J. reine angew. Math. **664** (2012), 115—140
DOI 10.1515/CRELLE.2011.104

Journal für die reine und
angewandte Mathematik

Local diophantine properties of modular curves of $\mathscr{D}$-elliptic sheaves

By *Mihran Papikian* at University Park

Abstract. We study the existence of rational points on modular curves of $\mathscr{D}$-elliptic sheaves over local fields and the structure of special fibres of these curves. We discuss some applications which include finding presentations for arithmetic groups arising from quaternion algebras, finding the equations of modular curves of $\mathscr{D}$-elliptic sheaves, and constructing curves violating the Hasse principle.

1. Introduction

The purpose of this paper is to discuss the function field analogues of certain problems about Shimura curves over local fields. To describe our results we first need to introduce some notation.

Let $C := \mathbb{P}^1_{\mathbb{F}_q}$ be the projective line over the finite field $\mathbb{F}_q$. Denote by $F = \mathbb{F}_q(T)$ the field of rational functions on C. The set of closed points on C (equivalently, places of F) is denoted by $|C|$. For each $v \in |C|$, we denote by $\mathcal{O}_v$ and F_v the completions of $\mathcal{O}_{C,v}$ and F at v, respectively. Let $A := \mathbb{F}_q[T]$. This is the subring of F consisting of functions which are regular away from the place generated by $1/T$ in $\mathbb{F}_q[1/T]$. The place generated by $1/T$ will be denoted by ∞ and called the *place at infinity*; it will play a role similar to the archimedean place for $\mathbb{Q}$. The places in $|C| - \infty$ are the *finite places*.

Let D be a quaternion division algebra over F, which is split at ∞, i.e., $D \otimes_F F_\infty \cong \mathbb{M}_2(F_\infty)$. Let R be the finite set of places where D ramifies; see §2.2 for the terminology and basic properties. Denote by $D^\times$ the multiplicative group of D. Fix a maximal A-order Λ in D. Since D is split at ∞, it satisfies the so-called *Eichler condition* relative to A, which implies that, up to conjugation, Λ is the unique maximal A-order in D, cf. [28], Corollary III.5.7. Let

$$\Gamma^R := \Lambda^\times = \{\lambda \in \Lambda \mid \mathrm{Nr}(\lambda) \in \mathbb{F}_q^\times\}$$

The author was supported in part by NSF grant DMS-0801208 and Humboldt Research Fellowship.

be the group of units of Λ. Via an isomorphism $D^\times(F_\infty) \cong \mathrm{GL}_2(F_\infty)$, the group Γ^R can be considered as a discrete subgroup of $\mathrm{GL}_2(F_\infty)$. There are two analogues of the Poincaré upper half-plane in this setting. One is the *Bruhat–Tits tree* $\mathscr{T}$ of $\mathrm{PGL}_2(F_\infty)$ and the other is the *Drinfeld half-plane* $\Omega := \mathbb{P}^{1,\mathrm{an}}_{F_\infty} - \mathbb{P}^{1,\mathrm{an}}_{F_\infty}(F_\infty)$, where $\mathbb{P}^{1,\mathrm{an}}_{F_\infty}$ is the rigid-analytic space associated to the projective line over F_∞. These two versions of the upper half-plane are related to each other: $\mathscr{T}$ is the dual graph of an analytic reduction of Ω, cf. [27]. As a subgroup of $\mathrm{GL}_2(F_\infty)$, Γ^R acts naturally on both $\mathscr{T}$ and Ω (these actions are compatible with respect to the reduction map). The quotient $\Gamma^R\backslash\Omega$ is a one-dimensional, connected, smooth analytic space over F_∞. It is the rigid-analytic space associated to a smooth, projective curve X^R over F_∞ ([27], Theorem 3.3). In fact, X^R is a moduli scheme of certain objects, called *$\mathscr{D}$-elliptic sheaves*, so it has a model over F; cf. §2.3. The curve X^R is the function field analogue of a Shimura curve parametrizing abelian surfaces with multiplication by a maximal order in an indefinite division quaternion algebra over $\mathbb{Q}$.

Now we describe the main results of the paper. Let K be a finite extension of F_v. We determine whether X^R has K-rational points. This problem naturally breaks into three cases, which need to be examined separately: $v \in |C| - R - \infty$, $v \in R$ and $v = \infty$. The corresponding theorems are Theorem 3.1, 4.1 and 5.10. These results are the function field analogues of the results of Jordan and Livné [9], and Shimura [25].

Next, we study the quotient graphs $\Gamma^R\backslash\mathscr{T}$, which are the analogues of fundamental domains of Shimura curves in the Poincaré upper half-plane. The study of such domains over $\mathbb{C}$ is a classical problem which can be traced back to the 19th century. Nevertheless, determining explicitly such a domain for a given arithmetic group is a computationally difficult problem; in fact, a large portion of the recent book [1] is devoted to this problem (see also [10]). We give a description of $\Gamma^R\backslash\mathscr{T}$ in Corollary 5.4 and Theorem 5.5.

Finally, we discuss some applications of our results. We give an upper-bound on the number of generators of Γ^R, determine the cases when Γ^R is generated by torsion elements and find a presentation for Γ^R in those cases (see Theorems 5.7 and 5.8). In §6, we find explicitly the torsion units which generate Γ^R in terms of a basis of D. We also determine in some special cases the equation defining X^R as a curve over F (Theorem 6.3); as far as I am aware, these are the first known examples of such equations. In §7, we use the knowledge of local points on X^R to show that there exist quadratic extensions of F over which X^R violates the so-called Hasse principle (Theorem 7.9).

2. Preliminaries

The purpose of this section is to fix the notation and terminology, and recall some basic facts which will be used later in the paper.

2.1. Notation. Besides the notation in the introduction, the following will be used throughout the paper. Let $v \in |C|$. The residue field of $\mathcal{O}_v$ is denoted by $\mathbb{F}_v$, the cardinality of $\mathbb{F}_v$ is denoted by q_v, the degree m extension of $\mathbb{F}_v$ is denoted by $\mathbb{F}_v^{(m)}$, and $\deg(v) := \dim_{\mathbb{F}_q}(\mathbb{F}_v)$. We assume that the valuation $\mathrm{ord}_v : F_v \to \mathbb{Z}$ is normalized by $\mathrm{ord}_v(\varpi_v) = 1$, where ϖ_v is a uniformizer of $\mathcal{O}_v$. Denote the adele ring of F by $\mathbb{A} = \prod'_{v\in|C|} F_v$, and for a finite set $S \subset |C|$, let $\mathbb{A}^S := \prod'_{v\in|C|-S} F_v$ be the adele ring outside of S. For each $v \in |C| - \infty$, let $\mathfrak{p}_v \lhd A$ be the

corresponding prime ideal of A and $\wp_v \in A$ be the monic generator of $\mathfrak{p}_v$. For $a \in A$, let $\deg(a)$ be the degree of a as a polynomial in T. Note that $\deg(\wp_v) = \deg(v)$.

For a ring H with a unit element, we denote by $H^\times$ the group of all invertible elements of H.

For $S \subset |C|$, put

$$\mathrm{Odd}(S) = \begin{cases} 1, & \text{if all places in } S \text{ have odd degrees,} \\ 0, & \text{otherwise.} \end{cases}$$

2.2. Quaternion algebras. Let D be a *quaternion algebra* over F, i.e., a 4-dimensional F-algebra with center F which does not possess non-trivial two-sided ideals. If L is a field containing F, then $D \otimes_F L$ is a quaternion algebra over L, cf. [28], page 4. By Wedderburn's theorem [19], (7.4), $D \otimes_F L$ is either a division algebra or is isomorphic to the matrix algebra $\mathbb{M}_2(L)$. In the second case, we say that L *splits* D, or is a *splitting field* for D, cf. [19], page 96. We say that D *splits* (resp. *ramifies*) at $v \in |C|$ if F_v is a splitting field for D (resp. is not a splitting field). Let $R \subset |C|$ be the set of places where D ramifies. It is known that R is a finite set of even cardinality, and for any choice of a finite set $R \subset |C|$ of even cardinality there is a unique, up to isomorphism, quaternion algebra ramified exactly at the places in R; see [28], page 74. In particular, $D \cong \mathbb{M}_2(F)$ if and only if $R = \emptyset$. The *discriminant* of D is

$$\mathfrak{r} := \prod_{\substack{x \in R \\ x \neq \infty}} \wp_x \in A.$$

Let $D^\times$ be the algebraic group over F defined by $D^\times(B) = (D \otimes_F B)^\times$ for any F-algebra B; this is the multiplicative group of D.

Notation 2.1. For $a, b \in F^\times$, let $H(a, b)$ be the F-algebra with basis 1, i, j, ij (as an F-vector space), where $i, j \in H(a, b)$ satisfy:

- If q is odd,

$$i^2 = a, \quad j^2 = b, \quad ij = -ji.$$

- If q is even,

$$i^2 + i = a, \quad j^2 = b, \quad ij = j(i + 1).$$

It is easy to show that $H(a, b)$ is a quaternion algebra; cf. [28], pages 1–5.

Proposition 2.2. *Let L be a field of degree n over F. Then L embeds into D, i.e., there is an F-isomorphism of L onto an F-subalgebra of D, if and only if n divides 2 and no place in R splits in L. Any two such F-isomorphisms are conjugate in D. If L is a quadratic extension of F, then L splits D if and only if L embeds into D.*

Proof. See [19], (32.15), and [28], Theorem I.2.8. □

We denote by $\alpha \mapsto \alpha'$ the canonical involution of D ([28], page 1); thus $\alpha'' = \alpha$ and $(\alpha\beta)' = \beta'\alpha'$. The *reduced trace* of α is $\mathrm{Tr}(\alpha) = \alpha + \alpha'$; the *reduced norm* of α is $\mathrm{Nr}(\alpha) = \alpha\alpha'$; the *reduced characteristic polynomial* of α is

$$f(x) = (x - \alpha)(x - \alpha') = x^2 - \mathrm{Tr}(\alpha)x + \mathrm{Nr}(\alpha).$$

If D is a division algebra and $\alpha \notin F$, then the field $F(\alpha)$ generated by α over F is quadratic over F, and the reduced trace and norm of α are simply the images of α under the trace and norm of $F(\alpha)/F$.

2.3. $\mathscr{D}$-elliptic sheaves. From now on we assume that D is a division algebra and D is split at ∞ (this is the analogue of indefinite quaternion algebra over $\mathbb{Q}$). Fix a locally free sheaf $\mathscr{D}$ of $\mathscr{O}_C$-algebras with stalk at the generic point equal to D and such that $\mathscr{D}_v := \mathscr{D} \otimes_{\mathscr{O}_C} \mathscr{O}_v$ is a maximal order in $D_v := D \otimes_F F_v$. For $S \subset |C|$, denote $\mathscr{D}^S := \prod_{v \in |C| - S} \mathscr{D}_v$.

Let W be an $\mathbb{F}_q$-scheme. Denote by Frob_W its Frobenius endomorphism, which is the identity on the points and the q-th power map on the functions. Denote by $C \times W$ the fibred product $C \times_{\mathrm{Spec}(\mathbb{F}_q)} W$.

Let $z : W \to C$ be a morphism of $\mathbb{F}_q$-schemes. A *$\mathscr{D}$-elliptic sheaf over W*, with pole ∞ and zero z, is a sequence $\mathbb{E} = (\mathscr{E}_i, j_i, t_i)_{i \in \mathbb{Z}}$, where each $\mathscr{E}_i$ is a locally free sheaf of $\mathscr{O}_{C \times W}$-modules of rank 4 equipped with a right action of $\mathscr{D}$ compatible with the $\mathscr{O}_C$-action, and where

$$j_i : \mathscr{E}_i \to \mathscr{E}_{i+1},$$

$$t_i : {}^{\tau}\mathscr{E}_i := (\mathrm{Id}_C \times \mathrm{Frob}_W)^* \mathscr{E}_i \to \mathscr{E}_{i+1}$$

are injective $\mathscr{O}_{C \times W}$-linear homomorphisms compatible with the $\mathscr{D}$-action. The maps j_i and t_i are sheaf modifications at ∞ and z, respectively, which satisfy certain conditions, and it is assumed that for each closed point w of W, the Euler–Poincaré characteristic $\chi(\mathscr{E}_0|_{C \times w})$ is in the interval $[0, 2)$; we refer to [12], §2, and [8], §1, for the precise definition. Moreover, to obtain moduli schemes with good properties, at the closed points w of W such that $z(w) \in R$ one imposes an extra condition on $\mathbb{E}$ to be "special", which is essentially a requirement that the trace of the induced action of $g \in \mathscr{D}_o$, $o \in R$, on the Lie algebra of $\mathbb{E}$ at o is equal to the reduced trace of g as an element of the quaternion algebra D_o (see [8], page 1305). Note that, unlike the original definition in [12], ∞ is allowed to be in the image of W; here we refer to [2], §4.4, for the details. Denote by $\mathscr{Ell}^{\mathscr{D}}(W)$ the set of isomorphism classes of $\mathscr{D}$-elliptic sheaves over W.

