SUPERSINGULAR REDUCTION OF DRINFELD MODULES

CHANTAL DAVID

Abstract. We present here an improvement of the results obtained by Brown in [1], on lower bounds for the number of supersingular primes of a rank 2 Drinfeld module ϕ over $\mathbb{F}_q(T)$. The improvement follows from a theorem giving a bound on certain supersingular primes of ϕ. This is similar to the case of elliptic curves, but the results obtained here for Drinfeld modules hold unconditionally, the Riemann hypothesis being known to hold over function fields.

1. Introduction.

Let $R = \mathbb{F}_q[T]$ and $F = \mathbb{F}_q(T)$ be, respectively, the ring of polynomials and the field of rational functions in one indeterminate over the finite field $\mathbb{F}_q$, q a power of an odd prime.

Let ϕ be a rank 2 Drinfeld R-module defined over $\mathbb{F}_q(T)$. For $p \in \mathbb{F}_q[T]$ a prime of good reduction for ϕ, let ϕ_p denote the reduction of ϕ at p; ϕ_p is then a rank 2 Drinfeld R-module over the finite field

$$\mathbb{F}_{(p)} = \mathbb{F}_q[T]/(p) \simeq \mathbb{F}_{q^{\deg p}}.$$

Depending on the structure of the endomorphism ring $\mathrm{End}(\phi_p)$, the Drinfeld module ϕ_p is said to be ordinary or supersingular (see Section 2). Let

$$P(x) = \left\{ \text{ monic prime polynomials } p \in \mathbb{F}_q[T] \,:\, |p| = q^{\deg p} \leq x \right\}.$$

In this paper, we investigate the asymptotic behavior of

$$\pi_\phi(x) = \#\left\{ p \in P(x) \ :\ \phi \text{ has good supersingular reduction at } p \right\}.$$

A quadratic extension K/F is said to be imaginary if the prime at infinity does not split in K/F. We say that a Drinfeld module ϕ has complex multiplication by an order $\mathcal{O}$ of a quadratic imaginary extension K/F if $\mathcal{O} \simeq \mathrm{End}(\phi)$. In this case, by Deuring's criterion (Theorem 2.2) and Čebotarev density theorem (Theorem 5.1), we get that

Partially supported by CICMA.

(i) when $K \neq F(\sqrt{u})$, u a non-square in $\mathbb{F}_q^*$,

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

where $\overline{x}$ is the largest power of q smaller than or equal to x;

(ii) when $K = F(\sqrt{u})$, u a non-square in $\mathbb{F}_q^*$,

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

where $\overline{x}$ is the largest *odd* power of q smaller than or equal to x.

When ϕ does not have complex multiplication, by analogy with the case of elliptic curves over $\mathbb{Q}$, it is natural to ask if

Conjecture 1.1 (Lang-Trotter conjecture for Drinfeld modules)**.** *There is a constant C_ϕ such that*

$$\pi_\phi(x) = C_\phi \frac{x^{1/2}}{\log_q x} + \underline{o}\left(\frac{x^{1/2}}{\log_q x}\right)$$

when $x \to \infty$.

We show in [2] that, on average, this conjecture holds for each degree k.

Brown showed in [1] that if ϕ is a *non-exceptional* (see Section 3) rank 2 Drinfeld R-module, then

$$\pi_\phi(x) \gg \log\log\log x \tag{1.1}$$

when $x \to \infty$. We show in this paper that this bound can be improved to

$$\pi_\phi(x) \gg \log\log x \tag{1.2}$$

when $x \to \infty$. This is similar to the case of elliptic curves, where conditional results, assuming the generalised Riemman hypothesis for L-series over number fields, were proved by Murty [15] and Elkies [7, 8]. Recently, some unconditional results were obtained by Fouvry and Murty [10]. It should be noted that the results obtained here are unconditional, since the Riemann hypothesis is true over function fields.

2. Supersingular Drinfeld modules.

For the basic definitions and properties of Drinfeld modules, see for example [11] or [13]. We just recall here some facts about supersingular reduction of Drinfeld modules.

