Journal of Number Theory 237 (2022) 15–39

Contents lists available at ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt

General Section

The growth of the discriminant of the endomorphism ring of the reduction of a rank 2 generic Drinfeld module

Alina Carmen Cojocaru [a,b,1], Mihran Papikian [c,*,2]

[a] *Department of Mathematics, Statistics and Computer Science, University of Illinois at Chicago, 851 S Morgan St, 322 SEO, Chicago, 60607, IL, USA*
[b] *Institute of Mathematics "Simion Stoilow" of the Romanian Academy, 21 Calea Grivitei St, Bucharest, 010702, Sector 1, Romania*
[c] *Department of Mathematics, Pennsylvania State University, University Park, PA 16802, USA*

ARTICLE INFO

Article history:
Received 16 January 2020
Received in revised form 26 September 2020
Accepted 5 March 2021
Available online 6 June 2021
Communicated by F. Breuer

Dedicated to Professor Ernst-Ulrich Gekeler

MSC:
primary 11G09, 11R58
secondary 11R29, 11R44

Keywords:
Drinfeld modules

ABSTRACT

For q an odd prime power, $A = \mathbb{F}_q[T]$, and $F = \mathbb{F}_q(T)$, let $\psi : A \to F\{\tau\}$ be a Drinfeld A-module over F of rank 2 and without complex multiplication, and let $\mathfrak{p} = pA$ be a prime of A of good reduction for ψ, with residue field $\mathbb{F}_\mathfrak{p}$. We study the growth of the absolute value $|\Delta_\mathfrak{p}|$ of the discriminant of the $\mathbb{F}_\mathfrak{p}$-endomorphism ring of the reduction of ψ modulo $\mathfrak{p}$ and prove that, for all $\mathfrak{p}$, $|\Delta_\mathfrak{p}|$ grows with $|p|$. Moreover, we prove that, for a density 1 of primes $\mathfrak{p}$, $|\Delta_\mathfrak{p}|$ is as close as possible to its upper bound $|a_\mathfrak{p}^2 - 4\mu_\mathfrak{p} p|$, where $X^2 + a_\mathfrak{p} X + \mu_\mathfrak{p} p \in A[X]$ is the characteristic polynomial of $\tau^{\deg p}$.

* Corresponding author.
E-mail addresses: cojocaru@uic.edu (A.C. Cojocaru), papikian@psu.edu (M. Papikian).

[1] A.C.C. was partially supported by a Collaboration Grant for Mathematicians from the Simons Foundation under Award No. 318454.
[2] M.P. was partially supported by a Collaboration Grant for Mathematicians from the Simons Foundation under Award No. 637364.

https://doi.org/10.1016/j.jnt.2021.03.026
0022-314X/

Orders
Endomorphism rings

1. Introduction

Let $\mathbb{F}_q$ be a finite field with q elements, $A := \mathbb{F}_q[T]$ be the ring of polynomials in T over $\mathbb{F}_q$, $F := \mathbb{F}_q(T)$ be the field of fractions of A, and F^{alg} be a fixed algebraic closure of F. We call a nonzero prime ideal of A simply a *prime* of A. The main results of this paper concern the reductions modulo primes of A of a fixed Drinfeld module over F. To state these results, we first recall some basic concepts from the theory of Drinfeld modules.

An *A-field* is a field L equipped with a homomorphism $\gamma : A \to L$. Two A-fields of particular prominence in this paper are F and $\mathbb{F}_{\mathfrak{p}} := A/\mathfrak{p}$, where $\mathfrak{p} \lhd A$ is a prime. When L is an extension of F, we implicitly assume that $\gamma : A \hookrightarrow L$ is obtained from the natural embedding of A into its field of fractions $A \hookrightarrow F \hookrightarrow L$; when L is a finite extension of $\mathbb{F}_{\mathfrak{p}}$, we implicitly assume that $\gamma : A \to A/\mathfrak{p} \hookrightarrow L$ is obtained from the natural quotient map.

For an A-field L, denote by $L\{\tau\}$ the noncommutative ring of polynomials in τ with coefficients in L and subject to the commutation rule $\tau c = c^q \tau$, $c \in L$. A *Drinfeld A-module of rank $r \geq 1$ defined over L* is a ring homomorphism $\psi : A \to L\{\tau\}$, $a \mapsto \psi_a$, uniquely determined by the image of T:

$$\psi_T = \gamma(T) + \sum_{1 \leq i \leq r} g_i(T)\tau^i, \quad g_r(T) \neq 0.$$

The *endomorphism ring* of ψ is the centralizer of the image $\psi(A)$ of A in $L\{\tau\}$:

$$\begin{aligned} \mathrm{End}_L(\psi) &:= \{u \in L\{\tau\} : u\psi_a = \psi_a u \text{ for all } a \in A\} \\ &= \{u \in L\{\tau\} : u\psi_T = \psi_T u\}. \end{aligned}$$

As $\mathrm{End}_L(\psi)$ contains $\psi(A) \cong A$ in its center, it is an A-algebra. It can be shown that $\mathrm{End}_L(\psi)$ is a free A-module of rank $\leq r^2$; see [Dr74, Sec. 2].

Now let $\psi : A \to F\{\tau\}$ be a Drinfeld A-module of rank r over F defined by

$$\psi_T = T + g_1\tau + \ldots + g_r\tau^r.$$

We say that a prime $\mathfrak{p} \lhd A$ is a *prime of good reduction* for ψ if $\mathrm{ord}_{\mathfrak{p}}(g_i) \geq 0$ for all $1 \leq i \leq r-1$ and if $\mathrm{ord}_{\mathfrak{p}}(g_r) = 0$. If that is the case, we view $g_1, \ldots, g_r$ as elements of the completion $A_{\mathfrak{p}}$ of A at $\mathfrak{p}$ and define the *reduction of ψ at $\mathfrak{p}$* as the Drinfeld A-module $\psi \otimes \mathbb{F}_{\mathfrak{p}} : A \to \mathbb{F}_{\mathfrak{p}}\{\tau\}$ given by

$$(\psi \otimes \mathbb{F}_{\mathfrak{p}})_T = \overline{T} + \overline{g_1}\tau + \cdots + \overline{g_r}\tau^r,$$

where $\overline{g}$ is the image of $g \in A_{\mathfrak{p}}$ under the canonical homomorphism $A_{\mathfrak{p}} \to A_{\mathfrak{p}}/\mathfrak{p}$. Note that $\psi \otimes \mathbb{F}_{\mathfrak{p}}$ has rank r since $\overline{g_r} \neq 0$. It is clear that all but finitely many primes of A are primes of good reduction for ψ; we denote the set of these primes by $\mathcal{P}(\psi)$.

Let $\mathfrak{p} = pA$ be a prime of good reduction of ψ, where p denotes the monic generator of $\mathfrak{p}$. Denote by $\mathcal{E}_{\psi,\mathfrak{p}} = \mathrm{End}_{\mathbb{F}_\mathfrak{p}}(\psi \otimes \mathbb{F}_\mathfrak{p})$ the endomorphism ring of $\psi \otimes \mathbb{F}_\mathfrak{p}$. It is easy to see that $\pi_\mathfrak{p} := \tau^{\deg p}$ is in the center of $\mathbb{F}_\mathfrak{p}\{\tau\}$, hence $\pi_\mathfrak{p} \in \mathcal{E}_{\psi,\mathfrak{p}}$. Using the theory of Drinfeld modules over finite fields, it is easy to show that $A[\pi_\mathfrak{p}]$ and $\mathcal{E}_{\psi,\mathfrak{p}}$ are A-orders in the imaginary field extension $F(\pi_\mathfrak{p})$ of F of degree r ("imaginary" means that there is a unique place of $F(\pi_\mathfrak{p})$ over the place $\infty := 1/T$ of F); see [GaPa19, Prop. 2.1]. Here we remind the reader that $A[\pi_\mathfrak{p}] = \psi(A)[\pi_\mathfrak{p}]$, i.e. that $A \cong \psi(A)$ also denotes the image of A under ψ. Then, denoting by $\mathcal{O}_{F(\pi_\mathfrak{p})}$ the integral closure of A in $F(\pi_\mathfrak{p})$, we obtain a natural inclusion of A-orders

$$A[\pi_\mathfrak{p}] \subseteq \mathcal{E}_{\psi,\mathfrak{p}} \subseteq \mathcal{O}_{F(\pi_\mathfrak{p})}.$$

It is an interesting problem, with important applications to the arithmetic of F, to compare the above orders as $\mathfrak{p}$ varies. For example, it is proved in [CoPa15, Thm. 1] (for $r = 2$) and in [GaPa19, Thm. 1.2], [GaPa20, Thm. 1.1] (for $r \geq 2$) that the quotient $\mathcal{E}_{\psi,\mathfrak{p}}/A[\pi_\mathfrak{p}]$ captures the splitting behavior of $\mathfrak{p}$ in the division fields of ψ; this result then leads to non-abelian reciprocity laws in function field arithmetic. Also, in [GaPa19, Thm. 1.1], it is shown that the quotients $\mathcal{E}_{\psi,\mathfrak{p}}/A[\pi_\mathfrak{p}]$ and $\mathcal{O}_{F(\pi_\mathfrak{p})}/\mathcal{E}_{\psi,\mathfrak{p}}$ can be arbitrarily large as $\mathfrak{p}$ varies, whereas in [CoPa15, Thm. 6] an explicit formula is given for the density of primes for which $A[\pi_\mathfrak{p}] = \mathcal{E}_{\psi,\mathfrak{p}}$.

In this paper, we are interested in the growth of the discriminant of $\mathcal{E}_{\psi,\mathfrak{p}}$ as $\mathfrak{p}$ varies, and in applications of this growth to the arithmetic of ψ. Our results assume that q is odd and $r = 2$. These assumptions are to be kept from here on without further notice.

Choosing a basis $\mathcal{E}_{\psi,\mathfrak{p}} = A\alpha_1 + A\alpha_2$ of $\mathcal{E}_{\psi,\mathfrak{p}}$ as a free A-module of rank 2, the discriminant $\Delta_\mathfrak{p} := \Delta_{\psi,\mathfrak{p}}$ of $\mathcal{E}_{\psi,\mathfrak{p}}$ is $\det(\mathrm{Tr}_{F(\pi_\mathfrak{p})/F}(\alpha_i\alpha_j))_{1\leq i,j\leq 2}$, which is well-defined up to a multiple by a square in $\mathbb{F}_q^\times$. If we write $\Delta_\mathfrak{p} = c_\mathfrak{p}^2 \cdot \Delta_{F(\pi_\mathfrak{p})}$, where $c_\mathfrak{p}, \Delta_{F(\pi_\mathfrak{p})} \in A$ with $\Delta_{F(\pi_\mathfrak{p})}$ square-free, then $\mathcal{E}_{\psi,\mathfrak{p}} = A + c_\mathfrak{p}\mathcal{O}_{F(\pi_\mathfrak{p})}$, $\Delta_{F(\pi_\mathfrak{p})}$ is the discriminant of $\mathcal{O}_{F(\pi_\mathfrak{p})}$, and $\mathcal{O}_{F(\pi_\mathfrak{p})}/\mathcal{E}_{\psi,\mathfrak{p}} \cong A/c_\mathfrak{p}A$ as A-modules. Note that, similarly to $\Delta_\mathfrak{p}$, the polynomial $c_\mathfrak{p}$ also depends on ψ, although this will not be explicitly indicated in our notation.