Theorem 2.3. *The functor $W \mapsto \mathscr{Ell}^{\mathscr{D}}(W)$ has a coarse moduli scheme $X^{\mathscr{D}}$, which is projective of pure relative dimension* 1 *over C and is smooth over $C - R - \infty$.*

Proof. Let I be a closed non-empty subscheme of C such that $I \cap (R \cup \infty) = \emptyset$. It is possible to add level-I structure to the moduli problem, assuming one considers only those schemes W for which $z(W) \cap I = \emptyset$. The resulting moduli problem is representable by a projective 1-dimensional scheme over $C - I$, which is smooth over $C - I - R - \infty$; see [8], Theorem 6.4, and [2], §4.4. (The proof of this result bases on the techniques in [12].) Dividing by the level structure, we obtain $X^{\mathscr{D}}$ over $C - I - R - \infty$. To extend this scheme

over I, repeat the same argument using some J disjoint from I, and glue the resulting scheme to $X^{\mathscr{D}}$ over $C - J - I - R - \infty$. □

2.4. Graphs. We recall some of the terminology related to graphs, as presented in [24] and [11]. A graph $\mathscr{G}$ consists of a set of *vertices* $X = \mathrm{Ver}(\mathscr{G})$ and a set of *edges* $Y = \mathrm{Ed}(\mathscr{G})$. Every edge y has an *inverse* edge $\bar{y} \in Y$, an *origin* $o(y) \in X$ and a *terminus* $t(y) \in X$. Moreover, $\bar{\bar{y}} = y$, $\bar{y} \neq y$ and $o(y) = t(\bar{y})$. The vertices $o(y)$ and $t(y)$ are the *extremities* of y. Note that it is allowed for distinct edges $y \neq z$ to have $o(y) = o(z)$ and $t(y) = t(z)$, and it is also allowed to have $y \in Y$ with $o(y) = t(y)$, in which case y is called a *loop*. We say that two vertices are *adjacent* if they are the extremities of some edge. We will assume that for any $v \in X$ the number of edges $y \in Y$ with $o(y) = v$ is finite; this number is the *degree* of v. A vertex $v \in X$ is called *terminal* if it has degree 1. A graph can be represented by a diagram where a marked point corresponds to a vertex and a line joining two marker points corresponds to a set of edges of the form $\{y, \bar{y}\}$; see [24], §I.2.1. A *path* (without backtracking) of length m between two vertices v, w in $\mathscr{G}$ is a collection of edges $y_1, y_2, \ldots, y_m \in \mathrm{Ed}(\mathscr{G})$ such that $y_i \neq \bar{y}_{i+1}$, $t(y_i) = o(y_{i+1})$ for $1 \leqq i \leqq m-1$, and $v = o(y_1)$, $w = t(y_m)$. We assume that $\mathscr{G}$ is connected, i.e., a path between any two distinct vertices exists. A path of minimal length is called a *geodesic*; the distance $d(v, w)$ between v and w is the length of a geodesic. A graph which has no non-trivial paths from a vertex to itself is called a *tree*. Note that in a tree a path between any two vertices is unique. A graph is *finite* if it has finitely many vertices and edges. A finite graph $\mathscr{G}$ can be interpreted as a 1-dimensional CW-complex ([24], page 22). The *first Betti number* $h_1(\mathscr{G})$ of $\mathscr{G}$ is the dimension of the homology group $\dim_{\mathbb{Q}} H_1(\mathscr{G}, \mathbb{Q})$.

$\mathscr{G}$ is a *graph with lengths* if we are given a map

$$\ell = \ell_{\mathscr{G}} : \mathrm{Ed}(\mathscr{G}) \to \mathbb{N} = \{1, 2, 3, \ldots\}$$

such that $\ell(y) = \ell(\bar{y})$. An *automorphism* of $\mathscr{G}$ is a pair $\phi = (\phi_1, \phi_2)$ of bijections $\phi_1 : X \to X$ and $\phi_2 : Y \to Y$ such that $\phi_1\big(o(y)\big) = o\big(\phi_2(y)\big)$, $\overline{\phi_2(y)} = \phi_2(\bar{y})$, and $\ell(y) = \ell\big(\phi_2(y)\big)$.

Let Γ be a group acting on a graph $\mathscr{G}$ (i.e., Γ acts via automorphisms). We say that $v, w \in X$ are Γ-*equivalent* if there is $\gamma \in \Gamma$ such that $\gamma v = w$; similarly, $y, z \in Y$ are Γ-*equivalent* if there is $\gamma \in \Gamma$ such that $\gamma y = z$. For $v \in X$, denote

$$\Gamma_v = \mathrm{Stab}_\Gamma(v) = \{\gamma \in \Gamma \mid \gamma v = v\}$$

the stabilizer of v in Γ. Similarly, let $\Gamma_y = \Gamma_{\bar{y}}$ be the stabilizer of $y \in Y$. The group Γ acts with *inversion* if there is $\gamma \in \Gamma$ and $y \in Y$ such that $\gamma y = \bar{y}$. If Γ acts without inversion, then we have a natural quotient graph $\Gamma\backslash\mathscr{G}$ such that $\mathrm{Ver}(\Gamma\backslash\mathscr{G}) = \Gamma\backslash\mathrm{Ver}(\mathscr{G})$ and $\mathrm{Ed}(\Gamma\backslash\mathscr{G}) = \Gamma\backslash\mathrm{Ed}(\mathscr{G})$.

Definition 2.4 (cf. [24], page 70). Let $\mathcal{O}$ be a complete discrete valuation ring with fraction field K, finite residue field $k \cong \mathbb{F}_q$ and a uniformizer π. Let V be a two-dimensional vector space over K. A *lattice* of V is a free rank-2 $\mathcal{O}$-submodule of V which generates the K-vector space V. Two lattices Λ and Λ' are *homothetic* if there is $x \in K^\times$ such that $\Lambda' = x\Lambda$. We denote the homothety class of Λ by $[\Lambda]$.

Let $\mathscr{T}$ be the graph whose vertices $\mathrm{Ver}(\mathscr{T}) = \{[\Lambda]\}$ are the homothety classes of lattices in V, and two vertices $[\Lambda]$ and $[\Lambda']$ are adjacent if we can choose representatives

$L \in [\Lambda]$ and $L' \in [\Lambda']$ such that $L' \subset L$ and $L/L' \cong k$. One shows that $\mathscr{T}$ is an infinite tree in which every vertex has degree $(q+1)$. This is the *Bruhat–Tits tree* of $\mathrm{PGL}_2(K)$. The group $\mathrm{GL}_2(K)$, as the group of linear automorphisms of V, naturally acts on $\mathscr{T}$ and preserves the distances between vertices.

Lemma 2.5. *Let $g \in \mathrm{GL}_2(K)$ and $v \in \mathrm{Ver}(\mathscr{T})$. Then*

$$d(v, gv) \equiv \mathrm{ord}_K\big(\det(g)\big) \pmod 2.$$

Proof. See [24], Corollary, page 75. □

2.5. Admissible curves. Let $\mathcal{O}$ be a complete discrete valuation ring with fraction field K, finite residue field k and a uniformizer π. Let $S = \mathrm{Spec}(\mathcal{O})$, $\mathcal{O}^{\mathrm{ur}}$ be the maximal unramified extension of $\mathcal{O}$, $\hat{\mathcal{O}}^{\mathrm{ur}}$ be its completion, and $\overline{k} = \mathcal{O}^{\mathrm{ur}}/\pi\mathcal{O}^{\mathrm{ur}}$.

Definition 2.6 (cf. [9], §3). A curve $X \to S$ is called *admissible* if:

(1) X is proper and flat over S and its generic fibre X_K is a smooth curve.

(2) The special fibre X_k is reduced with normal crossing singularities, and every irreducible component is isomorphic to $\mathbb{P}^1_k$.

(3) If x is a double point on the special fibre of X, then there exists a unique integer m_x for which the completion of $\mathcal{O}_{x,X} \otimes_{\mathcal{O}} \hat{\mathcal{O}}^{\mathrm{ur}}$ is isomorphic to the completion of $\hat{\mathcal{O}}^{\mathrm{ur}}[t,s]/(ts - \pi^{m_x})$.

The *dual graph* $\mathscr{G} = \mathrm{Gr}(X)$ of X is the following graph with lengths. The vertices of $\mathscr{G}$ are the irreducible components of X_k. The edges of $\mathscr{G}$, ignoring the orientation, are the singular points of X_k. If x is a double point and $\{y, \bar{y}\}$ is the corresponding edge of $\mathscr{G}$, then the extremities of y and $\bar{y}$ are the irreducible components passing through x; choosing between y or $\bar{y}$ corresponds to choosing one of the branches through x. Finally, $\ell(y) = \ell(\bar{y}) = m_x$.

The admissible curves are closely related to Mumford curves. Let $\Gamma \subset \mathrm{PGL}_2(K)$ be a discrete subgroup with compact quotient. There is an admissible curve X_Γ over S uniquely determined by Γ. The curve X_Γ is obtained as follows (see [11], §3). Let Γ_1 be a torsion-free normal subgroup of Γ with finite index (such a subgroup always exists). Mumford constructed a formal scheme $\hat{\mathbf{\Omega}}$ over $\mathrm{Spf}(\mathcal{O})$ such that the dual graph of its closed fibre is isomorphic to the Bruhat-Tits tree $\mathscr{T}$ of $\mathrm{PGL}_2(K)$, and proved that there exists a unique admissible curve X_{Γ_1} over S whose completion along its special fibre is isomorphic to the quotient $\Gamma_1 \backslash \hat{\mathbf{\Omega}}$ in the category of formal schemes. Now define X_Γ as the quotient $X_{\Gamma_1}/(\Gamma/\Gamma_1)$; this is independent of the choice of Γ_1. Next, Γ naturally acts on $\mathscr{T}$. Assume Γ acts without inversion. We assign lengths to the edges of the quotient graph $\Gamma\backslash\mathscr{T}$: for $y \in \mathrm{Ed}(\Gamma\backslash\mathscr{T})$ let $\ell(y) = \#\Gamma_{\tilde{y}}$, where $\tilde{y}$ is a preimage of y in $\mathscr{T}$.

Theorem 2.7. *There is an isomorphism $\mathrm{Gr}(X_\Gamma) \cong \Gamma\backslash\mathscr{T}$ of graphs with lengths. This implies that the genus of $(X_\Gamma)_K$ is equal to $h_1(\Gamma\backslash\mathscr{T})$.*

Proof. This is [11], Proposition 3.2 (note that since Γ acts without inversion on $\mathscr{T}$ the graph $(\Gamma\backslash\mathscr{T})^*$ in [11] is $(\Gamma\backslash\mathscr{T})$ itself). □

Remark 2.8. $\hat{\Omega}$ is the formal scheme associated to Drinfeld's non-archimedean half-plane $\Omega = \mathbb{P}_K^{1,\mathrm{an}} - \mathbb{P}_K^{1,\mathrm{an}}(K)$ over K. For the description of the rigid-analytic structure of Ω and the construction of $\hat{\Omega}$ we refer to [3], Chapter I.

3. Places of good reduction

Theorem 3.1. *Let $o \in |C| - R - \infty$. Let K be a finite extension of F_o of residue degree $f = f(K/F_o)$ and ramification index $e = e(K/F_o)$.*

- *If f is even, then $X^{\mathscr{D}}(K) \neq \emptyset$.*

- *If f is odd, then $X^{\mathscr{D}}(K) = \emptyset$ if and only if for every α satisfying a polynomial of the form*

$$X^2 + aX + c\wp_o^f \quad \text{with } a \in A \text{ and } c \in \mathbb{F}_q^\times,$$

and such that $F(\alpha)$ is quadratic over F, either some place in $(R \cup \infty)$ splits in $F(\alpha)$, or $\wp_o$ divides α and o splits in $F(\alpha)$.

Before proving the theorem we make some comments about its consequences.

Remark 3.2. Theorem 3.1 implies that if q is even then $X^{\mathscr{D}}(F_o) \neq \emptyset$, and hence also $X^{\mathscr{D}}(K) \neq \emptyset$ for any extension K of F_o. Indeed, if q is even, then $X^2 + \wp_o = 0$ is purely inseparable over F, so all the places in $(R \cup \infty \cup o)$ ramify in $F(\sqrt{\wp_o})$.

Remark 3.3. If q is odd, then to determine whether $X^{\mathscr{D}}(K) = \emptyset$ one needs to examine only a finite number of quadratic extensions of F. Indeed, ∞ splits in $F(\alpha)$, with α satisfying $X^2 + aX + c\wp_o^f = 0$, once $\deg(a) > f \cdot \deg(o)/2$.

Remark 3.4. Assume q is odd and fix a non-square $c \in \mathbb{F}_q^\times$. Using the Chinese Remainder Theorem, it is easy to show that if $\deg(o) > 2\deg(\mathfrak{r})$ then there exists $a \in A$ such that $X^2 + aX + c\wp_o$ is irreducible over F_v for $v \in R \cup \infty$. Theorem 3.1 then implies that $X^{\mathscr{D}}(F_o) \neq \emptyset$. The same conclusion can be drawn also using the Weil bound. The genus g of $X^{\mathscr{D}}$ is approximately $q^{\deg \mathfrak{r}}$ (see Corollary 5.4), so $q_o + 1 - 2g\sqrt{q_o} > 0$ if $\deg(o) > 2\deg(\mathfrak{r})$. Then the Weil bound implies $X^{\mathscr{D}}(\mathbb{F}_o) \neq \emptyset$, so $X^{\mathscr{D}}(F_o) \neq \emptyset$ by Hensel's Lemma (cf. the proof of Theorem 3.1).

Remark 3.5. If q is odd, then for a fixed K with odd residue degree there always exist (infinitely many) $X^{\mathscr{D}}$ with good reduction at o such that $X^{\mathscr{D}}(K) = \emptyset$. Indeed, let $S(a,c) \subset |C|$ be the set of primes splitting in the quadratic extension generated by the solutions of $X^2 + aX + c\wp_o^f = 0$. Each set $S(a,c)$ is infinite, but there are only finitely many a, c with $c \in \mathbb{F}_q^\times$ and $\deg(a) \leqq f \cdot \deg(o)/2$. Hence we can choose $R \subset |C| - \infty - o$ of even cardinality which has non-empty intersection with each $S(a,c)$ (and obviously there are infinitely many such R). By Theorem 3.1, the corresponding $X^{\mathscr{D}}$ will have no K-rational points.

Example 3.6. Let $q = 3$ and $R = \{x, y\}$ with $\wp_x = T$ and $\wp_y = T - 1$. Let $\wp_o = T - 2$. In the extension generated by the solutions of $X^2 + X + (T-2) = 0$ the

places x and ∞ ramify, and y remains inert. On the other hand, o splits but $\wp_o$ does not divide α. Hence $X^{\mathscr{D}}(F_o) \neq \emptyset$.

