Math. Ann. 327, 409–428 (2003) **Mathematische Annalen**

DOI: 10.1007/s00208-003-0448-3

Local points of twisted Mumford quotients and Shimura curves

Bruce W. Jordan · Ron Livné · Yakov Varshavsky

Received: 15 April 2002 / Revised version: 13 November 2002 /
Published online: 1 October 2003 –

Abstract. We determine over which fields twisted Mumford quotients have rational points. Using the p-adic uniformization, we apply these results to Shimura curves, and show some new cases for which the jacobians are even in the sense of [PS].

Mathematics Subject Classification (2000): 14G20, 14G35

1. Introduction and notation

The real points on certain Shimura varieties were determined by Shimura in [Shi]. In [JL1] the case of p-adic points was treated for Shimura curves associated to maximal orders in indefinite rational quaternion division algebras. The case of good reduction turned out to reduce to the trace formula via Hensel's lemma. The case of bad reduction was handled through the result of Cherednik and Drinfeld, which assured that these curves admit a p-adic uniformization.

A general result of Varshavsky, Rapoport and Zink (see [Va1, Va2]) gives the known cases when Shimura varieties admit a p-adic uniformization. Of special interest in this context is the case of curves, because of the recent results of [PS] and [JL3]. In this work we answer the question of existence of local points for some of these varieties. Using this we show in some new curve cases that the jacobians are even in the sense of [PS].

We now set some notation. Let F be a totally real number field of degree g over $\mathbb{Q}$, let $\infty_1, \dots, \infty_g$ be all the real embeddings of F, and let F_∞ be the product $\prod_{i=1}^g F_{\infty_i}$. Denote by F_∞^+ and $F_+^\times$ the set of totally positive elements of F_∞ and F respectively.

B.W. Jordan
Department of Mathematics, Baruch College, Box B6-230, CUNY, One Bernard Baruch Way, New York, NY 10010, USA (e-mail: bruce_jordan@baruch.cuny.edu)

R. Livné, Y. Varshavsky
Mathematics Institute, The Hebrew University of Jerusalem, Givat-Ram, Jerusalem 91904, Israel (e-mail: rlivne@math.huji.ac.il; vyakov@math.huji.ac.il)

The first author was partially supported by grants from the NSF and PSC-CUNY

The first two authors were partially supported by a joint Binational Israel-USA Foundation grant

Let $\mathbb{A} = \mathbb{A}_F$, $\mathbb{A}_{\mathrm{f}}$, $\mathbb{O}_{\mathrm{f}}$ and $\mathbb{A}_{\mathrm{f}}^v$ denote the rings of adèles of F, the finite adèles of F, the finite integral adèles of F and the finite adèles of F without the v component for a certain finite place v. Also for any ring A we denote by $A^\times$ the group of invertible elements of A.

For an algebraic group $\mathbf{G}/F$, we abbreviate $G = \mathbf{G}(F)$, $G_v = \mathbf{G}(F_v)$, $G_{\mathrm{f}} = \mathbf{G}(\mathbb{A}_{\mathrm{f}})$ and $G_{\mathrm{f}}^v = \mathbf{G}(\mathbb{A}_{\mathrm{f}}^v)$. We view G as contained in $\mathbf{G}(\mathbb{A})$ and in each G_{f}^v and G_v via the natural embeddings.

For a local field L, denote by val_L the valuation of L which sends the uniformizer to 1. Denote by L^{nr} the completion of the maximal unramified extension of L. For each positive integer r, denote by $L^{(r)}$ the extension of degree r of L in L^{nr}. We denote the center of a group G by $Z(G)$.

2. Local points of twisted Mumford quotients

Let K be a finite extension field of $\mathbb{Q}_p$, let $d \geq 2$ be an integer, and let $\Gamma \subset \mathrm{GL}_d(K)$ be a subgroup. Set $Z\Gamma := \Gamma \cap Z(\mathrm{GL}_d(K))$, and for every subgroup $\Delta \subset \Gamma$ containing $Z\Gamma$, we will write $P\Delta$ instead of $\Delta/Z\Gamma$. Finally, let k and k_+ be non-negative integers such that $\mathrm{val}_K(Z\Gamma) = k\mathbb{Z}$ and $\mathrm{val}_K(\det\Gamma) = k_+\mathbb{Z}$. In particular, dk is a multiple of k_+.

