ON THE VARIATION OF TATE-SHAFAREVICH GROUPS OF ELLIPTIC CURVES OVER HYPERELLIPTIC CURVES

MIHRAN PAPIKIAN

ABSTRACT. Let E be an elliptic curve over $F = \mathbb{F}_q(t)$ having conductor $(\mathfrak{p})\cdot\infty$, where $(\mathfrak{p})$ is a prime ideal in $\mathbb{F}_q[t]$. Let $\mathfrak{d} \in \mathbb{F}_q[t]$ be an irreducible polynomial of odd degree, and let $K = F(\sqrt{\mathfrak{d}})$. Assume $(\mathfrak{p})$ remains prime in K. We prove the analogue of the formula of Gross for the special value $L(E\otimes_F K, 1)$. As a consequence, we obtain a formula for the order of the Tate-Shafarevich group $Ш(E/K)$ when $L(E \otimes_F K, 1) \neq 0$.

1. Introduction

Let E be an elliptic curve over the function field $F := \mathbb{F}_q(t)$ of $\mathbb{P}^1_{\mathbb{F}_q}$, where q is odd. Assume E has conductor $(\mathfrak{p})\cdot\infty$, where ∞ is the place corresponding to $1/t$ and $\mathfrak{p} \in A := \mathbb{F}_q[t]$ is a prime. Further assume that the reduction of E at ∞ is split multiplicative. In this situation it is known that E is a quotient of the Drinfeld Jacobian variety $J := J_0(\mathfrak{p})$; see [9].

Let $S := \{x_1, x_2, \dots, x_n\}$ be the set of isomorphism classes of super-singular Drinfeld modules over $\overline{\mathbb{F}}_\mathfrak{p}$, where we write $\mathbb{F}_\mathfrak{p} := A/(\mathfrak{p})$. It is known that $n = \dim(J) + 1$. For each $x_i \in S$ we let ϕ_i denote a super-singular Drinfeld module representing the isomorphism class corresponding to x_i. Let $\mathcal{M}$ denote the free $\mathbb{Z}$-module on the set S, and $\deg : \mathcal{M} \to \mathbb{Z}$ denote the $\mathbb{Z}$-linear map obtained by sending each $x_i \in S$ to $1 \in \mathbb{Z}$, and let $\mathcal{M}^0$ denote the kernel of deg. Define a symmetric, bilinear, $\mathbb{Z}$-valued pairing on $\mathcal{M}$ by the formula

$$\langle x_i, x_j\rangle = \frac{1}{q-1}\#\mathrm{Isom}(\phi_i, \phi_j). \tag{1.1}$$

In particular, $\langle x_i, x_j\rangle = 0$ for $i \neq j$. It is known that $\mathrm{Aut}(\phi_i) \cong \mathbb{F}_q^\times$ or $\mathbb{F}_{q^2}^\times$ (the latter case can occur only when $\deg\mathfrak{p}$ is odd), so $\langle x_i, x_i\rangle = 1$ or $(q + 1)$.

Denote by $\mathcal{E}$ the Néron model of E over $\mathbb{P}^1_{\mathbb{F}_q}$. Let $\mathcal{E}^0$ be the relative connected component of the identity of $\mathcal{E}$, i.e., the largest open subgroup-scheme of $\mathcal{E}$ in which all fibres are connected. Similarly, denote by $\mathcal{J}$ and $\mathcal{J}^0$ the Néron model of J and its relative connected component of the identity. It is known, c.f. §3, that the closed fibre $\mathcal{J}^0_{\overline{\mathbb{F}}_\mathfrak{p}}$ is a torus and the character group $\mathrm{Hom}_{\overline{\mathbb{F}}_\mathfrak{p}}(\mathcal{J}^0_{\overline{\mathbb{F}}_\mathfrak{p}}, \mathbb{G}_{m,\overline{\mathbb{F}}_\mathfrak{p}})$ is canonically isomorphic to $\mathcal{M}^0$. Moreover, the pairing in (1.1) restricted to $\mathcal{M}^0$ is Grothendieck's monodromy pairing discussed in [12]. The character group Υ of $\mathcal{E}^0_{\overline{\mathbb{F}}_\mathfrak{p}}$ is isomorphic to $\mathbb{Z}$. We choose the quotient map $\pi : J \to E$ canonically to satisfy a ceratin minimality property; see §5.2. Let ρ be a generator of Υ. There

1991 *Mathematics Subject Classification.* Primary 11G05, 11G40; Secondary 11G18.
Key words and phrases. Formula of Gross, Tate-Shafarevich group, Drinfeld modular curves.
Supported in part by the European Postdoctoral Institute Fellowship.

results a functorial homomorphism between character groups $\pi^* : \Upsilon \to \mathcal{M}^0$. Let $H_E := \pi^*(\rho) \in \mathcal{M}^0$.

Now let $\mathfrak{d}$ be an irreducible polynomial in A of odd degree. Let $K = F(\sqrt{\mathfrak{d}})$. The field K is the function field of a hyperelliptic curve over $\mathbb{F}_q$. The extension K/F is ramified only at $(\mathfrak{d})$ and ∞. Let $\mathcal{O}$ be the integral closure of A in K. If we assume that the ideal $(\mathfrak{p})$ remains prime in $\mathcal{O}$ then the endomorphism rings of some super-singular Drinfeld modules ϕ_i contain $\mathcal{O}$ as a subring. There results an action of $\mathrm{Pic}(\mathcal{O})$ on a subset of S, and one produces from this action an element $H_K \in \mathcal{M}$; see §2.

Denote by $E_K := E \otimes_F K$ the base change of E to K. The first main result of this paper is the following theorem:

Theorem 1.1. *$L(E_K, 1) = 0$ if and only if $\langle H_E, H_K\rangle = 0$.*

If we assume $L(E_K, 1) \neq 0$ then Tate [23] proved that $E(K)$ and the Tate-Shafarevich group $Ш(E/K)$ are finite, and the formula for $L(E_K, 1)$ predicted by the conjecture of Birch and Swinnerton-Dyer holds; see also [14]. Our next main result gives a formula for the order of $Ш(E/K)$ in terms of $\langle H_E, H_K\rangle$:

Theorem 1.2. *If $\langle H_E, H_K\rangle \neq 0$ then*

$$\#Ш(E/K) = \left(\langle H_E, H_K\rangle \cdot \frac{\#E(F)}{\#\Phi_{E,\mathfrak{p}}} \cdot q^{(\deg \Omega^1_{\mathcal{E}/\mathbb{P}^1}|_O - 1)}\right)^2,$$

where $\Phi_{E,\mathfrak{p}} := \mathcal{E}_{\overline{\mathbb{F}}_\mathfrak{p}}/\mathcal{E}^0_{\overline{\mathbb{F}}_\mathfrak{p}}$ is the group of connected components of $\mathcal{E}_{\overline{\mathbb{F}}_\mathfrak{p}}$ and $\Omega^1_{\mathcal{E}/\mathbb{P}^1}|_O$ is the pullback of $\Omega^1_{\mathcal{E}/\mathbb{P}^1}$ along the relative zero section.

In particular, this theorem says that the variation of $\#Ш(E/K)$ over different K depends only on the relative position of H_K and H_E in $\mathcal{M}$. Also, the formula in the theorem can be used to compute $\#Ш(E/K)$, c.f. Example 5.5.

To prove Theorem 1.1 we will prove a more general result which gives a formula for the special values of L-functions of Drinfeld cusp forms at the center of the critical strip. This formula is the function field analogue of the result of Gross over $\mathbb{Q}$ [11]. Our proof follows closely the strategy in *loc.cit.* The required analytic calculations involving Rankin convolutions are already carried out in [18], where the authors prove the analogue of the Gross-Zagier formula for the derivatives of L-functions. Hence we only need to explicitly compute the pairing (1.1) between certain special elements of $\mathcal{M}$. Theorem 1.2 is a consequence of the analogue of Gross' formula and the theorem of Tate [23]. We make the restriction on $\mathfrak{d}$ being irreducible and the characteristic being odd mainly because the analytic formulae in [18] are proven under these assumptions.

The contents of the paper are as follows. We start section 2 by proving some auxiliary results about endomorphism rings of super-singular Drinfeld modules. Using these results, later in the same section we carry out the main technical calculation of the paper, which is an explicit formula for the pairing between certain elements of $\mathcal{M}$. In section 3 we prove the analogue of Eichler's theorem over F. We show that a certain set of explicit theta series arising from quaternion algebras over F spans the whole space of Drinfeld automorphic forms. (This theorem might be of some independent interest.) In section 4 we combine our previous results with the calculations in [18] to deduce the analogue of the formula of Gross. Finally, section 5 discusses the applications of aforementioned formula to the arithmetic of elliptic curves. In particular, it contains the proof of Theorem 1.2. We close this introduction by remarking that it would be very interesting to have some cohomological explanation for our results.

Acknowledgement. The author wishes to thank Brian Conrad for numerous helpful remarks on an earlier version of this paper.

2. The arithmetic of super-singular Drinfeld modules

The proof of the main result in [11] consists of two, fairly independent, parts. The first part, which is very analytic in nature, is a calculation of a Rankin integral. The output of this calculation is the fact that the values of certain L-functions at the center of their critical strip are equal, up to a non-zero constant, to the Petersson product of two modular forms. One of those modular forms is a cusp form of weight two and the other is a modular form with very explicit Fourier expansion. The second part of the proof in [11] is an algebraic calculation involving maximal orders in quaternion algebras over $\mathbb{Q}$. This calculation shows that the modular form obtained in the first step is a certain distinguished theta series arising from a quaternion algebra. Using these two steps, Gross deduces interesting arithmetic facts which complement his results with Zagier on the the special values of the derivatives of L-functions.

The analogue over F of the analytic portion of calculations in [11] was done by Rück and Tipp [18] (it is an intermediate step in their proof of the analogue of the Gross-Zagier formula). In this section we carry out the analogue of algebraic calculations. The main result is Corollary 2.12. Since the calculations are somewhat tedious and might seem not very motivated at this stage, we point out that the expression in Corollary 2.12 is a Fourier coefficient of a certain theta series which comes up in later sections. In particular, this theta series appears in the statement of the analogue of Gross' formula; see Theorem 4.1. The reader might choose to simply skim though this section as the proofs in the section are not essential for understanding the main results of the paper.

2.1. **Quaternion algebras over function fields.** Let $F = \mathbb{F}_q(t)$ and let $A = \mathbb{F}_q[t]$; we will assume the characteristic is not 2. A central simple algebra B over F is a *quaternion algebra* if $\dim_F B = 4$. From Wedderburn's structure theorem [16, (7.4)] one concludes that a quaternion algebra is either isomorphic to the matrix algebra $M_2(F)$ or is a division algebra. The quaternion algebra B is said to be *split* at a place v of F if $B_v := B \otimes_F F_v \cong M_2(F_v)$; it is said to be *ramified* if B_v is a division algebra. The fundamental exact sequence of Brauer groups from global class field theory implies that any quaternion algebra is split at all but finitely many places and the number of places where it is ramified is even. Conversely, for any even set of places of F there is a unique quaternion algebra ramified exactly at those places and split at all the others. In particular, $B \cong M_2(F)$ if and only if it is split at all places of F. For $a, b \in F^\times$, let $H(a, b)$ be the F-algebra with basis $1, i, j, k$ (as a F-vector space) and relations $i^2 = a$, $j^2 = b$, $ij = k = -ji$. One easily checks that this is a quaternion algebra. Conversely, using the Skolem-Noether theorem [16, (7.21)], it is not hard to show that every quaternion algebra is isomorphic to $H(a, b)$ for some (non-unique) $a, b \in F^\times$.

For any finite dimensional F-vector space V, a *full A-lattice* in V is a finitely generated A-submodule M in V such that $F \otimes_A M \cong V$. An *A-order* in the F-algebra B is a subring Λ of B, having the same unity element as A, and such that Λ is a full A-lattice in B. A *maximal A-order* in B is an A-order which is not contained in any other A-order in B. Orders exist and every order is contained in a maximal order [16, (10.4)]. Given a full A-lattice M in B, define the *left order of M* to be

$$O_l(M) = \{a \in B \mid aM \subseteq M\}.$$

One easily checks that this is indeed an order. Similarly to $O_l(M)$, one also defines the right order $O_r(M)$ of M.

Let Λ be an A-order in B. A full A-lattice I in B is called a *left ideal of* Λ (resp. *right ideal*, *two-sided ideal*) if it is stable under the left multiplication by Λ (resp. under the right multiplication, under multiplication on the right and on the left). Define $\mathrm{Nr}(I) \subset F$, the *reduced norm of* I, to be the fractional A-ideal generated by $\{\mathrm{Nr}(a) \mid a \in I\}$, where $\mathrm{Nr} = \mathrm{Nr}_{B/F}$ is the canonical reduced norm on B.

If S is a finite-length A-module, let $\chi(S)$ be the *Euler-Poincaré characteristic* of S, which is an ideal of A uniquely determined by the conditions

(i) $\chi(S) = \mathfrak{q}$ if $S \cong A/\mathfrak{q}$ with a prime ideal $\mathfrak{q}$ of A;
(ii) If $0 \to S_1 \to S \to S_2 \to 0$ is exact, then $\chi(S) = \chi(S_1)\chi(S_2)$.

The statements in the next proposition are well-known (the proofs, which are not hard, can be found in [16]). From now on we assume B is a division algebra.

Proposition 2.1. *Let I be a left ideal of some maximal order Λ in B. Let $I^{-1} = \{a \in B \mid IaI \subseteq I\}$.*

(1) *Let M be any full A-lattice in B. The order $O_l(M)$ is maximal if and only if $O_r(M)$ is maximal.*
(2) *If I is an integral ideal of Λ, i.e., $I \subseteq \Lambda$, then* $\mathrm{Nr}(I)^2 = \chi(\Lambda/I)$.
(3) *For any $\alpha \in \Lambda$,* $\mathrm{Nr}(\alpha) \in A$.
(4) *I^{-1} is a right Λ-ideal, and left $O_r(I)$-ideal.*
(5) $II^{-1} = \Lambda$, $I^{-1}I = O_r(I)$, $(I^{-1})^{-1} = I$.
(6) *If J is a left $O_r(I)$-ideal, then* $\mathrm{Nr}(IJ) = \mathrm{Nr}(I)\mathrm{Nr}(J)$. *In particular,*
$$\mathrm{Nr}(I^{-1}) = \mathrm{Nr}(I)^{-1}.$$
(7) *If $J \subset I$ is another left Λ-ideal and* $\mathrm{Nr}(J) = \mathrm{Nr}(I)$ *then $J = I$. In particular, if there is an element $\alpha \in I$ such that* $\mathrm{Nr}(\alpha) = \mathrm{Nr}(I)$ *then $I = \Lambda\alpha$.*

Let Λ be a maximal A-order in B. Two left Λ-ideals I and J are said to be *equivalent* if there is $a \in B$ with $J = Ia$. The number of equivalence classes of left Λ-ideals is called the *class number of B*. It is known that the class number is finite and is independent of the choice of Λ. If $\{I_1, I_2, \dots, I_n\}$ is a set of left Λ-ideals representing the distinct ideal classes, then each conjugacy class of maximal A-orders in B is represented in the set of right orders $\{O_r(I_1), O_r(I_2), \dots, O_r(I_n)\}$.

Let $\mathfrak{p} \in A$ be a monic irreducible polynomial. We will denote $\mathbb{F}_\mathfrak{p} := A/(\mathfrak{p})$. The finite field $\mathbb{F}_\mathfrak{p}$ is the field extension of $\mathbb{F}_q$ of degree equal to the degree of $\mathfrak{p}$. For $\mu \in A$ we will denote by (μ) the principal ideal in A generated by μ.

Let $\mathfrak{d}$ be an irreducible polynomial in A of *odd* degree. Let $K = F(y)$, where $y^2 = \mathfrak{d}$. Let $\mathcal{O} := A[y]$; this ring is the integral closure of A in K since we are assuming the characteristic of F is not 2, c.f. [13, §9]. The ideal $\mathcal{D} = (y)$ is the different of $\mathcal{O}/A$. The only primes of F which ramify in K are $(\mathfrak{d})$ and ∞.