Proof of Theorem 3.1. We start with a reduction. Denote $M := X^{\mathscr{D}} \times_C \mathrm{Spec}(\mathbb{F}_o)$. By Theorem 2.3, $X^{\mathscr{D}}$ has good reduction at o, so by the geometric version of Hensel's Lemma ([9], Lemma 1.1), $X^{\mathscr{D}}(K) \neq \emptyset$ if and only if $M(\mathbb{F}_o^{(f)}) \neq \emptyset$.

Let k be a fixed algebraic closure of $\mathbb{F}_o$. In [12], Chapter 9, the authors, following Drinfeld, develop a Honda–Tate type theory for $\mathscr{D}$-elliptic sheaves of characteristic o over k. A foundational block of this theory is a construction which attached to each $\mathscr{D}$-elliptic sheaf over k a pair $(\tilde{F}, \tilde{\Pi})$, called (D, ∞, o)-*type*, having the following properties, cf. [12], (9.11):

(1) $\tilde{F}$ is a separable field extension of F of degree dividing 2.

(2) $\tilde{\Pi} \in \tilde{F}^{\times} \otimes_{\mathbb{Z}} \mathbb{Q}$ is such that $\tilde{\Pi} \notin F^{\times} \otimes_{\mathbb{Z}} \mathbb{Q}$ unless $\tilde{F} = F$.

(3) ∞ does not split in $\tilde{F}$.

(4) The valuations of F naturally extend to the group $\tilde{F}^{\times} \otimes_{\mathbb{Z}} \mathbb{Q}$. There are exactly two places $\tilde{x} = \tilde{\infty}$ and $\tilde{x} = \tilde{o}$ of $\tilde{F}$ such that $\mathrm{ord}_{\tilde{x}}(\Pi) \neq 0$. The place $\tilde{\infty}$ is the unique place of $\tilde{F}$ over ∞ and $\tilde{o}$ divides o. Moreover,

$$\mathrm{ord}_{\tilde{\infty}}(\tilde{\Pi}) \cdot \deg(\tilde{\infty}) = -[\tilde{F} : F]/2.$$

(5) For each place x of F and each place $\tilde{x}$ of $\tilde{F}$ dividing x, we have

$$(2[\tilde{F}_{\tilde{x}} : F_x]/[\tilde{F} : F]) \cdot \mathrm{inv}_x(D) \in \mathbb{Z}.$$

Next, using (1)–(5), one deduces the following property of $\tilde{F}$ depending on the value of $h := 2[\tilde{F}_{\tilde{o}} : F_o]/[\tilde{F} : F]$ (see [16], Lemma 4.1). If $h = 1$, then $\tilde{F}$ is a separable quadratic extension of F in which o splits and each $x \in R \cup \infty$ does not split. If $h = 2$, then $\tilde{F} = F$ and the (D, ∞, o)-type (F, Π) is unique.

By [12], Theorem 9.13, the map which associates to a $\mathscr{D}$-elliptic sheaf of characteristic o over k its (D, ∞, o)-type decomposes the set $M(k)$ into a disjoint union of non-empty subsets (called *isogeny classes*)

$$M(k) = \bigsqcup M(k)_{(\tilde{F}, \tilde{\Pi})}.$$

The union is over all (D, ∞, o)-types, the points in the subset $M(k)_{(\tilde{F}, \tilde{\Pi})}$ have (D, ∞, o)-type $(\tilde{F}, \tilde{\Pi})$, and each such subset is non-empty. Moreover, the geometric Frobenius $\mathrm{Frob}_o : x \mapsto x^{-q_o}$ preserves $M(k)_{(\tilde{F}, \tilde{\Pi})}$.

We will examine when a given isogeny class contains an $\mathbb{F}_o^{(f)}$-rational point. For this we will employ the group-theoretic description of each isogeny class along with the action of the geometric Frobenius given in [12], §10.

We start with the case $F = \tilde{F}$. Let $\overline{D}$ be the quaternion algebra over F which is ramified exactly at the places $R \cup o \cup \infty$. There is a bijection

$$M(k)_{(F,\Pi)} \xrightarrow{\sim} \overline{D}^{\times}(F) \backslash [\overline{D}^{\times}(\mathbb{A}^{\infty,o})/(\mathscr{D}^{\infty,o})^{\times} \times \mathbb{Z}],$$

where $\overline{D}^{\times}(F)$ is embedded diagonally into $\overline{D}^{\times}(\mathbb{A}^{\infty,o})$, and $(\mathscr{D}^{\infty,o})^{\times}$ is considered as a subgroup of $\overline{D}(\mathbb{A}^{\infty,o})$ via an isomorphism $\overline{D}(\mathbb{A}^{\infty,o}) \cong D(\mathbb{A}^{\infty,o})$. The group $\overline{D}^{\times}(F)$ acts on $\overline{D}^{\times}(\mathbb{A}^{\infty,o})/(\mathscr{D}^{\infty,o})^{\times}$ by left multiplication, and it acts on $\mathbb{Z}$ via the composition $\mathrm{ord}_o \circ \mathrm{Nr}$. The action of Frob_o on $M(k)_{(F,\Pi)}$ corresponds to the translation by 1 on $\mathbb{Z}$.

Hence $M(\mathbb{F}_o^{(f)})_{(F,\Pi)} \neq \emptyset$ if and only if there is an element $\delta \in \overline{D}^{\times}(F) \cap (\mathscr{D}^{\infty,o})^{\times}$ whose reduced norm generates the ideal $\mathfrak{p}_o^f$, cf. [12], page 278. This is equivalent to the existence of $\delta \in \overline{D}^{\times}(F)$ such that $\mathrm{Tr}(\delta) = a \in A$, $\mathrm{Nr}(\delta) = b \in A$ and $(b) = \mathfrak{p}_o^f$.

If f is even, such δ always exists since $\wp_o^{f/2} \in F^{\times}$ satisfies the required conditions.

Now suppose f is odd, and δ with the required properties exists. If $\delta \in F$, then $\mathrm{Nr}(\delta)$ is a square in F which contradicts f being odd. Hence the reduced characteristic polynomial of δ is of the form $P_\delta(X) = X^2 + aX + c\wp_o^f$, with $a \in A$ and $c \in \mathbb{F}_q^{\times}$, and the solutions of this polynomial generate a quadratic subfield $F' := F(\delta)$ of $\overline{D}$. In particular, F' is a splitting field for $\overline{D}$, so by Proposition 2.2 the places in $(R \cup \infty \cup o)$ do not split in F'. Conversely, suppose there is a polynomial $P(X) = X^2 + aX + b$ whose solutions generate a quadratic extension F' of F in which the places in $(R \cup \infty \cup o)$ do not split and $(b) = \mathfrak{p}_o^f$. Again, by Proposition 2.2, F' embeds into $\overline{D}$. If δ is such that $P(\delta) = 0$, then the image of δ in $\overline{D}$ is an element which is integral over A and has reduced norm generating $\mathfrak{p}_o^f$.

We conclude that if f is even, then $M(\mathbb{F}_o^{(f)})_{(F,\Pi)} \neq \emptyset$. On the other hand, if f is odd, then $M(\mathbb{F}_o^{(f)})_{(F,\Pi)} = \emptyset$ if and only if for every α which is quadratic over F and satisfies a polynomial of the form $X^2 + aX + c\wp_o^f$, with $a \in A$ and $c \in \mathbb{F}_q^{\times}$, some place in $(R \cup \infty \cup o)$ splits in $F(\alpha)$.

Next, consider a (D, ∞, o)-type $(\tilde{F}, \tilde{\Pi})$ such that $\tilde{F}$ is quadratic over F. The valuations of $\tilde{\Pi}$ at the places of $\tilde{F}$ are zero except at the unique place $\tilde{\infty}$ over ∞ and a place $\tilde{o}$ dividing o. Since o splits in $\tilde{F}$, let $\tilde{\tilde{o}} \neq \tilde{o}$ be the other place of $\tilde{F}$ over o. Identify $\tilde{F}_{\tilde{\tilde{o}}}$ with F_o. There is a bijection

$$M(k)_{(\tilde{F},\tilde{\Pi})} \xrightarrow{\sim} \tilde{F}^{\times} \backslash [D^{\times}(\mathbb{A}^{\infty,o})/(\mathscr{D}^{\infty,o})^{\times} \times (F_o^{\times}/\mathscr{O}_o^{\times}) \times \mathbb{Z}],$$

where $\tilde{F}^{\times}$ is embedded diagonally into $D^{\times}(\mathbb{A}^{\infty,o})$ (such embedding exists since $\tilde{F}$ is a splitting field for D) and into $F_o^{\times}$ via $\tilde{F} \hookrightarrow \tilde{F}_{\tilde{\tilde{o}}} \cong F_o$. The group $\tilde{F}^{\times}$ acts on $D^{\times}(\mathbb{A}^{\infty,o})/(\mathscr{D}^{\infty,o})^{\times}$ and $(F_o^{\times}/\mathscr{O}_o^{\times})$ via left multiplication, and it acts on $\mathbb{Z}$ via the composition $\mathrm{ord}_o \circ \mathrm{Nr}_{\tilde{F}/F}$. The action of Frob_o on $M(k)_{(\tilde{F},\tilde{\Pi})}$ corresponds to the translation by 1 on $\mathbb{Z}$.

The previous paragraph implies that $M(\mathbb{F}_o^{(f)})_{(\tilde{F},\tilde{\Pi})} \neq \emptyset$ if and only if there is $\delta \in \tilde{F}$ which has zero valuations away from $\tilde{o}$ and $\tilde{\infty}$ and $\mathrm{Nr}_{\tilde{F}/F}(\delta)$ generates $\mathfrak{p}_o^f$. The characteristic polynomial of such an element has the form $P_\delta(X) = X^2 + aX + c\wp_o^f$, where $a \in A$ and $c \in \mathbb{F}_q^{\times}$. If α is a root of this polynomial, then the places in $(R \cup \infty)$ do not split in $F(\alpha)$ and o splits (since $F(\alpha) \cong \tilde{F}$). Moreover, $\wp_o$ does not divide α, as otherwise δ will have non-zero valuations at both places over o. Conversely, suppose there is a polynomial

$P(X) = X^2 + aX + b$ whose solutions generate a quadratic extension F' of F in which the places in $(R \cup \infty)$ do not split, o splits, and $(b) = \mathfrak{p}_o^f$. Let δ be a root of $P(X)$. Let $\tilde{o}$ and $\tilde{\tilde{o}}$ be the two places in F' over F. The valuations of δ at the places of F' are zero, except at the place $\tilde{\infty}$ over ∞, and one or both of $\tilde{o} \cup \tilde{\tilde{o}}$. Suppose $\mathrm{ord}_{\tilde{\tilde{o}}}(\delta) = 0$. Then, since there is a (D, ∞, o)-type $(\tilde{F}, \tilde{\Pi})$ with $\tilde{F} = F'$ and $\mathrm{ord}_{\tilde{o}}(\tilde{\Pi}) \neq 0$, $M(\mathbb{F}_o^{(f)})_{(\tilde{F}, \tilde{\Pi})}$ will be non-empty.

We conclude that $\bigsqcup_{\tilde{F} \neq F} M(\mathbb{F}_o^{(f)})_{(\tilde{F}, \tilde{\Pi})} = \emptyset$ if and only if for every α which is quadratic over F and satisfies a polynomial of the form $X^2 + aX + c\wp_o^f$, with $a \in A$ and $c \in \mathbb{F}_q^\times$, one of the following holds: (1) some place in $(R \cup \infty)$ splits in $F(\alpha)$; (2) o does not split in $F(\alpha)$; (3) $\wp_o$ divides α. Combining this with the conditions from the case $\tilde{F} = F$, we obtain Theorem 3.1. $\square$

Remark 3.7. The analogue of Theorem 3.1 over $\mathbb{Q}$ is [9], Theorem 2.5. Jordan and Livné prove this theorem by "deconstructing" the zeta-function of the reduction of Shimura curve at a place of good reduction. The approach via Honda–Tate theory, as is done presently, has the advantage of giving an interpretation to the conditions appearing in Theorem 3.1 in terms of isogeny classes.

4. Finite places of bad reduction

Theorem 4.1. *Let $o \in R$. Let K be a finite extension of F_o of residue degree $f = f(K/F_o)$ and ramification index $e = e(K/F_o)$.*

(1) *If f is even, then $X^{\mathscr{D}}(K) \neq \emptyset$.*

(2) *If f is odd and e is even, then $X^{\mathscr{D}}(K) = \emptyset$ if and only if in every quadratic extension $F(\sqrt{c\wp_o})/F$, with $c \in \mathbb{F}_q^\times$, some place in $(R - o) \cup \infty$ splits.*

(3) *If f and e are both odd, then $X^{\mathscr{D}}(K) = \emptyset$.*

Remark 4.2. An immediate consequence of Part (3) is that $X^{\mathscr{D}}(F_v) = \emptyset$ for $v \in R$. In particular, $X^{\mathscr{D}}(F) = \emptyset$. Also note that if q is even then $F(\sqrt{c\wp_o}) = F(\sqrt{\wp_o})$ is a purely inseparable extension, so the places $(R - o) \cup \infty$ ramify. In particular, if q and $[K : F_o] = fe$ are even, then $X^{\mathscr{D}}(K) \neq \emptyset$.

The rest of this section is devoted to the proof of Theorem 4.1. We start by recalling the analogue of Cherednik–Drinfeld uniformization for $X^{\mathscr{D}} \otimes F_o$ due to Hausberger [8].