Assume that:

(A) $P\Gamma$ is a cocompact lattice in $\mathrm{PGL}_d(K)$;
(B) $Z\Gamma$ is not relatively compact in $K^\times$.

Assumpion (B) imply that k and k_+ are non-zero. Let

$$\Gamma' := \{\gamma \in \Gamma | dk \text{ divides } \mathrm{val}_K(\det(\gamma))\}.$$

Then Γ' is a normal subgroup of Γ containing $Z\Gamma$, and Γ/Γ' is cyclic of order dk/k_+. For a subgroup $\Delta \subset \Gamma$ we denote by Δ' the intersection of Δ with Γ'.

Let Ω_K^d be Drinfeld's symmetric space. It is the K-analytic space ([Ber]) Ω_K^d obtained by removing all K-rational hyperplanes from $\mathbb{P}_K^{d-1}$. It is equipped with a natural action of $\mathrm{PGL}_d(K)$. Moreover the K-analytic space $\Omega_K^{d,\mathrm{nr}} := \Omega_K^d \hat{\otimes}_K K^{\mathrm{nr}}$ is equipped with a K-rational action of $\mathrm{GL}_d(K)$ such that $g \in \mathrm{GL}_d(K)$ acts on $\Omega_K^{d,\mathrm{nr}}$ via the natural (left) action on Ω_K^d and the action of $\mathrm{Fr}_K^{\mathrm{val}_K(\det g)}$ on K^{nr}.

Consider the quotient $\widetilde{X} = \widetilde{X}_\Gamma := \Gamma\backslash\Omega_K^{d,\mathrm{nr}}$. Then

$$\widetilde{X} = P\Gamma\backslash(Z\Gamma\backslash\Omega_K^{d,\mathrm{nr}}) = P\Gamma\backslash(\Omega_K^d \otimes_K K^{(dk)}),$$

hence assumption (A) implies that $\widetilde{X}$ algebraizes canonically to a projective geometrically connected variety X over $K^{(k_+)}$. More precisely, assumption (A) implies that the quotient $\Gamma'\backslash\Omega_K^d$ algebraizes canonically to a projective geometrically connected variety X' over K (see [Mus]), and $X = (\Gamma/\Gamma')\backslash(X' \otimes_K K^{(dk)})$. We say that X is a (*Frobenius*) *twist* of the *Mumford uniformized* variety X'.

Let L be any finite extension of $K^{(k_+)}$, and let $e = e(L/K^{(k_+)})$ and $f = f(L/K^{(k_+)})$ be the ramification index and the residue class degree of L over $K^{(k_+)}$ respectively. Notice that $[L : K] = efk_+$.

Finally, it will be sometimes convenient for us to assume that Γ satisfies

(C) $\det\Gamma \subset Z\Gamma$.

Notice that most interesting subgroups (e.g. congruence ones) satisfy assumption (C). Actually, what we will use is a consequence of (C) which asserts that k divides k_+.

Theorem 2.1. *Let* Γ *be a subgroup satisfying assumptions (A) and (B).*

a) If $X(L) \neq \emptyset$*, then there exists a subgroup* $\Delta \subset \Gamma$ *containing* $Z\Gamma$ *such that:*
  (i) the group $P\Delta$ *is finite;*
  (ii) $\mathrm{val}_K(\det(\Delta)) = dk\mathbb{Z} + fk_+\mathbb{Z}$*;*
  (iii) $d|efk_+m$*, where* m *is the order of* $P\Delta'$*.*

b) The converse of a) holds if we assume in addition either that d *is prime and* Γ *satisfies assumption (C) or that* $d|efk_+$*. In particular, the converse of a) holds if* $P\Gamma'$ *is torsion-free.*

Proof. Let d' be the least positive integer for which $L^{(d')}$ contains $K^{(dk)}$. Then d' is the smallest positive integer such that dk divides fk_+d', hence we have that $d' = dk/\gcd(dk, fk_+)$. Observe that conditions (ii) and (iii) of the theorem can be restated as