Lemma 2.2. *Let $B_{\mathfrak{p}}$ be the unique quaternion algebra over F which is ramified exactly at $(\mathfrak{p})$ and ∞. Assume $(\mathfrak{d}) \neq (\mathfrak{p})$. The field K embeds in $B_{\mathfrak{p}}$ if and only if $\left(\frac{\mathfrak{d}}{\mathfrak{p}}\right) = -1$. In case $K \hookrightarrow B_{\mathfrak{p}}$, there is a canonical isomorphism $B_{\mathfrak{p}} = K \oplus Kj$, where $j\alpha = \overline{\alpha}j$ for $\alpha \in K$ and $j^2 = c\mathfrak{p}$ for an appropriate $c \in \mathbb{F}_q^\times$.*

Proof. We know that $B_{\mathfrak{p}} \cong H(a,b)$ for some $a, b \in F^\times$. The algebra $H(a,b)$ is split over a field L if and only if the quadratic form $Q = X^2 - aY^2 - bZ^2 + abT^2$ corresponding to the reduced norm on $H(a,b)$ has a non-zero solution in L. To show that for particular a and b there is an isomorphism $B_{\mathfrak{p}} \cong H(a,b)$, it is enough to show that $H(a,b)$ is ramified at $\mathfrak{p}$ and is split at every other place not equal to ∞ (it then automatically will be ramified at ∞, since the number of ramified places must be even). Since the characteristic is not 2, using Hensel's lemma, it is enough to show that Q has a non-zero solution in $\mathbb{F}_{\mathfrak{l}}$ for every $\mathfrak{l} \neq \mathfrak{p}, \infty$, and has no non-zero solutions in $\mathbb{F}_{\mathfrak{p}}$. By an easy counting argument, any quadratic form of more than two variables has a non-zero solution over a finite field.

Suppose $K \hookrightarrow B_{\mathfrak{p}}$. Since the completion $F_{\mathfrak{p}}$ is flat over F, there is an injection $K \otimes_F F_{\mathfrak{p}} \hookrightarrow B_{\mathfrak{p}} \otimes_F F_{\mathfrak{p}}$. The algebra on the right hand-side is a division algebra by assumption. Hence $K \otimes_F F_{\mathfrak{p}}$ is a field, which implies that $\mathfrak{d}$ is not a square modulo $\mathfrak{p}$, i.e., $\left(\frac{\mathfrak{d}}{\mathfrak{p}}\right) = -1$. Conversely, suppose $\left(\frac{\mathfrak{d}}{\mathfrak{p}}\right) = -1$ and let $c \in \mathbb{F}_q^\times \setminus (\mathbb{F}_q^\times)^2$. Using the remarks in the previous paragraph, one easily checks that in case $\left(\frac{\mathfrak{p}}{\mathfrak{d}}\right) = 1$ the algebra $H(\mathfrak{d}, \mathfrak{p})$ is ramified exactly at $\mathfrak{p}$ and ∞. If $\left(\frac{\mathfrak{p}}{\mathfrak{d}}\right) = -1$ then $H(\mathfrak{d}, c\mathfrak{p})$ has the same property. In both cases we obviously have an injection $K \hookrightarrow B_{\mathfrak{p}}$ and the decomposition $B_{\mathfrak{p}} = K \oplus Kj$ stated in the lemma. □

Lemma 2.3. *Assume $\left(\frac{\mathfrak{d}}{\mathfrak{p}}\right) = -1$, so that $B_{\mathfrak{p}} = K \oplus Kj$. Let $c \in \mathbb{F}_q^\times$ be as in Lemma 2.2, and let $\varepsilon \in A$ be a solution of the congruence $\varepsilon^2 \equiv c\mathfrak{p} \pmod{\mathfrak{d}}$. If we let Λ be the set*

$$\{\alpha + \beta j \mid \alpha, \beta \in \mathcal{D}^{-1},\ \alpha \equiv \varepsilon\beta \pmod{\mathcal{O}_{\mathcal{D}}}\},$$

where $\mathcal{D}^{-1}$ is the inverse different of $\mathcal{O}/A$ and $\mathcal{O}_{\mathcal{D}}$ is the localization of $\mathcal{O}$ at the prime ideal $\mathcal{D}$, then Λ is a maximal order which contains $\mathcal{O} \oplus \mathcal{O}j$.

Proof. It is clear that Λ is a full A-lattice in $B_{\mathfrak{p}}$ and that it contains $\mathcal{O} \oplus \mathcal{O}j$. Let $\alpha_1 + \beta_1 j$ and $\alpha_2 + \beta_2 j$ be two elements of Λ. We have

$$(\alpha_1 + \beta_1 j)(\alpha_2 + \beta_2 j) = \alpha' + \beta' j,$$

where $\alpha' = \alpha_1\alpha_2 + c\mathfrak{p}\beta_1\bar{\beta}_2$ and $\beta' = \alpha_1\beta_2 + \beta_1\bar{\alpha}_2$. To check that Λ is a ring we need to check that $\alpha', \beta' \in \mathcal{D}^{-1}$ and $\alpha' \equiv \varepsilon\beta' \pmod{\mathcal{O}_{\mathcal{D}}}$. This is a straightforward but tedious calculation which we omit (one needs to use along the way that $\mathrm{Tr}_{K/F}(\beta_2) \in A$ and $\mathfrak{d}\beta_1\beta_2 \in \mathcal{O}$). Thus, Λ is an order.

Denote $\Delta = \mathcal{O} \oplus \mathcal{O}j$; this is an order in $B_{\mathfrak{p}}$. An A-basis for Δ is given by $1, i, j, ij$, where $i^2 = \mathfrak{d}$. As one easily checks, the discriminant of Δ with respect to the reduced trace on $B_{\mathfrak{p}}$ is equal to the ideal $(\mathfrak{p}\mathfrak{d})^2$. The discriminant of any A-order in $B_{\mathfrak{p}}$ is divisible by $(\mathfrak{p})^2$ and the maximal orders are characterized by the property that their discriminants are equal to the ideal $(\mathfrak{p})^2$. We have a strict containment $\Delta \subset \Lambda$. Hence

$$(\mathfrak{p}\mathfrak{d})^2 = \mathrm{disc}(\Lambda) \cdot \chi(\Lambda/\Delta)^2.$$

Since $\mathfrak{d}$ is a prime, we must have $\mathrm{disc}(\Lambda) = (\mathfrak{p})^2$, so Λ is maximal as claimed. □

Lemma 2.3 will be used in §2.4, but first we need few facts about the endomorphism rings of super-singular Drinfeld modules.

2.2. **Super-singular Drinfeld modules.** Let k be an algebraic extension of $\mathbb{F}_\mathfrak{p}$. There is a canonical A-structure on k given by $\gamma : A \to \mathbb{F}_\mathfrak{p} \hookrightarrow k$. Let τ be the Frobenius endomorphism relative to $\mathbb{F}_q$, i.e., the map $x \mapsto x^q$. Denote by $k\{\tau\}$ the non-commutative polynomial algebra in τ subject to the commutation rule $\tau x = x^q\tau$, $x \in k$.

A *Drinfeld module* (of rank 2) over k is a structure of A-module on k given by a ring homomorphism

$$\begin{aligned} \phi : A = \mathbb{F}_q[t] &\to k\{\tau\} \\ a &\mapsto \phi_a \end{aligned}$$

such that $\phi_t = \gamma(t) + g\tau + \Delta\tau^2$ and $\Delta \neq 0$. A *k-isogeny* between two Drinfeld modules ϕ and ψ is an element $u \in k\{\tau\}$ such that $u \circ \phi_a = \psi_a \circ u$ for all $a \in A$. Each $0 \neq f \in k\{\tau\}$ can uniquely be written as $f = f_s \circ \tau^h$, where f_s has a non-zero constant coefficient. The number $h = \mathrm{ht}(f)$ is called the *height* of f. The *height of the Drinfeld module* ϕ is the height of $\phi_\mathfrak{p}$ divided by $\deg(\mathfrak{p})$. It is equal to 1 or 2.

Suppose $u = \gamma(a) + g_1\tau + \cdots + g_s\tau^s \in k\{\tau\}$. We will denote by

$$u(X) = \gamma(a)X + g_1X^q + \cdots + g_sX^{q^s} \in k[X]$$

the corresponding q-additive polynomial. The scheme-theoretic kernel $\ker(u) = k[X]/\phi_a(X)$ is a commutative finite flat group-scheme of $\mathbb{F}_q$-vector spaces. Conversely, it is easy to see that given a finite subgroup scheme of $\mathbb{F}_q$-vector spaces $H \subset \mathbb{G}_{a,k}$, there is a unique polynomial $u \in k\{\tau\}$ with $H = \ker(u)$

Lemma 2.4. *With notation as above, assume in addition that H has a structure of an A-module via the Drinfeld module ϕ over k. Then u is an isogeny from ϕ if and only if* $\mathrm{ht}(u)$ *is divisible by* $\deg \mathfrak{p}$.

Proof. See [10, Prop.2.5]. □

If H satisfies the conditions of Lemma 2.4, then we will say that H is a subgroup-scheme of ϕ and will denote the corresponding isogeny by u_H. The Drinfeld module ϕ is called *super-singular* (s.s.) if $\ker(\phi_\mathfrak{p})$ is connected (equivalent conditions are: $\phi_\mathfrak{p}(X)$ is purely inseparable, or $\mathrm{ht}(\phi) = 2$). Let

$$\mathrm{End}(\phi) = \{u \in k\{\tau\} \mid u \circ \phi_a = \phi_a \circ u \text{ for all } a \in A\}.$$

Theorem 2.5. *Let ϕ be a s.s. Drinfeld module over $\overline{\mathbb{F}}_\mathfrak{p}$. The endomorphism ring* $\mathrm{End}(\phi)$ *is a maximal order in $B_\mathfrak{p}$.*

Proof. See [6]. □

Fix a s.s. Drinfeld module ϕ over $\overline{\mathbb{F}}_\mathfrak{p}$, and denote $\Lambda = \mathrm{End}(\phi)$. Let I be a left integral Λ-ideal (i.e., I is a full A-lattice in $B_\mathfrak{p}$, $I \subseteq \Lambda$ and $\Lambda I \subseteq I$). To such an ideal one can associate another Drinfeld module $\phi^{(I)}$ and an isogeny $u_I : \phi \to \phi^{(I)}$ (since $\phi^{(I)}$ is isogenous to ϕ it is necessarily s.s.). Indeed, consider the group-scheme

$$H_I = \bigcap_{i \in I} \ker(i),$$

with the scheme-theoretic intersection taken inside of $\mathbb{G}_{a,\overline{\mathbb{F}}_\mathfrak{p}}$. It is easy to check that H_I satisfies the conditions in Lemma 2.4 , hence gives an isogeny u_I. We will denote $\ker(I) := H_I$.

Define the *norm* $\mathfrak{n}(u)$ *of the isogeny* u of ϕ by

$$\mathfrak{n}(u) = (\mathfrak{p})^{\mathrm{ht}(u)/\deg \mathfrak{p}} \cdot \chi(\ker(u)(\overline{\mathbb{F}}_\mathfrak{p})).$$

Theorem 2.6. *With previous notation, we have*

1. $\mathfrak{n}(u_I) = \mathrm{Nr}(I)$*;*
2. *Every isogeny from* ϕ *to another Drinfeld module has the form* u_I *for some left integral ideal* I *of* Λ*;*
3. $\mathrm{End}(\phi^{(I)}) \cong O_r(I)$*;*
4. *There is a one-to-one correspondence between the isomorphism classes of s.s. Drinfeld modules over* $\overline{\mathbb{F}}_\mathfrak{p}$ *and the left ideal classes in* $B_\mathfrak{p}$*;*
5. *All s.s. Drinfeld modules over* $\overline{\mathbb{F}}_\mathfrak{p}$ *are isogenous to each other.*

Proof. See [6, §§3-4]. □

Let Λ be a fixed maximal order in $B_\mathfrak{p}$, $\{I_1, \dots, I_n\}$ be integral representatives of distinct left ideal classes of Λ with $I_1 = \Lambda$. Denote $\Lambda_i = O_r(I_i)$. From Theorem 2.6 we know that there exist s.s. Drinfeld modules $\phi_1, \dots, \phi_n$ with $\phi_i \cong \phi_1^{(I_i)}$ and $\mathrm{End}(\phi_i) = \Lambda_i$. Denote $M_{ij} = I_j^{-1} I_i$. Since $O_r(I_j^{-1}) = \Lambda$, this is a lattice in $B_\mathfrak{p}$, and it is naturally a left Λ_j and right Λ_i module.

Proposition 2.7.

1. *There is an isomorphism*
$$M_{ij} \cong \mathrm{Hom}(\phi_i, \phi_j)$$
as left Λ_j *and right* Λ_i *modules.*
2. *If* $v_b : \phi_i \to \phi_j$ *is the isogeny corresponding to the non-zero element* $b \in M_{ij}$ *then*
$$\mathfrak{n}(v_b) = (\mathrm{Nr}(b)/m_{ij}),$$
where m_{ij} *is a generator of the fractional ideal* $\mathrm{Nr}(M_{ij})$*.*

Proof. Let $\alpha \in I_i$. Consider the endomorphism of $\phi := \phi_1$ induced by α. Since $\ker(\alpha) \supseteq \ker(I_i)$, $\alpha : \phi \to \phi$ must factor through u_{I_i}

$$\begin{tikzcd}
\phi \arrow[rr, "\alpha"] \arrow[dr, "u_{I_i}"'] & & \phi \\
& \phi_i \arrow[ur, "v_\alpha"'] &
\end{tikzcd}$$

where $v_\alpha \in \mathrm{Hom}(\phi_i, \phi)$. One easily checks that $\alpha \mapsto v_\alpha$ defines an injection $I_i \hookrightarrow \mathrm{Hom}(\phi_i, \phi)$ of left Λ and right Λ_i modules. Now let $v \in \mathrm{Hom}(\phi_i, \phi)$. The composite $v \circ u_{I_i}$ is an endomorphism w of ϕ. We claim that $w \in I_i$. Indeed, consider the left integral Λ-ideal generated by w and I_i, $\Lambda w + I_i$. We have $\ker(\Lambda w + I_i) = \ker(w) \cap \ker(I_i)$. Since by construction $\ker(w)$ contains $\ker(I_i)$, we get $\ker(\Lambda w + I_i) = \ker(I_i)$. Hence by Theorem 2.6 and Proposition 2.1, $w + I_i = I_i$, i.e., $w \in I_i$ as required. We conclude that the map $\alpha \mapsto v_\alpha$ constructed above is also surjective, in particular

$$I_i \cong \mathrm{Hom}(\phi_i, \phi). \tag{2.1}$$

Let I be a left integral Λ_j-ideal. The lattice $I_j I$ is a left Λ-ideal. We claim that

$$\phi^{(I_j I)} \cong \phi_j^{(I)}. \tag{2.2}$$

After scaling by an element of A, we can assume $I_j I$ is an integral Λ-ideal. Since $O_r(I_j) = \Lambda_j$ and $I \subseteq \Lambda_j$, we have $I_j I \subseteq I_j$. Hence $\ker(I_j I) \supseteq \ker(I_j)$, and

$$\ker(I_j I) \bmod \ker(I_j) \cong \ker(I).$$

We conclude $u_I \circ u_{I_j} = u_{I_j I}$, which is equivalent to the claim.

Now apply (2.1) with ϕ replaced by ϕ_j and ϕ_i replaced by $\phi_j^{(M_{ij})}$. (Here we consider M_{ij} as a left Λ_j-ideal.) We have

$$\begin{aligned} M_{ij} &\cong \mathrm{Hom}(\phi_j^{(M_{ij})}, \phi_j) \quad \text{(by (2.1))} \\ &\cong \mathrm{Hom}(\phi^{(I_j M_{ij})}, \phi_j) \quad \text{(by (2.2))} \\ &\cong \mathrm{Hom}(\phi^{(I_i)}, \phi_j) \quad \text{(by Proposition 2.1)} \\ &\cong \mathrm{Hom}(\phi_i, \phi_j), \end{aligned}$$

where all the isomorphisms are isomorphisms of left Λ_j and right Λ_i ideals.