Let $\phi = \phi(a, b)$ be the rank 2 Drinfeld R-module of generic characteristic over $\mathbb{F}_q(T)$ with equation

$$\phi(T) = T + af + bf^2, \quad a, b \in \mathbb{F}_q[T], \; b \neq 0, \tag{2.1}$$

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

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

The j-invariant of ϕ is then

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

We will consider only Drinfeld R-modules of rank 2, and we simply call them Drinfeld modules.

Let p be a monic prime polynomial of $\mathbb{F}_q[T]$. If $p \not| b$, then p is a prime of good reduction of ϕ, and the reduction of ϕ at p is the Drinfeld module ϕ_p with equation

$$\phi_p(T) = T + (a \bmod p)\, f + (b \bmod p)\, f^2 = T + a'\, f + b' f^2,$$

where

$$a', b' \in \mathbb{F}_{(p)} = \mathbb{F}_q[T]/(p) \simeq \mathbb{F}_{q^{\deg p}}, \quad \text{and } b' \neq 0.$$

Definition 2.1. *A Drinfeld module ψ defined over $\mathbb{F}_{(p)} = \mathbb{F}_q[T]/(p)$ is supersingular if the following equivalent conditions hold:*

(i) $\psi(p)$ is purely inseparable, i.e. $\psi(p) = f^h$ for some integer h;
(ii) There are no p-torsion points, i.e. Ker $\psi(p) = 0$;
(iii) $End_{\overline{\mathbb{F}_{(p)}}}(\psi)$ is a non-commutative ring;
(iv) $End_{\overline{\mathbb{F}_{(p)}}}(\psi)$ is a maximal order in the unique quaternion algebra over F which is ramified exactly at p and ∞.

The equivalence of these properties is proved in [11, Thm 5.3] and [12, Proposition 4.1]. A Drinfeld module which is not supersingular is said to be ordinary. For p a prime of good reduction of ϕ, we say p is a supersingular (respectively ordinary) prime for ϕ if ϕ_p is a supersingular (respectively ordinary) Drinfeld module over $\mathbb{F}_{(p)}$.

The following theorem is the statement of the criterion of Deuring [3], which allows the detection of supersingular primes of elliptic curves, in the context of Drinfeld modules.

Theorem 2.2 (Deuring's Criterion)**.** [1, Lemma 2.9.3] *Let $\phi(a, b)$ be a Drinfeld module as defined by (2.1). Let p be a prime of good reduction of ϕ. Then ϕ has supersingular reduction at p if and only if there exists an order $\mathcal{O}$ of a quadratic imaginary extension K/F such that*

(i) $P_{\mathcal{O}}(j_\phi) \equiv 0 \bmod p$;
(ii) p is inert or ramified in K.

In the previous theorem, $P_{\mathcal{O}}(x)$ denotes the monic polynomial whose roots are exactly the j-invariants of Drinfeld modules defined over C with complex multiplication by the order $\mathcal{O}$ of the quadratic imaginary extension K/F ; C is the completion at the infinite prime of the algebraic closure $\overline{F}_\infty$, and plays the role of the complex plane for Drinfeld modules over $\mathbb{F}_q(T)$. Let $K = F(\sqrt{d})$, $\mathcal{O} = R[\sqrt{d}]$ for some square-free $d \in \mathbb{F}_q[T]$. We then denote $P_{\mathcal{O}}(x)$ by $P_d(x)$, and the roots of $P_d(x)$ are then called the singular moduli associated to d. In [6], Drinfeld proved the existence of an analytic parametrisation for Drinfeld modules over C, given by the analytic function $j(z)$. Using this, we can write

$$P_d(x) = \prod_{R[\sqrt{d}] \subseteq \mathrm{End}(\phi)} (x - j_\phi) = \prod_{\substack{[z] \\ \mathrm{disc}(z) = d}} (x - j(z)) \tag{2.2}$$

where the product $\prod_{[z]}$ runs over equivalence classes $[z]$ of discriminant d. $P_d(x)$ is then a polynomial of degree $h(d)$, the class number of $F(\sqrt{d})$, over R.