(ii)′ $\mathrm{val}_K(\det(\Delta)) = (dk/d')\mathbb{Z}$ and
(iii)′ $d'|ekm$

respectively. Then

$$K^{(dk)} \otimes_{K^{(k_+)}} L \simeq \oplus_{\mathrm{Hom}_{K^{(k_+)}}(K^{(kd/d')},L)} L^{(d')}.$$

This yields the following description of X_L:

$$\begin{aligned} X_L = X \otimes_{K^{(k_+)}} L &\simeq (\Gamma/\Gamma')\backslash \left(\sqcup_{\mathrm{Hom}_{K^{(k_+)}}(K^{(kd/d')},L)} X' \otimes_K L^{(d')}\right) \\ &\simeq (\Gamma_1/\Gamma')\backslash(X' \otimes_K L^{(d')}), \end{aligned}$$

where Γ_1 is the stabilizer in Γ of any (and hence of each) connected component of $X' \otimes_K (K^{(dk)} \otimes_{K^{(k_+)}} L)$. Thus

$$\Gamma_1 = \{\gamma \in \Gamma | dk/d' \text{ divides } \mathrm{val}_K(\det(\gamma))\}.$$

The quotient Γ_1/Γ' is cyclic of order d', generated by the projection of any element $\gamma_0 \in \Gamma_1$ such that $\mathrm{val}_K(\det(\gamma_0)) = dk/d'$. Fix such a γ_0. Then

$$X(L) = \{P' \in X'(L^{(d')}) | \gamma_0(P') = P'\}. \tag{1}$$

These considerations prove the following

Lemma 2.2. *$X(L) \neq \emptyset$ if and only if there exists $P \in \Omega^d_K(\overline{L})$ such that for every $\sigma \in \mathrm{Gal}(\overline{L}/L)$ there exists an element $\phi(\sigma) \in \Gamma_1$ satisfying $\sigma(P) = \phi(\sigma)(P)$ and $\phi(\sigma) \in \gamma_0^i \Gamma'$ if $\sigma_{|L^{(d')}} = Fr_L^i$. (Here Γ_1 acts on $\Omega^d_K(\overline{L})$ through its projection to $\mathrm{PGL}_d(K)$.)*

We return to the proof of the Theorem:

a) Assume that $X(L) \neq \emptyset$, and let P be as in the lemma. Set

$$\Delta := \{\gamma \in \Gamma_1 | \gamma(P) = \tau(P) \text{ for some } \tau = \tau(\gamma) \in \mathrm{Gal}(\overline{L}/L)\}.$$

Then Δ is a subgroup of Γ_1, containing $Z\Gamma$, so it will suffice to show that Δ satisfies the conditions (i)-(iii) of the Theorem.

(i) Since the natural $\mathrm{GL}_d(K)$-equivariant map from Ω^d_K to the Bruhat-Tits building $\mathcal{B}^d_K$ of $\mathrm{PGL}_d(K)$ is constant on the Galois orbits, Δ stabilizes a certain point of $\mathcal{B}^d_K$. By assumption (A) on Γ, the group $P\Delta \subset \mathrm{PGL}_d(K)$ is compact and discrete. Hence it is finite.

(ii) By Lemma 2.2, the existence of P forces Δ to contain an element from $\gamma_0\Gamma'$. Since $\Delta \supset Z\Gamma$, the statement follows.

(iii) Let δ_0 be an element from $\gamma_0\Gamma' \cap \Delta \subset \Gamma_1$. Multiplying δ_0 by an element of $Z\Gamma$ we may and will assume that $\mathrm{val}_K(\det(\delta_0)) = \mathrm{val}_K(\det(\gamma_0)) = kd/d'$. Let n be the order of the image of δ_0 in $P\Delta$, and let $\delta_0^n = a \in K^\times \subset L^\times$. Then $\det(\delta_0)^n = a^d$, hence $\mathrm{val}_L(a) = n\,\mathrm{val}_L(\det(\delta_0))/d = ekn/d'$.