Let $\overline{D}$ be the quaternion algebra over F which is ramified exactly at $(R - o) \cup \infty$. Fix a maximal A-order $\mathfrak{D}$ in $\overline{D}(F)$, and denote

$$A^o = A[\wp_o^{-1}],$$
$$\mathfrak{D}^o = \mathfrak{D} \otimes_A A^o,$$
$$\Gamma = (\mathfrak{D}^o)^\times,$$
$$\Gamma_+ = \{\gamma \in \Gamma \mid \mathrm{ord}_o(\mathrm{Nr}(\gamma)) \in 2\mathbb{Z}\}.$$

If we fix an identification of $\overline{D}_o$ with $\mathbb{M}_2(F_o)$, then Γ and Γ_+ are discrete cocompact subgroups of $\mathrm{GL}_2(F_o)$ containing $\begin{pmatrix} \wp_o & 0 \\ 0 & \wp_o \end{pmatrix}$. Hence both Γ and Γ_+ act naturally on Drinfeld's o-adic half-plane $\Omega := \mathbb{P}^{1,\mathrm{an}}_{F_o} - \mathbb{P}^{1,\mathrm{an}}_{F_o}(F_o)$ and its formal analogue $\hat{\Omega}$ (see §2.5). Denote by $\mathrm{Fr}_o : \hat{\mathscr{O}}_o^{\mathrm{ur}} \to \hat{\mathscr{O}}_o^{\mathrm{ur}}$ the lift of the Frobenius homomorphism $x \mapsto x^{q_o}$ on $\overline{\mathbb{F}}_o$ to an $\mathscr{O}_o$-homomorphism. Consider the formal scheme

$$\hat{\Omega}^{\mathrm{ur}} := \hat{\Omega} \times_{\mathrm{Spf}(\mathscr{O}_o)} \mathrm{Spf}(\hat{\mathscr{O}}_o^{\mathrm{ur}})$$

over $\mathrm{Spf}(\mathscr{O}_o)$. Define an action of $\mathrm{GL}_2(F_o)$ on $\hat{\Omega}^{\mathrm{ur}}$ as follows: For an element $\gamma \in \mathrm{GL}_2(F_o)$ denote by $[\gamma]$ the element defined by γ in $\mathrm{PGL}_2(F_o)$ and set $n(\gamma) = -\mathrm{ord}_o\big(\det(\gamma)\big)$. Then define for $x \in \hat{\Omega}$ and $u \in \mathrm{Spf}(\hat{\mathscr{O}}_o^{\mathrm{ur}})$

$$\gamma : (x, u) \mapsto ([\gamma]x, \mathrm{Fr}_o^{n(\gamma)} u).$$

Let $M := X^{\mathscr{D}} \times_C \mathrm{Spec}(\mathscr{O}_o)$, and denote by $\hat{M}$ the completion of M along its special fibre. Note that $\overline{D}^\times(\mathbb{A}^{\infty,o}) \cong D^\times(\mathbb{A}^{\infty,o})$, so the group $(\mathscr{D}^{\infty,o})^\times$ can be considered as a subgroup of $\overline{D}^\times(\mathbb{A}^{\infty,o})$. Let

$$\mathscr{Z} := \overline{D}^\times(F) \backslash \overline{D}^\times(\mathbb{A}^\infty) / (\mathscr{D}^{\infty,o})^\times.$$

The set $\mathscr{Z}$ is equipped with an obvious right action of $\overline{D}^\times(F_o) = \mathrm{GL}_2(F_o)$. With this notation, we have the following uniformization ([8], Theorem 8.1):

$$\hat{M} \cong \mathrm{GL}_2(F_o) \backslash [\hat{\Omega}^{\mathrm{ur}} \times \mathscr{Z}]. \tag{4.1}$$

Since by the Strong Approximation Theorem [28], page 81,

$$\overline{D}^\times(\mathbb{A}^\infty) = D^\times(F) \cdot \mathrm{GL}_2(F_o) \cdot (\mathscr{D}^{\infty,o})^\times,$$

the isomorphism (4.1) can be rewritten as

$$\hat{M} \cong \Gamma \backslash \hat{\Omega}^{\mathrm{ur}}.$$

Denote by $\mathscr{O}_o^{(2)}$ the quadratic unramified extension of $\mathscr{O}_o$. Let $W = \Gamma/\Gamma_+ = \{1, w_o\}$, where w_o may be represented by any element $\gamma_o \in \Gamma$ whose norm generates $\mathfrak{p}_o$. Now the argument in [3], page 143, implies

$$\hat{M} \cong W \backslash [(\Gamma_+ \backslash \hat{\Omega}) \otimes \mathscr{O}_o^{(2)}], \tag{4.2}$$

where the action of W is given by $w_o : (x, u) \mapsto (w_o x, \mathrm{Fr}_o^{-1} u)$ for a point $x \in \hat{\Omega}$ and $u \in \mathrm{Spec}(\mathscr{O}_o^{(2)})$.

The existence of the uniformization (4.2) implies that M is an admissible curve, cf. §2.5. The vertices of the Bruhat–Tits tree $\mathscr{T}$ of $\mathrm{PGL}_2(F_o)$ can be partitioned into two disjoint classes such that the vertices in the same class are an even distance apart; see [24], page 71. Therefore, by Lemma 2.5, Γ_+ preserve the two classes of $\mathrm{Ver}(\mathscr{T})$ and w_o interchanges these two classes. This implies that Γ_+ acts without inversion on $\mathscr{T}$, and that w_o has no fixed vertices in $\Gamma_+ \backslash \mathscr{T}$.

Proposition 4.3. *With notation of Theorem* 4.1, *if f is even, then $M(K) \neq \emptyset$. If f is odd, then $M(K) \neq \emptyset$ if and only if there is an edge $y \in \mathrm{Ed}(\Gamma_+\backslash\mathscr{T})$ such that $e \cdot \ell(y)$ is even and $w_o(y) = \bar{y}$.*

Proof. This follows from the previous discussion combined with the arguments in the proofs of Theorems 5.1 and 5.2 in [9] (essentially verbatim). □

Proposition 4.3 establishes Part (1) of Theorem 4.1. Next, we examine when there is an edge $y \in \mathrm{Ed}(\Gamma_+\backslash\mathscr{T})$ such that $w_o(y) = \bar{y}$. Let $y \in \mathrm{Ed}(\Gamma_+\backslash\mathscr{T})$ and $\tilde{y}$ be a preimage of y in $\mathscr{T}$. If $w_o y = \bar{y}$ then there exits $\gamma \in \Gamma$ such that $\gamma\tilde{y} = \bar{\tilde{y}}$. Let $v, w \in \mathrm{Ver}(\mathscr{T})$ be the extremities of $\tilde{y}$. Then $\gamma(v) = w$, $\gamma(w) = v$, and so $\gamma^2(v) = v$. This implies $\gamma^2 \in F_o^\times \mu \mathfrak{D}_o^\times \mu^{-1}$ for some $\mu \in \mathrm{GL}_2(F_o)$. From this we conclude that $\gamma^2 = \wp_o^n c$, where $n \in \mathbb{Z}$ and $c \in \mu\mathfrak{D}_o^\times\mu^{-1}$. Since the distance between v and γv is 1, $\mathrm{ord}_o\big(\mathrm{Nr}(\gamma)\big) = n$ is odd. Put $n = 2m+1$ and replace γ by $\wp_o^{-m}\gamma$. Then we get $\gamma^2 = c\wp_o$ and $c \in \mu\mathfrak{D}_o^\times\mu^{-1} \cap \Gamma \subset (\mathfrak{D}')^\times$, where $\mathfrak{D}'$ is a maximal A-order in $\overline{D}$. Since $\overline{D}$ is ramified at ∞, $(\mathfrak{D}')^\times \cong \mathbb{F}_q^\times$ or $\mathbb{F}_{q^2}^\times$; see [6], page 383. Therefore, c is algebraic over $\mathbb{F}_q$. The field $L := F(\gamma)$ embeds into $\overline{D}$, so by Proposition 2.2, L/F is a quadratic extension. Since o ramifies in L, $\mathbb{F}_q$ is algebraically closed in L. We get $c \in \mathbb{F}_{q^2}^\times \cap L = \mathbb{F}_q^\times$. Conversely, suppose there is $c \in \mathbb{F}_q^\times$ such that $F(\sqrt{c\wp_o})$ embeds into $\overline{D}$. The image of $\sqrt{c\wp_o}$ is contained in some maximal A^o-order of $\overline{D}$. Since $\overline{D}$ is split at o and $\mathrm{Pic}(A^o) = 1$, a theorem of Eichler implies that all such orders are conjugate in $\overline{D}$; see [28], Corollary III.5.7. Therefore, we can assume that $\mathfrak{D}^o$ contains an element γ such that $\gamma^2 = c\wp_o$. Such an element is obviously in Γ. We can choose an embedding $\Gamma \hookrightarrow \mathrm{GL}_2(F_o)$ such that γ maps to the matrix $\begin{pmatrix} 0 & 1 \\ c\wp_o & 0 \end{pmatrix}$. Using this matrix representation, it is easy to check that there is an edge $\tilde{y} \in \mathrm{Ed}(\mathscr{T})$ such that $\gamma\tilde{y} = \bar{\tilde{y}}$. Then the image y of $\tilde{y}$ in $\Gamma_+\backslash\mathscr{T}$ will satisfy $w_o y = \bar{y}$. Finally, observe that $F(\sqrt{c\wp_o})$ embeds into $\overline{D}$ if and only if the places in $(R-o)\cup\infty$ do not split in this extension (Proposition 2.2). Combining the previous discussion with Proposition 4.3, we obtain Part (2) of Theorem 4.1.

From now on we assume that f and e are both odd. We start the proof of Part (3) of Theorem 4.1 with a lemma:

Lemma 4.4. *An edge of $\Gamma_+\backslash\mathscr{T}$ has length* 1 *or $q+1$. The number of edges of length $q+1$ is equal to*

$$2^{\#R-1} \cdot \mathrm{Odd}(R-o) \cdot \big(1 - \mathrm{Odd}(o)\big).$$

Proof. Let k be a fixed algebraic closure of $\mathbb{F}_o$. The singular points of $M \times_{\mathscr{C}_o} k$ represent the isomorphism classes of $\mathscr{D}$-elliptic sheaves of characteristic o over k which are *superspecial*; see [18], Proposition 5.9. Let x be a singular point and let $\mathbb{E}$ be the superspecial $\mathscr{D}$-elliptic sheaf corresponding to x. There is a natural notion of an automorphism group $\mathrm{Aut}(\mathbb{E})$ of $\mathbb{E}$. This is a finite group isomorphic to $\mathbb{F}_q^\times$ or $\mathbb{F}_{q^2}^\times$; see [18], Lemma 5.7. An argument similar to [5], Theorem VI.6.9, implies that the integer m_x attached to x in Definition 2.6 is equal to $\#\big(\mathrm{Aut}(\mathbb{E})/\mathbb{F}_q^\times\big)$. Thus, m_x is equal to 1 or $q+1$.

Next, since $\mathbb{E}$ is superspecial, $\mathrm{Aut}(\mathbb{E})$ is the group of units in an Eichler A-order $\mathscr{H}$ in $\overline{D}$ of level $\mathfrak{p}_o$; see [18], Theorem 5.3. Let $I_1, \ldots, I_h$ represent the isomorphism classes of locally free left $\mathscr{H}$-ideals. For $1 \leqq i \leqq h$, we denote with $\mathscr{H}_i$ the right order of the respective I_i. Each $\mathscr{H}_i$ is an Eichler A-order of level $\mathfrak{p}_o$. By [18], Theorem 5.4, the singular points

$x_1, \dots, x_h$ of $M \times_{\mathscr{O}_o} k$ are in natural bijection with $I_1, \dots, I_h$ and $m_{x_i} = \#(\mathscr{H}_i^\times / \mathbb{F}_q^\times)$. Now the class number formula for Eichler orders ([6], Theorem 9) implies

$$\#\{1 \leqq i \leqq h \,|\, m_{x_i} = q+1\} = 2^{\#R-1} \cdot \mathrm{Odd}(R-o) \cdot \big(1 - \mathrm{Odd}(o)\big).$$

Finally, Theorem 2.7, [9], Proposition 3.7, and (4.2) imply that the dual graph $\mathrm{Gr}(M)$, as a graph with lengths, is isomorphic to $\Gamma_+ \backslash \mathscr{T}$, so the claim of the lemma follows from the previous paragraph. □

Thanks to Proposition 4.3 and Lemma 4.4, to show that $M(K) = \emptyset$ when f and e are both odd we can assume that q is odd and $\deg(o)$ is even.

Let ξ be a fixed non-square in $\mathbb{F}_q^\times$. Let $y \in \mathrm{Ed}(\Gamma_+ \backslash \mathscr{T})$ be an edge with $\ell(y) = q+1$. Let $\tilde{y} \in \mathrm{Ed}(\mathscr{T})$ be any edge of $\mathscr{T}$ lying above y. By the argument in the proof of Lemma 4.4, there exists $\gamma \in \Gamma_+$ such that $\gamma^2 = \xi$ and $\mathrm{Stab}_{\Gamma_+}(\tilde{y}) = \mathbb{F}_q(\gamma)^\times$.

Now let $y \in \mathrm{Ed}(\Gamma_+ \backslash \mathscr{T})$ be an edge such that $w_o(y) = \bar{y}$, and let $\tilde{y} \in \mathrm{Ed}(\mathscr{T})$ be any edge of $\mathscr{T}$ lying above y. From our earlier discussions we know that there exists $\gamma_0 \in \Gamma$ such that $\gamma_0^2 = c\wp_o$ with $c \in \mathbb{F}_q^\times$, and $\gamma_0 \tilde{y} = \bar{\tilde{y}}$. Since $\overline{D}$ is ramified at ∞, in the extension $F(\gamma_0)/F$ the place ∞ does not split. On the other hand, by assumption $\deg(o)$ is even, so we can assume $c = \xi$ (as ∞ splits in the extension $F(\sqrt{\wp_o})/F$).