Denote by $|\cdot| = |\cdot|_\infty$ the absolute value on F corresponding to $1/T$, normalized so that $|a| = q^{\deg a}$ for $a \in A$, with $\deg a$ denoting the degree of a as a polynomial in T and subject to the convention that $\deg 0 = -\infty$. The first main result of this paper is the following:

Theorem 1. *Assume* $\mathrm{End}_{F^{\mathrm{alg}}}(\psi) = A$. *Then*

$$|\Delta_\mathfrak{p}| \gg_\psi \frac{\log|p|}{(\log\log|p|)^2},$$

where the implied $\gg_\psi$*-constant depends on* q *and on the coefficients of the polynomial* $\psi_T \in F\{\tau\}$.

By considering τ as the Frobenius automorphism of $\mathbb{F}_\mathfrak{p}$ relative to $\mathbb{F}_q$, that is, as the map $\alpha \mapsto \alpha^q$, we can also consider $\mathbb{F}_\mathfrak{p}$ as an A-module via $\psi \otimes \mathbb{F}_\mathfrak{p}$ (hence T acts on $\mathbb{F}_\mathfrak{p}$ as $(\psi \otimes \mathbb{F}_\mathfrak{p})_T$). This module will be denoted ${}^\psi\mathbb{F}_\mathfrak{p}$. The properties of the torsion elements of this module lead to an A-module isomorphism

$$ {}^\psi\mathbb{F}_\mathfrak{p} \cong A/d_{1,\mathfrak{p}}A \times A/d_{2,\mathfrak{p}}A $$

for uniquely determined nonzero monic polynomials $d_{1,\mathfrak{p}}, d_{2,\mathfrak{p}} \in A$ such that $d_{1,\mathfrak{p}} \mid d_{2,\mathfrak{p}}$; as above, the polynomials $d_{1,\mathfrak{p}}, d_{2,\mathfrak{p}}$ also depend on ψ, although this will not be explicitly indicated in our notation.

Note that $d_{2,\mathfrak{p}}$ may be regarded as the exponent of the A-module ${}^\psi\mathbb{F}_\mathfrak{p}$, and that $|d_{1,\mathfrak{p}} \cdot d_{2,\mathfrak{p}}| = |p|$; thus we have the trivial lower bound $|d_{2,\mathfrak{p}}| \geq |p|^{\frac{1}{2}}$. Theorem 1 allows us to deduce a stronger lower bound on $|d_{2,\mathfrak{p}}|$.

Theorem 2. *Assume* $\mathrm{End}_{F^{\mathrm{alg}}}(\psi) = A$. *Then*

$$ |d_{2,\mathfrak{p}}| \gg_\psi |p|^{\frac{1}{2}} \frac{(\log |p|)^{\frac{1}{2}}}{\log\log |p|}, $$

where the implied $\gg_\psi$*-constant depends on* q *and on the coefficients of the polynomial* $\psi_T \in F\{\tau\}$.

Theorems 1 and 2 are the Drinfeld module analogues of results by Schoof for elliptic curves over $\mathbb{Q}$; see the statement and proof of the main result of [Sc91]. Our proof of Theorem 1 is inspired by Schoof's arguments. It relies on Drinfeld's now-classical function field analogue of the analytic theory of elliptic curves [Dr74], on the growth properties of the function field counterpart of the j-function, proved by Gekeler [Ge99], and on the more recent Drinfeld module analogue of Deuring's lifting lemma, proved in an earlier paper by the present authors [CoPa15].

Remark 3. According to Theorem 1, $|\Delta_\mathfrak{p}|$ grows with $\deg p$. In relation to the growth of $|\Delta_\mathfrak{p}|$, Theorem 1.1 of [GaPa20] implies that, for any fixed number $\kappa > 0$, we can find $\mathfrak{p}$ such that $|c_\mathfrak{p}| > \kappa$; therefore, for such $\mathfrak{p}$, $|\Delta_\mathfrak{p}| = |c_\mathfrak{p}|^2 \cdot |\Delta_{F(\pi_\mathfrak{p})}| > \kappa$. However, Theorem 1.1 of [GaPa20] does not imply that $|\Delta_\mathfrak{p}|$ has to grow with $\deg p$. In fact, computationally, Garai and the second author have found that it happens that $c_\mathfrak{p} = 1$; in this case, their aforementioned theorem does not give any lower bound on $|\Delta_\mathfrak{p}|$. On the other hand, Theorem 1 of the present paper does not imply that we can find some $\mathfrak{p}$ such that $|c_\mathfrak{p}| > \kappa$. Thus these two results are complementary to each other.

Remark 4. If $\mathrm{End}_{F^{\mathrm{alg}}}(\psi) \neq A$, then $\mathrm{End}_{F^{\mathrm{alg}}}(\psi) = \mathcal{O}$ is an order in an imaginary quadratic extension K of F, in which case the growth of $|\Delta_\mathfrak{p}|$ is vastly different from that shown in Theorem 1. On one hand, if $\mathfrak{p} \in \mathcal{P}(\psi)$ splits in K, then

$$ \mathcal{O} \subseteq \mathrm{End}_{\mathbb{F}_\mathfrak{p}}(\psi \otimes \mathbb{F}_\mathfrak{p}) \subseteq \mathcal{O}_K $$

(see [Ge83, Lem. 3.3]), which implies that $|\Delta_{\mathfrak{p}}| \leq |\Delta_{\mathcal{O}}|$, where $\Delta_{\mathcal{O}}$ is the discriminant of $\mathcal{O}$. Hence $|\Delta_{\mathfrak{p}}|$ remains bounded as $\mathfrak{p}$ varies over the primes that split in K. In particular, Theorem 1 is false without its assumption. On the other hand, if $\mathfrak{p} \in \mathcal{P}(\psi)$ is inert in K, then $\psi \otimes \mathbb{F}_{\mathfrak{p}}$ is supersingular, which implies that $A[\pi_{\mathfrak{p}}] = A[\sqrt{\alpha p}]$ for some $\alpha \in \mathbb{F}_q^{\times}$, and that $A[\pi_{\mathfrak{p}}] = \mathcal{E}_{\mathfrak{p}} = \mathcal{O}_{F(\pi_{\mathfrak{p}})}$ (see Lemma 5.2 and Theorem 5.3 of [Ge83]). Hence $|\Delta_{\mathfrak{p}}| = |p|$, a much larger growth than that shown in Theorem 1. One can also prove that, in the supersingular case, $d_{1,\mathfrak{p}} = 1$ and $d_{2,\mathfrak{p}} = p - \beta$ for some $\beta \in \mathbb{F}_q^{\times}$ (see [CoPa15, Cor. 3]). Hence $|d_{2,\mathfrak{p}}| = |p|$, which is as large as possible.

Remark 5. From the theory of Drinfeld modules over finite fields, one can deduce that the discriminant of $A[\pi_{\mathfrak{p}}]$ has degree $\leq \deg p$. More precisely, the characteristic polynomial of $\pi_{\mathfrak{p}}$ is of the form $X^2 + a_{\mathfrak{p}} X + \mu_{\mathfrak{p}} p \in A[X]$, where $\mu_{\mathfrak{p}} \in \mathbb{F}_q^{\times}$ and $\deg a_{\mathfrak{p}} \leq \frac{\deg p}{2}$. This implies that $|\Delta_{\mathfrak{p}}| \leq \left|a_{\mathfrak{p}}^2 - 4\mu_{\mathfrak{p}} p\right| \leq |p|$. Note that the coefficients $a_{\mathfrak{p}}$ and $\mu_{\mathfrak{p}}$ also depend on ψ, although this will not be explicitly indicated in our notation.

The lower bound on $|\Delta_{\mathfrak{p}}|$ in Theorem 1 holds for *all* primes $\mathfrak{p} = pA \lhd A$, with finitely many exceptions. The next theorem gives a stronger lower bound, almost as close as the upper bound of Remark 5, which holds for *a set* of primes $\mathfrak{p} = pA \lhd A$ *of Dirichlet density 1*:

Theorem 6. *Assume* $\mathrm{End}_{F^{\mathrm{alg}}}(\psi) = A$. *For any positive valued function* $f : \mathbb{N} \to (0, \infty)$ *with* $\lim_{x \to \infty} f(x) = \infty$, *we have that, as* $x \to \infty$,

$$\# \left\{ \mathfrak{p} \in \mathcal{P}(\psi) : \deg p = x, |\Delta_{\mathfrak{p}}| > \frac{\left|a_{\mathfrak{p}}^2 - 4\mu_{\mathfrak{p}} p\right|}{q^{f(\deg p)}} \right\} \sim \pi_F(x),$$

where $\pi_F(x) := \#\{\mathfrak{p} \lhd A \ : \deg p = x\}$. *Moreover, the Dirichlet density of the set*

$$\left\{ \mathfrak{p} \in \mathcal{P}(\psi) : |\Delta_{\mathfrak{p}}| > \frac{\left|a_{\mathfrak{p}}^2 - 4\mu_{\mathfrak{p}} p\right|}{q^{f(\deg p)}} \right\}$$

exists and equals 1.

Theorem 6 is a Drinfeld module unconditional analogue of a recent result of the first author and Fitzpatrick for elliptic curves over $\mathbb{Q}$; see [CoFi21]. It is inspired by the results of [CoSh15] and relies on some of the main results of [CoPa15].

In Sections 2, 3, and 4 we review and prove several results about orders, quadratic forms, and j-invariants of Drinfeld modules needed in the proofs of the main theorems. In Sections 5 and 6 we present the proofs of Theorems 1, 2, and 6.

Notation. Throughout the paper, we use the standard $\sim$, o, O, $\ll$, $\gg$ notation, which we now recall: given suitably defined real functions h_1, h_2, we say that $h_1 \sim h_2$ if $\lim_{x \to \infty} h_1(x)/h_2(x) = 1$; we say that $h_1 = \mathrm{o}(h_2)$ if $\lim_{x \to \infty} h_1(x)/h_2(x) = 0$; we say that

$h_1 = \mathrm{O}(h_2)$ or $h_1 \ll h_2$ or $h_2 \gg h_1$ if h_2 is positive valued and there exists a positive constant C such that $|h_1(x)| \leq Ch_2(x)$ for all x in the domain of h_1; we say that $h_1 = \mathrm{O}_D(h_2)$ or $h_1 \ll_D h_2$ or $h_2 \gg_D h_1$ if $h_1 \ll h_2$ and the implied O-constant C depends on priorly given data D. We make the convention that any implied O-constant may depend on q without any explicit specification.

2. A-orders

Let K/F be a quadratic imaginary extension. Let B be the integral closure of A in K. An *A-order* in K is an A-subalgebra $\mathcal{O}$ of B with the same unity element and such that $B/\mathcal{O}$ has finite cardinality. Note that an A-order $\mathcal{O}$ is a free A-module of rank 2 and that there is an A-module isomorphism $B/\mathcal{O} \cong A/cA$ for a unique nonzero monic polynomial $c \in A$, called the *conductor* of $\mathcal{O}$ in B. It is easy to show that $\mathcal{O} = A + cB$.