Let L' be the field of rationality of P (corresponding by Galois theory to the stabilizer $H \subset \mathrm{Gal}(\overline{L}/L)$ of P). Then for every $\sigma \in \mathrm{Gal}(\overline{L}/L)$ and every $\tau \in H$ we have

$$\tau(\sigma(P)) = \tau(\phi(\sigma)(P)) = \phi(\sigma)(\tau(P)) = \phi(\sigma)(P) = \sigma(P),$$

hence L' is a Galois extension of L. Also we have a natural surjective homomorphism $\pi : \Delta \to \mathrm{Gal}(L'/L)$ such that $\pi(\delta)(P) = \delta(P)$ for each $\delta \in \Delta$.

Let $v \in (L')^d$ be a representative of $P \in \Omega^d_L(L') \subset \mathbb{P}^{d-1}(L')$. Then by our assumption, there exist $\tau \in \mathrm{Gal}(\overline{L}/L)$ and $\lambda \in L'$ such that $\delta_0(v) = \lambda\tau(v)$. Since the action of $\delta_0 \in \mathrm{GL}_d(K)$ commutes with that of τ, we get $av = \delta_0^n(v) = \lambda\tau(\lambda)\tau^2(\lambda)\cdots\tau^{n-1}(\lambda)(v)$. Hence $a = \lambda\tau(\lambda)\tau^2(\lambda)\cdots\tau^{n-1}(\lambda)$. Taking valuations, we get $\mathrm{val}_L(\lambda) = \mathrm{val}_L(a)/n = ek/d'$. Since $\mathrm{val}_{L'}(\lambda)$ is an integer, $d'|eke(L'/L)$, so it will suffice to show that $e(L'/L)$ divides m.

But $e(L'/L)$ obviously equals the ramification degree of $L'L^{(d')}$ over $L^{(d')}$, hence it divides the degree $[L'L^{(d')} : L^{(d')}]$. This degree is equal to the number of conjugates of P over $L^{(d')}$. But conjugates of P over $L^{(d')}$ form a homogeneous space for the action of the group $\Delta'/Z\Gamma$, hence the number of conjugates divides the order of $\Delta'/Z\Gamma$, which is m. This completes the proof of part a).

b) We will show the existence of local points by a case-by-case analysis.

I) Assume first that $d|efk_+$ or, equivalently, that $d'|ek$. Let δ_0, n and a be as in the proof of iii) in a). It will suffice us to show that there exists a point $P \in \Omega^d_K(L^{(n)})$ such that $\delta_0(P) = Fr_L(P)$.

The assumption $d'|ek$ implies that $n|\,\mathrm{val}_L(a)$. Therefore there exist $\lambda \in L^{(n)}$ such that $N_{L^{(n)}/L}(\lambda) = a$. Hence $\delta' := \lambda^{-1}\delta_0 \in \mathrm{GL}_d(L^{(n)})$ satisfies $\mathrm{Fr}_L^{n-1}(\delta')\,\mathrm{Fr}_L^{n-2}(\delta')\cdots\delta' = 1$. By Hilbert Theorem 90 for GL_d, there exists $B \in \mathrm{GL}_d(L^{(n)})$ such that $\delta' = \mathrm{Fr}_L(B)\cdot B^{-1}$. Hence for every vector $v \in L^d$, the image $P = P_v$ of $Bv \in (L^{(n)})^d$ in $\mathbb{P}^{d-1}(L^{(n)})$ satisfies $\delta_0(P) = \mathrm{Fr}_L(P)$. Therefore it remains to show that there exists $v \in L^d$ such that the corresponding P_v belongs to Ω^d_K.

Let W be the $L^{(n)}$-vector subspace of $\mathrm{Mat}_d(L^{(n)})$ spanned by the Galois conjugates of B over L. Then W is invariant under the action of the Galois group $\mathrm{Gal}(L^{(n)}/L)$, hence is defined over L by descent theory. Therefore W contains an element $B' \in \mathrm{GL}_d(L)$.