3. Supersingular primes of ϕ.

All the material of this section can be found in [1]. Fix some Drinfeld module ϕ as defined by (2.1). We also suppose that ϕ is a *non-exceptional* Drinfeld module. Let F_∞ be the completion of F at the infinite prime. To simplify the discussion, we will consider only non-exceptional Drinfeld modules ϕ which satisfy one of the following

(i) $q \equiv 3(4)$ and $j_\phi T$ is not a square in F_∞ ,
(ii) $q \equiv 1(4)$ and j_ϕ is not a square in F_∞ ,

but our proof applies to all non-exceptional Drinfeld modules, as defined in [1, Definition 1.1.5] . Let $P = \{p_1, p_2, \dots, p_n\}$ be a set of distinct monic prime polynomials of $\mathbb{F}_q[T]$, where each p_i is a either a prime of bad reduction or a supersingular prime of ϕ. We also suppose that P contains all primes of bad reduction.

Any $f \in F^*$ can be written uniquely in F_∞ as $f = \omega(f)\, u T^{\deg f}$, where $\omega(f) \in \mathbb{F}_q^*$, and u is an element of the valuation ring of F_∞ such that $u \equiv 1 \bmod \infty$. We also define

$$\mathrm{sgn}\ f = \begin{cases} 1 & \text{if } \omega(f) \text{ is a square in } \mathbb{F}_q^* \\ -1 & \text{if } \omega(f) \text{ is not a square in } \mathbb{F}_q^*. \end{cases}$$

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

$$(-\beta)^{(q-1)/2} = -\omega(j_\phi)^{(q-1)/2}. \tag{3.1}$$

Let π be a prime polynomial of $\mathbb{F}_q[T]$ such that

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

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

We say that π is an *admissible prime associated to P and β*. Let N_π be the numerator of $P_\pi(j_\phi)$, i.e.

$$N_\pi = P_\pi(j_\phi) b^{h(\pi)}, \tag{3.2}$$

where $j_\phi = \frac{a}{b}$ and $h(\pi)$ is the class number of $F(\sqrt{\pi})$. We will see in Section 5 that there is an infinite number of such primes. Then, since ϕ is non-exceptional and (3.1) holds, one can show that [1, (4.2.10)]

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

There is then a prime $p(\pi) \in \mathbb{F}_q[T]$ dividing N_π such that

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

By Deuring's criterion (Theorem 2.2), $p(\pi)$ is a supersingular prime for ϕ, and $p(\pi)$ cannot be one of the p_i's, since π is a quadratic non-residue mod $p(\pi)$. This shows that there exist an infinite number of supersingular primes for ϕ.

Finally, it is clear that

$$|p(\pi)| \leq |N_\pi|. \tag{3.3}$$

4. A bound for N_d.

We prove in this section that

Theorem 4.1. *Let $d \in \mathbb{F}_q[T]^*$ be a square-free polynomial such that $F(\sqrt{d})/F$ is a quadratic imaginary extension, and let ϕ be a Drinfeld module as given by (2.1). Let N_d be the numerator $P_d(j_\phi)$. 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.

As in the classical case of elliptic curves over $\mathbb{Q}$, we can write the singular moduli associated to d as $j(z_i)$, where for $1 \leq i \leq h(d)$

$$z_i = \frac{-b_i \pm \sqrt{b_i^2 - 4a_ic_i}}{2a_i}, \qquad b_i^2 - 4a_ic_i = d \tag{4.1}$$

with

$$a_i, b_i, c_i \in \mathbb{F}_q[T], \quad \text{ and } \quad |b_i| < |a_i| \leq |c_i|. \tag{4.2}$$

It can also be shown that

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

where C_q depends only on q ([1, Lemma 2.8.2]). Choose

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

Then

$$P_d(j_\phi) \;=\; \prod_{i=1}^{h(d)} \left(j_\phi - j(z_i)\right) \;\ll\; 2^{h(d)} \exp\left(C|d|^{1/2} \sum_{i=1}^{h(d)} \frac{1}{|a_i|}\right),$$

so we have to bound $h(d)$ and $\sum_{i=1}^{h(d)} \frac{1}{|a_i|}$.