Let $\{\alpha_1, \alpha_2\}$ be a basis of $\mathcal{O}$ as a free A-module, and $\sigma \in \mathrm{Gal}(K/F) \cong \mathbb{Z}/2\mathbb{Z}$ be the generator of $\mathrm{Gal}(K/F)$. The discriminant of $\{\alpha_1, \alpha_2\}$ is

$$\mathrm{disc}(\alpha_1, \alpha_2) = \det \begin{pmatrix} \alpha_1 & \sigma(\alpha_1) \\ \alpha_2 & \sigma(\alpha_2) \end{pmatrix}^2.$$

If $\{\beta_1, \beta_2\}$ is another A-basis of $\mathcal{O}$, then $\mathrm{disc}(\beta_1, \beta_2) = \kappa^2 \cdot \mathrm{disc}(\alpha_1, \alpha_2)$ for some $\kappa \in \mathbb{F}_q^\times$. The *discriminant* $\Delta_{\mathcal{O}}$ of $\mathcal{O}$ is defined to be $\mathrm{disc}(\alpha_1, \alpha_2)$, up to an $(\mathbb{F}_q^\times)^2$-multiple. It is elementary to show that $\mathcal{O} = A[\sqrt{\Delta_{\mathcal{O}}}]$ and $(\Delta_{\mathcal{O}}) = c^2 \cdot (\Delta_B)$, where (a) denotes the ideal generated by an element $a \in A$. Note that Δ_B is square-free.

Remark 7. The splitting behavior of $\infty = 1/T$ in any quadratic extension K/F can be described using the discriminant Δ_B. Namely, ∞ ramifies in $K/F \iff \deg \Delta_B$ is odd; ∞ splits in $K/F \iff \deg \Delta_B$ is even and the leading coefficient of Δ_B is a square in $\mathbb{F}_q^\times$; ∞ is inert in $K/F \iff \deg \Delta_B$ is even and the leading coefficient of Δ_B is not a square in $\mathbb{F}_q^\times$.

There are two important groups associated to an A-order $\mathcal{O}$: the *unit group* $\mathcal{O}^\times$ of invertible elements of $\mathcal{O}$ and the *ideal class group* $\mathrm{Cl}(\mathcal{O})$ of classes of proper (invertible) fractional ideals of $\mathcal{O}$; see [Cox89, p. 136]. The ideal class group is finite and its cardinality $h(\mathcal{O})$ is called the *class number* of $\mathcal{O}$. The class numbers of $\mathcal{O}$ and B are related by the following well-known formula (see [Cox89, Thm. 7.24, p. 146] or [Yu95a, pp. 323–324]):

$$h(\mathcal{O}) = h(B) \frac{|c|}{[B^\times : \mathcal{O}^\times]} \prod_{\substack{\ell \mid c \\ \ell \text{ monic irreducible}}} \left(1 - \left(\frac{K}{\ell}\right) \frac{1}{|\ell|}\right), \tag{1}$$

where

$$\left(\frac{K}{\ell}\right) := \begin{cases} 1 & \text{if } (\ell) \text{ splits in } K, \\ -1 & \text{if } (\ell) \text{ is inert in } K, \\ 0 & \text{if } (\ell) \text{ ramifies in } K. \end{cases}$$

Hence

$$h(\mathcal{O}) \leq h(B) \cdot |c| \prod_{\substack{\ell | c \\ \ell \text{ monic irreducible}}} \left(1 + \frac{1}{|\ell|}\right). \tag{2}$$

The product on the right-hand side of (2) may be bounded from above as follows:

Lemma 8.

$$\prod_{\substack{\ell | c \\ \ell \text{ monic irreducible}}} \left(1 + \frac{1}{|\ell|}\right) \ll \log\log|c|. \tag{3}$$

Proof. To simplify the notation, we assume that ℓ is always monic and irreducible in this proof. Note that

$$\prod_{\ell | c} \left(1 + \frac{1}{|\ell|}\right) < \prod_{\ell | c} \frac{|\ell|}{|\ell| - 1} = \frac{|c|}{\varphi_A(c)},$$

where $\varphi_A(c) = |c| \prod_{\ell | c}(1 - 1/|\ell|)$ is the analogue of the classical Euler function. On the other hand, the well-known bound

$$|c|/\varphi_A(c) \ll \log\log|c|$$

for the classical Euler function is valid also for its function field analogue (see [Br10, Lem. 2.2]). By combining these two observations, the lemma follows. □

The class number $h(B)$ of the maximal order may be estimated from above as follows:

Lemma 9.

$$h(B) \leq \begin{cases} \frac{\sqrt{|\Delta_B|}\deg \Delta_B}{\sqrt{q}}, & \textit{if } \deg \Delta_B \textit{ is odd,} \\ \\ \frac{2\sqrt{|\Delta_B|}\deg \Delta_B}{q+1}, & \textit{otherwise.} \end{cases}$$

Proof. The quadratic symbol $\left(\frac{K}{\ell}\right)$ gives rise to a quadratic character $\chi_{\Delta_B}(\cdot)$ and to an associated L-function $L(s, \chi_{\Delta_B})$; see [Ro02, p. 316].

On one hand, by the function field analogue of the classical class number formula (see [Ro02, Thm. 17.8A]),

$$L(1,\chi_{\Delta_B}) = \begin{cases} \frac{\sqrt{q}}{\sqrt{|\Delta_B|}} h(B), & \text{if } \deg \Delta_B \text{ is odd,} \\ \frac{q+1}{2\sqrt{|\Delta_B|}} h(B), & \text{otherwise.} \end{cases}$$

Note that, above, we made use of our assumption that K/F is imaginary.

On the other hand, by [Ro02, Lem. 17.10],

$$L(1,\chi_{\Delta_B}) = \sum_{\substack{0 \neq m \in A \\ m \text{ monic} \\ \deg m < \deg \Delta_B}} \frac{\chi_{\Delta_B}(m)}{|m|}.$$

Hence

$$|L(1,\chi_{\Delta_B})| \leq \sum_{\substack{0 \neq m \in A \\ m \text{ monic} \\ \deg m < \deg \Delta_B}} \frac{1}{|m|} = \sum_{0 \leq d \leq \deg(\Delta_B)-1} q^{-d} \sum_{\substack{0 \neq m \in A \\ m \text{ monic} \\ \deg m = d}} 1 = \deg \Delta_B,$$

where $|L(1,\chi_{\Delta_B})|$ denotes the usual absolute value on $\mathbb{C}$.

By combining this bound with the class number formula, we obtain the stated bound for $h(B)$. □

Putting together (2), Lemma 8, and Lemma 9, we obtain an upper bound for the class number $h(\mathcal{O})$ of the arbitrary order $\mathcal{O}$:

$$h(\mathcal{O}) \ll \sqrt{|\Delta_{\mathcal{O}}|} \cdot (\deg \Delta_{\mathcal{O}})^2. \tag{4}$$

3. Quadratic forms

Let $f(x,y) = ax^2 + bxy + cy^2 \in A[x,y]$ be a quadratic form. The *discriminant* of $f(x,y)$ is $b^2 - 4ac$. The quadratic form $f(x,y)$ is *primitive* if $\gcd(a,b,c) = 1$.

The group $\mathrm{GL}_2(A)$ acts on the set of primitive quadratic forms as follows: if $\begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix}$ is the matrix of f, that is, $f(x,y) = \begin{pmatrix} x & y \end{pmatrix} \begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}$, and if $\mathcal{M} \in \mathrm{GL}_2(A)$, then $\mathcal{M}^t \begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix} \mathcal{M}$ is the matrix of $\mathcal{M}f$.

Two primitive quadratic forms f and g are *properly equivalent* if $g = \mathcal{M}f$ for some $\mathcal{M} \in \mathrm{SL}_2(A)$.

In the proof of Theorem 1 we will need the following analogue of a well-known classical result:

Theorem 10. *Let $\mathcal{O}$ be an imaginary quadratic A-order, of discriminant $\Delta_{\mathcal{O}}$. If $ax^2 + bxy + cy^2 \in A[x,y]$ is a primitive quadratic form of discriminant $\Delta_{\mathcal{O}}$, then $A + \frac{-b+\sqrt{\Delta_{\mathcal{O}}}}{2a} A$ is a proper fractional ideal of $\mathcal{O}$. The map*

$$ax^2 + bxy + cy^2 \longmapsto A + \frac{-b + \sqrt{\Delta_{\mathcal{O}}}}{2a} A$$

induces a bijection between the proper equivalence classes of primitive quadratic forms of discriminant $\Delta_{\mathcal{O}}$ *and* $\mathrm{Cl}(\mathcal{O})$.

Proof. The proof of Theorem 7.7 in [Cox89, pp. 137–140] works also in this context; see [Be09] for the details. □

Lemma 11. *Every primitive quadratic form over* A *is properly equivalent to a quadratic form* $ax^2 + bxy + cy^2$ *such that*

$$\deg b < \deg a \leq \deg c. \tag{5}$$

Proof. Among all forms properly equivalent to the given one, pick $f(x, y) = ax^2 + bxy + cy^2$ so that $\deg b$ is as small as possible (note that b can be zero, in which case, by our convention, $\deg 0 = -\infty$).

If $\deg a \leq \deg b$, then f is properly equivalent to

$$g(x, y) = f(x + my, y) = ax^2 + (2am + b)xy + c'y^2$$

for some $m \in A$. Using the division algorithm in A, we can choose m so that $\deg(2am + b) < \deg a$, which contradicts our choice of $f(x, y)$. Thus $\deg b < \deg a$. The inequality $\deg b < \deg c$ follows similarly.

If $\deg a > \deg c$, then we interchange the outer coefficients via the proper equivalence $(x, y) \mapsto (-y, x)$. The resulting form satisfies $\deg b < \deg a \leq \deg c$. □

Let F_∞ be the completion of F with respect to the absolute value $|\cdot|$, and $\mathbb{C}_\infty$ be the completion of the algebraic closure F_∞^{alg}. We use the same notation for the unique extension of $|\cdot|$ to $\mathbb{C}_\infty$. The *imaginary part* of $z \in \mathbb{C}_\infty$ is

$$|z|_i := \min_{x \in F_\infty} |z - x|.$$

Obviously, $|z|_i \leq |z|$.

Lemma 12. *Let* $f(x, y) = ax^2 + bxy + cy^2$ *be a primitive quadratic form over* A *with discriminant* Δ. *Assume* $F(\sqrt{\Delta})$ *is imaginary and* $f(x, y)$ *satisfies* (5). *Then*

$$1 \leq \left| \frac{-b + \sqrt{\Delta}}{2a} \right|_i = \left| \frac{-b + \sqrt{\Delta}}{2a} \right| \leq |\sqrt{\Delta}|. \tag{6}$$

Proof. Since $\Delta = b^2 - 4ac$ and $\deg b < \deg a \leq \deg c$, we obtain that

$$\deg \Delta = \deg(b^2 - 4ac) = \deg(ac) \geq 2 \deg a.$$

Hence

$$|\sqrt{\Delta}| \geq |a| > |b|.$$

Then, using the strong triangle inequality, we obtain that

$$\left|\frac{-b+\sqrt{\Delta}}{2a}\right| = \frac{|-b+\sqrt{\Delta}|}{|a|} = \frac{|\sqrt{\Delta}|}{|a|}. \tag{7}$$

Since $|a| \geq 1$, we deduce that

$$1 \leq \frac{|\sqrt{\Delta}|}{|a|} \leq |\sqrt{\Delta}|.$$

Thus the two outer inequalities of (6) hold, that is,

$$1 \leq \left|\frac{-b+\sqrt{\Delta}}{2a}\right| \leq |\sqrt{\Delta}|.$$

To prove the middle equality of (6), we proceed in two different ways, according to the parity of $\deg \Delta$.