To prove (2), consider the left principal ideal $\Lambda_j b$. The isogeny v_b is the isogeny for which $u_{\Lambda_j b} = v_b \circ u_{M_{ij}}$

$$\begin{tikzcd} \phi_j \arrow[rr, "u_{\Lambda_j b}"] \arrow[dr, "u_{M_{ij}}"'] & & \phi_j \\ & \phi_i \arrow[ur, "v_b"'] & \end{tikzcd}$$

From this it is easy to see that v_b is invariant under scaling M_{ij} by elements of A, so we can assume M_{ij} is an integral left Λ_j-ideal. Moreover,

$$\mathfrak{n}(v_b) = \mathfrak{n}(u_{\Lambda_j b}) / \mathfrak{n}(u_{M_{ij}}).$$

The claim follows from Theorem 2.6 and Proposition 2.1. Note that the expression $\mathrm{Nr}(b)/m_{ij}$ is invariant under scaling M_{ij} by elements of A. $\square$

2.3. **Brandt matrices.** Let $\phi_1, \phi_2, \dots, \phi_n$ be the isomorphism classes of s.s. Drinfeld modules over $\overline{\mathbb{F}}_\mathfrak{p}$ arranged in some fixed order. Let $\mathfrak{m}$ be any monic element of A. Let $b_{i,j}(\mathfrak{m})$ be the number of subgroup-schemes H of ϕ_i such that $u_H(\phi_i) = \phi_j$ and $\mathfrak{n}(u_H) = (\mathfrak{m})$. The $n \times n$ matrix $B(\mathfrak{m}) = (b_{i,j}(\mathfrak{m}))_{1 \le i,j \le n}$ is called the $\mathfrak{m}$-*th Brandt matrix*. Using Proposition 2.7, the Brandt matrices can also be defined using only the data of the quaternion algebra $B_\mathfrak{p}$.

Let $\mathcal{M} = \oplus_{i=1}^n \mathbb{Z} x_i$ be a free $\mathbb{Z}$-module of rank n, where x_i corresponds to ϕ_i, $1 \le i \le n$. For each $\mathfrak{m}$ we have $B(\mathfrak{m}) \in \mathrm{End}_\mathbb{Z}(\mathcal{M})$. Let $w_i = \#\mathrm{Aut}(\phi_i)/(q-1)$. It is known that w_i is equal either to 1 or $q+1$; c.f. [4]. Define a positive definite $\mathbb{Z}$-valued pairing

$$\begin{aligned} \langle , \rangle : \mathcal{M} \times \mathcal{M} &\to \mathbb{Z} \\ x_i, x_j &\mapsto \langle x_i, x_j \rangle = w_i \delta_{ij}, \end{aligned} \tag{2.3}$$

where δ_{ij} is the Kroneker symbol.

Theorem 2.8.

(1) *The row sums* $\sum_j b_{i,j}(\mathfrak{m})$ *are independent of* i *and are equal to*

$$\sigma_{\mathfrak{p}}(\mathfrak{m}) := \sum_{\substack{\mathfrak{m}' \text{monic} \\ \mathfrak{m}'|\mathfrak{m}, \mathfrak{p}\nmid \mathfrak{m}'}} q^{\deg(\mathfrak{m}')}.$$

(2) *The matrices* $\{B(\mathfrak{m}) \mid \mathfrak{m} \in A, \mathfrak{m}$ *monic*$\}$ *generate a commutative subring* $\mathbb{B}$ *of* $\mathrm{Mat}(n, \mathbb{Z})$.
(3) *The action of* $B(\mathfrak{m})$ *is symmetric with respect to the pairing* $\langle , \rangle$ *on* $\mathcal{M}$*, i.e., for* $e, e' \in \mathcal{M}$ *we have* $\langle B(\mathfrak{m})e, e'\rangle = \langle e, B(\mathfrak{m})e'\rangle$.
(4) *The commutative algebra* $\mathbb{B} \otimes_{\mathbb{Z}} \mathbb{Q}$ *is semi-simple and isomorphic to the product of totally real number fields.*

Proof. The proof is very similar to the proof of [11, Prop.2.7]. □

Remark 2.9. The traces of $B(\mathfrak{m})$'s are important arithmetic invariants, which will be related to the traces of Hecke operators on the Drinfeld modular curves in §3.

2.4. **Main technical calculation.** Let $\mathfrak{d}$ be an odd degree irreducible polynomial in A. Assume $\left(\frac{\mathfrak{d}}{\mathfrak{p}}\right) = -1$. Let $K = F(y)$, where $y^2 = \mathfrak{d}$. By Lemma 2.2 K embeds in $B_{\mathfrak{p}}$ and gives a decomposition $B_{\mathfrak{p}} = K \oplus Kj$, where $j^2 = c\mathfrak{p}$ for an appropriate $c \in \mathbb{F}_q^\times$, $j\alpha = \bar{\alpha}j$ for all $\alpha \in K$. Let Λ be a maximal order which contains $\mathcal{O}$, and let I be an integral ideal of $\mathcal{O}$. Consider a s.s. Drinfeld module ϕ over $\overline{\mathbb{F}}_{\mathfrak{p}}$ with endomorphism ring Λ. Since ΛI is a left Λ-ideal, we can form $\phi^{(\Lambda I)}$. The left ideal class of ΛI in $B_{\mathfrak{p}}$ depends on the ideal class $\mathcal{I} \in \mathrm{Pic}(\mathcal{O})$ of I rather than on I itself. Hence $\phi^{(\Lambda I)}$ is well-defined by $\mathcal{I}$ and we denote it by $\phi^{(\mathcal{I})}$. In this way we get an action of the group $\mathrm{Pic}(\mathcal{O})$ on the set of isomorphism classes of s.s. Drinfeld modules over $\overline{\mathbb{F}}_{\mathfrak{p}}$ whose endomorphism rings contain $\mathcal{O}$ under the above fixed embedding of K into $B_{\mathfrak{p}}$. (To see how $\mathcal{O}$ embeds in $\mathrm{End}(\phi^{(\mathcal{I})}) = \mathcal{O}_r(\Lambda I)$ note that $\mathcal{O}$ naturally acts on the right of ΛI.)

Now let Λ be a maximal order which contains $\mathcal{O} \oplus \mathcal{O}j$. Let $\mathcal{M} = \oplus_{i=1}^n \mathbb{Z}x_i$ be the free $\mathbb{Z}$-module defined in §2.3, and assume $\mathrm{End}(\phi_1) = \Lambda$. We have defined an action of $\mathrm{Pic}(\mathcal{O})$ on ϕ_1, which we can transport in a formal manner into an action on x_1. The image of x_1 under the action of ideals in the class $\mathcal{I}$ will be denoted by $x_{\mathcal{I}}$. We had an action of the $\mathbb{Z}$-algebra of Brandt matrices on $\mathcal{M}$. The main result of this subsection is the calculation of

$$\langle x_{\mathcal{J}}, B(\mathfrak{m})x_{\mathcal{I}\mathcal{J}}\rangle,$$

where $\langle \cdot, \cdot \rangle$ is the pairing in (2.3) and $B(\mathfrak{m}) \in \mathbb{B}$. From definitions

$$\langle x_{\mathcal{J}}, B(\mathfrak{m})x_{\mathcal{I}\mathcal{J}}\rangle = \frac{1}{q-1}\#\{u \in \mathrm{Hom}(x_{\mathcal{I}\mathcal{J}}, x_{\mathcal{J}}) \mid \mathfrak{n}(u) = (\mathfrak{m})\}. \tag{2.4}$$

Proposition 2.10. *Let* $\mathfrak{a}$ *and* $\mathfrak{b}$ *be integral ideals in classes* $\mathcal{I}$ *and* $\mathcal{J}$ *which are relatively prime to* $\mathcal{D} = (\sqrt{\mathfrak{d}})$. *We have a bijection*

$$\mathrm{Hom}(x_{\mathcal{I}\mathcal{J}}, x_{\mathcal{J}}) \cong \{\alpha + \beta j \mid \alpha \in \mathcal{D}^{-1}\mathfrak{a},\ \beta \in \mathcal{D}^{-1}\mathfrak{b}^{-1}\bar{\mathfrak{b}}\bar{\mathfrak{a}},\ \alpha \equiv \varepsilon\beta \pmod{\mathcal{O}_{\mathcal{D}}}\},$$

where $\varepsilon^2 \equiv c\mathfrak{p} \pmod{\mathfrak{d}}$. *If* u *corresponds to* $\alpha + \beta j$ *then*

$$\mathfrak{n}(u) = (\mathrm{Nr}_{K/F}(\alpha) + c\mathfrak{p}\mathrm{Nr}_{K/F}(\beta))/\mathrm{Nr}_{K/F}(\mathfrak{a}).$$

Here c *is the constant appearing in Lemma 2.2.*

Proof. By the definition of the action of $\mathrm{Pic}(\mathcal{O})$, the left ideal class of $x_{\mathcal{I}\mathcal{J}}$ is $\Lambda\mathfrak{a}\mathfrak{b}$, and similarly the left ideal class of $x_{\mathcal{J}}$ is $\Lambda\mathfrak{b}$. By Proposition 2.7

$$\mathrm{Hom}(x_{\mathcal{I}\mathcal{J}}, x_{\mathcal{J}}) \cong (\Lambda\mathfrak{b})^{-1}(\Lambda\mathfrak{a}\mathfrak{b}) = \mathfrak{b}^{-1}\Lambda\mathfrak{a}\mathfrak{b}.$$

From Lemma 2.3 we get the desired expression for $\mathrm{Hom}(x_{\mathcal{I}\mathcal{J}}, x_{\mathcal{J}})$. Indeed, the factors $\bar{\mathfrak{b}}\bar{\mathfrak{a}}$ are due to the relation $jx = \bar{x}j$ for all $x \in K$, and since we assumed $\mathfrak{a}$ and $\mathfrak{b}$ to be relatively prime to $\mathcal{D}$, locally at $\mathcal{D}$ these ideals are the unit ideals so the congruence relation is preserved.

The final statement of the proposition follows from Proposition 2.7. In fact, $\mathrm{Nr}(\alpha + \beta j) = \mathrm{Nr}_{K/F}(\alpha) + c\mathfrak{p}\mathrm{Nr}_{K/F}(\beta)$ and

$$\mathrm{Nr}(\mathfrak{b}^{-1}\Lambda\mathfrak{a}\mathfrak{b}) = \mathrm{Nr}_{K/F}(\mathfrak{b})^{-1}\mathrm{Nr}_{K/F}(\mathfrak{b})\mathrm{Nr}_{K/F}(\mathfrak{a}) = \mathrm{Nr}_{K/F}(\mathfrak{a}).$$

□

For an integral ideal $\mathfrak{a}$ of $\mathcal{O}$ and a fixed element $\lambda_0 \in A$ define

$$r_{\mathfrak{a},\lambda_0}(\lambda) = \#\{\mu \in \mathfrak{a} \mid \mathrm{Nr}_{K/F}(\mu) = \lambda_0\lambda\}.$$

Let L be an integral ideal of A. For an ideal class $\mathcal{A}$ of $\mathcal{O}$ define

$$r_{\mathcal{A}}(L) = \#\{\mathfrak{a} \in \mathcal{A} \mid \mathfrak{a} \text{ integral with } \mathrm{Nr}_{L/K}(\mathfrak{a}) = L\}.$$

and

$$R(L) = \sum_{\mathcal{A} \in \mathrm{Pic}(\mathcal{O})} r_{\mathcal{A}}(L).$$

For $0 \neq \mu \in A$, define

$$\sigma(\mu) = \begin{cases} q-1 & \text{if } \mu \equiv 0 \bmod \mathfrak{d}, \\ 1 & \text{otherwise.} \end{cases}$$

Let δ_z, $z \in F_\infty^\times$, be the local norm symbol at ∞, i.e., δ_z is equal to 1 if z is the norm of an element of $F_\infty(\sqrt{\mathfrak{d}})/F_\infty$ and -1 otherwise.

Proposition 2.11. *We have the equality*

$$\begin{aligned}\langle x_{\mathcal{J}}, B(\mathfrak{m})x_{\mathcal{I}\mathcal{J}}\rangle &= r_{\mathcal{I}^{-1}}((\mathfrak{d}\mathfrak{m})) \\ &+ \sum_{\substack{0 \neq \mu \in A \\ \deg\mu \leq \deg(\mathfrak{m}\mathfrak{d}) - \deg(\mathfrak{p})}} r_{\mathcal{I}^{-1}}((\mathfrak{d}\mathfrak{m} - \mathfrak{p}\mu)) \cdot r_{\mathcal{I}\mathcal{J}^2}((\mu)) \cdot \sigma(\mu)\frac{1 - \delta_{(\mathfrak{d}\mathfrak{m} - \mathfrak{p}\mu)\mathfrak{p}\mu}}{2}.\end{aligned}$$

Proof. Let $\mathfrak{a}$ be a fixed ideal of $\mathcal{I}$ and let $\lambda_0 \in A$ be a fixed generator of $\mathrm{Nr}_{K/F}(\mathfrak{a})$. By (2.4) and Proposition 2.10 we need to count the number of solutions to the identity

$$(\mathrm{Nr}_{K/F}(\alpha) + c\mathfrak{p}\mathrm{Nr}_{K/F}(\beta)) = (\mathfrak{m}\lambda_0), \tag{2.5}$$

with $\alpha \in \mathcal{D}^{-1}\mathfrak{a}$, $\beta \in \mathcal{D}^{-1}\mathfrak{b}^{-1}\bar{\mathfrak{b}}\bar{\mathfrak{a}}$, $\alpha \equiv \varepsilon\beta \pmod{\mathcal{O}_{\mathcal{D}}}$, where $\varepsilon^2 \equiv c\mathfrak{p} \pmod{\mathfrak{d}}$. Define

$$\nu := \mathrm{Nr}_{K/F}(\alpha)\mathfrak{d}\lambda_0^{-1} \in A, \quad \text{ and } \quad \mu := c\mathrm{Nr}_{K/F}(\beta)\mathfrak{d}\lambda_0^{-1} \in A.$$

Since $(\nu\lambda_0\mathfrak{d}^{-1} + \mathfrak{p}\lambda_0\mathfrak{d}^{-1}\mu) = (\mathfrak{m}\lambda_0)$, we are looking for ν and μ such that

$$(\nu + \mathfrak{p}\mu) = (\mathfrak{d}\mathfrak{m}).$$

This is equivalent to the existence of a unique $s \in \mathbb{F}_q$ such that $\nu = s\mathfrak{d}\mathfrak{m} - \mathfrak{p}\mu$. From the definition of ν, we must have $\mathrm{Nr}_{K/F}(\alpha) = (s\mathfrak{d}\mathfrak{m} - \mathfrak{p}\mu)\mathfrak{d}^{-1}\lambda_0$. The number of such α, with μ and s being fixed, is equal to $r_{\mathfrak{a},\lambda_0}(s\mathfrak{d}\mathfrak{m}-\mathfrak{p}\mu)$. To count the number of β's, consider the integral ideal

$$\mathcal{L}=(\beta)\mathcal{D}\mathfrak{b}\bar{\mathfrak{b}}^{-1}\bar{\mathfrak{a}}^{-1}.$$

We must have $\mathrm{Nr}_{K/F}(\mathcal{L})=(\mu)$. If $\mu=0$ then $\beta=0$, so we will assume $\mu\neq 0$. Since the ideal $\bar{\mathfrak{a}}\mathfrak{a}$ is principal, $\bar{\mathfrak{a}}$ is in $\mathcal{I}^{-1}$. Similarly $\bar{\mathfrak{b}}\in\mathcal{J}^{-1}$. As $\mathcal{D}=(\sqrt{\mathfrak{d}})$ is principal, we conclude that the ideal $\mathcal{L}$ lies in the class of $\mathcal{I}\mathcal{J}^2$. The number of integral ideals satisfying the last two properties is equal to $r_{\mathcal{I}\mathcal{J}^2}((\mu))$. If an element β exists at all, it is uniquely determined, up to a $\mathbb{F}_q^\times$ multiple, by the ideal $\mathcal{L}$. The existence of β is equivalent to $c^{-1}\mu\mathfrak{d}^{-1}\lambda_0$ being a norm of an element in K, and by Hasse's principle this last condition is equivalent to $c^{-1}\mu\mathfrak{d}^{-1}\lambda_0$ being a norm locally at all places of F. The element $\mathfrak{d}^{-1}=\mathrm{Nr}_{K/F}(\sqrt{\mathfrak{d}}^{-1})$ is a global norm, so we can ignore it. Since $(\mu\lambda_0)$ is the norm of the $\mathcal{O}$ integral ideal $\mathcal{L}\mathfrak{a}$, the element $c^{-1}\mu\lambda_0$ is a local norm at all finite places, and the existence of β is equivalent to $\delta_{c^{-1}\mu\lambda_0}=1$. Since our quaternion is ramified at ∞, we must have $\delta_{c\mathfrak{p}}=-1$. Thus, the existence of β is equivalent to $\delta_{\mathfrak{p}\mu\lambda_0}=-1$. Finally, we have to take into account the congruence relation between α and β. If μ is divisible by $\mathfrak{d}$, then α and β are integral at $\mathcal{D}$ and the congruence relation is satisfied for any choice of $\mathbb{F}_q^\times$ multiple of β. On the other hand, if μ is coprime to $\mathfrak{d}$, then there is a unique choice of a multiple of β, with α being fixed, for which the congruence holds. We conclude that for a given α the number of possible non-zero β's is

$$\sigma(\mu)\cdot r_{\mathcal{I}\mathcal{J}^2}((\mu))\frac{1-\delta_{\mathfrak{p}\mu\lambda_0}}{2}.$$