Lemma 4.2.

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

where the O-constant depends only on q.

Proof: Define the L-series

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

where

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

and where the sum is taken over monic polynomials $a \in \mathbb{F}_q[T]$. By quadratic reciprocity, one shows that $L(s, \chi_d)$ is the finite sum

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

which gives

$$L(1, \chi_d) \ll \log|d|. \tag{4.3}$$

We now use the class number formula for function fields. Since $F(\sqrt{d})$ is a quadratic imaginary extension of F, we only have to consider the following cases

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

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

With (4.3), this completes the proof of Lemma 4.2. □

Lemma 4.3.

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

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 than 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 (4.2). Then

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

where the sum runs over monic polynomials $a \in A$, and $\delta(a)$ is the number of monic prime divisors of a. But

$$\sum_{|a| \leq |d|^{1/2}} \frac{2^{\delta(a)}}{|a|} \leq \sum_{|a| \leq |d|^{1/2}} \sum_{|b| \leq |d|^{1/2}} \frac{1}{|a||b|} \ll \log^2 |d|. \quad \square$$

This completes the proof of Theorem 4.1, since

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

where $j_\phi = \frac{a}{b}$ with $a, b \in \mathbb{F}_q[T]$.
Remark: This improves the bound given in [1], which is $N_d \ll \exp(|d|^4)$.

5. Distribution of primes.

Let E be a finite Galois extension of $F = \mathbb{F}_q(T)$, with Galois group $G = \text{Gal}(E/F)$, and genus g_E. Let L be the algebraic closure of $\mathbb{F}_q$ in E, and

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

For C a conjugacy class in G, we denote

$$\begin{aligned} P_k(F) &= \{p \text{ monic prime } \in \mathbb{F}_q[T] \ : \ \deg p = k\} \\ P_k(E/F; C) &= \left\{ p \in P_k(F) \ : \ p \text{ is unramified in } E/F \text{ and } \left(\frac{E/F}{p}\right) = C \right\}. \end{aligned}$$

Then, since the Riemann hypothesis is true over function fields, we get

Theorem 5.1 (Čebotarev Density Theorem). *([9, Proposition 5.16]) Let f be the Frobenius element of $\mathbb{F}_q$, i.e.*

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

Let a be a positive integer such that

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

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

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

and for $k \equiv a$ mod N

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

where the O-constant is absolute.

Remark: This is in fact stronger than the statement of Proposition 5.16 of [9], since we are in the particular case of a Galois extension over $\mathbb{F}_q(T)$.

We now apply the last theorem to count the number of admissible primes π, as defined above. Let $P = \{p_1, \ldots, p_n\}$ be a set of monic prime polynomials of $\mathbb{F}_q[T]$, and $\beta \in \mathbb{F}_q^*$. Let

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

with α a non-square of $\mathbb{F}_q^*$. Then the algebraic closure of $\mathbb{F}_q$ in K_n is $L = \mathbb{F}_{q^2}$ and

$$\begin{aligned} N &= [\mathbb{F}_{q^2} : \mathbb{F}_q] = 2 \\ M &= [K_n : \mathbb{F}_{q^2}(T)] = 2^n \\ \mathrm{Gal}(K_n/F) &\simeq (\mathbb{Z}/2\mathbb{Z})^{n+1}. \end{aligned}$$

Let $\pi^k_{P,\beta}$ be the number of prime polynomials π of $\mathbb{F}_q[T]$ such that

(i) π is unramified in K_n/F;
(ii) π is an admissible prime associated to P and β;
(iii) $\deg \pi = k$.

Lemma 5.2. *There exists a unique $g(P,\beta) \in Gal\ (K_n/F)$ such that for a prime polynomial $\pi \in \mathbb{F}_q[T]$, unramified in K_n with $\omega(\pi) = \beta$, the following are equivalent:*

(i) $\deg \pi$ is odd, and for $1 \le i \le n$, $\left(\frac{\pi}{p_i}\right) = 1$;
(ii) $\left(\frac{K_n/F}{\pi}\right) = g(P,\beta)$.