First, suppose that $\deg \Delta$ is odd. Observe that (7) gives

$$\log_q \left|\frac{-b+\sqrt{\Delta}}{2a}\right| = \log_q \frac{|\sqrt{\Delta}|}{|a|} = \frac{\deg \Delta}{2} - \deg a.$$

Given our assumption on $\deg \Delta$, the above implies that $\log_q \left|\frac{-b+\sqrt{\Delta}}{2a}\right| \notin \mathbb{Z}$. In this case, the desired middle equality of (6) follows from the more general fact that, if $z \in \mathbb{C}_\infty$ is such that $\log_q |z| \notin \mathbb{Z}$, then $|z|_i = |z|$, which we now explain. On one hand, if $\log_q |z| \notin \mathbb{Z}$, then for any $x \in F_\infty$ we have $|z| \neq |x|$. As such, the strong triangle inequality implies $|z-x| = \max\{|z|, |x|\} \geq |z|$, showing that $|z|_i \geq |z|$. On the other hand, $|z|_i \leq |z|$. Thus we must have $|z|_i = |z|$.

Next, suppose that $u := \deg \Delta$ is even. Since $F(\sqrt{\Delta})$ is assumed to be imaginary, the leading coefficient of Δ is not a square in $\mathbb{F}_q^\times$ (see Remark 7) and $F_\infty(\sqrt{\Delta}) = \mathbb{F}_{q^2}F_\infty$. Choosing $1/T$ as the uniformizer of $\mathbb{F}_{q^2}F_\infty$, we can expand $\sqrt{\Delta}$ as

$$\sqrt{\Delta} = \alpha \left(\frac{1}{T}\right)^{-u/2} + \text{higher degree terms in } \frac{1}{T},$$

where $\alpha \in \mathbb{F}_{q^2} \backslash \mathbb{F}_q$. Since $u/2 \geq \deg a > \deg b$, the $1/T$-expansion of $(-b+\sqrt{\Delta})/2a$ is

$$\frac{-b+\sqrt{\Delta}}{2a} = \beta \left(\frac{1}{T}\right)^{-v} + \text{higher degree terms in } \frac{1}{T},$$

where $v := \frac{u}{2} - \deg a \geq 0$ and $\beta \in \mathbb{F}_{q^2} \backslash \mathbb{F}_q$.

If $\left|\frac{-b+\sqrt{\Delta}}{2a} - x\right| < \left|\frac{-b+\sqrt{\Delta}}{2a}\right|$ for some $x \in F_\infty$, then the $1/T$-expansion of x must have the form

$$\beta \left(\frac{1}{T}\right)^{-v} + \text{higher degree terms in } \frac{1}{T}.$$

But this is not possible, since $\beta \notin \mathbb{F}_q$. Therefore, $\left|\frac{-b+\sqrt{\Delta}}{2a} - x\right| \geq \left|\frac{-b+\sqrt{\Delta}}{2a}\right|$ for all $x \in F_\infty$, which implies that $\left|\frac{-b+\sqrt{\Delta}}{2a}\right|_i = \left|\frac{-b+\sqrt{\Delta}}{2a}\right|$. □

4. The j-invariant of a rank 2 Drinfeld module

Let $\gamma : A \longrightarrow L$ be an A-field and let $\psi : A \longrightarrow L\{\tau\}$ be a Drinfeld A-module over L of rank 2, defined by $\psi_T = \gamma(T) + g_1\tau + g_2\tau^2$ for some $g_1, g_2 \in L$ with $g_2 \neq 0$. The quantity

$$j(\psi) := \frac{g_1^{q+1}}{g_2} \in L \tag{8}$$

is called the *j-invariant of ψ*.

In general, two Drinfeld A-modules ψ and ϕ are said to be isomorphic over an extension L' of L if $\psi_T = c^{-1}\phi_T c$ for some $c \in L'$. It is easy to show that two Drinfeld A-modules ϕ and ψ of rank 2 are isomorphic over L^{alg} if and only if $j(\phi) = j(\psi)$.

Now assume that $L = \mathbb{C}_\infty$ and let $\Omega := \mathbb{C}_\infty - F_\infty$ be the Drinfeld half-plane. The group $\mathrm{GL}_2(A)$ acts on Ω by linear fractional transformations,

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} z := \frac{az+b}{cz+d},$$

and the set

$$\mathcal{F} := \{z \in \Omega \ : \ |z| = |z|_i \geq 1\} \tag{9}$$

is a "fundamental domain" for the action of $\mathrm{GL}_2(A)$ on Ω; see [Ge99, Prop. 6.5]. In particular, every element of Ω is $\mathrm{GL}_2(A)$-equivalent to some element of $\mathcal{F}$.

To each $z \in \Omega$, we associate the lattice $A + Az \subset \mathbb{C}_\infty$. By the analytic theory of Drinfeld modules, the lattice $A + Az$ corresponds to a Drinfeld A-module ψ^z of rank 2 defined over $\mathbb{C}_\infty$. Moreover, it can be shown that $\psi^z \cong \psi^{z'}$ (over $\mathbb{C}_\infty$) if and only if $z = \gamma z'$ for some $\gamma \in \mathrm{GL}_2(A)$, and the map $z \longmapsto \psi^z$ induces a bijection between the orbits $\mathrm{GL}_2(A) \setminus \Omega$ and the isomorphism classes of rank 2 Drinfeld A-modules over $\mathbb{C}_\infty$; see [Dr74, Sec. 6].

Thanks to the above properties, there exists a $\mathrm{GL}_2(A)$-invariant function

$$j : \Omega \longrightarrow \mathbb{C}_\infty, \quad j(z) := j\left(\psi^z\right). \tag{10}$$

Theorem 13. *For $z \in \mathcal{F}$, we have* $\log_q |j(z)| < q^2|z|$.

Proof. See Theorem 6.6 in [Ge99]. □

A Drinfeld A-module ψ of rank 2 over $\mathbb{C}_\infty$ is said to have *complex multiplication* if $\mathrm{End}_{\mathbb{C}_\infty}(\psi) \neq A$.

Theorem 14. *Suppose that the Drinfeld A-module $\psi := \psi^z$ defined by $z \in \Omega$ has complex multiplication. Then the following properties hold.*

(i) $K := F(z)$ *is an imaginary quadratic extension of* F.
(ii) $\mathcal{O} := \mathrm{End}_{\mathbb{C}_\infty}(\psi)$ *is an A-order in* K.
(iii) $K(j(\psi))/K$ *is a finite abelian extension.*
(iv) $j(\psi)$ *is integral over* A.
(v) $\mathrm{Gal}(K(j(\psi))/K) \cong \mathrm{Cl}(\mathcal{O})$.
(vi) $\{\sigma(j(\psi)) \mid \sigma \in \mathrm{Gal}(K(j(\psi))/K)\} = \left\{ j\left(\frac{-b+\sqrt{\Delta_\mathcal{O}}}{2a}\right) \;\middle|\; [ax^2+bxy+cy^2]_{\Delta_\mathcal{O}} / \mathrm{SL}_2(A) \right\}$, *where $[ax^2+bxy+cy^2]_{\Delta_\mathcal{O}} / \mathrm{SL}_2(A)$ denotes the proper equivalence class of the primitive quadratic form $ax^2+bxy+cy^2$ of discriminant $\Delta_\mathcal{O}$.*

Proof. For (i)-(v), see Section 4 in [Ge83]. For (vi), proceed as follows. On one hand, by [Ge83, Cor. 4.5], the set of Galois conjugates of $j(\psi)$ is equal to the set $\{j(z')\}$, where $A + Az'$ runs over the equivalence classes of proper fractional ideals of $\mathcal{O}$. On the other hand, Theorem 10 gives explicit expressions for representatives of these ideal classes in terms of the equivalence classes of quadratic forms. This completes the proof. □

5. Proof of Theorems 1 and 2

Let ψ be a Drinfeld A-module of rank 2 over F and let $\mathfrak{p} \lhd A$ be a fixed prime where ψ has good reduction. Let $\psi \otimes \mathbb{F}_\mathfrak{p}$ be the reduction of ψ at $\mathfrak{p}$. As we mentioned in the introduction, $\mathcal{E}_{\psi,\mathfrak{p}} := \mathrm{End}_{\mathbb{F}_\mathfrak{p}}(\psi \otimes \mathbb{F}_\mathfrak{p})$ is an A-order in the imaginary quadratic extension $F(\pi_\mathfrak{p})$ of F. Since $\mathfrak{p}$ remains fixed in this section, for simplicity of notation, in the proofs below we will write

$$\mathcal{E} := \mathcal{E}_{\psi,\mathfrak{p}}, \ \Delta := \Delta_\mathfrak{p}, \ \text{and} \ K := F(\pi_\mathfrak{p}).$$

5.1. Proof of Theorem 1

Proposition 15. *There exists a Drinfeld A-module Ψ of rank 2 over $\mathbb{C}_\infty$ for which the following properties hold.*

(i) $\mathrm{End}_{\mathbb{C}_\infty}(\Psi) = \mathcal{E}$.
(ii) *There exists a prime $\mathfrak{P}$ of $K(j(\Psi))$ lying over $\mathfrak{p}$ such that* $j(\Psi) \equiv j(\psi) \bmod \mathfrak{P}$.

Proof. Note that in (ii) we implicitly use Theorem 14: assuming (i), by Theorem 14, $j(\Psi)$ is algebraic over A, so $K(j(\psi))$ is a finite algebraic extension of F and $j(\Psi) \bmod \mathfrak{P}$ makes sense.

Since the rank of $\psi \otimes \mathbb{F}_\mathfrak{p}$ is 2, by [CoPa15, Prop. 24], the field K is "good" for $\psi \otimes \mathbb{F}_\mathfrak{p}$ in the sense therein. Then by Theorem 22 and its proof in [CoPa15], there exists a discrete valuation ring R with maximal ideal $\mathcal{M}$, equipped with an injective homomorphism $\gamma : A \to R$, and having the properties:

(a) $\mathcal{M} \cap A = \mathfrak{p}$ and $R/\mathcal{M} \cong A/\mathfrak{p}$;
(b) there exists a Drinfeld A-module $\Psi : A \to R\{\tau\}$ of rank 2 such that $\mathcal{E} \subseteq \mathrm{End}_R(\Psi)$;
(c) $\Psi \otimes \mathbb{F}_\mathfrak{p} := \Psi \bmod \mathcal{M}$ is isomorphic to $\psi \otimes \mathbb{F}_\mathfrak{p}$ over $\mathbb{F}_\mathfrak{p}$.