By our assumption, $d|efk_+$, hence $[L:K] = efk_+ \geq d$. In particular, L contains d elements which are linearly independent over K. Equivalently, there exists $v' \in L^d$ not lying in any K-rational hyperplane. We claim that for $v := (B')^{-1}(v')$ the corresponding P_v lies in Ω^d_K. In fact, let $w \in K^n$ be a row vector such that $wBv = 0$. Since w and v are L-rational, we get $wCv = 0$ for every matrix $C \in W$. In particular, we have $wv' = wB'v = 0$. By our choice of v', the vector w is therefore the trivial vector, so that $P_v \in \Omega^d_K$.

II) It remains to consider the case when Γ satisfies assumption (C) and d is prime not dividing efk_+. Then $d' = d$, $k_+ = k$ and $[\Delta:\Delta'] = d$. Let δ_0, n and a be as above.

We claim that for every field extension $\widetilde{L}/K$ whose ramification degree $e(\widetilde{L}/K)$ is prime to d (in particular for $\widetilde{L} = L$), the subalgebra $\widetilde{L}_0 = \widetilde{L}[\delta_0] \subset \mathrm{Mat}_d(\widetilde{L})$ is a totally ramified field extension of $\widetilde{L}$ of degree d. Indeed, since the minimal polynomial of δ_0 divides $x^n - a$, the algebra $\widetilde{L}_0$ is either a field or a direct sum of fields. Let $\widetilde{L}'_0$ be one of the direct factors of $\widetilde{L}_0$, and let δ'_0 be the image of δ_0 in $\widetilde{L}'_0$. Then $(\delta'_0)^n = a$, therefore

$$\mathrm{val}_{\widetilde{L}'_0}(\delta'_0) = \mathrm{val}_{\widetilde{L}'_0}(a)/n = e(\widetilde{L}'_0/K)ekn/nd = e(\widetilde{L}'_0/K)ek/d.$$

Since $\mathrm{val}_{\widetilde{L}'_0}(\delta'_0)$ is an integer, our assumption implies that

$$d|e(\widetilde{L}'_0/\widetilde{L})|[\widetilde{L}'_0:\widetilde{L}] \leq [\widetilde{L}_0:\widetilde{L}] = d.$$

From this the statement follows.

It follows from our assumption that d^2 divides the order of $P\Delta$. We distinguish two cases: i) $d^2|n$ and ii) d^2 does not divide n.

Case i) We will prove that there is a cyclic extension M/L of degree n, whose ramification degree is d such that $a \in \mathrm{Nm}_{M/L}\,M^\times$. Write n as a product $d^t n'$, where n' is prime to d. As before, $\mathrm{val}_L(a) = ekn/d = d^{t-1}ekn'$, hence $n'|\,\mathrm{val}_L(a)$. It follows that a belongs to $\mathrm{Nm}_{L^{(n')}/L}(L^{(n')})^\times$. If we find a cyclic extension M'/L

of degree d^t with ramification degree d such that $a \in \mathrm{Nm}_{M'/L}(M')^\times$, then the composite field $M := M'L^{(n')}$ satisfies the required property. Indeed, as M' and $L^{(n')}$ are linearly disjoint over L, we have

$$\mathrm{Nm}_{M'L^{(n')}/L}(M'L^{(n')})^\times = \mathrm{Nm}_{M'/L}(M')^\times \cap \mathrm{Nm}_{L^{(n')}/L}(L^{(n')})^\times.$$

By Local Class Field Theory, to construct M' it is equivalent to construct an open subgroup $H \subset L^\times$, containing a and contained in $\{l \in L^\times | d^{t-1}$ divides $\mathrm{val}_L(l)\}$ such that $L^\times/H \cong \mathbb{Z}/d^t\mathbb{Z}$.

First we show that a is not a d^{th} power in L. In fact, suppose that $a = b^d$ for some $b \in L$. Let η be a primitive d^{th} root of unity inside $\overline{L}$. Then the ramification degree of $\widetilde{L} := L(\eta)$ over L (hence over K) is prime to d, so by the claim above the algebra $\widetilde{L}_0 = \widetilde{L}[\delta_0] \subset \mathrm{Mat}_d(\widetilde{L})$ is a field. The equality

$$(\delta_0^{n/d} - b)(\delta_0^{n/d} - \eta b)\ldots(\delta_0^{n/d} - \eta^{d-1}b) = \delta_0^n - a = 0$$

then implies that some $\delta_0^{n/d} - \eta^i b$ equal to 0. Hence $\delta_0^{n/d}$ is central in $\mathrm{Mat}_d(\widetilde{L})$, contradicting the fact that δ_0 has an order n modulo center.