Proof: This is a consequence of quadratic reciprocity over function fields, which reads as

$$\left(\frac{\alpha}{\pi}\right) = (-1)^{\deg \pi}$$

for α a non-square of $\mathbb{F}_q[T]$, and

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

for p_i a polynomial of $\mathbb{F}_q[T]$ with $\deg p_i \ge 1$. $\square$

Applying the Čebotarev density theorem to the extension K_n/F, with $C = \{g(P,\beta)\}$, we obtain

$$\pi^k_{P,\beta} = \pi_C(K_n/F;k) = 0 \qquad \text{when } k \text{ is even,}$$

and

$$\pi^k_{P,\beta} = \pi_C(K_n/F;k) = \frac{1}{2^n}\frac{q^k}{k} + O\left(\frac{q^{k/2}}{k}\left(k + \sum_{i=1}^{n} \deg p_i\right)\right) \qquad \text{when } k \text{ is odd ,} \tag{5.1}$$

with an absolute O-constant.

We then show

Proposition 5.3. *There is a sufficiently large absolute constant C such that for any odd k such that*

$$q^k \geq C\ 4^n \left(\sum_{i=1}^{n} \deg p_i\right)^2, \tag{5.2}$$

we have

$$\pi^k_{P,\beta} \gg \frac{1}{2^n}\frac{q^k}{k}.$$

Proof: For k odd such that (5.2) holds, we can choose C big enough such that the error term in (5.1) is bounded by a fraction of the main term. The result follows. □

We also define

$$\pi_{P,\beta}(x) = \sum_{q^k \leq x} \pi^k_{P,\beta}\ ,$$

and rewrite last proposition as

Proposition 5.4. *There is a sufficiently large absolute constant C such that for*

$$x \geq C\ q^2\ 4^n \left(\sum_{i=1}^{n} \deg p_i\right)^2, \tag{5.3}$$

we have

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

Proof: Let l be the unique odd integer such that $q^l \leq x < q^{l+2}$. Then, by the last proposition,

$$\pi_{P,\beta}(x) \geq \pi^l_{P,\beta} \gg \frac{1}{2^n}\frac{q^l}{l} \geq \frac{\log q}{q^2}\frac{1}{2^n}\frac{x}{\log x}$$

when $q^l \geq C\ 4^n\ \left(\sum_{i=1}^n \deg p_i\right)^2$, which is insured by (5.3). □

Remark: With Proposition 5.4 and Theorem 4.1, it follows by induction that

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

which is a first improvement of (1.1).

6. Supersingular primes of Drinfeld modules with two complex multiplications.

Theorem 6.1. *Let ϕ be a Drinfeld module defined over $\mathbb{F}_q(T)$. Let $d_1,\, d_2 \in \mathbb{F}_q[T]$ be two distinct fundamental discriminants, and let p be a prime of good reduction of ϕ such that*

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

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

Proof: 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

$$J(d_1, d_2) = \prod_{\substack{[\tau_1],[\tau_2] \\ \mathrm{disc}(\tau_1)=d_1 \\ \mathrm{disc}(\tau_2)=d_2}} \left(j(\tau_1) - j(\tau_2)\right)^{\left(q^2-1/\omega_1\omega_2\right)},$$

where ω_1 and ω_2 are the number of roots of unity in the quadratic orders of discriminant d_1 and d_2 respectively. This is not sufficient here, since all admissible primes π as chosen in Section 3 are odd degree polynomials.