The previous discussion, combined with Proposition 4.3, implies that if $M(K) \neq 0$, then there exists $\tilde{y} \in \mathrm{Ed}(\mathscr{T})$ and $\gamma, \gamma_0 \in \Gamma$ such that

$$\gamma^2 = \xi, \quad \gamma_0^2 = \xi \wp_o, \quad \gamma \tilde{y} = \tilde{y}, \quad \gamma_0 \tilde{y} = \bar{\tilde{y}}. \tag{4.3}$$

Note that $\gamma_0^{-1} \gamma \gamma_0$ is in Γ and moreover, $\mathrm{ord}_o\big(\mathrm{Nr}(\gamma_0^{-1}\gamma\gamma_0)\big) = \mathrm{ord}_o\big(\mathrm{Nr}(\gamma)\big) = 0$, as γ is algebraic over $\mathbb{F}_q$. Hence $\gamma_0^{-1}\gamma\gamma_0 \in \Gamma_+$. On the other hand, $\gamma_0^{-1}\gamma\gamma_0 \cdot \tilde{y} = \tilde{y}$. Therefore,

$$\gamma_0^{-1}\gamma\gamma_0 \in (A^o)^\times \mathbb{F}_q(\gamma)^\times.$$

We conclude that there is $s \in \mathbb{Z}$ and $a, b \in \mathbb{F}_q$ (a, b are not both zero) such that

$$\gamma\gamma_0 = \wp_o^s \gamma_0 (a + b\gamma).$$

Comparing the norms of both sides, we must have $s = 0$. Thus,

$$\gamma\gamma_0 = \gamma_0(a + b\gamma). \tag{4.4}$$

Note that γ and γ_0 are pure quaternions, so $\gamma' = -\gamma$ and $\gamma_0' = -\gamma_0$. In particular, $(\gamma\gamma_0)' = \gamma_0'\gamma' = \gamma_0\gamma$. On the other hand, using (4.4),

$$(\gamma\gamma_0)' = \big(\gamma_0(a+b\gamma)\big)' = (a+b\gamma)'\gamma_0' = (a-b\gamma)(-\gamma_0) = -a\gamma_0 + b\gamma\gamma_0.$$

Using (4.4) again, this last expression is equal to

$$-a\gamma_0 + b\gamma_0(a+b\gamma) = -a\gamma_0 + ab\gamma_0 + b^2\gamma_0\gamma.$$

Overall,

$$\gamma_0\gamma = (ab - a)\gamma_0 + b^2\gamma_0\gamma.$$

Multiplying both sides by γ_0^{-1} from the left, we conclude that either $b = -1$ and $a = 0$, or $b = 1$ and $a \in \mathbb{F}_q$. In the first case, (4.4) becomes $\gamma_0\gamma = -\gamma\gamma_0$, so $\overline{D} \cong H(\xi, \xi\wp_o)$. Now, since both ξ and $\xi\wp_o$ are units at the places in $R - o$, the Hilbert symbols $(\xi, \xi\wp_o)_v$ for $v \in R - o$ are equal to 1; see [21], Chapter XIV, §3. This implies that $\overline{D}$ is split at the places in $R - o$ (see [28], page 32), which is a contradiction. Therefore, we must have $b = 1$ and

$$\gamma\gamma_0 = \gamma_0(a + \gamma).$$

Multiplying both sides of this equality by $\gamma_0\gamma$ from the right, we get $\xi^2\wp_o$ on the left-hand side and

$$a\gamma_0^2\gamma + \gamma_0\gamma\gamma_0\gamma = a\xi\wp_o\gamma + \gamma_0\gamma_0(a + \gamma)\gamma = a\xi\wp_o\gamma + \xi\wp_o(a\gamma + \xi),$$

on the right-hand side. This forces $2a\xi\wp_o = 0$, so $a = 0$. But if $a = 0$ and $b = 1$, then (4.4) says that γ and γ_0 commute in $\overline{D}$. Therefore, $F(\gamma, \gamma_0)$ is a subfield of $\overline{D}$. This subfield is necessarily quadratic over F. On the other hand, $F(\gamma_0)$ and $F(\gamma)$ are both quadratic and linearly disjoint over F. This leads to a contradiction. Overall, we conclude that the conditions (4.3) cannot hold simultaneously, which finishes the proof of Part (3) of Theorem 4.1.

5. The place at infinity

As in the introduction, let Λ be a maximal A-order in D. From now on we denote $K := F_\infty$, $\mathcal{O} := \mathcal{O}_\infty$, $k := \mathbb{F}_\infty \cong \mathbb{F}_q$, and $\Gamma := \Lambda^\times$. The group Γ can be considered as a discrete subgroup of $\mathrm{GL}_2(K)$ via an embedding

$$\iota : \Gamma \hookrightarrow D^\times(F) \hookrightarrow D^\times(K) \cong \mathrm{GL}_2(K).$$

Note that for $\gamma \in \Gamma$, $\det\big(\iota(\gamma)\big) = \mathrm{Nr}(\gamma) \in \mathbb{F}_q^\times$, so $\mathrm{ord}_\infty \det\big(\iota(\gamma)\big) = 0$. We fix some embedding ι and omit it from notation. The group Γ acts on Drinfeld's ∞-adic half-plane $\Omega := \mathbb{P}^{1,\mathrm{an}}_K - \mathbb{P}^{1,\mathrm{an}}_K(K)$ and its associated formal scheme $\hat{\Omega}$. Let $M := X^{\mathscr{D}} \times_C \mathrm{Spec}(\mathcal{O})$, and denote by $\hat{M}$ the completion of M along its special fibre. We have the following uniformization theorem due to Blum and Stuhler ([2], Theorem 4.4.11):

$$\hat{M} \cong D^\times(F)\backslash\big[\hat{\Omega} \times \big(D^\times(\mathbb{A}^\infty)/(\mathscr{D}^\infty)^\times\big)\big]. \tag{5.1}$$

Since D is split at ∞, the Strong Approximation Theorem for $D^\times$ implies (cf. [28], page 89)

$$D^\times(F)\backslash D^\times(\mathbb{A}^\infty)/(\mathscr{D}^\infty)^\times \cong F^\times\backslash(\mathbb{A}^\infty)^\times/\prod_{x \in |C| - \infty} \mathcal{O}_x^\times \cong \mathrm{Pic}(A) = 1. \tag{5.2}$$

Note that $\Gamma \cong D^\times(F) \cap (\mathscr{D}^\infty)^\times$. Therefore, (5.1) reduces to

$$\hat{M} \cong \Gamma\backslash\hat{\Omega}. \tag{5.3}$$

The uniformization (5.3) will play a key role in our examination of rational points on $X^{\mathscr{D}}$ over finite extensions of K. We start with an analysis of the quotient graph $\Gamma\backslash\mathscr{T}$, which can be considered as an analogue of fundamental domains of Shimura curves (here $\mathscr{T}$ is the Bruhat–Tits tree of $\mathrm{PGL}_2(K)$). By Lemma 2.5, Γ acts without inversion on $\mathscr{T}$ and, by Theorem 2.7, $\Gamma\backslash\mathscr{T}$ is the dual graph of M; in particular, $\Gamma\backslash\mathscr{T}$ is a finite graph. This last fact can easily be proved directly, without an appeal to the uniformization theorem:

Lemma 5.1. *The quotient graph $\Gamma\backslash\mathscr{T}$ is finite.*

Proof. It is enough to show that $\Gamma\backslash\mathscr{T}$ has finitely many vertices. The group $\mathrm{GL}_2(K)$ acts transitively on the set of lattices in K^2. The stabilizer of a vertex is isomorphic to $Z(K)\cdot\mathrm{GL}_2(\mathscr{O})$, where Z denotes the center of $\mathrm{GL}(2)$. This yields a natural bijection $\mathrm{Ver}(\mathscr{T})\cong\mathrm{GL}_2(K)/Z(K)\cdot\mathrm{GL}_2(\mathscr{O})$, and

$$\mathrm{Ver}(\Gamma\backslash\mathscr{T})\cong\Gamma\backslash\mathrm{GL}_2(K)/Z(K)\cdot\mathrm{GL}_2(\mathscr{O}).$$

We will show that the above double coset space is finite. Since D is a division algebra, $D^\times(F)\backslash D^\times(\mathbb{A})/Z(K)$ is compact, cf. [28], Chapter III.1. Thus, using (5.2), we see that $\Gamma\backslash\mathrm{GL}_2(K)/Z(K)$ is compact since it is the image of $D^\times(F)\backslash D^\times(\mathbb{A})/Z(K)$ under the natural quotient map $D^\times(\mathbb{A})\to D^\times(\mathbb{A})/(\mathscr{D}^\infty)^\times$. Finally, since $\mathrm{GL}_2(\mathscr{O})$ is open in $\mathrm{GL}_2(K)$, $\#\mathrm{Ver}(\Gamma\backslash\mathscr{T})$ is finite. □

Proposition 5.2. *Let $v\in\mathrm{Ver}(\mathscr{T})$ and $y\in\mathrm{Ed}(\mathscr{T})$. Then $\Gamma_v\cong\mathbb{F}_q^\times$ or $\Gamma_v\cong\mathbb{F}_{q^2}^\times$, and $\Gamma_y\cong\mathbb{F}_q^\times$.*

Proof. By choosing an appropriate basis of K^2, we can assume that v represents the homothety class of $\mathscr{O}^2$. The stabilizer of v in $\mathrm{GL}_2(K)$ is $Z(K)\cdot\mathrm{GL}_2(\mathscr{O})$. Since $\mathrm{GL}_2(\mathscr{O})$ is compact in $\mathrm{GL}_2(K)$, whereas Γ is discrete, $\Gamma_v=\Gamma\cap\mathrm{GL}_2(\mathscr{O})$ is finite. In particular, if $\gamma\in\Gamma_v$, then $\gamma^n=1$ for some $n\geqq 1$. We claim that the order n of γ is coprime to the characteristic p of F. Indeed, if $p\,|\,n$ then $(\gamma^{n/p}-1)\in D$ is non-zero but $(\gamma^{n/p}-1)^p=0$. This is not possible since D is a division algebra. Consider the subfield $F(\gamma)$ of D generated by γ over F. By Proposition 2.2, $[F(\gamma):F]=1$ or 2. Since $\gamma\in D$ is algebraic over $\mathbb{F}_q$, we conclude that $[\mathbb{F}_q(\gamma):\mathbb{F}_q]=1$ or 2.

It is obvious that $\mathbb{F}_q^\times\subset\Gamma_v$. Assume there is $\gamma\in\Gamma_v$ which is not in $\mathbb{F}_q^\times$. From the previous paragraph, γ generates $\mathbb{F}_{q^2}$ over $\mathbb{F}_q$, so every element of Γ_v is of order dividing q^2-1. In particular, by Sylow's Theorem, the order of Γ_v is coprime to p. Considering γ as an element of $\mathrm{GL}_2(\mathscr{O})$, we clearly have $a+b\gamma\in\mathbb{M}_2(\mathscr{O})$ for $a,b\in\mathbb{F}_q$ (embedded diagonally into $\mathrm{GL}_2(K)$). But if a and b are not both zero, then $a+b\gamma\in\Lambda$ is invertible, hence belongs to Γ and $\mathrm{GL}_2(\mathscr{O})$. This implies $\mathbb{F}_q(\gamma)^\times\cong\mathbb{F}_{q^2}^\times\subset\Gamma_v$. Suppose there is $\delta\in\Gamma_v$ which is not in $\mathbb{F}_q(\gamma)^\times$. Since δ is algebraic over $\mathbb{F}_q$, δ and γ do not commute in D (otherwise $F(\gamma,\delta)$ is a subfield of D of degree >2 over F). Then $\Gamma_v/\mathbb{F}_q^\times$ is a finite subgroup of $\mathrm{PGL}_2(K)$ whose elements have orders dividing $q+1$ and which contains two non-commuting elements of order $(q+1)$. This contradicts the classification of finite subgroups of $\mathrm{PGL}_2(K)$ of order coprime to p, cf. [22], page 281. Indeed, suppose H is such a subgroup. If $p=2$ or 3, then H is either cyclic or dihedral. In general, if H is not cyclic or dihedral, then it must be isomorphic to A_4, A_5 or S_5, so the elements of H have orders 1, 2, 3, 4 or 5.

Now consider Γ_y. Clearly $\mathbb{F}_q^\times\subset\Gamma_y$. Let v and w be the extremities of y. Note that there are natural inclusions $\Gamma_y\subset\Gamma_v$, $\Gamma_y\subset\Gamma_w$ and $\Gamma_y=\Gamma_v\cap\Gamma_w$. If Γ_y is strictly larger

than $\mathbb{F}_q^\times$, then from the discussion about the stabilizers of vertices, we have $\Gamma_v = \Gamma_w \cong \mathbb{F}_{q^2}^\times$ (an equality of subgroups of Γ). Therefore, $\Gamma_y \cong \mathbb{F}_{q^2}^\times$. On the other hand, the stabilizer of y in $\mathrm{GL}_2(K)$ is isomorphic to $Z(K)\cdot\mathscr{I}$, where $\mathscr{I}$ is the Iwahori subgroup $\mathscr{I}$ of $\mathrm{GL}_2(\mathcal{O})$ consisting of matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ such that $\mathrm{ord}_\infty(c) \geqq 1$. Since $\mathscr{I}$ does not contain a subgroup isomorphic to $\mathbb{F}_{q^2}^\times$, we get a contradiction. □

Corollary 5.3. *Let $v \in \mathrm{Ver}(\mathscr{T})$ be such that $\Gamma_v \cong \mathbb{F}_{q^2}^\times$. Then Γ_v acts transitively on the edges with origin v.*

Proof. By Proposition 5.2, a subgroup of $\mathbb{F}_{q^2}^\times$ which stabilizes an edge with origin v is $\mathbb{F}_q^\times$. Hence $\Gamma_v/\mathbb{F}_q^\times$ acts freely on the set of such edges. Since this quotient group has $q+1$ elements, which is also the number of edges with origin v, it has to act transitively. □

Corollary 5.4. *The length of any edge $y \in \mathrm{Ed}(\Gamma\backslash\mathscr{T})$ is equal to* 1. *In particular, M is a proper, flat and regular scheme over* $\mathrm{Spec}(\mathcal{O})$ *with* $\mathrm{Gr}(M) \cong \Gamma\backslash\mathscr{T}$. *The first Betti number $h_1(\Gamma\backslash\mathscr{T})$ is equal to*

$$g(R) := 1 + \frac{1}{q^2-1}\prod_{x\in R}(q_x - 1) - \frac{q}{q+1}\cdot 2^{\#R-1}\cdot \mathrm{Odd}(R).$$

(*M is not necessarily the minimal regular model of $X^{\mathscr{D}}$ over* $\mathrm{Spec}(\mathcal{O})$; *one obtains the minimal model by removing the terminal vertices from* $\Gamma\backslash\mathscr{T}$.)