The group $A := L^\times/(L^\times)^{d^t}$ is a finite abelian d-group. Let $\bar{a}$ and $\bar{\pi}$ be the images in A of a and of some uniformizer of L respectively, and set $A' := \mathcal{O}_L^\times/(\mathcal{O}_L^\times)^{d^t} \subset A$. We claim that there exists a subgroup $H' \subset A'$ such that A decomposes as a direct sum $\langle\bar{\pi}\rangle \oplus \langle\bar{a}\rangle \oplus H'$, where by $\langle\bar{\pi}\rangle$ (resp. $\langle\bar{a}\rangle$) we denote the cyclic subgroup generated by $\bar{\pi}$ (resp. $\bar{a}$). Indeed, using the fact that $d^{t-1} | \mathrm{val}_L(a)$ and that a is not a d^{th} power in L, we first see that the cyclic subgroups $\langle\bar{\pi}\rangle$ and $\langle\bar{a}\rangle$ have a trivial intersection. Put $a' := a\pi^{-\mathrm{val}_L(a)} \in \mathcal{O}_L^\times$. It remains to show that $\langle\bar{a'}\rangle$ is a direct summand in A', or equivalently that a' is not a d^{th} power. As $d | \mathrm{val}_L(a)$ and a is not a d^{th} power in L, the statement follows. Now we can take $H \subset L^\times$ be the inverse image of $\langle\bar{a}\rangle \oplus H'$ in $L^\times$.

Let σ be a generator of $\mathrm{Gal}(M/L)$ such that $\sigma_{|L^{(n/d)}} = \mathrm{Fr}_L$. As in the previous case, it will suffice to find a point $P \in \Omega_K^d(M)$ such that $\delta_0(P) = \sigma(P)$. Let λ be an element of M such that $\mathrm{Nm}_{M/L}(\lambda) = a$. As before, there exists $B \in \mathrm{GL}_d(M)$ such that $\sigma(B) = \lambda^{-1}\delta_0 B$. Then for every $v \in L^d$ the image $P = P_v \in \mathbb{P}^{d-1}(M)$ of $Bv \in M^d$ satisfies $\delta_0(P) = \sigma(P)$, so it remains to show that some Bv does not lie in a K-rational hyperplane. In fact, suppose that $wBv = 0$ for some row vector $w \in K^d$. Since $\sigma(Bv) = \lambda^{-1}\delta_0 Bv$, it follows that $w\delta_0^i Bv = 0$ for all i. Since the minimal polynomial of δ_0 has degree d, we get that for a generic v the vectors $\delta_0^i Bv = B(B^{-1}\delta_0 B)^i v$ span all of M^d. For such a v we therefore get $w = 0$, as claimed.

Case ii) Let $\bar{\delta}_0$ be the image of $\delta_0^{n/d}$ in $P\Delta$, and let Δ_d be a d-Sylow subgroup of $P\Delta$ containing $\bar{\delta}_0$. By our assumptions, $\Delta_d \cap P\Delta'$ is a non-trivial d-subgroup, hence it contains a central element $\bar{\delta}_1$ of Δ_d of order d. Since n/d is prime to d, we get that $\bar{\delta}_0 \notin P\Delta'$. Therefore $\bar{\delta}_0$ and $\bar{\delta}_1$ generate a subgroup isomorphic to $(\mathbb{Z}/d\mathbb{Z})^2$.

Let $\delta_1 \in \Delta$ be a representative of $\bar{\delta}_1$, then $(\delta_1)^d \in K^\times$. Replacing δ_0 by $\delta_0^{n/d}$, we get $\delta_0\delta_1 = b\delta_1\delta_0$ for some $b \in K^\times$. Taking determinants we see that $b^d = 1$.