Hence

$$\begin{aligned}(q-1)\langle x_{\mathcal{J}},B(\mathfrak{m})x_{\mathcal{I}\mathcal{J}}\rangle &= \sum_{s\in\mathbb{F}_q^\times} r_{\mathfrak{a},\lambda_0}(s\mathfrak{d}\mathfrak{m})\\ &+\sum_{\substack{0\neq\mu\in A\\ \deg\mu\leq\deg(\mathfrak{m}\mathfrak{d})-\deg(\mathfrak{p})}}\sum_{s\in\mathbb{F}_q^\times} r_{\mathfrak{a},\lambda_0}(s\mathfrak{d}\mathfrak{m}-\mathfrak{p}\mu)\cdot r_{\mathcal{I}\mathcal{J}^2}((\mu))\cdot\sigma(\mu)\frac{1-\delta_{\mathfrak{p}\mu\lambda_0}}{2}.\end{aligned}$$

If $r_{\mathfrak{a},\lambda_0}(s\mathfrak{d}\mathfrak{m}-\mathfrak{p}\mu)\neq 0$ then $\lambda_0(s\mathfrak{d}\mathfrak{m}-\mathfrak{p}\mu)$ is a norm of an element in K. Hence $\delta_{\lambda_0(s\mathfrak{d}\mathfrak{m}-\mathfrak{p}\mu)}=\delta_{\lambda_0}\delta_{s\mathfrak{d}\mathfrak{m}-\mathfrak{p}\mu}=1$. In particular, $\delta_{\lambda_0}=\delta_{s\mathfrak{d}\mathfrak{m}-\mathfrak{p}\mu}$ and also $\delta_{\lambda_0\mathfrak{p}\mu}=\delta_{(s\mathfrak{d}\mathfrak{m}-\mathfrak{p}\mu)\mathfrak{p}\mu}$. Under the substitution $\mu\mapsto s\mu$ the expression $r_{\mathcal{I}\mathcal{J}^2}((\mu))\cdot\sigma(\mu)$ clearly remain invariant. The local norm symbol becomes $\delta_{(s\mathfrak{d}\mathfrak{m}-s\mathfrak{p}\mu)s\mathfrak{p}\mu}=\delta_{(\mathfrak{d}\mathfrak{m}-\mathfrak{p}\mu)\mathfrak{p}\mu}\delta_{s^2}=\delta_{(\mathfrak{d}\mathfrak{m}-\mathfrak{p}\mu)\mathfrak{p}\mu}$. Hence we have

$$\begin{aligned}(q-1)\langle x_{\mathcal{J}},B(\mathfrak{m})x_{\mathcal{I}\mathcal{J}}\rangle &= \sum_{s\in\mathbb{F}_q^\times} r_{\mathfrak{a},\lambda_0}(s\mathfrak{d}\mathfrak{m})\\ &+\sum_{\substack{0\neq\mu\in A\\ \deg\mu\leq\deg(\mathfrak{m}\mathfrak{d})-\deg(\mathfrak{p})}} r_{\mathcal{I}\mathcal{J}^2}((\mu))\cdot\sigma(\mu)\frac{1-\delta_{(\mathfrak{d}\mathfrak{m}-\mathfrak{p}\mu)\mathfrak{p}\mu}}{2}\sum_{s\in\mathbb{F}_q^\times} r_{\mathfrak{a},\lambda_0}(s(\mathfrak{d}\mathfrak{m}-\mathfrak{p}\mu)).\end{aligned}$$

It is easy to check that for $\lambda\in A$

$$\frac{1}{q-1}\sum_{s\in\mathbb{F}_q^\times} r_{\mathfrak{a},\lambda_0}(s\lambda)=r_{\mathcal{I}^{-1}}((\lambda)).$$

Finally, we get the desired expression

$$\langle x_{\mathcal{J}}, B(\mathfrak{m})x_{\mathcal{I}\mathcal{J}}\rangle = r_{\mathcal{I}^{-1}}((\mathfrak{d}\mathfrak{m}))$$
$$+ \sum_{\substack{0\neq\mu\in A\\ \deg\mu\leq\deg(\mathfrak{m}\mathfrak{d})-\deg(\mathfrak{p})}} r_{\mathcal{I}^{-1}}((\mathfrak{d}\mathfrak{m}-\mathfrak{p}\mu))\cdot r_{\mathcal{I}\mathcal{J}^2}((\mu))\cdot\sigma(\mu)\frac{1-\delta_{(\mathfrak{d}\mathfrak{m}-\mathfrak{p}\mu)\mathfrak{p}\mu}}{2}.$$

□

Corollary 2.12. *Let $h_{\mathcal{O}} := \#\mathrm{Pic}(\mathcal{O})$ be the class number of $\mathcal{O}$. There is an equality*

$$\sum_{\mathcal{J}\in\mathrm{Pic}(\mathcal{O})}\langle x_{\mathcal{J}}, B(\mathfrak{m})x_{\mathcal{I}\mathcal{J}}\rangle = h_{\mathcal{O}}\cdot r_{\mathcal{I}}((\mathfrak{d}\mathfrak{m}))$$
$$+ \sum_{\substack{0\neq\mu\in A\\ \deg\mu\leq\deg(\mathfrak{m}\mathfrak{d})-\deg(\mathfrak{p})}} r_{\mathcal{I}}((\mathfrak{d}\mathfrak{m}-\mathfrak{p}\mu))\cdot R((\mu))\cdot\sigma(\mu)\frac{1-\delta_{(\mathfrak{d}\mathfrak{m}-\mathfrak{p}\mu)\mathfrak{p}\mu}}{2}.$$

Proof. An integral ideal $\mathfrak{a}$ is in $\mathcal{I}$ if and only if its conjugate $\bar{\mathfrak{a}}$ is in $\mathcal{I}^{-1}$. Moreover, $\mathrm{Nr}_{K/F}(\mathfrak{a}) = \mathrm{Nr}_{K/F}(\bar{\mathfrak{a}})$, so we conclude that $r_{\mathcal{I}^{-1}} = r_{\mathcal{I}}$. Next, we claim that $\mathrm{Pic}(\mathcal{O})[2] = 1$. Assuming this for a moment, we get $\sum_{\mathcal{J}} r_{\mathcal{I}\mathcal{J}^2} = R$, and the corollary follows from Proposition 2.11.

It remains to show that $h_{\mathcal{O}}$ is odd. Let $C/\mathbb{F}_q$ be the smooth, projective, geometrically connected curve with function field K. This is a hyperelliptic curve, and by Hurwitz's formula its genus is equal to $(\deg\mathfrak{d}-1)/2$. Denote by J the Jacobian variety of C. There is an exact sequence

$$0\to J(\mathbb{F}_q)\to\mathrm{Pic}(\mathcal{O})\to\mathbb{Z}/d_\infty\mathbb{Z}\to 0,$$

where $d_\infty = [\mathbb{F}_\infty : \mathbb{F}_q]$. Since ∞ ramifies in K/F, $d_\infty = 1$. We get $\mathrm{Pic}(\mathcal{O})[2] = J[2](\mathbb{F}_q)$. Hence we are reduced to showing that J has no non-trivial $\mathbb{F}_q$-rational 2-torsion. Let $\mathfrak{d} = a\cdot\prod_{i=1}^d(t-b_i)$ be the decomposition of the polynomial $\mathfrak{d}$ over $\overline{\mathbb{F}}_q$, where $d = \deg(\mathfrak{d})$, $a\in\mathbb{F}_q^\times$ and $b_i\in\overline{\mathbb{F}}_q$, $1\leq i\leq d$. Denote by P_i the point on $C(\overline{\mathbb{F}}_q)$ corresponding to the solution $(b_i, 0)$ of $y^2 = \mathfrak{d}$, $1\leq i\leq d$. For the Weil divisor $D_i := P_i - \infty$ on C we have $2D_i = \mathrm{div}(t-b_i)$. Hence each D_i gives a 2-torsion point on J. There is one linear relation $\sum_{i=1}^d D_i = \mathrm{div}(y) = 0$ in $\mathrm{Div}^0(C)$, so D_i's generate $J[2]\cong(\mathbb{Z}/2)^{d-1}$. Since we are assuming $\mathfrak{d}$ is irreducible, non of these divisors is $\mathbb{F}_q$-rational. The claim follows. □

3. The analogue of Eichler's theorem

It is a classical result that certain theta series arising from quaternion algebras generate the space of modular forms of of weight 2 and prime level. This was conjectured by Hecke and proved by Eichler using a trace formula. In this section we will prove the analogue of Eichler's theorem over F. Our argument will be geometric – it uses the existence of Néron models of abelian varieties and integral models of Drinfeld modular curves. The idea of this proof is due to Matthew Emerton [3]. We start with recalling the necessary facts form the theory of Drinfeld automorphic forms.

3.1. **Harmonic cochains.** Denote the completion of F at ∞ by F_∞. Let R_∞ be the ring of integers in F_∞, and $\pi_\infty = t^{-1}$ be the uniformizer at ∞. Let $\mathcal{T}$ be the *Bruhat-Tits tree* of $\mathrm{PGL}_2(F_\infty)$. The oriented edges $Y(\mathcal{T})$ of $\mathcal{T}$ are parametrized by the set $\mathrm{GL}_2(F_\infty)/\mathcal{I}\cdot Z(F_\infty)$, where Z is the center of $\mathrm{GL}(2)$ and

$$\mathcal{I} := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(R_\infty) \;\middle|\; c \in (\pi_\infty) \right\}.$$

We denote by $X(\mathcal{T})$ the vertices of $\mathcal{T}$. For an edge $e \in Y$ we denote by $\bar{e}$, $t(e)$, $o(e)$ the inversely oriented edge, the terminus of e, and the origin of e, respectively. Multiplication from the *right* by $\begin{pmatrix} 0 & 1 \\ \pi & 0 \end{pmatrix}$ corresponds to the map $e \mapsto \bar{e}$ on $Y(\mathcal{T})$. The set $Y(\mathcal{T})$ can be represented as the union of two disjoint sets: the positively oriented edges

$$Y^+(\mathcal{T}) := \left\{ \begin{pmatrix} \pi_\infty^k & u \\ 0 & 1 \end{pmatrix} \;\middle|\; k \in \mathbb{Z}, u \in F_\infty/(\pi_\infty^k) \right\},$$

and the negatively oriented edges $Y^-(\mathcal{T}) = \{\bar{e} \mid e \in Y^+\}$. Denote $\Gamma_0(1) := \mathrm{GL}_2(A)$ and $\Gamma_\infty = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in \mathrm{GL}_2(A) \right\}$. For $\mathfrak{n} \in A$ let

$$\Gamma_0(\mathfrak{n}) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(1) \;\middle|\; c \in (\mathfrak{n}) \right\}.$$

be the *Hecke congruence subgroup* of level $\mathfrak{n}$ (it is clear that $\Gamma_0(\mathfrak{n})$ depends only on the ideal $(\mathfrak{n})$).

Let B be a subring of $\mathbb{C}$. Let Γ be a subgroup of $\Gamma_0(1)$; for example, $\Gamma = \Gamma_0(\mathfrak{n})$. Consider the following conditions on B valued functions of $Y(\mathcal{T})$:

(i) $\varphi(\bar{e}) = -\varphi(e)$ for any $e \in Y(\mathcal{T})$; functions satisfying this condition will be called *alternating*.
(ii) $\sum_{t(e)=v} \varphi(e) = 0$ for any $v \in X(\mathcal{T})$; functions satisfying this condition will be called *harmonic*.
(iii) $\varphi(\gamma e) = \varphi(e)$ for any $\gamma \in \Gamma$; functions satisfying this condition will be called Γ*-invariant*.
(iv) φ has compact (=finite) support modulo Γ.

We will denote by $\underline{\mathrm{H}}_!(\mathcal{T}, B)^\Gamma \subset \underline{\mathrm{H}}(\mathcal{T}, B)^\Gamma \subset \underline{\mathrm{H}}(\mathcal{T}, B)$ the spaces of B-valued functions on $Y(\mathcal{T})$ satisfying the conditions (i)-(iv), (i)-(iii), and (i)-(ii) respectively. The B-module $\underline{\mathrm{H}}(\mathcal{T}, B)$ is called the *space of B-valued harmonic cochains*.

3.2. **Fourier analysis.** The theory of Fourier analysis on $\mathcal{T}$ was developed by Weil in [24]. We follow the exposition in [8], which gives ∞-adic formulae.

Since Γ_∞ preserves the orientation on $\mathcal{T}$, we have $\Gamma_\infty \setminus Y^+(\mathcal{T}) = Y^+(\Gamma_\infty \setminus \mathcal{T})$. Any function on $Y^+(\mathcal{T})$, which is invariant under Γ_∞ acting on the left, can be regarded as a function on $Y^+(\Gamma_\infty \setminus \mathcal{T})$. Any such function has a Fourier expansion. Let β be a non-negative divisor of F,

$$\beta = (\alpha) \cdot \infty^{\deg \beta} = (\alpha)_f \cdot \infty^{\deg \beta - \deg \alpha},$$

where (α) is the principal divisor of $\alpha \in A$ with finite part $(\alpha)_f$.

If φ is a function on $Y^+(\Gamma_\infty \setminus \mathcal{T})$ then (see [8], (2.6) to (2.8))

$$\varphi\left(\begin{pmatrix} \pi_\infty^k & y \\ 0 & 1 \end{pmatrix}\right) = c_0(\varphi, \pi_\infty^k) + \sum_{\substack{\deg \alpha \leq k-2 \\ 0 \neq \alpha \in A}} c(\varphi, (\alpha) \cdot \infty^{k-2}) \psi_\infty(\alpha y),$$

where

$$c_0(\varphi, \pi_\infty^k) = \begin{cases} q^{1-k} \sum_{y \in (\pi_\infty)/(\pi_\infty^k)} \varphi\left(\begin{pmatrix} \pi_\infty^k & y \\ 0 & 1 \end{pmatrix}\right) & k \geq 1 \\ \varphi\left(\begin{pmatrix} \pi_\infty^k & 0 \\ 0 & 1 \end{pmatrix}\right) & k \leq 1, \end{cases} \tag{3.1}$$

$$c(\varphi, \beta) = q^{-1-\deg \beta} \sum_{y \in (\pi_\infty)/(\pi_\infty^{2+\deg \beta})} \varphi\left(\begin{pmatrix} \pi_\infty^{2+\deg \beta} & y \\ 0 & 1 \end{pmatrix}\right) \psi_\infty(-\alpha y),$$

and $\psi_\infty : F_\infty \mapsto \mathbb{C}^\times$ is $\sum a_i \pi_\infty^i \mapsto \psi(\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(a_{-1}))$ with ψ a non-trivial additive character of $\mathbb{F}_p$, for example, $\psi = \exp(\frac{2\pi i}{p})$.

Lemma 3.1. *Let φ be alternating and invariant under Γ_∞. Then φ is harmonic if and only if its Fourier coefficients satisfy:*

(i) *There exists a constant c such that $c_0(\varphi, \pi_\infty^k) = c \cdot q^{-k}$.*
(ii) *For any non-negative divisor $\beta = \beta_f \cdot \infty^k$, $c(\varphi, \beta) = c(\varphi, \beta_f) q^{-k}$.*

Proof. See [8, Lem.2.13]. □

3.3. **Eisenstein series.** Following [8, (5.4)], we say that the collection

$$\{c(\beta) \mid \beta \text{ is a positive divisor of } F\}$$

of Fourier coefficients is *eulerian* in the prime divisor $\wp$ with *Euler factor* $P(X) = 1 + a_1 X + \cdots + a_d X^d$ if the following holds: Write $P(X)^{-1} = \sum_{k \geq 0} b_k X^k$ as a formal power series. Then

$$c(\beta \cdot \wp^k) = c(\beta) \cdot b_k$$

whenever $\wp$ and β are coprime. For a divisor β define its norm $|\beta| = q^{\deg \beta}$.