Proof. Let $y \in \mathrm{Ed}(\Gamma\backslash\mathscr{T})$. According to Proposition 5.2, the image of Γ_y in $\mathrm{PGL}_2(K)$ is trivial, so $\ell(y) = 1$ by definition. Next, by Theorem 2.7, $h_1(\Gamma\backslash\mathscr{T})$ is equal to the genus of $X_K^{\mathscr{D}}$. A formula for the genus of $X_K^{\mathscr{D}}$ is computed in [16], Theorem 5.4, and it is given by $g(R)$, so $h_1(\Gamma\backslash\mathscr{T}) = g(R)$. □

Theorem 5.5. (1) *The graph $\Gamma\backslash\mathscr{T}$ has no loops.*

(2) *Every vertex of $\Gamma\backslash\mathscr{T}$ is either terminal or has degree $q+1$.*

(3) *Let V_1 and V_{q+1} be the number of terminal and degree $q+1$ vertices of $\Gamma\backslash\mathscr{T}$, respectively. Then*

$$V_1 = 2^{\#R-1}\,\mathrm{Odd}(R) \quad \textit{and} \quad V_{q+1} = \frac{2}{q-1}\big(g(R) - 1 + 2^{\#R-2}\,\mathrm{Odd}(R)\big).$$

Proof. The graph $\Gamma\backslash\mathscr{T}$ has no loops since adjacent vertices of $\mathscr{T}$ are not Γ-equivalent, as follows from Lemma 2.5.

Let $v \in \mathrm{Ver}(\mathscr{T})$. By Proposition 5.2, $\Gamma_v \cong \mathbb{F}_q^\times$ or $\mathbb{F}_{q^2}^\times$. In the second case, by Corollary 5.3, the image of v in $\Gamma\backslash\mathscr{T}$ is a terminal vertex. Now assume $\Gamma_v \cong \mathbb{F}_q^\times$. We claim that the image of v in $\Gamma\backslash\mathscr{T}$ has degree $q+1$. Let $e, y \in \mathrm{Ed}(\mathscr{T})$ be two distinct edges with origin v. It is enough to show that e is not Γ-equivalent to y or $\bar{y}$. On the one hand, e cannot be Γ-equivalent to y since $\Gamma_v \cong \mathbb{F}_q^\times$ stabilizes every edge with origin v. On the other hand, if e is Γ-equivalent to $\bar{y}$ then v is Γ-equivalent to an adjacent vertex, and that cannot happen.

Using (2), the number of non-oriented edges $\{y, \bar{y}\}$ of $\Gamma\backslash\mathscr{T}$ is equal to

$$E := \big(V_1 + (q+1)V_{q+1}\big)/2.$$

On the other hand, by Euler's formula $E + 1 = g(R) + V_1 + V_{q+1}$, so to prove (3) it is enough to prove the formula for V_1.

Let S be the set of terminal vertices of $\Gamma\backslash\mathscr{T}$. Let G be the set of conjugacy classes of subgroups of Γ isomorphic to $\mathbb{F}_{q^2}^\times$. We claim that there is a bijection $\varphi : S \to G$ given by $\tilde{v} \mapsto \Gamma_v$, where v is a preimage of the terminal vertex $\tilde{v} \in S$. The map is well-defined since if w is another preimage of $\tilde{v}$ then $v = \gamma w$ for some $\gamma \in \Gamma$, and so $\Gamma_w = \gamma^{-1}\Gamma_v\gamma$ is a conjugate of Γ_v. If φ is not injective, then there are two vertices $v, w \in \mathrm{Ver}(\mathscr{T})$ such that $\Gamma_v \cong \mathbb{F}_{q^2}^\times$, $\Gamma_w = \gamma^{-1}\Gamma_v\gamma$ for some $\gamma \in \Gamma$, but v and w are not in the same Γ-orbit. Then $\Gamma_{\gamma w} = \gamma\Gamma_w\gamma^{-1} = \Gamma_v$, but $\gamma w \neq v$. The geodesic connecting v to γw is fixed by Γ_v, so every edge on this geodesic has stabilizer equal to Γ_v. This contradicts Proposition 5.2. Finally, to see that φ is surjective it is enough to show that every finite subgroup Γ' of Γ fixes some vertex. If Γ' is finite, then the orbit $\Gamma' \cdot v$ is finite for any $v \in \mathrm{Ver}(\mathscr{T})$, so Γ' fixes some vertex by [24], Proposition 19, page 36.

Let $\mathscr{A} := \mathbb{F}_{q^2}[T]$ and $L := \mathbb{F}_{q^2}F$ (note that $\mathscr{A}$ is the integral closure of A in L). If q is odd, let ξ be a fixed non-square in $\mathbb{F}_q$. If q is even, let ξ be a fixed element of $\mathbb{F}_q$ such that $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_2}(\xi) = 1$ (such ξ always exists, cf. [13], Theorem 2.24). Consider the polynomial $f(x) = x^2 - \xi$ if q is odd, and $f(x) = x^2 + x + \xi$ if q is even. Note that $f(x)$ is irreducible over $\mathbb{F}_q$; this is obvious for q odd, and follows from [13], Corollary 3.79, for q even. Thus, a solution of $f(x) = 0$ generates $\mathbb{F}_{q^2}$ over $\mathbb{F}_q$. Denote by P the set of Γ-conjugacy classes of elements of Λ whose reduced characteristic polynomial is $f(x)$. By a theorem of Eichler ([28], Corollaries 5.12, 5.13, and 5.14, pages 94–96),

$$\#P = h(\mathscr{A}) \prod_{x \in R} \left(1 - \left(\frac{L}{x}\right)\right),$$

where $h(\mathscr{A})$ is the class number of $\mathscr{A}$, and $\left(\frac{L}{x}\right)$ is the *Artin–Legendre symbol*:

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

Note that a place of even degree splits in L and a place of odd degree remains inert in L, so

$$\prod_{x \in R} \left(1 - \left(\frac{L}{x}\right)\right) = 2^{\#R}\,\mathrm{Odd}(R).$$

Since $h(\mathscr{A}) = 1$, we get $\#P = 2^{\#R}\,\mathrm{Odd}(R)$.

If $\lambda \in \Lambda$ is an element with reduced characteristic polynomial $f(x)$, then it is clear that $\lambda \in \Gamma$ and $\mathbb{F}_q(\lambda)^\times \subset \Gamma$ is isomorphic to $\mathbb{F}_{q^2}^\times$. Hence $\lambda \mapsto \mathbb{F}_q(\lambda)^\times$ defines a map $\chi : P \to G$. As before, it is easy to check that χ is well-defined and surjective. We will show that χ is 2-to-1, which implies the formula for V_1. Obviously $\lambda \neq \lambda'$ and these elements generate

the same subgroup in Γ, as the canonical involution on D restricted to $F(\lambda)$ is equal to the Galois conjugation on $F(\lambda)/F$. Since λ and λ' are the only elements in $\mathbb{F}_q(\lambda)$ with the given characteristic polynomial, it is enough to show that λ and λ' are not Γ-conjugate. Suppose there is $\gamma \in \Gamma$ such that $\lambda' = \gamma\lambda\gamma^{-1}$. One easily checks that 1, λ, γ, $\gamma\lambda$ are linearly independent over F, hence generate D. If q is odd, then $\lambda' = -\lambda$. If q is even, then $\lambda' = \lambda + 1$. Using this, one easily checks that γ^2 commutes with λ, e.g., for q odd:

$$\gamma^2\lambda\gamma^{-2} = \gamma\lambda'\gamma^{-1} = -\gamma\lambda\gamma^{-1} = -\lambda' = \lambda.$$

Hence γ^2 lies in the center of D, and therefore, $\gamma^2 = b \in \mathbb{F}_q^\times$. Looking at the relations between λ and γ, we see that D is isomorphic to $H(\xi, b)$. We claim that this last algebra is isomorphic to $\mathbb{M}_2(F)$, which leads to a contradiction. Indeed, an easy consequence of Chevalley–Warning's Theorem is that a quadratic form in $n \geqq 3$ variables over a finite field has a non-trivial zero. Thus, since $\xi, b \in \mathbb{F}_q^\times$, the quadratic form associated to the reduced norm on $H(\xi, b)$ has a non-trivial zero over the subfield $\mathbb{F}_q$ of F. This obviously implies that $H(\xi, b)$ has zero divisors, hence cannot be a division algebra. □

Remark 5.6. It is easy to check directly that the formulas giving $h_1(\Gamma\backslash\mathscr{T})$ and V_{q+1} assume non-negative integer values. Interestingly, the presence of $\mathrm{Odd}(R)$ is necessary to make this happen.

The next theorem is the group-theoretic incarnation of Theorem 5.5.

Theorem 5.7. *Let* Γ_{tor} *be the normal subgroup of* Γ *generated by torsion elements.*

(1) $\Gamma/\Gamma_{\mathrm{tor}}$ *is a free group on* $g(R)$ *generators.*

(2) *If* $\mathrm{Odd}(R) = 0$, *then* $\Gamma_{\mathrm{tor}} = \mathbb{F}_q^\times$.

(3) *If* $\mathrm{Odd}(R) = 1$, *then the maximal finite order subgroups of* Γ *are isomorphic to* $\mathbb{F}_{q^2}^\times$, *and, up to conjugation,* Γ *has* $2^{\#R-1}$ *such subgroups.*

(4) Γ *can be generated by* $\left(2^{\#R-1} + g(R)\right)$ *elements.*

Proof. By [24], Corollary 1, page 55, $\Gamma/\Gamma_{\mathrm{tor}}$ is the fundamental group of the graph $\Gamma\backslash\mathscr{T}$. The topological fundamental group of any finite graph is a free group. Hence $\Gamma/\Gamma_{\mathrm{tor}}$ is a free group. The number of generators of this group is equal to the number of generators of the commutator group $(\Gamma/\Gamma_{\mathrm{tor}})^{\mathrm{ab}} \cong H_1(\Gamma\backslash\mathscr{T}, \mathbb{Q})$, which is a free abelian group on $g(R)$ generators. This proves (1). Parts (2) and (3) follow from the proofs of Proposition 5.2 and Theorem 5.5. Part (4) is a consequence of (1)–(3), cf. [24], Theorem 13, page 55. □

The main point of [24], Chapter I, is that the knowledge of $\Gamma\backslash\mathscr{T}$ gives a presentation for Γ. We apply this theory in the case when $\Gamma\backslash\mathscr{T}$ is itself a tree:

Corollary 5.8. $\Gamma = \Gamma_{\mathrm{tor}}$ *if and only if one of the following holds*:

(1) $R = \{x, y\}$ *and* $\deg(x) = \deg(y) = 1$. *In this case,* Γ *has a presentation*

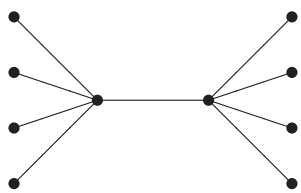
$$\Gamma \cong \langle \gamma_1, \gamma_2 \,|\, \gamma_1^{q^2-1} = \gamma_2^{q^2-1} = 1, \gamma_1^{q+1} = \gamma_2^{q+1} \rangle.$$

(2) $q = 4$ *and* R *consists of the four degree*-1 *places in* $|C| - \infty$. *In this case,* Γ *has a presentation*

$$\Gamma \cong \langle \gamma_1, \ldots, \gamma_8 \,|\, \gamma_1^{15} = \cdots = \gamma_8^{15} = 1, \gamma_1^5 = \cdots = \gamma_8^5 \rangle.$$

Proof. By Theorem 5.7, $\Gamma = \Gamma_{\mathrm{tor}}$ if and only if $g(R) = 0$. From the formula for $g(R)$ one easily concludes that $g(R) = 0$ exactly in the two cases listed in the theorem. In Case (1), according to Theorem 5.5, $V_1 = 2$ and $V_{q+1} = 0$, so $\Gamma\backslash\mathscr{T}$ is a segment:

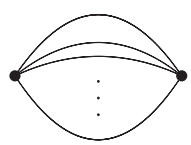
In Case (2), $V_1 = 8$ and $V_5 = 2$, so $\Gamma\backslash\mathscr{T}$ is the tree:



By [24], I.4.4, Γ is the graph of groups $\Gamma\backslash\mathscr{T}$, where each terminal vertex of $\Gamma\backslash\mathscr{T}$ is labeled by $\mathbb{F}_{q^2}^\times$, each non-terminal vertex is labeled by $\mathbb{F}_q^\times$, and each edge is labeled by $\mathbb{F}_q^\times$. In other words, Γ is the amalgam of the groups labeling the vertices of $\Gamma\backslash\mathscr{T}$ along the subgroups labeling the edges. The presentation for Γ follows from the definition of amalgam; see [24], I.1. □

Theorem 5.5 allows to determine $\Gamma\backslash\mathscr{T}$ in some other cases, besides the case when $\Gamma\backslash\mathscr{T}$ is a tree treated in Corollary 5.8:

Corollary 5.9. *Suppose* $R = \{x, y\}$ *and* $\{\deg(x), \deg(y)\} = \{1, 2\}$. *Then* $\Gamma\backslash\mathscr{T}$ *is the graph which has* 2 *vertices and* $q + 1$ *edges connecting them*:



Proof. From Theorem 5.5, $h_1(\Gamma\backslash\mathscr{T}) = q$, $V_1 = 0$ and $V_{q+1} = 2$. This implies the claim. □

The example in Corollary 5.9 is significant for arithmetic reasons. Assume q is odd. As is shown in [17], the curve $X^{\mathscr{D}}$ is hyperelliptic if and only if $R = \{x, y\}$ and $\{\deg(x), \deg(y)\} = \{1, 2\}$. Thus, Corollaries 5.9 and 5.4 imply that the special fibre of the minimal regular model over $\mathrm{Spec}(\mathscr{O})$ of a hyperelliptic $X^{\mathscr{D}}$ consists of two projective lines $\mathbb{P}^1_{\mathbb{F}_q}$ intersecting transversally at their $\mathbb{F}_q$-rational points.