It is not hard to deduce from [Ge83, Lem. 3.3] that, under reduction modulo $\mathcal{M}$, we get an injection $\mathrm{End}_L(\Psi) \hookrightarrow \mathrm{End}_{\mathbb{F}_\mathfrak{p}}(\Psi \otimes \mathbb{F}_\mathfrak{p})$, where L is the fraction field of R. Hence $\mathcal{E} \subseteq \mathrm{End}_L(\Psi) \subseteq \mathrm{End}_{\mathbb{F}_\mathfrak{p}}(\Psi \otimes \mathbb{F}_\mathfrak{p}) = \mathcal{E}$, which implies that $\mathrm{End}_L(\Psi) = \mathcal{E}$. By considering the action of $\mathcal{E}$ on the tangent space of Ψ, one deduces that K is a subfield of L. Thus $K(j(\Psi))$ is a subfield of L.

Let $\mathfrak{P} := \mathcal{M} \cap K(j(\Psi))$. Since $A/\mathfrak{p} \subseteq \mathcal{O}_{K(j(\Psi))}/\mathfrak{P} \subseteq R/\mathcal{M}$, $\mathfrak{P}$ is a maximal ideal of the integral closure $\mathcal{O}_{K(j(\Psi))}$ of A in $K(j(\Psi))$, with residue field $\mathbb{F}_\mathfrak{p}$. From the construction, it is clear that $\Psi \bmod \mathfrak{P}$ is isomorphic to $\psi \otimes \mathbb{F}_\mathfrak{p}$ over $\mathbb{F}_\mathfrak{p}$. In particular, $j(\Psi) \equiv j(\psi) \bmod \mathfrak{P}$.

Finally, we embed L into $\mathbb{C}_\infty$ and consider Ψ as a Drinfeld A-module over $\mathbb{C}_\infty$. Since $\mathrm{End}_{\mathbb{C}_\infty}(\Psi)/\mathrm{End}_L(\Psi)$ is a free A-module and $\mathrm{rank}_A \mathrm{End}_{\mathbb{C}_\infty}(\Psi) \leq 2$, we conclude that $\mathrm{End}_{\mathbb{C}_\infty}(\Psi) = \mathcal{E}$. □

Now assume that $\mathrm{End}_{F^{\mathrm{alg}}}(\psi) = A$. Let Ψ be a Drinfeld A-module over $\mathbb{C}_\infty$ as in Proposition 15. We have $j(\psi) \neq j(\Psi)$ (as elements of $\mathbb{C}_\infty$), since, otherwise, $\psi \cong \Psi$ over $\mathbb{C}_\infty$, which implies $\mathrm{End}_{F^{\mathrm{alg}}}(\psi) = \mathrm{End}_{\mathbb{C}_\infty}(\psi) = \mathcal{E}$, a contradiction. Write $j(\psi) = n/m$ with relatively prime $n, m \in A$.

Let $\mathfrak{P}$ be the prime of $K(j(\Psi))$ from Proposition 15. Then $j(\Psi) \equiv \frac{n}{m} \bmod \mathfrak{P}$ and $j(\Psi) \neq \frac{n}{m}$ imply $0 \neq n - m \cdot j(\Psi) \in \mathfrak{P}$.

By Theorem 14, $K(j(\Psi))/K$ is an abelian extension and

$$\begin{aligned} \mathrm{Nr}_{K(j(\Psi))/K}(n - m \cdot j(\Psi)) &= \prod_{\sigma \in \mathrm{Gal}(K(j(\Psi))/K)} (n - m \cdot \sigma(j(\Psi))) \\ &= \prod_{[ax^2+bxy+cy^2]_\Delta / \mathrm{SL}_2(A)} \left(n - m \cdot j\left(\frac{-b + \sqrt{\Delta}}{2a} \right) \right). \end{aligned}$$

On one hand, since $n - m \cdot j(\Psi) \in \mathfrak{P}$, we have $\alpha := \mathrm{Nr}_{K(j(\Psi))/K}(n - m \cdot j(\Psi)) \in \mathfrak{p}'$, where $\mathfrak{p}'$ is the prime of K lying under $\mathfrak{P}$. Letting α' be the conjugate of α over F, we obtain that $\alpha\alpha' \in \mathfrak{p}$, which gives $|\alpha| \geq |p|^{1/2}$.

On the other hand, by the strong triangle inequality,

$$|\alpha| = \prod_{[ax^2+bxy+cy^2]_\Delta / \mathrm{SL}_2(A)} \max\left\{|n|, |m| \cdot \left| j\left(\frac{-b+\sqrt{\Delta}}{2a}\right)\right|\right\}.$$

Remark that, by Lemma 11, we can assume that the triples (a, b, c) above satisfy (5). Under this assumption, Lemma 12 implies that $\frac{-b+\sqrt{\Delta}}{2a} \in \mathcal{F}$, with $\mathcal{F}$ as defined in (9). Then Theorem 13 and Lemma 12 imply

$$\log_q \left| j\left(\frac{-b+\sqrt{\Delta}}{2a}\right)\right| \leq q^2 \left|\frac{-b+\sqrt{\Delta}}{2a}\right| \leq q^2 \left|\sqrt{\Delta}\right|.$$

Combining our estimates, we get

$$|p|^{\frac{1}{2}} \leq \prod_{[ax^2+bxy+cy^2]_\Delta / \mathrm{SL}_2(A)} \max\left\{|n|, |m| \cdot q^{q^2\left|\sqrt{\Delta}\right|}\right\} = \max\left\{|n|, |m| \cdot q^{q^2\left|\sqrt{\Delta}\right|}\right\}^{h(\mathcal{E})}.$$

Since n and m are determined by ψ, we deduce that

$$\deg p \ll_\psi h(\mathcal{E}) \cdot \left|\sqrt{\Delta}\right|.$$

Furthermore, since, by (4), $h(\mathcal{E}) \ll \sqrt{|\Delta|} \cdot (\deg \Delta)^2$, we deduce that

$$\deg p \ll_\psi |\Delta| \cdot (\deg \Delta)^2. \tag{11}$$

We claim that (11) implies

$$|\Delta| \gg_\psi \frac{\log |p|}{(\log\log |p|)^2}. \tag{12}$$

Indeed, if $|\Delta| \geq \log |p|$, then obviously $|\Delta| > \log |p|/(\log\log |p|)^2$. On the other hand, if $|\Delta| \leq \log |p|$, then $\log |\Delta| \leq \log\log |p|$, and so from (11) we get

$$|\Delta| \gg_\psi \frac{\log |p|}{(\deg \Delta)^2} = \frac{\log |p|}{(\log |\Delta|)^2} (\log q)^2 \gg_\psi \frac{\log |p|}{(\log\log |p|)^2}.$$

This completes the proof of Theorem 1.

5.2. Proof of Theorem 2

We start by recalling a few more general facts. Let $\gamma : A \to L$ be an A-field and let ϕ be a Drinfeld A-module of rank r over L. Then ϕ endows any field extension L' of L with an A-module structure, where $m \in A$ acts by ϕ_m. More precisely, if $\phi_m = \gamma(m) + \sum_{1 \le i \le r \deg m} g_i(m)\tau^i$, then put $\phi_m(x) = \gamma(m)x + \sum_{1 \le i \le r \deg m} g_i(m)x^{q^i} \in L[x]$ and, for $\lambda \in L'$, define $m \circ \lambda := \phi_m(\lambda)$. The *m-torsion* $\phi[m] \subset \overline{L}^{\mathrm{alg}}$ of ϕ is the set of zeros of the polynomial $\phi_m(x)$. It is clear that $\phi[m]$ has a natural structure of an A-module and it is not hard to show that, as A-modules, $\phi[m] \subseteq (A/mA)^{\oplus r}$, with an equality if and only if m is relatively prime to $\ker(\gamma)$; see [Go96, Ch. 4].

We return to the Drinfeld A-module ψ of rank 2 over F and, as in the introduction, we consider $\mathbb{F}_\mathfrak{p}$ as an A-module via the action of $\psi \otimes \mathbb{F}_\mathfrak{p}$ and denote it by ${}^{\psi}\mathbb{F}_\mathfrak{p}$; then

$$ {}^{\psi}\mathbb{F}_\mathfrak{p} \cong A/d_{1,\mathfrak{p}}A \times A/d_{2,\mathfrak{p}}A $$

for uniquely determined nonzero monic polynomials $d_{1,\mathfrak{p}}, d_{2,\mathfrak{p}} \in A$ such that $d_{1,\mathfrak{p}} \mid d_{2,\mathfrak{p}}$. (Note that there are at most two terms because ${}^{\psi}\mathbb{F}_\mathfrak{p}$ is a finite A-module, so for some $d \in A$ we have ${}^{\psi}\mathbb{F}_\mathfrak{p} \subseteq (\psi \otimes \mathbb{F}_\mathfrak{p})[d] \subseteq A/dA \times A/dA$.) Since $\mathfrak{p}$ remains fixed in this section, for simplicity of notation, in this proof we will write

$$ d_1 := d_{1,\mathfrak{p}}, \ d_2 := d_{2,\mathfrak{p}}. $$

Suppose $d_1 \neq 1$. Then $(\psi \otimes \mathbb{F}_\mathfrak{p})[d_1]$ is rational over $\mathbb{F}_\mathfrak{p}$, i.e., all the roots of $\psi_{d_1}(x)$ are in $\mathbb{F}_\mathfrak{p}$, and $p \nmid d_1$. Let $\pi_\mathfrak{p} = \tau^{\deg(p)} \in \mathcal{E}$ be the Frobenius endomorphism of $\psi \otimes \mathbb{F}_\mathfrak{p}$. The fact that $(\psi \otimes \mathbb{F}_\mathfrak{p})[d_1]$ is rational over $\mathbb{F}_\mathfrak{p}$ implies that $\pi_\mathfrak{p} = 1 + d_1\alpha$ for some $\alpha \in \mathcal{E}$; see the proof of Theorem 1.2 in [GaPa20]. From the theory of Drinfeld modules over finite fields (see [Yu95b, Thm. 1], [Ge91, Section 3]), we know that the minimal polynomial of $\pi_\mathfrak{p}$ over A has the form

$$ P_{\psi,\mathfrak{p}}(X) = X^2 + a_\mathfrak{p}X + \mu_\mathfrak{p}p, \tag{13} $$

where $\mu_\mathfrak{p} \in \mathbb{F}_q^\times$, and that

$$ \deg a_\mathfrak{p} \le \frac{\deg p}{2}. \tag{14} $$

Therefore $|\pi_\mathfrak{p}| = |\pi'_\mathfrak{p}| = |p|^{\frac{1}{2}}$, where $\pi'_\mathfrak{p}$ denotes the conjugate of $\pi_\mathfrak{p}$ over F. In particular,

$$ |p| = |\pi_\mathfrak{p}| \cdot |\pi'_\mathfrak{p}| = |1 + d_1\alpha| \cdot |1 + d_1\alpha'| = |d_1\alpha| \cdot |d_1\alpha'| = |d_1|^2 \cdot |\alpha\alpha'|, \tag{15} $$

where α' denotes the conjugate of α over F.