Let $E : Y(\Gamma_\infty \setminus \mathcal{T}) \to \mathbb{C}$ be the unique alternating function defined by the collection of Fourier coefficients c_0, $c(\beta)$, where

(i) $c((1)) = 1$;
(ii) $c(\beta)$ is eulerian at finite primes $\wp$ with Euler factor

$$1 - (1 + |\wp|^{-1})X + |\wp|^{-1} X^2;$$

(iii) $c(\beta)$ is eulerian at ∞ with Euler factor $1 - q^{-1}X$;
(iv) $c_0(\pi_\infty^k) = -\frac{q^2}{q^2-1} q^{-k}$;

Let $\mathfrak{n} \in A$ be monic. Let $E_\mathfrak{n}$ the function on $Y(\mathcal{T})$ defined by

$$E_\mathfrak{n}(e) = E(e) - E\left(\begin{pmatrix} \mathfrak{n} & 0 \\ 0 & 1 \end{pmatrix} e\right).$$

We call $E_\mathfrak{n}$ the *Eisenstein series of level* $\mathfrak{n}$.

Proposition 3.2. $E_\mathfrak{n} \in \underline{H}(\mathcal{T}, \mathbb{C})^{\Gamma_0(\mathfrak{n})}$.

Proof. Since E is alternating, it is clear that $E_{\mathfrak{n}}$ is also alternating. Let $G(e) := E\left(\begin{pmatrix}\mathfrak{n} & 0\\ 0 & 1\end{pmatrix} e\right)$. By [8, Prop.2.10],

$$c(G,\beta) = c(E, \beta\cdot(\mathfrak{n})_f^{-1}) \quad \text{and} \quad c_0(G,\pi_\infty^k) = c_0(E, \pi_\infty^{k-\deg\mathfrak{n}}).$$

In particular, $c(G,\beta)=0$ if $\mathfrak{n} \not| \beta_f$; c.f. [8, Cor.2.11]. Hence $E_{\mathfrak{n}}$ is eulerian at ∞ (with the same Euler factor as E), and

$$\begin{aligned} c_0(E_{\mathfrak{n}},\pi_\infty^k) &= c_0(E,\pi_\infty^k) - c_0(E,\pi_\infty^{k-\deg\mathfrak{n}}) \\ &= \frac{q^2}{q^2-1}\left(q^{\deg\mathfrak{n}}-1\right)q^{-k}. \end{aligned} \tag{3.2}$$

By Lemma 3.1, $E_{\mathfrak{n}}$ is harmonic. Finally, that $E_{\mathfrak{n}}$ is $\Gamma_0(\mathfrak{n})$-invariant is proved in [8, Cor.6.3]. □

Remark 3.3. E may also be represented, up to a scalar factor, as conditionally convergent Eisenstein series $\sum_{\gamma\in\Gamma_\infty\setminus\Gamma_0(1)} \operatorname{sgn}(\gamma e) q^{-\kappa(\gamma e)}$, and where the summation has to be taken in a fixed order. Here $\kappa(e)$ is defined as follows: Given an edge e, either e or $\bar{e}$ is positively oriented, and hence is represented by $\begin{pmatrix}\pi_\infty^k & u\\ 0 & 1\end{pmatrix}$. Take $\kappa(e)=k$. The function $\operatorname{sgn}(e)$ is equal to ±1 depending on the orientation of e. The exponential $q^{-\kappa(e)}$ can be thought of as the analogue of $\operatorname{Im}(z)$ over the complex numbers.

For a function $\varphi\in\underline{\mathrm{H}}(\mathcal{T},\mathbb{C})^\Gamma$ there is a relation between being compactly supported modulo Γ and the Fourier coefficient $c_0(\varphi)$. If Γ is a congruence subgroup of $\Gamma_0(1)$ then the quotient graph $\Gamma\setminus\mathcal{T}$ is the edge-disjoint union of a finite graph $(\Gamma\setminus\mathcal{T})^0$ and a finite number of half-lines h_s labelled by the cusps $s\in\Gamma\setminus\mathbb{P}^1(F)$ of Γ. Hence the function φ is in $\underline{\mathrm{H}}_!(\mathcal{T},\mathbb{C})^\Gamma$ if and only if it vanishes on all h_s. One of h_s, namely the one corresponding to the orbit of $\infty=(1:0)\in\mathbb{P}^1(F)$, has a preimage in $\mathcal{T}$ given by the matrices $\begin{pmatrix}\pi_\infty^k & 0\\ 0 & 1\end{pmatrix}$, $k\le 1$. Since the values of φ on these matrices coincides with $c_0(\varphi,\pi_\infty^k)=c\cdot q^{-k}$, c.f. (3.1) and Lemma 3.1, φ vanishes on h_∞ if and only if the constant Fourier coefficient $c_0(\varphi)=0$. It is known [20] that $\Gamma_0(1)\setminus\mathcal{T}=h_\infty$. Hence for every $s\in\Gamma\setminus\mathbb{P}^1(F)$ there is $\gamma_s\in\Gamma_0(1)$ such that $\gamma_s s=\infty$, and φ will be compactly supported if and only if $c_0(\varphi\circ\gamma_s)=0$ for all s.

Proposition 3.4. *If $\mathfrak{p}\in A$ be a prime then*

$$\underline{\mathrm{H}}(\mathcal{T},\mathbb{C})^{\Gamma_0(\mathfrak{p})} = \mathbb{C}E_{\mathfrak{p}} \oplus \underline{\mathrm{H}}_!(\mathcal{T},\mathbb{C})^{\Gamma_0(\mathfrak{p})}.$$

Proof. Let $\Gamma:=\Gamma_0(\mathfrak{p})$. From what was said, we already know that the space on the right hand-side is a subspace of $\underline{\mathrm{H}}(\mathcal{T},\mathbb{C})^\Gamma$, and the sum is direct. The elements of $\underline{\mathrm{H}}(\mathcal{T},\mathbb{C})^\Gamma$ may be considered as alternating functions on $Y(\Gamma\setminus\mathcal{T})$ with the harmonicity condition being replaced by $\sum_{t(e)=v} m(e)\varphi(e)=0$. Here $m(e)$ are certain multiplicities that count how many edges of $\mathcal{T}$ are identified modulo Γ. Using these two conditions, it is not hard to check that if $\varphi\in\underline{\mathrm{H}}(\mathcal{T},\mathbb{C})^\Gamma$ vanishes on all but possibly one of the half-lines of $\Gamma\setminus\mathcal{T}$, then in fact it must be compactly supported (i.e., has to vanish on all of the half-lines).

It is known that $\Gamma\setminus\mathcal{T}$ has only two cusps; see, for example, [5]. If $\varphi\in\underline{\mathrm{H}}(\mathcal{T},\mathbb{C})^\Gamma$ then, by subtracting from φ an appropriate multiple of $E_{\mathfrak{n}}$, we can guarantee that

$c_0(\varphi - cE_\mathfrak{p}) = 0$. Hence $\varphi - cE_\mathfrak{p}$ vanishes on h_∞, and from the previous paragraph $\varphi - cE_\mathfrak{p} \in \underline{\mathrm{H}}_!(\mathcal{T}, \mathbb{C})^\Gamma$. $\square$

3.4. **Hecke operators.** In this subsection we put $\Gamma := \Gamma_0(\mathfrak{p})$ with $\mathfrak{p}$ prime. Most of the facts stated below hold true without any restrictions on the level. We restrict to prime level to avoid discussing old cusp forms, and have Proposition 3.4 available.

Let $\mathfrak{m}$ be a monic polynomial in A. For a function φ on $\mathrm{GL}_2(F_\infty)$ put

$$(T_\mathfrak{m}\varphi)(g) = \sum \varphi\left(\begin{pmatrix} a & b \\ 0 & d\end{pmatrix} g\right),$$

where the sum is over the triples (a, b, d) of A such that a, d are monic, $ad = \mathfrak{m}$, $(a, \mathfrak{p}) = 1$, and $\deg b < \deg d$. We call $T_\mathfrak{m}$ the $\mathfrak{m}$*-th Hecke operator.* These Hecke operators have the usual properties, c.f. [7], [9]:

(i) All $T_\mathfrak{m}$ commute;
(ii) If $\mathfrak{m}$ and $\mathfrak{m}'$ are coprime then $T_{\mathfrak{m}\mathfrak{m}'} = T_\mathfrak{m} T_{\mathfrak{m}'}$;
(iii) If $\mathfrak{q}$ is a prime distinct form $\mathfrak{p}$ then
$$T_{\mathfrak{q}^{n+1}} = T_{\mathfrak{q}^n} T_\mathfrak{q} - |\mathfrak{q}| T_{\mathfrak{q}^{n-1}};$$
(iv) $T_\mathfrak{m}$ preserves $\underline{\mathrm{H}}(\mathcal{T}, \mathbb{C})^\Gamma$.

Denote $\mathbb{T} := \mathbb{Z}[\dots, T_\mathfrak{m}, \dots]$ the $\mathbb{Z}$-algebra generated by the Hecke operators acting on $\underline{\mathrm{H}}(\mathcal{T}, \mathbb{C})^\Gamma$. Since $\mathbb{T}$ preserves the integral structure $\underline{\mathrm{H}}(\mathcal{T}, \mathbb{Z})^\Gamma$, and it is known that $\underline{\mathrm{H}}(\mathcal{T}, \mathbb{Z})^\Gamma$ is a finitely generated free $\mathbb{Z}$-module, $\mathbb{T}$ is a finitely generated free $\mathbb{Z}$-module. One can express the Fourier expansion of $T_\mathfrak{m}\varphi$ in terms of the Fourier expansion of φ in a usual manner. Since the Fourier coefficients of $E_\mathfrak{p}$ are eulerian, $E_\mathfrak{p}$ is a $\mathbb{T}$-eigenvector, with the eigenvalue of $T_\mathfrak{q}$, $(\mathfrak{p}, \mathfrak{q}) = 1$, being $1 + |\mathfrak{q}|$. It is also known that $\underline{\mathrm{H}}_!(\mathcal{T}, \mathbb{C})^\Gamma$ is preserved by $\mathbb{T}$ and has a basis of simultaneous $\mathbb{T}$-eigenforms; c.f. [7]. In particular, $\mathbb{T}_\mathbb{C} := \mathbb{T} \otimes \mathbb{C}$ is a semi-simple $\mathbb{C}$-algebra. We will denote the quotient of $\mathbb{T}$ acting faithfully on $\underline{\mathrm{H}}_!(\mathcal{T}, \mathbb{C})^\Gamma$ by $\mathbb{T}^0$, and the quotient acting faithfully on $\mathbb{C}E_\mathfrak{p}$ by $\mathbb{T}^E$. To abbreviate the notation, we put

$$M := \underline{\mathrm{H}}(\mathcal{T}, \mathbb{C})^\Gamma \quad \text{and} \quad S := \underline{\mathrm{H}}_!(\mathcal{T}, \mathbb{C})^\Gamma.$$

Theorem 3.5.

(i) *There is a bilinear perfect pairing* $\mathbb{T}_\mathbb{C} \times M \to \mathbb{C}$ *given by*
$$(T_\mathfrak{m}, \varphi) \mapsto c((T_\mathfrak{m}\varphi), (1)).$$
(ii) *The same pairing restricts to a perfect pairing* $\mathbb{T}^0_\mathbb{C} \times S \to \mathbb{C}$.

Proof. Part (ii) is proved in [7, Thm.3.17]. The same argument applied to the pairing $\mathbb{T}_\mathbb{C} \times M \to \mathbb{C}$ shows that if the pairing is not perfect then there is $\varphi \in M$ all whose Fourier coefficients are 0 except possibly for $c_0(\varphi)$. In that case $\varphi = c_0(\varphi)$. Hence by Lemma 3.1, up to a scalar multiple, $\varphi(e) = \mathrm{sgn}(e) q^{-\kappa(e)}$, where $\mathrm{sgn}(e)$ and $\kappa(e)$ are as in Remark 3.3. This function is in $\underline{\mathrm{H}}(\mathcal{T}, \mathbb{C})$ but it is not invariant under Γ, c.f. [8, (2.12) and (4.7)]. This gives a contradiction. $\square$

It is clear that there is an injection $\mathbb{T} \hookrightarrow \mathbb{T}^0 \oplus \mathbb{T}^E$ with finite cokernel.

3.5. **Hecke operators as correspondences.** Let, as in §3.4, $\mathfrak{p}$ be a monic prime. The functor which associates to an A-scheme W the set of isomorphism classes of pairs $(D, Z_\mathfrak{p})$, where D is a Drinfeld module of rank 2 over W and $Z_\mathfrak{p}$ is a $\mathfrak{p}$-cyclic subgroup of D, possesses a coarse moduli scheme $M_0(\mathfrak{p})/A$ of pure relative dimension 1. There is a canonical compactification $X_0(\mathfrak{p})$ of $M_0(\mathfrak{p})$. We refer to [2], [9], and [5] for the details.

Theorem 3.6.

(a) $X_0(\mathfrak{p})$ *is a proper, normal, irreducible scheme of pure relative dimension* 1 *over* $\mathrm{Spec}(A)$.
(b) $X_0(\mathfrak{p}) \to \mathrm{Spec}\ A\left[\mathfrak{p}^{-1}\right]$ *is smooth.*
(c) $X_0(\mathfrak{p})_F$ *is a smooth proper geometrically connected curve over* F.
(d) $X_0(\mathfrak{p})_{\overline{\mathbb{F}}_\mathfrak{p}}$ *is reduced and is a union of two copies of* $X_0(1)_{\overline{\mathbb{F}}_\mathfrak{p}} = \mathbb{P}^1_{\overline{\mathbb{F}}_\mathfrak{p}}$ *intersecting transversally at the points representing the isomorphism classes of super-singular Drinfeld modules. A super-singular point* x *on the first copy of* $\mathbb{P}^1_{\overline{\mathbb{F}}_\mathfrak{p}}$ *is glued to* $\tau^{\deg \mathfrak{p}}(x)$ *on the second copy.*

Proof. See [2] and [5]. □

Let $\mathcal{M} = \oplus_{i=1}^n \mathbb{Z}x_i$ be as in §2.3. Let $\deg : \mathcal{M} \to \mathbb{Z}$ be the $\mathbb{Z}$-linear map obtained by sending each x_i to $1 \in \mathbb{Z}$, and let $\mathcal{M}^0$ be the kernel of deg. Denote $\mathcal{M}_\mathbb{C} := \mathcal{M} \otimes_\mathbb{Z} \mathbb{C}$. The kernel of $\deg : \mathcal{M}_\mathbb{C} \to \mathbb{C}$ is $\mathcal{M}^0_\mathbb{C} := \mathcal{M}^0 \otimes_\mathbb{Z} \mathbb{C}$.

Using moduli interpretation, one can define Hecke correspondences $T_\mathfrak{m}$ on $X_0(\mathfrak{p})$, $\mathfrak{m} \in A$ is monic. As in the case of classical modular curves, the Hecke correspondences induce endomorphisms of $\mathcal{M}$ and $\mathcal{M}^0$. Moreover, the action of $T_\mathfrak{m} \in \mathrm{End}_\mathbb{Z}(\mathcal{M})$ is given by the Brandt matrix $B(\mathfrak{m})$. Hence the $\mathbb{Z}$-subalgebra of $\mathrm{End}(\mathcal{M})$ generated by the Hecke operators (as correspondences) is the algebra of Brandt matrices $\mathbb{B}$. In the case of classical modular curves all the previous statements are carefully explained in [15, pp. 18-22]; see also [17, pp. 443-445]. Since the arguments for Drinfeld modular curves are essentially the same, we will simply refer to *loc.cit.* for the proofs. Denote $\mathbb{B}_\mathbb{C} := \mathbb{B} \otimes_\mathbb{Z} \mathbb{C}$.