Theorem 5.10. $M(K) = \emptyset$ *if and only if* $\mathrm{Odd}(R) = 0$. *If* L *is a finite non-trivial extension of* K, *then* $M(L) \neq \emptyset$.

Proof. Let L be a finite extension of K with residue degree f and ramification index e. Let $\mathcal{O}_L$ be the ring of integers of L. The argument which proves [9], Theorem 4.5, combined with Corollary 5.4, shows that the dual graph of $M \times_{\mathcal{O}} \mathcal{O}_L$ is isomorphic to $\Gamma\backslash\mathscr{T}$ but with $\ell(y) = e$ for any $y \in \mathrm{Ed}(\Gamma\backslash\mathscr{T})$. Moreover, the action induced by Fr_∞ on this graph is trivial. Using a geometric version of Hensel's Lemma [9], Lemma 1.1, one deduces from the previous statement that $M(L) \neq \emptyset$ if and only if either $e > 1$ or there is a vertex $x \in \mathrm{Ver}(\Gamma\backslash\mathscr{T})$ whose degree $< q^f + 1$; cf. [9], argument in the proofs of Theorems 5.1 and 5.2. But by Theorem 5.5 every vertex of $\Gamma\backslash\mathscr{T}$ has degree 1 or $q+1$, and there are vertices of degree 1 if and only if $\mathrm{Odd}(R) = 1$. Since $q + 1 < q^f + 1$ if $f > 1$, the claim follows. □

6. Explicit generators and equations

Let B be an indefinite division quaternion algebra over $\mathbb{Q}$ of discriminant d and let $\Lambda \subset B$ be a maximal $\mathbb{Z}$-order; recall that $d > 1$ is the product of primes where B ramifies. Let $\Gamma^d = \{\gamma \in \Lambda \mid \mathrm{Nr}(\gamma) = 1\}$. Upon fixing an identification of $B \otimes_{\mathbb{Q}} \mathbb{R}$ with $\mathbb{M}_2(\mathbb{R})$, we can view the group Γ^d as a discrete subgroup of $\mathrm{SL}_2(\mathbb{R})$. Only for a few d the explicit matrices generating Γ^d as a subgroup of $\mathrm{SL}_2(\mathbb{R})$ have been computed, cf. [1] or [10]. For example, Γ^6 is isomorphic to the subgroup of $\mathrm{SL}_2(\mathbb{R})$ generated by

$$\gamma_1 = \frac{1}{2}\begin{pmatrix} \sqrt{2} & 2-\sqrt{2} \\ -6-3\sqrt{2} & -\sqrt{2} \end{pmatrix}, \quad \gamma_2 = \frac{1}{2}\begin{pmatrix} \sqrt{2} & -2+\sqrt{2} \\ 6+3\sqrt{2} & -\sqrt{2} \end{pmatrix}$$

$$\gamma_3 = \frac{1}{2}\begin{pmatrix} 1 & 1 \\ -3 & 1 \end{pmatrix}, \qquad \gamma_4 = \frac{1}{2}\begin{pmatrix} 1 & 3-2\sqrt{2} \\ -9-6\sqrt{2} & 1 \end{pmatrix}$$

(which have orders 4, 4, 6, 6, respectively).

Let $\mathscr{H}$ be the Poincaré upper half-plane. The quotient $X^d := \Gamma^d\backslash\mathscr{H}$ is a compact Riemann surface. From the work of Shimura it is known that the algebraic curve X^d has a canonical model over $\mathbb{Q}$. The equations defining X^d as a curve over $\mathbb{Q}$ again are known only for a small number of d; cf. [11], [9]. For example, X^6 as a curve in $\mathbb{P}^2_{\mathbb{Q}}$ is isomorphic to the conic defined by

$$X^2 + Y^2 + 3Z^2 = 0.$$

In this section we keep the notation of §5, but assume q is odd. We will find explicit generators for Γ and determine the equation of $X^{\mathscr{D}}$ in Case (1) of Corollary 5.8. First, we explicitly describe D and a maximal A-order in D:

Lemma 6.1. *Let $\xi \in \mathbb{F}_q$ be a fixed non-square. If $\mathrm{Odd}(R) = 1$, then $H(\xi, \mathfrak{r}) \cong D$. The free A-module Λ in D generated by*

$$x_1 = 1, \quad x_2 = i, \quad x_3 = j, \quad x_4 = ij$$

is a maximal order.

Proof. To prove $H(\xi, \mathfrak{r}) \cong D$, it is enough to show that the Hilbert symbol $(\xi, \mathfrak{r})_v$ is -1 if and only if $v \in R$, cf. [28], page 32. By [21], Chapter XIV, §3, $(\xi, \mathfrak{r})_v = 1$ if and only if

$\xi^{\mathrm{ord}_v(\mathfrak{r})}$ is a square in $\mathbb{F}_v$. Now $\mathrm{ord}_v(\mathfrak{r}) = 0$ if $v \in |C| - R - \infty$, $\mathrm{ord}_v(\mathfrak{r}) = 1$ if $v \in R$, $\mathrm{ord}_\infty(\mathfrak{r})$ is even since $\#R$ is even and $\mathrm{Odd}(R) = 1$. It remains to observe that ξ is not a square in $\mathbb{F}_v$ for $v \in R$ since ξ is not a square in $\mathbb{F}_q$ and $\deg(v)$ is odd by assumption.

Next, it is obvious that Λ is an order. To show that it is maximal, we compute its discriminant, i.e., the ideal of A generated by $\det\big(\mathrm{Tr}(x_i x_j)\big)_{ij}$:

$$\det\big(\mathrm{Tr}(x_i x_j)\big)_{ij} = \det\begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 2\xi & 0 & 0 \\ 0 & 0 & 2\mathfrak{r} & 0 \\ 0 & 0 & 0 & -2\xi\mathfrak{r} \end{pmatrix} = -16\xi^2\mathfrak{r}^2.$$

Since q is odd and $\xi \in \mathbb{F}_q^\times$, the ideal generated by $-16\xi^2\mathfrak{r}^2$ is $\left(\prod_{x \in R} \mathfrak{p}_x\right)^2$. This implies that Λ is maximal, cf. [28], pages 84–85. $\square$

From Lemma 6.1 we see that finding the elements $\lambda = a + bi + cj + dij \in D$ which lie in Γ is equivalent to finding $a, b, c, d \in A$ such that

$$(a^2 - \xi b^2) - \mathfrak{r}(c^2 - \xi d^2) \in \mathbb{F}_q^\times. \tag{6.1}$$

We are particularly interested in torsion elements of Γ, so instead of looking for general units, we will try to find elements in Λ which are algebraic over $\mathbb{F}_q$ (such elements automatically lie in $\Lambda^\times$). Consider the equation $\gamma^2 = \xi$ in Λ. If we write $\gamma = a + bi + cj + dij$, then

$$\gamma^2 = a^2 + b^2\xi + c^2\mathfrak{r} - d^2\xi\mathfrak{r} + 2(abi + acj + adij).$$

Therefore, $\gamma^2 = \xi$ is equivalent to

$$a = 0 \quad \text{and} \quad b^2\xi + c^2\mathfrak{r} - d^2\xi\mathfrak{r} = \xi. \tag{6.2}$$

A possible solution is $b = 1$, $d = c = 0$. This gives the obvious $\theta_1 = i$ as a torsion unit. Now assume $R = \{x, y\}$ with $\deg(x) = \deg(y) = 1$. Then $\mathfrak{r} = (T - \alpha_1)(T - \alpha_2)$, where $\alpha_1, \alpha_2 \in \mathbb{F}_q$ and $\alpha_1 \neq \alpha_2$. For this $\mathfrak{r}$,

$$b_0 = \frac{2}{\alpha_1 - \alpha_2} T - \frac{\alpha_1 + \alpha_2}{\alpha_1 - \alpha_2}, \quad c_0 = 0, \quad d_0 = -\frac{2}{\alpha_1 - \alpha_2}$$

satisfy (6.2), so $\theta_2 = i(b_0 + d_0 j)$ is a torsion unit.

Next, we study the action of θ_1, θ_2 on $\mathscr{T}$. Since $\mathfrak{r}$ has even degree and is monic, $\sqrt{\mathfrak{r}} \in K$. The map

$$i \mapsto \begin{pmatrix} 0 & 1 \\ \xi & 0 \end{pmatrix}, \quad j \mapsto \begin{pmatrix} \sqrt{\mathfrak{r}} & 0 \\ 0 & -\sqrt{\mathfrak{r}} \end{pmatrix}, \tag{6.3}$$

defines an embedding of D into $\mathbb{M}_2(K)$. The $1/T$-adic expansion of $\sqrt{\mathfrak{r}}$ in K starts with

$$\sqrt{\mathfrak{r}} = T - \frac{\alpha_1 + \alpha_2}{2} - \frac{(\alpha_1 - \alpha_2)^2}{8T} + \cdots.$$

Therefore,

$$\pi := b_0 + d_0\sqrt{\mathfrak{r}} = \frac{\alpha_1 - \alpha_2}{4T} + \cdots$$

has valuation $\mathrm{ord}_\infty(\pi) = 1$. To simplify the notation in our calculations we take π as a uniformizer of $\mathcal{O}$. Note that $\pi^{-1} = b_0 - d_0\sqrt{\mathfrak{r}}$, so θ_2 under the embedding (6.3) maps to the matrix

$$\theta_2 = \begin{pmatrix} 0 & 1 \\ \xi & 0 \end{pmatrix}\begin{pmatrix} \pi & 0 \\ 0 & \pi^{-1} \end{pmatrix} = \begin{pmatrix} 0 & \pi^{-1} \\ \xi\pi & 0 \end{pmatrix}.$$

Let $e_1 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ and $e_2 = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$ be the standard basis of K^2. Let $v, w \in \mathrm{Ver}(\mathscr{T})$ be the vertices corresponding to the homothety classes of lattices $\mathcal{O}e_1 + \mathcal{O}e_2$ and $\mathcal{O}e_1 + \pi\mathcal{O}e_2$, respectively. Note that v and w are adjacent in $\mathscr{T}$. Now $\theta_1 e_1 = \xi e_2$ and $\theta_1 e_2 = e_1$, so

$$\theta_1 \cdot v = [\xi\mathcal{O}e_2 + \mathcal{O}e_1] = [\mathcal{O}e_1 + \mathcal{O}e_2] = v.$$

Similarly, $\theta_2 e_1 = \xi\pi e_2$ and $\theta_2 e_2 = e_1/\pi$, so

$$\theta_2 \cdot w = [\xi\pi\mathcal{O}e_2 + \mathcal{O}e_1] = [\mathcal{O}e_1 + \pi\mathcal{O}e_2] = w.$$

Thus, we found two adjacent vertices in $\mathscr{T}$ and elements in their stabilizers which are not in $\mathbb{F}_q^\times$. Proposition 5.2 implies that $\Gamma_v \cong \mathbb{F}_{q^2}^\times$ and $\Gamma_w \cong \mathbb{F}_{q^2}^\times$. By Corollary 5.3, the images of v and w in $\Gamma\backslash\mathscr{T}$ are adjacent terminal vertices. This implies that $\Gamma\backslash\mathscr{T}$ is an edge, and proves Theorem 5.5 in the case when $R = \{x, y\}$ and $\deg(x) = \deg(y) = 1$. By fixing generators γ_1, γ_2 of the finite cyclic groups $\mathbb{F}_q(\theta_1)^\times = \langle\gamma_1\rangle$ and $\mathbb{F}_q(\theta_2)^\times = \langle\gamma_2\rangle$, one obtains two torsion elements which generate Γ.

Example 6.2. Let $q = 3$, $\alpha_1 = 1$, $\alpha_2 = 0$. Then $\mathfrak{r} = T(T-1)$, $\xi = -1$. Since $\gamma_i = 1 - \theta_i$ generates $\mathbb{F}_q(\theta_i)^\times$, Γ is isomorphic to the subgroup of $\mathrm{GL}_2(K)$ generated by the matrices

$$\gamma_1 = \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix} \quad \text{and} \quad \gamma_2 = \begin{pmatrix} 1 & (T+1) - \sqrt{\mathfrak{r}} \\ -(T+1) - \sqrt{\mathfrak{r}} & 1 \end{pmatrix}$$

both of which have order 8 and satisfy $\gamma_1^4 = \gamma_2^4 = -1$.