We write $\alpha = a_1 + a_2\sqrt{\Delta}$ for some $a_1, a_2 \in A$. Note that $a_2 \neq 0$ since $\pi \notin A$. Then

$$ |\alpha\alpha'| = |a_1^2 - a_2^2\Delta|. \tag{16} $$

The leading terms of a_1^2 and $a_2^2\Delta$, as polynomials in T, cannot cancel. Indeed, a_1^2 and a_2^2 have even degrees and their leading coefficients are squares in $\mathbb{F}_q^\times$, whereas Δ either has odd degree or has a leading coefficient which is not a square in $\mathbb{F}_q^\times$ (see Remark 7). This implies that

$$|a_1^2 - a_2^2\Delta| \geq |\Delta|. \tag{17}$$

Combining Theorem 1 with (15), (16), (17), we obtain

$$|p| \geq |d_1|^2 \cdot |\Delta| \gg_\psi |d_1|^2 \cdot \frac{\log|p|}{(\log\log|p|)^2},$$

or, equivalently,

$$|d_1| \ll_\psi \frac{\sqrt{|p|} \cdot \log\log|p|}{\sqrt{\log|p|}}.$$

Recalling that $|d_1 d_2| = |p|$, we deduce that

$$|d_2| \gg_\psi \frac{\sqrt{|p| \cdot \log|p|}}{\log\log|p|}.$$

This completes the proof of Theorem 2.

6. Proof of Theorem 6

Let ψ be a Drinfeld A-module of rank 2 over F and let $\mathfrak{p} \lhd A$ be a fixed prime where ψ has good reduction. As before, let $\psi \otimes \mathbb{F}_\mathfrak{p}$ be the reduction of ψ at $\mathfrak{p}$. As we mentioned earlier, the rings $A[\pi_\mathfrak{p}] \subseteq \mathcal{E}_{\psi,\mathfrak{p}} \subseteq \mathcal{O}_{F(\pi_\mathfrak{p})}$ are A-orders in the imaginary quadratic extension $K_\mathfrak{p} := F(\pi_\mathfrak{p})$ of F. Since $\mathfrak{p}$ varies in this section, we will now specify the dependence on $\mathfrak{p}$ of $\Delta_\mathfrak{p}$ and of all other relevant data.

Similarly to the A-module isomorphism $\mathcal{O}_{F(\pi_\mathfrak{p})}/\mathcal{E}_{\psi,\mathfrak{p}} \cong A/c_\mathfrak{p} A$ mentioned in the introduction, there is an A-module isomorphism $\mathcal{E}_{\psi,\mathfrak{p}}/A[\pi_\mathfrak{p}] \cong A/b_\mathfrak{p} A$, where $b_\mathfrak{p} = b_{\psi,\mathfrak{p}} \in A$ is a monic polynomial.

Comparing the discriminants of $\mathcal{E}_{\psi,\mathfrak{p}}$ and $A[\pi_\mathfrak{p}]$ and remarking that the discriminant of $A[\pi_\mathfrak{p}]$ is the discriminant of the polynomial $P_{\psi,\mathfrak{p}}$ of (13), we find a (not necessarily monic) generator $\delta_\mathfrak{p} = \delta_{\psi,\mathfrak{p}} \in A$ of the ideal $(\Delta_\mathfrak{p})$ that is uniquely determined by the relation

$$a_\mathfrak{p}^2 - 4\mu_\mathfrak{p} p = b_\mathfrak{p}^2 \delta_\mathfrak{p}. \tag{18}$$

Then, by taking norms, we obtain

$$\frac{|\Delta_\mathfrak{p}|}{|a_\mathfrak{p}^2 - 4\mu_\mathfrak{p} p|} = \frac{|\delta_\mathfrak{p}|}{|a_\mathfrak{p}^2 - 4\mu_\mathfrak{p} p|} = \frac{1}{|b_\mathfrak{p}|^2}. \tag{19}$$

Letting f be any positive valued function such that $\lim_{x\to\infty} f(x) = \infty$, we deduce from (19) that proving that

$$\#\left\{\mathfrak{p} \in \mathcal{P}(\psi) : \deg p = x,\ |\Delta_{\mathfrak{p}}| > \frac{|a_{\mathfrak{p}}^2 - 4\mu_{\mathfrak{p}} p|}{q^{f(\deg p)}}\right\} \sim \pi_F(x)$$

is equivalent to proving that

$$\#\left\{\mathfrak{p} \in \mathcal{P}(\psi) : \deg p = x,\ |b_{\mathfrak{p}}| \geq q^{\frac{f(\deg p)}{2}}\right\} = \mathrm{o}(\pi_F(x))). \tag{20}$$

To prove (20), our strategy will be to partition the primes $\mathfrak{p}$ according to the values m taken by $b_{\mathfrak{p}}$, to relax each equality $b_{\mathfrak{p}} = m$ to the divisibility $m \mid b_{\mathfrak{p}}$, and to reinterpret this divisibility as a condition that may be studied via density theorems, as we explain below.

First, let us remark that the condition $m \mid b_{\mathfrak{p}}$ for some $\mathfrak{p}$ with $\deg p = x$ implies that

$$\deg m \leq \frac{\deg\left(a_{\mathfrak{p}}^2 - 4\mu_{\mathfrak{p}} p\right)}{2} \leq \frac{x}{2}, \tag{21}$$

since $\deg a_{\mathfrak{p}} \leq \frac{\deg p}{2}$, as we recalled in (14). Thus

$$\begin{aligned}
&\#\left\{\mathfrak{p} \in \mathcal{P}(\psi) : \deg p = x, |b_{\mathfrak{p}}| \geq q^{\frac{f(\deg p)}{2}}\right\} \\
&= \#\left\{\mathfrak{p} \in \mathcal{P}(\psi) : \deg p = x, |b_{\mathfrak{p}}| \geq q^{\frac{f(x)}{2}}\right\} \\
&= \sum_{\substack{0\neq m\in A \\ m \text{ monic} \\ \frac{f(x)}{2}\leq \deg m\leq \frac{x}{2}}} \#\left\{\mathfrak{p} \in \mathcal{P}(\psi) : \deg p = x, b_{\mathfrak{p}} = m\right\} \\
&\leq \sum_{\substack{0\neq m\in A \\ m \text{ monic} \\ \frac{f(x)}{2}\leq \deg m\leq \frac{x}{2}}} \#\left\{\mathfrak{p} \in \mathcal{P}(\psi) : \deg p = x, m \mid b_{\mathfrak{p}}\right\}.
\end{aligned} \tag{22}$$

To analyze the inner counting function, let $m \in A$ be a monic polynomial and denote by $F(\psi[m])$ the field obtained by adjoining to F the elements of $\psi[m]$. We obtain a finite Galois extension of F, whose Galois group $\mathrm{Gal}(F(\psi[m])/F)$ may be viewed as a subgroup of $\mathrm{GL}_2(A/mA)$. We distinguish the subfield

$$J_m := \left\{z \in F(\psi[m]) : \sigma(z) = z\ \forall \sigma \in \mathrm{Gal}(F[\psi[m]/F) \text{ a scalar element}\right\},$$

which is a finite Galois extension of F and whose Galois group $\mathrm{Gal}(J_m/F)$ may be viewed as a subgroup of $\mathrm{PGL}_2(A/mA)$.

An important consequence of [CoPa15, Thm. 1] is that, for any $\mathfrak{p} \in \mathcal{P}(\psi)$ with $\mathfrak{p} \nmid m$,

$$m \mid b_{\mathfrak{p}} \iff \mathfrak{p} \text{ splits completely in } J_m/F. \tag{23}$$

Thus the divisibility $m \mid b_{\mathfrak{p}}$ may be studied via the Chebotarev Density Theorem. For this, we use the standard notation

$$\Pi_1(x, J_m/F) := \#\left\{\mathfrak{p} \in \mathcal{P}(\psi) : \deg p = x, \mathfrak{p} \text{ splits completely in } J_m/F\right\},$$

and we recall that it was shown in [CoPa15, Thm. 15] that an effective version of the Chebotarev Density Theorem of [MuSc94] applied to the extension J_m/F gives

$$\Pi_1(x, J_m/F) = \frac{c_m(x)}{[J_m : F]} \cdot \frac{q^x}{x} + \mathrm{O}_\psi\left(\frac{q^{\frac{x}{2}}}{x} \deg m\right), \tag{24}$$

where

$$c_m := \left[J_m \cap \overline{\mathbb{F}}_q : \mathbb{F}_q\right]$$

and

$$c_m(x) := \begin{cases} c_m & \text{if } c_m \mid x, \\ 0 & \text{otherwise.} \end{cases} \tag{25}$$

Upon fixing a parameter $f(x)/2 \le y = y(x) \le x/2$, which will be chosen optimally later, by using (24) in (22) we obtain that

$$\begin{aligned}
&\#\left\{\mathfrak{p} \in \mathcal{P}(\psi) : \deg p = x, |b_{\mathfrak{p}}| \ge q^{\frac{f(\deg p)}{2}}\right\} \\
&\quad \le \sum_{\substack{0 \ne m \in A \\ m \text{ monic} \\ \frac{f(x)}{2} \le \deg m \le \frac{x}{2}}} \#\left\{\mathfrak{p} \in \mathcal{P}(\psi) : \deg p = x, m \mid b_{\mathfrak{p}}\right\} \\
&\quad = \sum_{\substack{0 \ne m \in A \\ m \text{ monic} \\ \frac{f(x)}{2} \le \deg m \le y}} \Pi_1(x, J_m/F) \\
&\qquad + \sum_{\substack{0 \ne m \in A \\ m \text{ monic} \\ y < \deg m \le \frac{x}{2}}} \#\left\{\mathfrak{p} \in \mathcal{P}(\psi) : \deg p = x, m \mid b_{\mathfrak{p}}\right\} \\
&\quad = \frac{q^x}{x} \sum_{\substack{0 \ne m \in A \\ m \text{ monic} \\ \frac{f(x)}{2} \le \deg m \le y}} \frac{c_m(x)}{[J_m : F]} + \mathrm{O}_\psi\left(\sum_{\substack{0 \ne m \in A \\ m \text{ monic} \\ \frac{f(x)}{2} \le \deg m \le y}} \frac{q^{\frac{x}{2}}}{x} \deg m\right) \qquad (26) \\
&\qquad + \sum_{\substack{0 \ne m \in A \\ m \text{ monic} \\ y < \deg m \le \frac{x}{2}}} \#\left\{\mathfrak{p} \in \mathcal{P}(\psi) : \deg p = x, m \mid b_{\mathfrak{p}}\right\}. \qquad (27)
\end{aligned}$$

To estimate the first summation in (26), we recall that it was proven in [Ge19, Thm. 4.1] that the integers c_m are absolutely bounded, that is,

$$c_m \ll 1. \tag{28}$$

Thus

$$\sum_{\substack{0\neq m\in A\\ m \text{ monic}\\ \frac{f(x)}{2}\leq \deg m\leq y}} \frac{c_m(x)}{[J_m:F]} \ll \sum_{\substack{0\neq m\in A\\ m \text{ monic}\\ \frac{f(x)}{2}\leq \deg m\leq y}} \frac{1}{[J_m:F]} \leq \sum_{\substack{0\neq m\in A\\ m \text{ monic}\\ \frac{f(x)}{2}\leq \deg m}} \frac{1}{[J_m:F]}. \tag{29}$$