Theorem 3.7. *There is a canonical algebra isomorphism* $\mathbb{T}_\mathbb{C} \cong \mathbb{B}_\mathbb{C}$*, where on the left we have the subalgebra of* $\mathrm{End}_\mathbb{C}(M)$ *generated by the Hecke operators acting on* M*. This algebra isomorphism makes* M *and* $\mathcal{M}_\mathbb{C}$ *into isomorphic* $\mathbb{T}_\mathbb{C}$*-modules.*

Proof. By Theorem 2.8 (1), $\mathbb{B}$ preserves $\mathcal{M}^0$. Denote the quotients of $\mathbb{B}$ acting faithfully on $\mathcal{M}^0$ and $\mathcal{M}/\mathcal{M}^0 \cong \mathbb{Z}$ by $\mathbb{B}^0$ and $\mathbb{B}^E$, respectively. Let $J := \mathrm{Pic}^0_{X_0(\mathfrak{p})_F/F}$ be the Jacobian variety of $X_0(\mathfrak{p})_F$. Let $\mathcal{J}$ be the Néron model of J over $\mathrm{Spec}(A)$, and let $\mathcal{J}^0$ be the relative connected component of the identity of $\mathcal{J}$. Since $X_0(\mathfrak{p})$ has a degenerate $\mathbb{F}_\mathfrak{p}$-fibre, by the example 9.2/8 in [1], $\mathcal{J}^0_{\overline{\mathbb{F}}_\mathfrak{p}}$ is a split torus. Moreover, $\mathcal{M}^0 = \mathrm{Hom}_{\overline{\mathbb{F}}_\mathfrak{p}}(\mathcal{J}^0_{\overline{\mathbb{F}}_\mathfrak{p}}, \mathbb{G}_{m,\overline{\mathbb{F}}_\mathfrak{p}})$ is the character group of $\mathcal{J}^0_{\overline{\mathbb{F}}_\mathfrak{p}}$. By the Néron mapping property the endomorphisms of J act on $\mathcal{J}^0_{\overline{\mathbb{F}}_\mathfrak{p}}$, and this action is faithful since the reduction is toric. Thus, the subalgebra of $\mathrm{End}_F(J)$ generated by the Hecke operators as correspondences acts faithfully on $\mathcal{M}^0$.

By Drinfeld's fundamental theorem [2, Thm. 2], there is a canonical isomorphism

$$\mathrm{H}^1_{\mathrm{et}}(X_0(\mathfrak{p})_{F^{\mathrm{sep}}}, \overline{\mathbb{Q}}_\ell) \cong \underline{\mathrm{H}}_!(\mathcal{T}, \overline{\mathbb{Q}}_\ell)^{\Gamma_0(\mathfrak{p})} \otimes \mathrm{sp}, \tag{3.3}$$

where sp is the two-dimensional special ℓ-adic ($\ell \neq p$) representation of $\mathrm{Gal}(F_\infty^{\mathrm{sep}}/F_\infty)$. Moreover, this isomorphism is compatible with the action of Hecke operators. Since

$$\mathrm{End}_F(J) \otimes \overline{\mathbb{Q}}_\ell \hookrightarrow \mathrm{End}_{\mathrm{Gal} F^{\mathrm{sep}}/F}(\mathrm{H}^1_{\mathrm{et}}(X_0(\mathfrak{p})_{F^{\mathrm{sep}}}, \overline{\mathbb{Q}}_\ell)^\vee),$$

the Hecke correspondences generate a subalgebra in $\mathrm{End}_F(J)$ which is isomorphic to $\mathbb{T}^0$. The action of Hecke operators on $\mathcal{M}^0$ induced by the correspondences on $X_0(\mathfrak{p})$ is canonically isomorphic to the action induced by extending the action on J to $\mathcal{J}^0$. This last fact is proved in [15]. Hence the homomorphism

$$\begin{aligned} \mathbb{T}_{\mathbb{C}} &\to \mathbb{B}_{\mathbb{C}} \\ T_{\mathfrak{m}} &\mapsto B(\mathfrak{m}) \end{aligned} \tag{3.4}$$

restricts to an isomorphism $\mathbb{T}^0_{\mathbb{C}} \cong \mathbb{B}^0_{\mathbb{C}}$. (For all our practical purposes, we can fix an isomorphism $\overline{\mathbb{Q}}_\ell \cong \mathbb{C}$ and work with either of the fields.)

By Theorem 2.8 (1), $B(\mathfrak{m})$ acts on $\mathcal{M}/\mathcal{M}^0$ by multiplication by $\sigma_{\mathfrak{p}}(\mathfrak{m})$. The Hecke operator $T_{\mathfrak{m}}$ acts on the Eisenstein series $E_{\mathfrak{p}}$ with the same eigenvalue. Hence (3.4) restricts to an isomorphism $\mathbb{T}^E_{\mathbb{C}} \cong \mathbb{B}^E_{\mathbb{C}}$. Since $\mathbb{T}_{\mathbb{C}} = \mathbb{T}^0_{\mathbb{C}} \oplus \mathbb{T}^E_{\mathbb{C}}$, and $\mathbb{B}_{\mathbb{C}} = \mathbb{B}^0_{\mathbb{C}} \oplus \mathbb{B}^E_{\mathbb{C}}$, the claim follows. □

3.6. **Theta series.** We keep the notation of the previous subsections. Recall the pairing on $\mathcal{M}$ that we defined in §2.3: Let $w_i = \#\mathrm{Aut}(x_i)/(q-1)$, and define a positive definite $\mathbb{Z}$-valued pairing via the formula $\langle x_i, x_j \rangle = w_i \delta_{ij}$. This pairing extends to a bilinear pairing on $\mathcal{M}_{\mathbb{C}}$ and the action of $\mathbb{T}$ is symmetric with respect to this pairing; c.f. Theorem 2.8. Let $x, y \in \mathcal{M}_{\mathbb{C}}$ be two fixed elements. Define a set of Fourier coefficients by

$$c_0(\pi_\infty^k) = q^2 \cdot \deg x \cdot \deg y \cdot q^{-k},$$

and for a non-negative divisor $\beta = (\mathfrak{m})_f \cdot \infty^k$ of F, $\mathfrak{m} \in A$ monic, define

$$c(\beta) = \langle x, T_{\mathfrak{m}} y \rangle \cdot q^{-k}.$$

Let $\Theta_{x,y}$ be the unique alternating $\mathbb{C}$-valued function on $Y(\Gamma_\infty \setminus \mathcal{T})$ defined by the collection of these Fourier coefficients. By Lemma 3.1, $\Theta_{x,y} \in \underline{\mathrm{H}}(\mathcal{T}, \mathbb{C})$.

Proposition 3.8. $\Theta_{x,y} \in M$.

Proof. The function deg on $\mathcal{M}_{\mathbb{C}}$ is $\mathbb{C}$-linear. Hence $\Theta : (x, y) \mapsto \Theta_{x,y}$ is a bilinear homomorphism from $\mathcal{M}_{\mathbb{C}} \times \mathcal{M}_{\mathbb{C}}$ into $\underline{\mathrm{H}}(\mathcal{T}, \mathbb{C})$. Since $\mathcal{M}_{\mathbb{C}} = \oplus_{i=1}^n \mathbb{C} x_i$, we can assume $x = x_i$ for some fixed i. Consider the element $x_E := \sum_{i=1}^n x_i/w_i \in \mathcal{M}_{\mathbb{C}}$. The image of x_E in $\mathcal{M}_{\mathbb{C}}/\mathcal{M}^0_{\mathbb{C}}$ is clearly non-zero, hence it generates this one dimensional space. Every element $y \in \mathcal{M}_{\mathbb{C}}$ can be uniquely written as $y = c x_E + x_0$, where $c \in \mathbb{C}$ and $x_0 \in \mathcal{M}^0_{\mathbb{C}}$. It is enough to prove that Θ_{x_i, x_E} and Θ_{x_i, x_0} are in $\underline{\mathrm{H}}(\mathcal{T}, \mathbb{C})^\Gamma$. We have

$$\begin{aligned} T_{\mathfrak{m}} x_E &= \sum_{i=1}^n \frac{1}{w_i} T_{\mathfrak{m}} x_i = \sum_{i=1}^n \frac{1}{w_i} \sum_{j=1}^n b_{i,j}(\mathfrak{m}) x_j \\ &= \sum_{j=1}^n x_j \sum_{i=1}^n \frac{1}{w_i} b_{i,j}(\mathfrak{m}) = \sum_{j=1}^n x_j \sum_{i=1}^n \frac{1}{w_j} b_{j,i}(\mathfrak{m}) \\ &= \sum_{j=1}^n \frac{1}{w_j} x_j \sum_{i=1}^n b_{j,i}(\mathfrak{m}) = \sigma_{\mathfrak{p}}(\mathfrak{m}) \sum_{j=1}^n \frac{1}{w_j} x_j \\ &= \sigma_{\mathfrak{p}}(\mathfrak{m}) x_E. \end{aligned}$$

Hence $\langle x_i, T_\mathfrak{m} x_E\rangle = \sigma_\mathfrak{p}(\mathfrak{m})\langle x_i, x_E\rangle = \sigma_\mathfrak{p}(\mathfrak{m})$. In particular, for any non-negative divisor β we have $c(E_\mathfrak{p}, \beta) = c(\Theta_{x_i,x_E}, \beta)$. There is a mass-formula [4, (5.9)]:

$$\sum_{i=1}^{n} \frac{1}{w_i} = \frac{q^{\deg \mathfrak{p}} - 1}{q^2 - 1}.$$

Thus, using (3.2), we also get $c_0(\Theta_{x_i,x_E}, \pi_\infty^k) = q^2 \deg(x_E) q^{-k} = c_0(E_\mathfrak{p}, \pi_\infty^k)$. The final conclusion is that $\Theta_{x_i,x_E} = E_\mathfrak{p}$.

Now consider Θ_{x_i,x_0}. Since $\deg(x_0) = 0$, $c_0(\Theta_{x_i,x_0}) = 0$. The map $\mathbb{T}^0_\mathbb{C} \to \mathbb{C}$ defined by $T_\mathfrak{m} \mapsto \langle x_i, T_\mathfrak{m} x_0\rangle$ is a $\mathbb{C}$-linear homomorphism. By Theorem 3.5, Θ_{x_i,x_0} is in S. □

Theorem 3.9. *The set of theta series $\{\Theta_{x_i,x_j} \mid 1 \le i, j \le n\}$ generates M.*

Proof. We need to show that $\mathbb{T}_\mathbb{C}$-module homomorphism

$$\Theta : \mathcal{M}_\mathbb{C} \otimes_{\mathbb{T}_\mathbb{C}} \mathcal{M}_\mathbb{C} \to M$$

defined by $x_i, x_j \mapsto \Theta_{x_i,x_j}$ is surjective. The pairing $\langle\cdot,\cdot\rangle$ gives an isomorphism

$$\mathcal{M}_\mathbb{C} \cong \mathcal{M}_\mathbb{C}^\vee := \mathrm{Hom}_\mathbb{C}(\mathcal{M}_\mathbb{C}, \mathbb{C}).$$

By Theorem 3.5, we have an isomorphism $M \cong \mathrm{Hom}_\mathbb{C}(\mathbb{T}_\mathbb{C}, \mathbb{C})$. Composing this last isomorphism with Θ, and the duality induced by $\langle\cdot,\cdot\rangle$, we get a pairing

$$\mathcal{M}_\mathbb{C} \otimes_{\mathbb{T}_\mathbb{C}} \mathcal{M}_\mathbb{C}^\vee \to \mathrm{Hom}_\mathbb{C}(\mathbb{T}_\mathbb{C}, \mathbb{C}).$$

This map is surjective if and only if its dual

$$\mathbb{T}_\mathbb{C} \to \mathrm{Hom}_\mathbb{C}(\mathcal{M}_\mathbb{C} \otimes_{\mathbb{T}_\mathbb{C}} \mathcal{M}_\mathbb{C}^\vee, \mathbb{C}) = \mathrm{Hom}_{\mathbb{T}_\mathbb{C}}(\mathcal{M}_\mathbb{C}, \mathcal{M}_\mathbb{C})$$

is injective. It is not hard to check that this last homomorphism coincides with the homomorphism induced by the natural action of $\mathbb{T}$ on $\mathcal{M}$. Since this action is faithful, the map is indeed injective. □

4. The analogue of a formula of Gross

In this section we will use the results of previous sections to prove the analogue of Prop. 11.2 in [11] over F.

4.1. **L-series of cusp forms.** Let, as in §3, $\Gamma := \Gamma_0(\mathfrak{p})$. Recall that the space $S := \underline{\mathrm{H}}_!(\mathcal{T}, \mathbb{C})^\Gamma$ is a space of functions on the set

$$Y(\Gamma \setminus \mathcal{T}) := \Gamma \setminus \mathrm{GL}_2(F_\infty)/\mathcal{I} \cdot Z(F_\infty),$$

and as such has a natural interpretation as a space of automorphic forms in the sense of Jacquet-Langlands. We will call S the space of *Drinfeld cusp forms.* It is known that $\dim_\mathbb{C} S$ is equal to the genus of $X_0(\mathfrak{p})_F$; c.f. (3.3).

The Haar measure on the locally compact group $\mathrm{GL}_2(F_\infty)$ induces a measure d on $Y(\Gamma \setminus \mathcal{T})$. Let $e \in Y(\mathcal{T})$, and let $\mathrm{Stab}_\Gamma(e) = \{\gamma \in \Gamma \mid \gamma(e) = e\}$ be the stabilizer of e in Γ. The group $\mathrm{Stab}_\Gamma(e)$ is finite. One can take

$$d(\tilde{e}) = \frac{q-1}{2}(\#\mathrm{Stab}_\Gamma(e))^{-1},$$

where e is a preimage of $\tilde{e} \in Y(\Gamma \setminus \mathcal{T})$ in $Y(\mathcal{T})$. From now on we will assume that the measure d is fixed as above. Let $\varphi, \phi \in M$, with $\varphi \in S$. We define the *Petersson product* with respect to measure $d(e)$ by

$$(\varphi, \phi) := \sum_{e \in Y(\Gamma \setminus \mathcal{T})} \varphi(e)\overline{\phi}(e)d(e).$$

Since φ has finite support, (φ, ϕ) is a finite sum. It is known that the action of the Hecke operators is self-adjoint with respect to the Petersson product.

Following Weil, one can attach an L-series to a cusp form. Define

$$L(\varphi, s) = \sum_{\beta \text{ pos. div.}} c(\varphi, \beta)|\beta|^{-s},$$

where $|\beta| = q^{\deg \beta}$ denotes the norm of the divisor β, and the sum is over all non-negative divisors of F, including those with an ∞-component.

We will say that $\varphi \in S$ is a *normalized eigenform* if it is an eigenform for all Hecke operators and $c(\varphi, (1)) = 1$. Since we are assuming $\mathfrak{p}$ is prime and it is known that $\dim_{\mathbb{C}} \underline{\mathrm{H}}_!(\mathcal{T}, \mathbb{C})^{\Gamma_0(1)} = 0$, the space S has a basis consisting of $\mathbb{T}$-eigenforms. The Fourier coefficients of a normalized eigenform φ are eulerian. Hence the L-function of φ has Euler product expansion

$$L(\varphi, s) = \prod_v \left(1 - \frac{a_v}{|v|^s}\right)^{-1} \left(1 - \frac{b_v}{|v|^s}\right)^{-1},$$

where the product is over all places of F (including ∞), and for $v \not| \mathfrak{p} \cdot \infty$, $a_v = \bar{b}_v$, $|a_v| = |b_v| = 1$.

4.2. **Main identity.** In this subsection f will be a fixed normalized eigenform in S. We will denote $c(f, \beta)$ simply by $c(\beta)$. Note that $c_0(\pi_\infty^k) = 0$ for all k as f is a cusp-form.

Let, as in §2.4, $\mathfrak{d}$ be an odd degree irreducible polynomial in A. Assume $\left(\frac{\mathfrak{d}}{\mathfrak{p}}\right) = -1$, so $K := F(\sqrt{\mathfrak{d}}) \hookrightarrow B_\mathfrak{p}$. Without loss of generality we can assume that $\Lambda = \mathrm{End}(x_1)$ is the maximal order in Lemma 2.3. We had an action of $\mathrm{Pic}(\mathcal{O})$ on x_1, and denoted the image of x_1 under the action of ideals in the class $\mathcal{I}$ by $x_\mathcal{I}$. Define

$$H_K := \sum_{\mathcal{I} \in \mathrm{Pic}(\mathcal{O})} x_\mathcal{I}.$$

$H_K \in \mathcal{M}$ has degree $\#\mathrm{Pic}(\mathcal{O})$.