Theorem 6.3. *Assume $R = \{x, y\}$ and $\deg(x) = \deg(y) = 1$. Then $X_F^{\mathscr{D}}$, as a curve over F, is isomorphic to the conic in $\mathbb{P}_F^2$ defined by the equation*

$$X^2 - \xi Y^2 - \mathfrak{r}Z^2 = 0.$$

Proof. Let $\mathscr{C}$ be a smooth conic in $\mathbb{P}_F^2$, and let $Q(X, Y, Z)$ be a homogeneous quadratic equation defining $\mathscr{C}$. Since the characteristic of F is odd by assumption, by the theory of quadratic forms [23], §IV.1, we can assume that Q is diagonal and non-degenerate:

$$Q(X, Y, Z) = aX^2 + bY^2 + cZ^2, \quad a, b, c \in F^\times. \tag{6.4}$$

Let $d := abc \neq 0$ be the discriminant of Q. The conic $\mathscr{C}$ obviously does not change if we replace Q with $\alpha \cdot Q$ for any $\alpha \in F^\times$. Next, $Q(X, Y, Z)$ and $Q(\alpha X, Y, Z)$ define isomorphic conics. Since $Q(dX, Y, Z)/d$ has discriminant 1, we can assume that Q is given by (6.4) and has discriminant 1. Let $\varepsilon_v(Q) = \pm 1$ be the *Hasse invariant* of Q at $v \in |C|$. The argument in the proof of [23], Theorem 6, page 36, shows that Q has a non-trivial zero over F_v if and only if $\varepsilon_v(Q) = (-1, -d)_v$. On the other hand, Q having non-trivial zeros over F_v is equivalent to $\mathscr{C}(F_v) \neq \emptyset$. By the Hasse–Minkowski Theorem [15], page 189, a non-degenerate quadratic form over F, up to a linear isomorphism, is uniquely determined by the number of variables, the discriminant and the local Hasse invariants for all places of F. We conclude that two conics $\mathscr{C}$ and $\mathscr{C}'$ in $\mathbb{P}^2_F$ are isomorphic over F if and only if

$$\mathscr{C}(F_v) \neq \emptyset \Leftrightarrow \mathscr{C}'(F_v) \neq \emptyset \quad \text{for all } v \in |C|.$$

The projective curve $X^{\mathscr{D}}_F$ is defined over F and is smooth, cf. Theorem 2.3. The existence of the uniformization (5.3) implies that $X^{\mathscr{D}}_F$ is geometrically connected. The genus of $X^{\mathscr{D}}_F$ is $g(R)$, so if $R = \{x, y\}$ and $\deg(x) = \deg(y) = 1$, then $X^{\mathscr{D}}_F$ has genus 0, i.e., is a conic. If $v \in |C| - R - \infty$, then by Theorem 2.3, $X^{\mathscr{D}}$ has good reduction at v. A curve of genus zero over a finite field always has rational points, so $X^{\mathscr{D}}(F_v) \supset X^{\mathscr{D}}(\mathbb{F}_v) \neq \emptyset$ for $v \in |C| - R - \infty$. The same conclusion for $v = \infty$ follows from Theorem 5.10, as $\mathrm{Odd}(R) = 1$. Finally, by Theorem 4.1, $X^{\mathscr{D}}(F_v) = \emptyset$ for $v \in R$.

Now to prove the theorem it is enough to show that the conic defined by $X^2 - \xi Y^2 - \mathfrak{r} Z^2$ has F_v-rational points exactly for $v \in |C| - R$. By the definition of the Hilbert symbol, $X^2 - \xi Y^2 - \mathfrak{r} Z^2$ has a non-trivial zero over F_v if and only if $(\xi, \mathfrak{r})_v = 1$. Thus, we need to show that $(\xi, \mathfrak{r})_v = -1$ if and only if $v \in R$. This calculation was already carried out in the proof of Lemma 6.1. □

7. On the Hasse principle

In this section X is a smooth, projective, geometrically irreducible curve over a field K.

Definition 7.1. If K is a global field, denote the set of places of K by $|K|$. We say that X *violates the Hasse principle* if $X(K_v) \neq \emptyset$ for all $v \in |K|$, but $X(K) = \emptyset$.

The study of varieties over global fields which violate the Hasse principle is an active research area in Number Theory, cf. [26]. In this section we show that there exist quadratic extensions of F over which $X^{\mathscr{D}}$ violates the Hasse principle if $\deg(\mathfrak{r}) \geqq 20$.

Definition 7.2. The *K-gonality* of X, denoted $\delta_K(X)$, is the least positive integer n for which there exists a degree n morphism $\pi : X \to \mathbb{P}^1_K$ defined over K.

Theorem 7.3. *Let K be a finite field extension of F. Assume that the Jacobian of X has no isotrivial quotients. If X has infinitely many points of degree d over K, then there exists a finite, purely inseparable extension $\tilde{K}$ of K such that $\delta_{\tilde{K}}(X) \leqq 2d$.*

Proof. This result is essentially due to Frey [7], Proposition 2. The statement of the theorem is proven in [20], Theorem 2.1, under the additional assumption that $X(K) \neq \emptyset$;

the main difference between [20] and the argument in [7] is that one needs to replace Faltings' proof of Mordell–Lang's conjecture over number fields by its analogue over function fields due to Hrushovski. Finally, as was observed by Clark [4], Theorem 5, the assumption $X(K) \neq \emptyset$ is not necessary for Frey's argument to work. □

Notation 7.4. Let $m(X)$ be the minimum degree of a finite field extension L/K such that $X(L) \neq \emptyset$. If K is a global field, let $m_v(X) := m(X \otimes K_v)$ and

$$m_{\mathrm{loc}}(X) = \operatorname*{lcm}_{v \in |K|} m_v(X).$$

Note that due to the Weil bound and Hensel's Lemma, $m_v(X) = 1$ for all but finitely many v, so m_{loc} is well-defined.

Theorem 7.5. *Let K be a finite field extension of F. Suppose $X(K) = \emptyset$, and moreover, suppose that for any finite, purely inseparable extension $\tilde{K}$ of K we have*

$$\delta_{\tilde{K}}(X) > 2m > 2$$

for some multiple m of $m_{\mathrm{loc}}(X)$. Then there exist infinitely many extensions L/K with $[L : K] = m$ such that X_L violates the Hasse principle.

Proof. Let S_m be the set of points on X of degree m over K. Due to our assumption on the gonality of X, Theorem 7.3 implies that S_m is finite. The rest of the proof is the same as in [4], Theorem 6. □

Lemma 7.6. *Assume K is a discrete valuation field with perfect residue field k. If X has good reduction X_k over k, then $\delta_K(X) \geqq \delta_k(X_k)$.*

Proof. See [14], Lemma 5.1 and Remark 5.2. □

Lemma 7.7. *Let $S \subset |C|$ be a finite subset of places. Denote $s := \sum_{x \in S} \deg(x)$. There exists a place $o \in |C| - S$ such that $\deg(o) \leqq \log_q(s) + 1$.*

Proof. Fix a natural number $n \geqq 1$. Let $S_n = \{x \in |C| \,|\, \deg(x) \leqq n\}$. Then

$$\sum_{x \in S_n} \deg(x) \geqq \sum_{\substack{x \in |C| \\ \deg(x) \,|\, n}} \deg(x) = \#C(\mathbb{F}_{q^n}) = q^n + 1.$$

Choose $o \in |C|$ of least possible degree subject to $o \notin S$. A moment of thought shows that it is enough to prove the statement of the lemma for $S = S_n$. In this case, the above inequality gives $s > q^n$. Since we can choose o of degree $n + 1$, the claim follows. □

Proposition 7.8. *The Jacobian of $X_F^{\mathscr{D}}$ has no isotrivial quotients. For any finite, purely inseparable extension $\tilde{F}$ of F we have*

$$\delta_{\tilde{F}}(X^{\mathscr{D}}) \geqq \frac{\prod_{x \in R} (q_x - 1)}{(q^2 - 1)\big(q \deg(\mathfrak{r}) + 3\big)} > \frac{q^{\frac{\deg(\mathfrak{r})}{2} - 3}}{\deg(\mathfrak{r}) + 3}.$$

Proof. The Jacobian $J^{\mathscr{D}}$ of $X_F^{\mathscr{D}}$ has no isotrivial quotients since $X^{\mathscr{D}}$ is totally degenerate at the places $R \cup \infty$, and hence the connected component of the identity of the Néron model of $J^{\mathscr{D}}$ has purely toric reduction at those places.

Let $\tilde{F}$ be a finite, purely inseparable extension of F. Fix some $o \in |C| - R - \infty$, and let $\tilde{o}$ be the (unique) place of $\tilde{F}$ over o. The residue field of the place $\tilde{o}$ is $\mathbb{F}_o$. Denote $X_o^{\mathscr{D}} := X^{\mathscr{D}} \times_C \operatorname{Spec}(\mathbb{F}_o)$. By Lemma 7.6, $\delta := \delta_{\mathbb{F}_o}(X_o^{\mathscr{D}}) \leqq \delta_{\tilde{F}}(X^{\mathscr{D}})$, so it is enough to give a lower bound on δ. On the one hand, we must have

$$\#X_o^{\mathscr{D}}(\mathbb{F}_o^{(2)}) \leqq \delta \#\mathbb{P}^1_{\mathbb{F}_o}(\mathbb{F}_o^{(2)}) = \delta(q_o^2 + 1).$$

On the other hand, by [16], Corollary 4.8,

$$\#X_o^{\mathscr{D}}(\mathbb{F}_o^{(2)}) \geqq \frac{1}{q^2-1} \prod_{x \in R \cup o} (q_x - 1) + \frac{q}{q+1} \cdot 2^{\#R} \cdot \operatorname{Odd}(R \cup o).$$

We conclude that

$$\frac{1}{q^2-1} \prod_{x \in R} (q_x - 1) \leqq \delta \frac{q_o^2 + 1}{q_o - 1} \leqq \delta(q_o + 3).$$

By Lemma 7.7, we can choose o such that $q_o \leqq q \deg(\mathfrak{r})$. With this choice, we get the desired lower bound on δ. The second inequality follows from the crude estimates

$$\prod_{x \in R} (q_x - 1) \geqq q^{\deg(\mathfrak{r})/2} \quad \text{and} \quad (q^2-1)\big(q \deg(\mathfrak{r}) + 3\big) < q^3\big(\deg(\mathfrak{r}) + 3\big). \quad \square$$

Theorem 7.9. *Suppose* $\deg(\mathfrak{r}) \geqq 20$. *Then there exist infinitely many quadratic extensions* L/F *such that* $X^{\mathscr{D}}$ *violates the Hasse principle over* L.

Proof. If $\deg(\mathfrak{r}) \geqq 20$, then Proposition 7.8 gives

$$\delta_{\tilde{F}}(X^{\mathscr{D}}) > \frac{q^{\frac{\deg(\mathfrak{r})}{2}-3}}{\deg(\mathfrak{r}) + 3} > 4.$$

As a consequence of Theorems 3.1, 4.1 and 5.10, we have $m_{\mathrm{loc}}(X^{\mathscr{D}}) = 2$ and $X^{\mathscr{D}}(F) = \emptyset$. The claim now follows from Theorem 7.5. $\square$

Acknowledgments. I thank E.-U. Gekeler and A. Schweizer for useful discussions. The article was mostly written while I was visiting the Department of Mathematics of Saarland University. I thank the members of the department for their warm hospitality.

References

[1] *M. Alsina* and *P. Bayer*, Quaternion orders, quadratic forms and Shimura curves, Amer. Math. Soc., 2004.

[2] *A. Blum* and *U. Stuhler*, Drinfeld modules and elliptic sheaves, in: Vector bundles on curves: New directions, Lect. Notes Math. **1649** (1997), 110–188.

[3] *J.-F. Boutot* and *H. Carayol*, Uniformisation p-adique des courbes de Shimura: les théorèmes de Čerednik et de Drinfeld, Astérisque **196** (1991), 45–158.

[4] *P. Clark*, On the Hasse principle for Shimura curves, Israel J. Math. **171** (2009), 349–365.
[5] *P. Deligne* and *M. Rapoport*, Les schémas de modules de courbes elliptiques, in: Modular fucnctions of one variable II, Lect. Notes Math. **349**, Springer (1973), 143–316.
[6] *M. Denert* and *J. Van Geel*, The class number of hereditary orders in non-Eichler algebras over global function fields, Math. Ann. **282** (1988), 379–393.
[7] *G. Frey*, Curves with infinitely many points of fixed degree, Israel J. Math. **85** (1994), 79–83.
[8] *T. Hausberger*, Uniformisation des variétés de Laumon–Rapoport–Stuhler et conjecture de Drinfeld–Carayol, Ann. Inst. Fourier **55** (2005), 1285–1371.
[9] *B. Jordan* and *R. Livné*, Local diophantine properties of Shimura curves, Math. Ann. **270** (1985), 235–248.
[10] *D. Kohel* and *H. Verrill*, Fundamental domains for Shimura curves, J. Théor. Nombres Bordeaux **15** (2003), 205–222.
[11] *A. Kurihara*, On some examples of equations defining Shimura curves and the Mumford uniformization, J. Fac. Sci. Univ. Tokyo **25** (1979), 277–300.
[12] *G. Laumon*, *M. Rapoport* and *U. Stuhler*, $\mathscr{D}$-elliptic sheaves and the Langlands correspondence, Invent. Math. **113** (1993), 217–338.
[13] *R. Lidl* and *H. Niederreiter*, Finite fields, Addison-Wesley, 1983.
[14] *K. V. Nguyen* and *M. Saito*, *d*-gonality of modular curves and bounding torsions, preprint 1996, arXiv:alg-geom/9603024v1.
[15] *O. T. O'Meara*, Introduction to quadratic forms, Springer, 1963.
[16] *M. Papikian*, Genus formula for modular curves of $\mathscr{D}$-elliptic sheaves, Arch. Math. **92** (2009), 237–250.
[17] *M. Papikian*, On hyperelliptic modular curves over function fields, Arch. Math. **92** (2009), 291–302.
[18] *M. Papikian*, Endomorphisms of exceptional $\mathscr{D}$-elliptic sheaves, Math. Z. **266** (2010), 407–423.
[19] *I. Reiner*, Maximal orders, Academic Press, 1975.
[20] *A. Schweizer*, On the uniform boundedness conjecture for Drinfeld modules, Math. Z. **244** (2003), 601–614.
[21] *J.-P. Serre*, Local fields, Grad. Texts Math. **67**, Springer, 1979.
[22] *J.-P. Serre*, Propriétés galoisiennes des points d'ordre fini des courbes elliptiques, Invent. Math. **15** (1972), 259–331.
[23] *J.-P. Serre*, A course in arithmetic, Grad. Texts Math. **7**, Springer, 1973.
[24] *J.-P. Serre*, Trees, Springer Monogr. Math., 2003.
[25] *G. Shimura*, On the real points of an arithmetic quotient of a bounded symmetric domain, Math. Ann. **215** (1975), 135–164.
[26] *A. Skorobogatov*, Torsors and rational points, Cambridge University Press, 2001.
[27] *M. van der Put*, Discrete groups, Mumford curves and theta functions, Ann. Fac. Sci. Toulouse Math. **1** (1992), 399–438.
[28] *M.-F. Vignéras*, Arithmétique des algèbres de quaternions, Lect. Notes Math. **800**, Springer, 1980.

Department of Mathematics, Pennsylvania State University, University Park, PA 16802, USA
e-mail: papikian@math.psu.edu

Eingegangen 2. Dezember 2009