Furthermore, under the assumption $\mathrm{End}_{F^{\mathrm{alg}}}(\psi) = A$, it was proven in [CoJo21, Cor. 3] that

$$|m|^3 \ll_\psi [J_m : F] \leq |m|^3. \tag{30}$$

(Note that only the lower bound requires the assumption on the endomorphism ring.) Using the above lower bound in (29), we deduce that

$$\sum_{\substack{0\neq m\in A\\ m \text{ monic}\\ \frac{f(x)}{2}\leq \deg m\leq y}} \frac{c_m(x)}{[J_m:F]} \ll_\psi \sum_{\substack{0\neq m\in A\\ m \text{ monic}\\ \frac{f(x)}{2}\leq \deg m}} \frac{1}{|m|^3} \ll \frac{1}{q^{f(x)}}. \tag{31}$$

To estimate the second summation in (26), we observe that

$$\sum_{\substack{0\neq m\in A\\ m \text{ monic}\\ \frac{f(x)}{2}\leq \deg m\leq y}} \deg m \leq \sum_{\substack{0\neq m\in A\\ m \text{ monic}\\ \deg m\leq y}} \deg m \leq q^y. \tag{32}$$

By putting together (26), (27), (31), and (32), we deduce that

$$\#\left\{\mathfrak{p}\in\mathcal{P}(\psi) : \deg p = x, |b_{\mathfrak{p}}| \geq q^{\frac{f(\deg p)}{2}}\right\} \ll_\psi \frac{q^{x-f(x)}}{x} + q^{\frac{x}{2}+y} \tag{33}$$

$$+ \sum_{\substack{0\neq m\in A\\ m \text{ monic}\\ y<\deg m\leq \frac{x}{2}}} \#\left\{\mathfrak{p}\in\mathcal{P}(\psi) : \deg p = x, m \mid b_{\mathfrak{p}}\right\}. \tag{34}$$

Let us remark that, since we are seeking to prove that (33) is $\mathrm{o}\left(\frac{q^x}{x}\right)$, we will need to choose y such that $y \lneq x/2$. Thus the sum in (34) is non-empty.

An upper bound for the remaining sum in (34) can be obtained as an application of the Square Sieve, which, once again, makes use of (24), (28), and (30), though in a much more elaborate way than what we explained above. This application gives rise to the

non-trivial estimate [CoPa15, (40)], which we recall below: for any squarefree $g \in A$, we have

$$\begin{aligned} &\#\left\{\mathfrak{p} \in \mathcal{P}(\psi) : \deg p = x, g\left(a_{\mathfrak{p}}^2 - 4\mu_{\mathfrak{p}} p\right) \text{ is a square in } A\right\} \\ &\ll_{\psi} q^{\frac{7x}{8}}(x + \deg g) + q^{\frac{3x}{4}} x(x + \deg g)^2. \end{aligned} \tag{35}$$

Now let us show how (35) enables us to complete the proof of (20). Let $0 \neq m \in A$ be such that m is monic and $y < \deg m \leq x/2$, and let $\mathfrak{p} \in \mathcal{P}(\psi)$ be such that $\deg p = x$ and $m \mid b_{\mathfrak{p}}$. Observe that

$$m^2 \mid (a_{\mathfrak{p}}^2 - 4\mu_{\mathfrak{p}} p) \tag{36}$$

and that there exist a unit $u_{\mathfrak{p}} \in \mathbb{F}_q^{\times}$ and monic polynomials $h_{\mathfrak{p}}, g_{\mathfrak{p}} \in A$, with $g_{\mathfrak{p}}$ squarefree, uniquely determined by $\mathfrak{p}$ (and ψ) such that

$$a_{\mathfrak{p}}^2 - 4\mu_{\mathfrak{p}} p = u_{\mathfrak{p}} h_{\mathfrak{p}}^2 g_{\mathfrak{p}}. \tag{37}$$

Furthermore, observe that $m \mid h_{\mathfrak{p}}$,

$$y \leq \deg m \leq \deg h_{\mathfrak{p}} \leq \frac{x}{2}, \tag{38}$$

and

$$\deg g_{\mathfrak{p}} \leq x - 2\deg h_{\mathfrak{p}}. \tag{39}$$

Using these observations, we obtain that

$$\begin{aligned} &\sum_{\substack{0 \neq m \in A \\ m \text{ monic} \\ y < \deg m \leq \frac{x}{2}}} \#\left\{\mathfrak{p} \in \mathcal{P}(\psi) : \deg p = x, m \mid b_{\mathfrak{p}}\right\} \\ \leq &\sum_{\substack{0 \neq m \in A \\ m \text{ monic} \\ y < \deg m \leq \frac{x}{2}}} \#\left\{\mathfrak{p} \in \mathcal{P}(\psi) : \deg p = x, m^2 \mid (a_{\mathfrak{p}}^2 - 4\mu_{\mathfrak{p}} p)\right\} \\ \leq &\sum_{\substack{0 \neq m \in A \\ m \text{ monic} \\ y < \deg m \leq \frac{x}{2}}} \#\left\{\mathfrak{p} \in \mathcal{P}(\psi) : \deg p = x, m \mid h_{\mathfrak{p}}\right\}. \end{aligned}$$

Partitioning the primes $\mathfrak{p}$ according to $h_{\mathfrak{p}}$, we deduce that

$$\sum_{\substack{0 \neq m \in A \\ m \text{ monic} \\ y < \deg m \leq \frac{x}{2}}} \#\left\{\mathfrak{p} \in \mathcal{P}(\psi) : \deg p = x, m \mid h_{\mathfrak{p}}\right\}.$$

$$= \sum_{\substack{0\neq m\in A\\ m \text{ monic}\\ y<\deg m\le \frac{x}{2}}} \sum_{\substack{h\in A\\ h \text{ monic}\\ m\mid h\\ y\le \deg h\le \frac{x}{2}}} \#\{\mathfrak{p}\in\mathcal{P}(\psi): \deg p = x, h_{\mathfrak{p}} = h\}$$

$$\le \sum_{\substack{h\in A\\ h \text{ monic}\\ y\le \deg h\le \frac{x}{2}}} \tau_A(h) \#\{\mathfrak{p}\in\mathcal{P}(\psi): \deg p = x, h_{\mathfrak{p}} = h\}$$

$$= \sum_{\substack{h\in A\\ h \text{ monic}\\ y\le \deg h\le \frac{x}{2}}} \tau_A(h) \#\left\{\mathfrak{p}\in\mathcal{P}(\psi): \deg p = x, a_{\mathfrak{p}}^2 - 4\mu_{\mathfrak{p}} p = u_{\mathfrak{p}} h^2 g_{\mathfrak{p}}\right\},$$

where $\tau_A(h)$ denotes the number of monic divisors of h in A. Partitioning the primes $\mathfrak{p}$ according to $u_{\mathfrak{p}}$ and $g_{\mathfrak{p}}$, we deduce that the above summation satisfies the bounds:

$$= \sum_{\substack{h\in A\\ h \text{ monic}\\ y\le \deg h\le \frac{x}{2}}} \tau_A(h) \sum_{\substack{g\in A\\ g \text{ monic, squarefree}\\ \deg g\le x-2\deg h}} \#\left\{\mathfrak{p}\in\mathcal{P}(\psi): \deg p = x, a_{\mathfrak{p}}^2 - 4\mu_{\mathfrak{p}} p = u_{\mathfrak{p}} h^2 g\right\}$$

$$\le \sum_{u\in\mathbb{F}_q^\times} \sum_{\substack{h\in A\\ h \text{ monic}\\ y\le \deg h\le \frac{x}{2}}} \tau_A(h) \sum_{\substack{g\in A\\ g \text{ monic, squarefree}\\ \deg g\le x-2y}} \#\left\{\mathfrak{p}\in\mathcal{P}(\psi): \deg p = x, a_{\mathfrak{p}}^2 - 4\mu_{\mathfrak{p}} p = u h^2 g\right\}$$

$$\le \sum_{u\in\mathbb{F}_q^\times} \sum_{\substack{g\in A\\ g \text{ monic, squarefree}\\ \deg g\le x-2y}} \sum_{\substack{h\in A\\ h \text{ monic}\\ y\le \deg h\le \frac{x}{2}}} \tau_A(h) \#\big\{\mathfrak{p}\in\mathcal{P}(\psi): \deg p = x, g(a_{\mathfrak{p}}^2 - 4\mu_{\mathfrak{p}} p) = u(hg)^2\big\}$$

$$\ll_\varepsilon q^{x\varepsilon} \sum_{u\in\mathbb{F}_q^\times} \sum_{\substack{g\in A\\ g \text{ monic, squarefree}\\ \deg g\le x-2y}} \sum_{\substack{h\in A\\ h \text{ monic}\\ y\le \deg h\le \frac{x}{2}}} \#\big\{\mathfrak{p}\in\mathcal{P}(\psi): \deg p = x, g(a_{\mathfrak{p}}^2 - 4\mu_{\mathfrak{p}} p) = u(hg)^2\big\},$$

where we have also used the estimate $\tau_A(h) \ll_\varepsilon |h|^\varepsilon$, valid for any $\varepsilon > 0$. Let us remark that, for each $u \in \mathbb{F}_q^\times$, each monic squarefree g and each $\mathfrak{p}$, there is at most one monic $h \in A$ such that $y \le \deg h \le x/2$ and $a_{\mathfrak{p}}^2 - 4\mu_{\mathfrak{p}} p = u h^2 g$. Thus

$$q^{x\varepsilon} \sum_{u\in\mathbb{F}_q^\times} \sum_{\substack{g\in A\\ g \text{ monic, squarefree}\\ \deg g\le x-2y}} \sum_{\substack{h\in A\\ h \text{ monic}\\ y\le \deg h\le \frac{x}{2}}} \#\big\{\mathfrak{p}\in\mathcal{P}(\psi): \deg p = x, g(a_{\mathfrak{p}}^2 - 4\mu_{\mathfrak{p}} p) = u(hg)^2\big\}$$

$$\le q^{x\varepsilon+1} \sum_{\substack{g\in A\\ g \text{ monic, squarefree}\\ \deg g\le x-2y}} \#\left\{\mathfrak{p}\in\mathcal{P}(\psi): \deg p = x, g(a_{\mathfrak{p}}^2 - 4\mu_{\mathfrak{p}} p) \text{ is a square in } A\right\}.$$

By invoking (35) and linking all the above estimates, we deduce that

$$\sum_{\substack{0\neq m\in A\\ m \text{ monic}\\ y<\deg m\le \frac{x}{2}}} \#\{\mathfrak{p}\in\mathcal{P}(\psi): \deg p = x, m \mid b_{\mathfrak{p}}\} \ll_{\psi,\varepsilon} q^{\frac{15x}{8} - 2y + x\varepsilon + 1} x^3, \tag{40}$$

valid for any $\varepsilon > 0$, an arbitrary value of which we now fix.

Choosing

$$y = y(x) := \frac{(11+\varepsilon)x}{24} \tag{41}$$

and recalling that q is fixed, x varies, and $\lim_{x\to\infty} f(x) = \infty$, we deduce from (33), (34), and (40) that

$$\#\left\{\mathfrak{p} \in \mathcal{P}(\psi) : \deg p = x, |b_{\mathfrak{p}}| \geq q^{\frac{f(\deg p)}{2}}\right\} \ll_{\psi,\varepsilon,q} q^{x-f(x)} + q^{\frac{23x}{24}+\varepsilon x} = \mathrm{o}\left(\frac{q^x}{x}\right), \tag{42}$$

which confirms (20).