Let $\mathcal{A} \in \mathrm{Pic}(\mathcal{O})$. We can consider the finite part β_f of the non-negative divisor β as an ideal in A. Define

$$L(f, \mathcal{A}, s) = \sum_{\beta \text{ pos. div.}} c(\beta) r_\mathcal{A}(\beta_f)|\beta|^{-s}$$

and

$$L^{(\mathfrak{p},\mathfrak{d})}(s) = \frac{1}{q-1} \sum_{\substack{\lambda \in A \\ (\lambda, \mathfrak{p})=1}} \left(\frac{\mathfrak{d}}{\lambda}\right) q^{-s \deg \lambda}.$$

Here $\left(\frac{\mathfrak{d}}{\lambda}\right)$ denotes the Jacobi symbol. The series $L^{(\mathfrak{p},\mathfrak{d})}(2s+1)L(f, \mathcal{A}, s)$ admits a holomorphic continuation to the whole complex plane and satisfies a functional equation [18, Thm.2.7.3]. Finally, define

$$L_K(f,s) = \sum_{\mathcal{A}\in \mathrm{Pic}(\mathcal{O})} L^{(\mathfrak{p},\mathfrak{d})}(2s+1)L(f,\mathcal{A},s).$$

We will be interested in the special value of this function at the center $s=0$ of the critical strip. Let $\Theta_K := \Theta_{H_K,H_K} \in M$ be the theta series we have constructed in §3.6.

Theorem 4.1.

$$L_K(f,0) = 2q^{-\frac{1+\deg \mathfrak{d}}{2}}(f,\Theta_K).$$

Proof. Using Corollary 2.12, we can explicitly compute the Fourier coefficients of Θ_K. Using Rankin's method, in [18] the authors show that $L_K(f,0)$ is equal, up to an explicit constant, to the Petersson product of f and some $G \in M$. Moreover, by unfolding the Rankin's integral, they are able to compute explicitly the Fourier coefficients of G; see [18, Lem. 2.7.1 and Prop. 2.7.2]. The theorem follows from the comparison of the Fourier coefficients of G and Θ_K. □

If $f_1, f_2, \dots, f_{n-1}$ is the basis of S consisting of normalized $\mathbb{T}$-eigenforms then

$$M = \mathbb{C}E_{\mathfrak{p}} \oplus \mathbb{C}f_1 \oplus \cdots \oplus \mathbb{C}f_{n-1}$$

is a decomposition into eigenspaces. By Theorem 3.7, M and $\mathcal{M}_{\mathbb{C}}$ are isomorphic $\mathbb{T}$-modules, so we have a similar decomposition

$$\mathcal{M}_{\mathbb{C}} = \mathcal{M}^E \oplus \mathcal{M}^{f_1} \oplus \cdots \oplus \mathcal{M}^{f_{n-1}}.$$

Let $H_f \in \mathcal{M}_{\mathbb{C}}$ be a non-zero element in the f-isotypical component $\mathcal{M}^f$.

Corollary 4.2.

$$L_K(f,0) = 2q^{-\frac{1+\deg \mathfrak{d}}{2}}(f,f)\frac{\langle H_f, H_K\rangle^2}{\langle H_f, H_f\rangle}.$$

In particular, $L_K(f,0)=0$ *if and only if* $\langle H_f, H_K\rangle = 0$.

Proof. Let H_{K,f_i} be the projection of H_K into $\mathcal{M}^{f_i}$, so we can write

$$H_K = H_{K,E} + \sum_{i=1}^{n-1} H_{K,f_i}.$$

Since the action of $\mathbb{T}$ is symmetric with respect to $\langle\cdot,\cdot\rangle$ and we have a multiplicity one theorem for M (i.e., two $\mathbb{T}$-eigenforms having the same eigenvalues for all $T_{\mathfrak{m}}$ must differ by a non-zero scalar multiple), it is clear that $\langle H_K, H_f\rangle = \langle H_{K,f}, H_f\rangle$. Hence

$$H_{K,f} = \frac{\langle H_f, H_K\rangle}{\langle H_f, H_f\rangle}H_f.$$

It is enough to show

$$L_K(f,0) = 2q^{-\frac{1+\deg \mathfrak{d}}{2}}(f,f)\langle H_{K,f}, H_{K,f}\rangle.$$

As we mentioned, the action of Hecke operators is self-adjoint with respect to the Petersson norm. Thus, by repeating the above argument, we need to show that in Theorem 4.1 the f-isotypical component of Θ_K is $\langle H_{K,f}, H_{K,f}\rangle f$. The map $\Theta : \mathcal{M}_{\mathbb{C}} \times \mathcal{M}_{\mathbb{C}} \to M$ in Theorem 3.9 is $\mathbb{T}$-bilinear, so $\Theta_{H_{K,E},H_{K,f_i}} = 0$ and $\Theta_{H_{K,f_j},H_{K,f_i}} = 0$ unless $i=j$. Hence, as one easily checks, the f-isotypical component is $\Theta_{H_{K,f},H_{K,f}}$. On the other hand, the Fourier coefficients of $\Theta_{H_{K,f},H_{K,f}}$ are given by $c(\Theta_{H_{K,f},H_{K,f}},\beta)=\langle H_{K,f},H_{K,f}\rangle c(f,\beta)$. That is,

$$\Theta_{H_{K,f},H_{K,f}}=\langle H_{K,f},H_{K,f}\rangle f,$$

as was required. □

5. Applications to elliptic curves

In this section we compare the formula in Corollary 4.2 with the formula of Birch and Swinnerton-Dyer (BSD). First we recall a special case of the statement of the BSD conjecture for elliptic curves over function fields.

5.1. **Formula of Birch and Swinnerton-Dyer.** Let C be a smooth projective geometrically connected curve over $\mathbb{F}_q$. Denote the function field of C by $K=\mathbb{F}_q(C)$, and its genus by $g(C)$. For each place v of K denote by $\mathcal{O}_v$ the ring of integers of the completion K_v, and denote the residue field by k_v.

Let E be a non-isotrivial elliptic curve over K. Denote by $\mathcal{E}$ the Néron model of E over C. Denote by $\mathcal{E}^0$ be the relative connected component of the identity of $\mathcal{E}$. Let $\mathcal{E}_v:=\mathcal{E}\times k_v$ and $\mathcal{E}_v^0:=\mathcal{E}^0\times k_v$. The group of connected components $\Phi_{E,v}=\mathcal{E}_v/\mathcal{E}_v^0$ of E at v is a finite étale group-scheme over k_v. The *Tamagawa number* $c_v(E)$ of E at v is the order of the subgroup $\Phi_{E,v}(k_v)$ of k_v-rational points in $\Phi_{E,v}(\bar{k}_v)$. The group $\Phi_{E,v}$ is trivial at almost all places (for example, it is trivial at the places where E has good reduction), hence almost all $c_v=1$. Let $\Omega^1_{\mathcal{E}/C}$ be the relative canonical sheaf on $\mathcal{E}$, and denote its restriction to the relative zero section by $\Omega^1_{\mathcal{E}/C}|_O$. Define

$$\tau(E/K)=\prod_v c_v(E)\cdot\left(q^{-\deg(\Omega^1_{\mathcal{E}/C}|_O)}\right)\cdot q^{1-g(C)}.$$

Assume that the L-function of E does not vanish at 1, $L(E,1)\neq 0$. Tate proved [23] (see also [14]) that $E(K)$ and the Tate-Shafarevich group $Ш(E/K)$ of E over K are finite, and

$$L(E,1)=\frac{\tau(E/K)\cdot\#Ш(E/K)}{\#E(K)^2}. \tag{5.1}$$

5.2. **Modular elliptic curves.** Let, as we have been denoting, $F=\mathbb{F}_q(t)(=\mathbb{F}_q(\mathbb{P}^1_{\mathbb{F}_q}))$. Let E be an elliptic curve over F of conductor $(\mathfrak{p})\cdot\infty$, where $(\mathfrak{p})\subset A$ is a prime ideal. Moreover, we assume that E has a split multiplicative reduction at ∞. In this situation it is known that E can be realized as a quotient of the Drinfeld modular curve $X:=X_0(\mathfrak{p})_F$; c.f. [9]. We will assume that the morphism $\pi: X\to E$ is chosen to have the minimal possible degree. Let $J:=\mathrm{Pic}^0_{X/F}$ be the Drinfeld Jacobian. By Albanese functoriality, π induces a homomorphism of $\pi_*: J\to E$, and by Picard functoriality, it induces a homomorphism $\pi^*: E\to J$. The composition $\pi_*\circ\pi^*$ is the endomorphism of E given by multiplication by $\deg(\pi)$.

Next, let $\mathcal{J}$ be the Néron model of J over $\mathbb{P}^1_{\mathbb{F}_q}$, and let $\mathcal{J}^0$ be the relative connected component of the identity of $\mathcal{J}$. As we already mentioned in §3.5, it can be shown that $\mathcal{M}^0=\mathrm{Hom}_{\overline{\mathbb{F}}_\mathfrak{p}}(\mathcal{J}^0_{\overline{\mathbb{F}}_\mathfrak{p}},\mathbb{G}_{m,\overline{\mathbb{F}}_\mathfrak{p}})$ is the character group of $\mathcal{J}^0_{\overline{\mathbb{F}}_\mathfrak{p}}$. Moreover, the pairing (2.3) on $\mathcal{M}$ restricted to $\mathcal{M}^0$ is *Grothendieck's monodromy pairing*; see [12], [17], [15, pp.16-18].

The curve E has a multiplicative reduction at $\mathfrak{p}$. Let $\mathcal{E}$ be its Néron model over $\mathbb{P}^1_{\mathbb{F}_q}$, and let $\Upsilon = \mathrm{Hom}_{\overline{\mathbb{F}}_\mathfrak{p}}(\mathcal{E}^0_{\overline{\mathbb{F}}_\mathfrak{p}}, \mathbb{G}_{m,\overline{\mathbb{F}}_\mathfrak{p}})$ be the character group at $\mathfrak{p}$. Then $\Upsilon \cong \mathbb{Z}$. There is a functorial homomorphism $\pi^* : \Upsilon \to \mathcal{M}^0$. Choose a generator ρ of Υ and denote $H_E := \pi^*(\rho)$. It is clear that H_E is well-defined up to a sign.

Lemma 5.1. *With previous notation,*

$$\deg(\pi) \cdot \#\Phi_{E,\mathfrak{p}} = \langle H_E, H_E \rangle.$$

Proof. This follows from the functorial properties of the monodromy pairing and Thm.11.5 in [12]. □

There is a unique normalized eigenform $f \in S$ corresponding to E. The L-series of E and f satisfy $L(E, s+1) = L(f, s)$; see [9], [7]. Let $K = F(\sqrt{\mathfrak{d}})$ be as in §4.2. Let $E_K := E \otimes_F K$ be the elliptic curve E over K. We also have $L(E_K, s+1) = L_K(f, s)$. Finally, one can take H_f to be H_E. The following is known [7]

$$\deg(\pi) \cdot \#\Phi_{E,\infty} = (f, f).$$

Hence we can rewrite the formula in Corollary 4.2 as

$$L(E_K, 1) = 2q^{-\frac{1+\deg \mathfrak{d}}{2}} \frac{\#\Phi_{E,\infty}}{\#\Phi_{E,\mathfrak{p}}} \langle H_E, H_K \rangle^2. \tag{5.2}$$

The nonsingular complete curve $C/\mathbb{F}_q$ such that $\mathbb{F}_q(C) = K$ is a hyperelliptic curve of genus $g(C) = (\deg \mathfrak{d} - 1)/2$. By construction, the prime $(\mathfrak{p})$ stays inert in K. Since E has multiplicative reduction at $\mathfrak{p}$, E_K necessarily will have split multiplicative reduction at $\mathfrak{p}$. Thus, the Tamagawa number $c_\mathfrak{p}(E_K) = \#\Phi_{E,\mathfrak{p}}$. The prime at ∞ ramifies in K, hence $c_\infty(E_K) = 2\#\Phi_{E,\infty}$. Since E_K has good reduction away form $\mathfrak{p}$ and ∞, we get

$$\tau(E/K) = 2\#\Phi_{E,\mathfrak{p}}\#\Phi_{E,\infty} \cdot \left(q^{-\deg(\Omega^1_{\mathcal{E}_K/C}|O)}\right) \cdot q^{\frac{3-\deg \mathfrak{d}}{2}}.$$

If we assume $\langle H_E, H_K \rangle \neq 0$, so that $L(E_K, 1) \neq 0$, then we can rewrite (5.1) for E_K as

$$L(E_K, 1) = 2\#\Phi_{E,\mathfrak{p}}\#\Phi_{E,\infty} \cdot \left(q^{-\deg(\Omega^1_{\mathcal{E}_K/C}|O)}\right) \cdot \left(q^{\frac{3-\deg \mathfrak{d}}{2}}\right) \cdot \frac{\#\text{Ш}(E/K)}{\#E(K)^2}. \tag{5.3}$$

Let $E_\mathfrak{d}$ be the twist of E by the quadratic character of $\mathrm{Gal}(K/F)$.

Proposition 5.2. *If $L(E_K, 1) \neq 0$ then $E(K) = E(F)$.*

Proof. By Tate's theorem [23], the assumption $L(E_K, 1) \neq 0$ implies $E(K)$ is finite. Obviously $E(F)$ will also be finite, and we need to prove the equality of torsion groups $E(F)$ and $E(K)$. Let m be an integer coprime to the characteristic p of F. Let $F_m := F(E[m])$ be the smallest subextension of F^{sep} over which the finite étale group-scheme $E[m]$ is constant. Since E has good reduction at $\mathfrak{d}$, by Néron-Ogg-Shafarevich criterion [21] the extension F_m/F is unramified at $\mathfrak{d}$ if $m \geq 3$. This immediately implies $E(F)[m] = E(K)[m]$ for all $m \geq 3$ coprime to p. Hence we need to prove $E(F)[2] = E(K)[2]$ and $E(F)[p^n] = E(K)[p^n]$ for all $n \geq 1$.

To prove the first statement, consider $E[2] - \{O\}$, an étale F-scheme of order 3. If this is irreducible, i.e., $E(F)[2] = 1$, it certainly cannot acquire a rational point over the quadratic extension K/F. Thus, we may assume it is reducible but not constant (i.e., $E(F)[2] = \mathbb{Z}/2$). Let Δ be the minimal discriminant of E/F. Since p is odd, the quadratic field extension F_2 of F must contain $F(\sqrt{\Delta})$. (This follows from the fact that if E is given in terms of a Weierstrass equation $y^2 = x^3 + ax^2 + bx + c$ then the 2-torsion points besides O are exactly the points with $y = 0$ and Δ is essentially the discriminant of the cubic on the right hand side.) Hence F_2 ramifies at $(\mathfrak{p})$, as (Δ) is a power of $(\mathfrak{p})$ (here we are using the fact that the finite part of the conductor of E is $\mathfrak{p}$). The only prime of A which ramifies in K is $(\mathfrak{d}) \neq (\mathfrak{p})$. In particular, F_2 and K are disjoint and we conclude $E(F)[2] = E(K)[2] = \mathbb{Z}/2$.