In general, one can prove Theorem 6.1 following the ideas of Kaneko [14] who proved a similar result for elliptic curves. By hypothesis, ϕ has good supersingular reduction ϕ_p at p. Then, $\mathrm{End}(\phi_p)$ is a maximal order in H, the unique quaternion algebra over F which ramifies exactly at p and ∞, and

$$\begin{aligned} R\left[\sqrt{d_1}\right] &\subseteq \mathrm{End}(\phi_p) \\ R\left[\sqrt{d_2}\right] &\subseteq \mathrm{End}(\phi_p). \end{aligned}$$

Let α_i be the image of $\sqrt{d_i}$ in $\mathrm{End}(\phi_p)$, $i = 1, 2$, and consider the R-submodule of $\mathrm{End}(\phi_p)$

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

This is an order in H; its reduced discriminant $d(L)$ is given by

$$d(L)^2 = R\left(\,\det \mathrm{tr}(\mu_i\mu_j)\,\right),$$

where

$$\mu_1 = 1, \;\; \mu_2 = \alpha_1, \;\; \mu_3 = \alpha_3, \;\; \mu_4 = \alpha_1\alpha_2$$

[16, Chapter 1, Lemma 4.7]. One computes

$$\det \operatorname{tr}(\mu_i \mu_j) = -\left(4d_1d_2 - s^2\right)^2,$$

where $s = \operatorname{tr}(\alpha_1\alpha_2)$. Then, since L is contained in the maximal order $\operatorname{End}(\phi_p)$

$$p^2 \mid -\left(4d_1d_2 - s^2\right)^2,$$

which gives

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

If

$$|s^2| > |d_1d_2|,$$

$h = \operatorname{tr}^2(\alpha_1\alpha_2) - 4\operatorname{n}(\alpha_1\alpha_2)$ is a polynomial of even degree with leading coefficient in $(\mathbb{F}_q^*)^2$, i.e. ∞ splits in the quadratic extension $F(\sqrt{h})/F$. Since $F(\sqrt{h}) \subseteq H$, this is impossible. Then

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

and

$$|p| \leq |d_1d_2| \quad \Leftrightarrow \quad \deg p \leq \deg d_1d_2. \quad \square$$

7. Lower bound for $\pi_\phi(x)$.

Given $P = \{p_1, \ldots, p_n\}$, we choose admissible primes π associated to $p_1, \ldots, p_n$, as in Section 3. For each of these admissible π, we get a new supersingular prime $p(\pi) \mid N_\pi$, and by construction $p(\pi) \notin P = \{p_1, \ldots, p_n\}$. If we can also insure that they are all distinct, we can use Proposition 5.4 to count the new supersingular primes $p(\pi)$. Theorem 6.1 gives the criterion which insures that the primes $p(\pi)$ are distinct.

Theorem 7.1. *Let ϕ a non-exceptional Drinfeld module, as given by (2.1). 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, $\log x_{m+1} \ll x_m^{1/4} \log^2 x_m$.

Proof: Let K be any positive constant such that

$$K < \frac{1}{2\log 4}. \tag{7.1}$$

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

Then, let x be such that

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

and let $p_1, \dots, p_n$ be the n supersingular primes of ϕ with norm smaller than or equal to x. Then,

$$4^n \left(\sum_{i=1}^{n} \deg p_i \right)^2 \leq 4^n n^2 (\log_q x)^2 < x^{K \log 4} K^2 \log^2 x \ \ \log_q^2 x,$$

and by (7.1), we obtain

$$\sqrt{x} \geq C q^2 4^n \left(\sum_{i=1}^{n} \deg p_i \right)^2$$

for x large enough. Then, by Proposition 5.4,

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

For each of those admissible π with norm smaller than or equal to $\sqrt{x}$, we get a new supersingular prime $p(\pi)$. Suppose that $p = p(\pi_1) = p(\pi_2)$ for some $\pi_1 \neq \pi_2$. Then by Theorem 6.1, $|p| \leq x$, which is impossible since $p(\pi) \notin P = \{p_1, \dots, p_n\}$. Let $x' = \max |p(\pi)|$. Then by Theorem 4.1,

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

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

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

Then for x large enough, using 7.1, we get

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

This completes the proof of the Theorem. $\square$

Corollary 7.2.

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

Proof: Corollary 7.2 follows applying Theorem 7.1 to find $x_m \leq x \leq x_{m+1}$. Then

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

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

[2] C. David, Average distribution of supersingular Drinfeld modules, *preprint.*

[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 finite Drinfeld modules, *Journal of Algebra*, **141**, 187-203 (1991).

[13] 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) .

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

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

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

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

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