Now let us prove that the set $\left\{\mathfrak{p} \in \mathcal{P}(\psi) : |\Delta_{\mathfrak{p}}| > \frac{|a_{\mathfrak{p}}^2 - 4\mu_{\mathfrak{p}} p|}{q^{f(\deg p)}}\right\}$ has Dirichlet density 1. For this, let $s > 1$ and consider the sum

$$\begin{aligned}\sum_{\substack{\mathfrak{p}\in\mathcal{P}(\psi)\\ |\Delta_{\mathfrak{p}}| \leq \frac{|a_{\mathfrak{p}}^2 - 4\mu_{\mathfrak{p}} p|}{q^{f(\deg p)}}}} q^{-s\deg p} &= \sum_{x\geq 1} q^{-sx} \#\left\{\mathfrak{p} \in \mathcal{P}(\psi) : \deg p = x, |\Delta_{\mathfrak{p}}| \leq \frac{|a_{\mathfrak{p}}^2 - 4\mu_{\mathfrak{p}} p|}{q^{f(\deg p)}}\right\} \\ &= \sum_{x\geq 1} q^{-sx} \#\left\{\mathfrak{p} \in \mathcal{P}(\psi) : \deg p = x, |b_{\mathfrak{p}}| \geq q^{\frac{f(x)}{2}}\right\}.\end{aligned}$$

By (26), (27), (32), (40), and our earlier choice (41) of y, we obtain that the above is

$$\leq \sum_{x\geq 1} \frac{q^{(1-s)x}}{x} \sum_{\substack{0\neq m\in A\\ m \text{ monic}\\ \frac{f(x)}{2}\leq \deg m\leq \frac{x}{2}}} \frac{c_m(x)}{[J_m : F]} + \mathrm{O}_{\psi,\varepsilon,q}\left(\sum_{x\geq 1} q^{(\frac{23}{24}+\varepsilon-s)x}\right). \tag{43}$$

To estimate the first double sum in (43), we use (25) to rewrite $c_m(x)$:

$$\begin{aligned} T_1 &:= \sum_{x\geq 1} \frac{q^{(1-s)x}}{x} \sum_{\substack{0\neq m\in A\\ m \text{ monic}\\ \frac{f(x)}{2}\leq \deg m\leq \frac{x}{2}}} \frac{c_m(x)}{[J_m : F]} \\ &= \sum_{x\geq 1} \frac{q^{(1-s)x}}{x} \sum_{\substack{0\neq m\in A\\ m \text{ monic}\\ \frac{f(x)}{2}\leq \deg m\leq \frac{x}{2}\\ c_m | x}} \frac{c_m}{[J_m : F]} \\ &= \sum_{\substack{0\neq m\in A\\ m \text{ monic}}} \sum_{\substack{j\geq 1\\ \frac{f(c_m j)}{2}\leq \deg m\leq \frac{c_m j}{2}}} \frac{q^{(1-s)c_m j}}{j[J_m : F]}. \end{aligned} \tag{44}$$

Next we fix $M > 0$ and observe that, since $\lim_{x\to\infty} f(x) = \infty$, there exists $n(M) \in \mathbb{N}$ such that

$$f(n) > M \quad \forall n \geq n(M). \tag{45}$$

We split the inner sum over j in our last reformulation (44) of T_1 according to whether $c_m j \geq n(M)$ or $c_m j < n(M)$. For the first range $c_m j \geq n(M)$, we obtain

$$\begin{aligned}
T_{1,1} &:= \sum_{\substack{0\neq m\in A\\ m \text{ monic}}} \sum_{\substack{j\geq 1\\ c_m j\geq n(M)\\ \frac{f(c_m j)}{2}\leq \deg m\leq \frac{c_m j}{2}}} \frac{q^{(1-s)c_m j}}{j[J_m : F]} \\
&\leq \sum_{\substack{0\neq m\in A\\ m \text{ monic}\\ \frac{M}{2}\leq \deg m}} \frac{1}{[J_m : F]} \sum_{j\geq 1} \frac{q^{(1-s)c_m j}}{j} \\
&\ll \sum_{\substack{0\neq m\in A\\ m \text{ monic}\\ \frac{M}{2}\leq \deg m}} \frac{1}{[J_m : F]} \sum_{j\geq 1} \frac{q^{(1-s)j}}{j} \\
&\ll_\psi \sum_{\substack{0\neq m\in A\\ m \text{ monic}\\ \frac{M}{2}\leq \deg m}} \frac{1}{|m|^3} \sum_{j\geq 1} \frac{q^{(1-s)j}}{j} \\
&\ll \frac{1}{q^M} \left|\log\left(1-q^{1-s}\right)\right|,
\end{aligned}$$

where we used (45) to pass to the second line, (28) to pass to the third line, the lower bound in (30) to pass to the fourth line, and [CoSh15, Lem. 2.2], together $s > 1$, to pass to the fifth line. It follows that

$$\lim_{s\to 1+} \frac{T_{1,1}}{-\log\left(1-q^{1-s}\right)} \ll_\psi \frac{1}{q^M}. \tag{46}$$

For the second range $c_m j < n(M)$ in the inner sum of (44), we remark that

$$T_{1,2} := \sum_{\substack{0\neq m\in A\\ m \text{ monic}}} \sum_{\substack{j\geq 1\\ c_m j< n(M)\\ \frac{f(c_m j)}{2}\leq \deg m\leq \frac{c_m j}{2}}} \frac{q^{(1-s)c_m j}}{j[J_m : F]}$$

is a finite sum since $\deg m \leq \frac{c_m j}{2} \ll j$ (using (28) for the $\ll$-bound) and since $j < n(M)$. Observing that $\lim_{s\to 1+} \frac{q^{(1-s)\alpha}}{\log\left(1-q^{1-s}\right)} = 0$ for any $\alpha \geq 1$, it follows that

$$\lim_{s\to 1+} \frac{T_{1,2}}{-\log\left(1-q^{1-s}\right)} = 0. \tag{47}$$

To estimate the remaining O-term in (43), we consider the sum

$$T_2 := \sum_{x\geq 1} q^{\left(\frac{23}{24}+\varepsilon-s\right)x}$$

and observe that

$$\lim_{s\to 1+} \frac{T_2}{-\log\left(1-q^{1-s}\right)} = -\lim_{s\to 1+} \frac{q^{\frac{23}{24}+\varepsilon-s}}{\left(1-q^{\frac{23}{24}+\varepsilon-s}\right)\log\left(1-q^{1-s}\right)} = 0. \tag{48}$$

We now take $M\to\infty$ in (45) and put together (46), (47), and (48), completing the proof of Theorem 6.

Acknowledgments

We thank Zeev Rudnick for his comments on an earlier version of Theorem 1, which prompted us to obtain an improved bound. We thank the referee for the detailed comments and suggestions, which allowed us to improve the exposition of the paper. We dedicate the paper to Ernst-Ulrich Gekeler for support and encouragement over the years.

References

[Be09] Jeffrey Beyerl, Binary Quadratic Forms over $\mathbb{F}_q[T]$ and Principal Ideal Domains, Thesis (Masters)–Clemson University, U.S.A., 2009.

[Br10] Florian Breuer, Torsion bounds for elliptic curves and Drinfeld modules, J. Number Theory 130 (5) (2010) 1241–1250.

[CoFi21] Alina Carmen Cojocaru, Matthew Fitzpatrick, The absolute discriminant of the endomorphism ring of most reductions of a non-CM elliptic curve is close to maximal, to appear in Arithmetic, Geometry, Cryptography and Coding Theory, edited by Stéphane Ballet, Gaetan Bisson, and Irene Bouw, Contemporary Mathematics, Vol. 770, American Mathematical Society, Providence, Rhode Island.

[CoJo21] Alina Carmen Cojocaru, Nathan Jones, Degree bounds for projective division fields associated to elliptic modules with a trivial endomorphism ring, to appear in Journal de Théorie des Nombres de Bordeaux.

[CoPa15] Alina Carmen Cojocaru, Mihran Papikian, Drinfeld modules, Frobenius endomorphisms, and CM-liftings, Int. Math. Res. Not. 17 (2015) 7787–7825.

[CoSh15] Alina Carmen Cojocaru, Andrew Michael Shulman, The distribution of the first elementary divisor of the reductions of a generic Drinfeld module of arbitrary rank, Can. J. Math. 67 (6) (2015) 1326–1357.

[Cox89] David A. Cox, Primes of the Form x^2+ny^2. A Wiley-Interscience Publication, John Wiley & Sons, Inc., New York, 1989, Fermat, class field theory and complex multiplication.

[Dr74] Vladimir Drinfeld, Elliptic modules, Mat. Sb. (N.S.)) 94 (136) (1974) 594–627, 656.

[Ge83] Ernst-Ulrich Gekeler, Zur Arithmetik von Drinfeld-Moduln, Math. Ann. 262 (2) (1983) 167–182.

[Ge91] Ernst-Ulrich Gekeler, On finite Drinfeld modules, J. Algebra 141 (1) (1991) 187–203.

[Ge99] Ernst-Ulrich Gekeler, Some new results on modular forms for $\mathrm{GL}(2, \mathbb{F}_q[T])$, in: Recent Progress in Algebra, Taejon/Seoul, 1997, in: Contemp. Math., vol. 224, Amer. Math. Soc., Providence, RI, 1999, pp. 111–141.

[Ge19] Ernst-Ulrich Gekeler, On the field generated by the periods of a Drinfeld module, Arch. Math. (Basel) 113 (6) (2019) 581–591.

[Go96] David Goss, Basic Structures of Function Field Arithmetic, Ergebnisse der Mathematik und ihrer Grenzgebiete (3) (Results in Mathematics and Related Areas (3)), vol. 35, Springer-Verlag, Berlin, 1996.

[GaPa19] Sumita Garai, Mihran Papikian, Endomorphism rings of reductions of Drinfeld modules, J. Number Theory 212 (2019) 18–39.

[GaPa20] Sumita Garai, Mihran Papikian, Computing endomorphism rings and Frobenius matrices of Drinfeld modules, J. Number Theory (2020), https://doi.org/10.1016/j.jnt.2019.11.018.

[MuSc94] V. Kumar Murty, John Scherk, Effective versions of the Chebotarev density theorem for function fields, C. R. Acad. Sci. Paris, Ser. I 319 (1994) 523–528.

[Ro02] Michael Rosen, Number Theory in Function Fields, Graduate Texts in Mathematics, vol. 210, Springer-Verlag, New York, 2002.

[Sc91] René Schoof, The exponents of the groups of points on the reductions of an elliptic curve, in: Arithmetic Algebraic Geometry, Texel, 1989, in: Progr. Math., vol. 89, Birkhäuser Boston, Boston, MA, 1991, pp. 325–335.

[Yu95a] Jiu-Kang Yu, A class number relation over function fields, J. Number Theory 54 (2) (1995) 318–340.

[Yu95b] Jiu-Kang Yu, Isogenies of Drinfeld modules over finite fields, J. Number Theory 54 (1) (1995) 161–171.