Since p is odd, we have the eigenspace decomposition on p-primary parts

$$E(K)_p = E(F)_p \times E_{\mathfrak{d}}(F)_p$$

under the action of the non-trivial involution generating $\mathrm{Gal}(K/F)$. Thus, it is enough to show that $E_{\mathfrak{d}}(F)[p] = 1$. Let $\mathcal{E}$ be the Néron model of $E_{\mathfrak{d}}$ over A. There is the identity on L-functions $L(E_K, s) = L(E, s)L(E_{\mathfrak{d}}, s)$. Our assumption clearly implies $L(E, 1) \neq 0$. In particular, the sign of the functional equation of $L(E, s)$ must be $+1$. Since the reduction of E at ∞ is split multiplicative, the local root number of E at ∞ is $+1$. Thus, the local root number at $\mathfrak{p}$ also must be $+1$. We conclude that the reduction of E at $\mathfrak{p}$ is split, and since $\mathfrak{p}$ is inert in K, $E_{\mathfrak{d}}$ has non-split multiplicative reduction at $\mathfrak{p}$. Hence $\mathrm{Frob}_{\mathfrak{p}}$ induces a *non-trivial* automorphism of $\mathcal{E}^0_{\mathbb{F}_{\mathfrak{p}}}$ such that $\mathrm{Frob}^2_{\mathfrak{p}} = 1$. This implies that the action of $\mathrm{Frob}_{\mathfrak{p}}$ on the character group of $\mathcal{E}^0_{\mathbb{F}_{\mathfrak{p}}}$ is by -1. By [12, Thm.11.5], the same is true for the action on the finite cyclic group $\Phi_{E_{\mathfrak{d}},\mathfrak{p}}(\overline{\mathbb{F}}_{\mathfrak{p}})$. Hence $\Phi_{E_{\mathfrak{d}},\mathfrak{p}}(\mathbb{F}_{\mathfrak{p}}) = 1$ or $\mathbb{Z}/2$. Now suppose $E_{\mathfrak{d}}(F)[p] = \mathbb{Z}/p$. Denote the completion of A at $\mathfrak{p}$ by R, and denote the fraction field of R by L. The Néron model of $E_{\mathfrak{d}}$ over R is $\mathcal{E}_R := \mathcal{E} \times_A R$. The group-scheme $G_L = E_{\mathfrak{d}}(F)[p]$ is étale and constant. Let G be the schematic closure of G_L in $\mathcal{E}_R$. This is a finite flat group-scheme over R whose closed fibre $G_{\mathbb{F}_{\mathfrak{p}}}$ is either étale or multiplicative, since $\mathcal{E}_{\mathbb{F}_{\mathfrak{p}}}$ is an extension of the finite (cyclic) étale group scheme $\Phi_{E_{\mathfrak{d}},\mathfrak{p}}$ by the torus $\mathbb{G}_{m,\mathbb{F}_{\mathfrak{p}}}$. By Lemma 5.3, $G_{\mathbb{F}_{\mathfrak{p}}}$ must be an étale constant group scheme. This implies $\Phi_{E_{\mathfrak{d}},\mathfrak{p}}(\mathbb{F}_{\mathfrak{p}})[p] = \mathbb{Z}/p$, which is a contradiction. □

Lemma 5.3. *Let R be a discrete valuation ring, K be its field of fractions, and k be the residue field. Let p be the characteristic of k. Assume R is equicharacteristic. Let G_K be a finite étale group scheme of order p over K. If G_K extends to a finite flat group scheme G over R such that the closed fibre G_k is either étale or multiplicative, then G_k is necessarily étale.*

Proof. Suppose G_K has a finite flat R-model G with multiplicative special fibre. The Cartier dual of G would be a finite flat group-scheme over R with étale special fibre, and hence has to be étale. This implies that $G_K \cong \mu_p$, which is a contradiction as μ_p is not étale in characteristic p. (Note that the statement of the lemma is false without assuming R is equicharacteristic as the example of μ_2 over $\mathbb{Q}_2$ shows.) □

Theorem 5.4. *If $L(E_K, 1) \neq 0$ then*

$$\#Ш(E/K) = \left(\langle H_E, H_K \rangle \cdot \frac{\#E(F)}{\#\Phi_{E,\mathfrak{p}}} \cdot q^{(\deg \Omega^1_{\mathcal{E}/\mathbb{P}^1}|_O - 1)} \right)^2.$$

Proof. The sheaf $\Omega^1_{\mathcal{E}/A}|_O$ is isomorphic to a line bundle on $\mathrm{Spec}(A)$, hence must be trivial as A is a principal ideal domain (in other words, there is a holomorphic and non-vanishing relative differential form $\omega_{\mathcal{E}/A}$, and this is unique up to $\mathbb{F}_q^\times$). In particular, the divisor of $\Omega^1_{\mathcal{E}/\mathbb{P}^1}|_O$ is supported at ∞. The extension $\mathcal{O}/A$ is ramified only at $(\mathfrak{d})$. Since E has good reduction at $\mathfrak{d}$, the Néron model of E_K over $\mathcal{O}$ is

$\mathcal{E} \otimes_A \mathcal{O}$. Hence the divisor of $\Omega^1_{\mathcal{E}_K/C}|_O$ is also supported at the prime over ∞. Let R be the local ring of $\infty \in \mathbb{P}^1_{\mathbb{F}_q}$. Let R' be its integral closure in K. Since E has multiplicative reduction at ∞, there is an isomorphism $\mathcal{E}^0 \otimes_R R' \cong \mathcal{E}^0_K/R'$. Hence $\Omega^1_{\mathcal{E}_K/R'}|_O \cong \Omega^1_{\mathcal{E}/R}|_O \otimes R'$. As R'/R is ramified, we get $2\deg(\Omega^1_{\mathcal{E}/\mathbb{P}^1}|_O) = \deg(\Omega^1_{\mathcal{E}_K/C}|_O)$. Now the theorem follows by comparing (5.2) with (5.3) and using Proposition 5.2. □

Example 5.5. Some of the calculations below were performed using the computer package `Magma`.

Let $F = \mathbb{F}_7(T)$. Let $\mathfrak{p} = T^3 - 2$ and $\mathfrak{d} = T - 3$. Then $\left(\frac{\mathfrak{d}}{\mathfrak{p}}\right) = -1$, so that $\mathfrak{p}$ and $\mathfrak{d}$ is a pair of primes satisfying the conditions of Lemma 2.2. Let

$$E/F: \; Y^2 = X^3 + aX + b,$$

where $a = -3T(T^3+2)$ and $b = -2T^6 + 3T^3 + 1$. One can show that E has conductor $(\mathfrak{p}) \cdot \infty$, and split multiplicative reduction at both primes. By computing the j-invariant of E and using *Tate's algorithm* [22, IV.8-9], one also shows that $\#\Phi_{E,\mathfrak{p}} = \#\Phi_{E,\infty} = 3$. From Grothendieck's theory of L-functions over function fields it is known that the L-function $L(E,s)$ of an elliptic curve E over $\mathbb{F}_q(T)$ with conductor $\mathfrak{n}$ is a polynomial in q^{-s} of degree $(\deg \mathfrak{n} - 4)$ and constant term 1. This immediately implies that for our curve $L(E,s) = 1$. Hence by Tate [23], $E(F)$ is finite. It is not hard to show that the prime-to-p part of $\#E(F)$ is 3. On the other hand, the argument in the proof of Proposition 5.2 shows that $E(F)[p] = 1$, as $\#\Phi_{E,\mathfrak{p}}$ is coprime to p. That is, $\#E(F) = 3$.

To compute $\deg(\Omega^1_{\mathcal{E}/\mathbb{P}^1}|_O)$ we need to be able to restrict to O-section. Make a change of variables $X = u/v$, $Y = 1/v$. The equation becomes

$$v = u^3 + auv^2 + bv^3.$$

This is non-singular at $u = v = 0$. The relative differential

$$\omega_{\mathcal{E}/A} = \frac{du}{1 - 2auv - 3bv^2}$$

is regular and non-zero over A restricted to O-section ($u = v = 0$). To compute the relative differential over ∞ we make a substitution $T = 1/S$. Let $a' = -3\frac{1}{S}(\frac{1}{S^3} + 2)$ and $b' = -2\frac{1}{S^6} + 3\frac{1}{S^3} + 1$.The equation becomes

$$S^6 v = S^6 u^3 + S^6 a' u v^2 + S^6 b' v^3.$$

This is singular at $u = v = 0$, $S = 0$, and we have to desingularize by blowing-up (three times, as it turns out). Concretely, we make a substitution $u' = S^3 u$, $v' = S^3 v$ and get $v' = S^9 u'^3 + S^9 a' u v^2 + S^9 b' v^3$, which is non-singular at $u' = v' = S = 0$, and the relative differential is

$$\omega_{\mathcal{E}/\mathcal{O}_\infty} = \frac{S^3 du'}{1 - 2S^6 a' u' v' - 3S^6 b' v'^2}.$$

We conclude $\deg(\Omega^1_{\mathcal{E}/\mathbb{P}^1}|_O) = 3$. Now we can use (5.1) to compute the order of $Ш(E/F)$; the identity is

$$1 = \frac{3 \cdot 3 \cdot 7^{-3} \cdot 7}{3^2} \#Ш(E/F).$$

That is, $\#Ш(E/F) = 7^2$.

Now we proceed to verify the analogue of Gross's formula (5.2). It is much easier to compute L-functions over F rather than over $K = F(\sqrt{\mathfrak{d}})$, so we use the identity

$$L(E_K, s) = L(E, s)L(E_{\mathfrak{d}}, s),$$

and compute $L(E_{\mathfrak{d}}, s)$. The conductor of $E_{\mathfrak{d}}$ is $(\mathfrak{p})(\mathfrak{d})^2\infty^2$, and the L-function is $L(E_{\mathfrak{d}}, s) = 343q^{-3s} - 21q^{-3s} - 3q^{-s} + 1$ $(q = 7)$. Hence

$$L(E_K, 1) = 8/7.$$

The Brandt matrix calculations, necessary for determining $\mathbb{Z}H_E \subset \mathcal{M}^0$, are carried out in [19, p.66]. Before stating this result, we introduce some terminology and notation.

As we already mentioned, a Drinfeld $A(= \mathbb{F}_q[T])$-module over an A-field k is an $\mathbb{F}_q$-linear homomorphism $\phi : A \to k\{\tau\}$, $a \mapsto \phi_a$ defined by $\phi_T = t + g\tau + \Delta\tau^2$, where t is the image of T in k, $\Delta, g \in k$, and $\Delta \neq 0$. The element $j(\phi) = g^{q+1}/\Delta$ is called the *j-invariant* of ϕ. Two Drinfeld modules are isomorphic over $\bar{k}$ if and only if they have the same j-invariant.

Now let $k = \overline{\mathbb{F}}_{\mathfrak{p}}$. Denote

$$j_\alpha := (t^q - t)(1 - (t^q - \alpha)^{q-1}),$$

where $\alpha \in \mathbb{F}_q$. There are 8 super-singular j-invariants (that is, j-invariants of s.s. Drinfeld modules) over k, and they are given by 0 and j_α, $\alpha \in \mathbb{F}_7$; see [19, Prop.16]. Choose a basis of $\mathcal{M}$, $x_0, x_{j_0}, \dots, x_{j_6}$, in this order. It is known that $w(x_0) = 8$ and $w(x_{j_\alpha}) = 1$ for all $\alpha \in \mathbb{F}_7$. The $\mathbb{T}$-eigenspace corresponding to our elliptic curve E is spanned by the vector $(1, -4, -1, -1, 2, -1, 2, 2)$; see [19, Exm.19] (misprint in *loc.cit.*!) Hence H_E is an integer multiple of this vector. Gekeler calculated that the degree of the modular parametrization of E is 13. Using lemma 5.1, we deduce

$$H_E = (1, -4, -1, -1, 2, -1, 2, 2).$$

It remains to compute H_K. Since $\mathrm{Pic}(\mathcal{O}) = 1$, H_K is equal to one of the basis elements of $\mathcal{M}$, and we need to find the s.s. Drinfeld module with $\mathcal{O}$-action. First we construct explicitly a Drinfeld module with an action of $\mathcal{O}$. Let $U^2 = T - 3$. Consider the rank one $\mathcal{O}$-Drinfeld module over K given by

$$U \mapsto U + \tau.$$

Via the embedding $A \hookrightarrow B \to K\{\tau\}$, we get a rank 2 A-module determined by

$$\phi_{T-3} = (U + \tau)(U + \tau) = (T - 3) + (U + U^q)\tau + \tau^2.$$

Its j-invariant is $j(\phi) = (U + U^q)^{q+1}$ with $q = 7$. Modulo $\mathfrak{p}$ reduction of this module has j-invariant $j(\bar{\phi}) = ((t - 3) + 2(t - 3)^4 + (t - 3)^7)^4$, and one checks that this is equal to j_6 in our earlier notation. (In other words, ϕ is a singular lift of the s.s. x_{j_6}.) Hence $H_K = x_{j_6}$ and

$$\langle H_E, H_K \rangle = 2.$$

Substituting everything in (5.2), we get an equality

$$\frac{8}{7} = 2 \cdot 7^{-1}\frac{3}{3} \cdot 2^2.$$

Finally, from Theorem 5.4, we have $\#Ш(E/K) = 2^2 \cdot 7^4$.

We briefly indicate what happens for other monic $\mathfrak{d}$ of degree 1, with E being the same. Let $\mathfrak{d}_\beta = T - \beta$, where $\beta \in \mathbb{F}_q$, and let $K_\beta := F(\sqrt{\mathfrak{d}_\beta})$. Denote $E_\beta := E \otimes_F K_\beta$. One verifies that

$$\left(\frac{\mathfrak{d}_\beta}{\mathfrak{p}}\right) = 1 \text{ for } \beta = 0, 1, 2, 4.$$

To these cases our theorems do not apply. Still, it is easy to check on a computer that in all these cases $L(E_\beta, 1) = 0$.

On the other hand, if $\beta = 3, 5, 6$ then $\left(\frac{\mathfrak{d}_\beta}{\mathfrak{p}}\right) = -1$, and our theorems apply. We already discusses the case $\beta = 3$. The L-functions $L(E_\beta, s)$ in all three cases are the same and are equal to $343q^{-3s} - 21q^{-3s} - 3q^{-s} + 1$, where $q = 7$. Thus, for $\beta = 3, 5, 6$ we have $L(E_\beta, 1) = 8/7$. A calculation similar to the case of $\beta = 3$ gives $H_{K_5} = x_{j_3}$ and $H_{K_6} = x_{j_5}$. Hence in all cases $\langle H_E, H_{K_\beta}\rangle = 2$ and $\#\text{Ш}(E_\beta) = 2^2 \cdot 7^4$.

References

1. S. Bosch, W. Lütkebohmert, and M. Raynaud, *Néron models*, Springer, 1990.
2. V. Drinfeld, *Elliptic modules*, Math. Sbornik **94** (1974), 594–627.
3. M. Emerton, *Supersingular elliptic curves, theta series and weight two modular forms*, J. Amer. Math. Soc. **15** (2002), 671–714.
4. E.-U. Gekeler, *Zur arithmetic von Drinfeld-moduln*, Math. Ann. **262** (1983), 167–182.
5. ———, *Über Drinfeldsche modulkurven vom Hecke-Typ*, Compositio Math. **57** (1986), 219–236.
6. ———, *On finite Drinfeld modules*, J. Algebra **141** (1991), 187–203.
7. ———, *Analytic construction of Weil curves over function fields*, J. Théor. Nombres Bordeaux **7** (1995), 27–49.
8. ———, *Improper Eisenstein series on Bruhat-Tits trees*, manuscripta math. **86** (1995), 367–391.
9. E.-U. Gekeler and M. Reversat, *Jacobians of Drinfeld modular curves*, J. Reine Angew. Math. **476** (1996), 27–93.
10. E.-U. Gekeler and B. Snyder, *Drinfeld modules over finite fields*, in Drinfeld modules, modular schemes and applications (1995), 66–99.
11. B. Gross, *Heights and the special values of $L-$series*, Canad. Math. Soc. Conf. Proc. **7** (1987), 115–187.
12. A. Grothendieck, *Modèles de Néron et monodromie*, SGA 7, Exposé IX, 1972.
13. H. Matsumura, *Commuative ring theory*, Cambridge University Press, 1986.
14. J. S. Milne, *On a conjecture of Artin and Tate*, Ann. Math. **102** (1975), 517–533.
15. M. Raynaud, *Jacobienne des courbes modulaires et opérateurs de Hecke*, Astérisque **196-197** (1991), 9–25.
16. I. Reiner, *Maximal orders*, Academic Press, 1975.
17. K. Ribet, *On the modular representations of* $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ *arising from modular forms*, Invent. Math. **100** (1990), 431–476.
18. H.-G. Rück and U. Tipp, *Heegner points and L-series of automorphic cusp forms of Drinfeld type*, Documenta Math. **5** (2000), 365–444.
19. A. Schweizer, *On the Drinfeld modular polynomial* $\Phi_T(X, Y)$, J. Number Theory **52** (1995), 53–68.
20. J-P. Serre, *Trees*, Springer, Berlin, 1980.
21. J-P. Serre and J. Tate, *Good reduction of abelian varieties*, Ann. Math **68** (1968), 492–517.
22. J. Silverman, *Advanced topics in the arithmetic of elliptic curves*, GTM 151, Springer, 1994.
23. J. Tate, *On a conjecture of Birch and Swinnerton-Dyer and a geometric analogue*, Sém. Bourbaki **306** (1966).
24. A. Weil, *Dirichlet series and automorphic forms*, LNM 189, Springer, 1971.

Department of Mathematics, Stanford University, Stanford, CA 94305
E-mail address: `papikian@math.stanford.edu`