma(T) + a'\mathcal{F} + b'\mathcal{F}^2. \end{aligned}$$

Then, $\phi \simeq_L \psi$ if and only if there exists $c \in L^*$ such that

$$a' = c^{q-1}a \quad \textit{and} \quad b' = c^{q^2-1}b.$$

Let $\phi(a_{\mathfrak{p}}, b_{\mathfrak{p}})$ be a supersingular Drinfeld A-module defined over $\mathbb{F}_{\mathfrak{p}}$, i.e. $\phi(a_{\mathfrak{p}}, b_{\mathfrak{p}})$ is defined by

$$\phi_T = \gamma(T) + a_{\mathfrak{p}}\mathcal{F} + b_{\mathfrak{p}}\mathcal{F}^2, \quad a, b \in \mathbb{F}_{\mathfrak{p}},\ \ b \ne 0.$$

By last lemma, any Drinfeld A-module over $\mathbb{F}_{\mathfrak{p}}$ in the isomorphism class of ϕ can be written as

$$\phi(c^{q-1}a_{\mathfrak{p}}, c^{q^2-1}b_{\mathfrak{p}}),$$

with $c \in \mathbb{F}_{\mathfrak{p}}^*$. Then, the number of such modules is

(i) the number of $(q-1)^{th}$ powers in $\mathbb{F}_p^* \simeq F_{q^d}^*$ if $j_{\phi(a_p,b_p)} \neq 0$, or equivalently if $a_p \neq 0$;

(ii) the number of $(q^2-1)^{th}$ powers in $\mathbb{F}_p^* \simeq F_{q^d}^*$ if $j_{\phi(a_p,b_p)} = 0$, or equivalently $a_p = 0$.

As $\phi_(a_p, b_p)$ is supersingular, the latter case is only possible when $d = \deg p$ is odd ([11, Satz 5.9]). We then compute that the number of modules over $\mathbb{F}_p$ in the class of $\phi_(a_p, b_p)$ is

$$\frac{q^d-1}{q-1}. \tag{A.3}$$

Then, by (A.2) and (A.3), the number of supersingular modules over $\mathbb{F}_p$ is

$$\frac{q^d-1}{q-1}\, H(p).$$

Lemma A.2 *Let K_a and K_b be large enough to have $q^d = |p| \leq \min(K_a, K_b)$. Then for any $\alpha, \beta \in \mathbb{F}_p$,*

$$\#\{(a,b) : |a| \leq K_a,\ |b| \leq K_b,\ a \equiv \alpha(p),\ b \equiv \beta(p)\} = \frac{K_a K_b}{q^{2d}}\, q^{2-r_a-r_b}$$

where

$$\begin{aligned} r_a &= \log_q K_a - \lfloor \log_q K_a \rfloor \\ r_b &= \log_q K_b - \lfloor \log_q K_b \rfloor . \end{aligned}$$

With last lemma,

$$\begin{aligned} \sum_{\substack{|a| \leq K_a \\ |b| \leq K_b}} \pi_{\phi(a,b)}(x) &= \sum_{|p| \leq x} \frac{K_a K_b}{q^{2d}}\, q^{2-r_a-r_b}\, \#\{\text{supersingular modules over } \mathbb{F}_p\} \\ &= \frac{q^{2-r_a-r_b}}{q-1}\, K_a K_b \sum_{|p| \leq x} \frac{H(p)}{|p|} + O_q\left(K_a K_b \sum_{|p| \leq x} \frac{H(p)}{|p|^2} \right) \end{aligned}$$

where the O-constant depends on q. If we have, as in [10],

$$\sum_{|p|\leq x} \frac{H(p)}{|p|} \sim C\frac{\sqrt{x}}{\log x}, \tag{A.4}$$

it would imply that the Lang-Trotter conjecture is true in average for Drinfeld modules. We are presently working on the evaluation of (A.4). Very similar estimates hold averaging the class numbers of number fields and function fields (see [17]).

Bibliography

[1] E. Artin, Quadratische Körper im Gebiel der höheren Kongruenzen I, II (thesis), *Collected Papers*, ed. S. Lang and J. Tate, Addison-Wesley, 1-94 (1965).

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

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

[4] D.R. Dorman, On singular moduli of rank 2 Drinfeld modules, *Compositio Math.* **80**, 235-256 (1991).

[5] D.R. Dorman, Singular moduli for rank 2 Drinfeld modules II, *preprint.*

[6] V. Drinfel'd, Elliptic modules (russian), *Math. Sbornik*, **94**, 594-627 (1974); Elliptic Modules (english translation), *Math USSR-Sbornik*, **23**, 561-592 (1976).

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

[8] N. D. Elkies, Ph. D. thesis, Harvard University (1987).

[9] M. D. Fried and M. Jarden, *Field arithmetic*, Springer-Verlag (1986).

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

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

[12] E.-U. Gekeler, On the coefficients of Drinfeld modular forms, *Invent. Math.* **93**, 667-700 (1988).

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

[14] B.H. Gross and D.B. Zagier, On singular moduli, *J. Reine und ang. Math.* **335**, 191-220 (1985).

[15] 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, 1-32 (1992) .

[16] D. R. Hayes, Explicit class field theory in global function fields, in *Studies in Algebra and Number Theory*, Advances in Mathematics Supplementary Studies **16**, ed. G. Rota, Academic Press, 173-217 (1979).

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

[18] T. Ibukiyama, On maximal orders of division quaternion algebras over the rational number field with certain optimal embeddings, *Nagoya Math. J.* **88**, 181-195 (1982).

[19] M. Kaneko, Supersingular j-invariants as singular moduli mod p, *Osaka J. Math.* **26**, 849-855 (1989).

[20] J. C. Lagarias and A. M. Odlyzko, Effective version of the Chebotarev density theorem, in *Algebraic Number Fields* (A. Fröhlich, ed.), Academic Press, 409-464 (1977).

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

[22] J. Neukirch, *Class field theory*, Springer-Verlag (1986).

[23] M. Rosen, The Hilbert class field in function fields, *Expositiones Math.* **5**, 365-378 (1987).

[24] M.-F. Vignéras, *Arithmetique des algèbres de quaternions*, Lectures Notes in Math. **800**, Springer-Verlag (1980).