We claim that $b \neq 1$. In fact, if b were equal to 1, then δ_1 would belong to the centralizer of δ_0 in $\mathrm{Mat}_d(K)$, which is $K(\delta_0)$. Since $K(\delta_0)$ is a totally ramified extension of K, the only elements of $K(\delta_0)^\times$ whose d^{th} power is in $K^\times$ are of the form $c(\delta_0)^i$ for some $c \in K^\times$ and some i. But then we get $\bar{\delta}_1 = (\bar{\delta}_0)^i$, contradicting our assumptions. Hence b is a primitive d^{th} root of unity.

The characteristic polynomial of δ_0 is irreducible over K. Therefore δ_0 has d distinct eigenvectors $V_1, \ldots, V_d$ (conjugate over K). They correspond to d conjugate fixed points $P_1, \ldots, P_d \in \Omega_K^d$ of δ_0. To finish the proof of the theorem it will suffice to show that the cyclic group generated by $\bar{\delta}_1$ acts simply-transitively on the P_i's.

Let $\lambda_1, \ldots, \lambda_d$ be the eigenvalues of δ_0, corresponding the V_i's, that is, $\delta_0(V_i) = \lambda_i V_i$ for all $i = 1, \ldots, d$. Then for each $i = 1, \ldots, d$ and each $j = 1, \ldots, d-1$ we have $\delta_0(\delta_1)^j(V_i) = b^j(\delta_1)^j\delta_0(V_i) = b^j\lambda_i(\delta_1)^j(V_i)$. Thus $(\bar{\delta}_1)^j(P_i) \neq P_i$, as was claimed. □

Remarks 2.3. a) By similar analysis, we can show that the converse of a) holds in some more cases, but we do not know whether it holds in general. In particular, we do not know whether assumption (C) in part b) is neccessary.

b) We suspect that there should be a simpler "topological" proof of Theorem 2.1, which uses the fact that the Bruhat-Tits building of $\mathrm{PGL}_d(K)$ can be naturally embedded into (Berkovich's) Ω_K^d.

c) The curve case of Theorem 2.1 was studied in [JL1], and generalizing these results to the higher dimensional case is one of our aims here — see also Section 4. It is in fact possible to obtain our results here through a generalization of the method of loc. cit., namely by an analysis of the special fiber and the resolution of its singularities.

Corollary 2.4. *a) If $dk | fk_+$, then $X(L) \neq \emptyset$.*
b) The converse of a) holds, if $P\Gamma$ is torsion-free.

Proof. Since $\mathrm{val}_K(\det(Z\Gamma)) = dk\mathbb{Z}$, the statement follows immediately from the theorem applied to $\Delta = Z\Gamma$. □

3. *P*-adic uniformization of Shimura curves

First we recall the definition of Shimura curves (cf. [De2], [Va2, Sect. 5]):

Let B^{int}/F be a quaternion division algebra, Let $\mathbf{G}^{\text{int}}/F$ be the algebraic group associated to its multiplicative group, and let $\nu^{\text{int}} : \mathbf{G}^{\text{int}} \to \mathbb{G}_m$ be the F-morphism induced from the reduced norm from B^{int} to F. Assume that $B^{\text{int}} \otimes_{F,\infty_i} \mathbb{R}$ is indefinite for $i = 1$ and definite for $2 \leq i \leq g$. Fix identifications of $B^{\text{int}}_{\infty_i}$ with $\mathrm{Mat}_{2\times 2}(\mathbb{R})$ for $i = 1$ and with the Hamilton quaternions $\mathbb{H}$ for $2 \leq i \leq g$.

Then $B^{\mathrm{int}} \otimes_{\mathbb{Q}} \mathbb{R} \cong \mathrm{Mat}_{2\times 2}(\mathbb{R}) \times \mathbb{H}^{g-1}$. Let $h : \mathrm{Res}_{\mathbb{C}/\mathbb{R}}\, \mathbb{G}_m(\mathbb{R}) \to \mathrm{Res}_{F/\mathbb{Q}}\, \mathbf{G}^{\mathrm{int}}(\mathbb{R})$ be the Hodge type

$$h(z) = (m(z), 1, \dots , 1) \in \mathrm{GL}_2(\mathbb{R}) \times (\mathbb{H}^\times)^{g-1} = \mathrm{Res}_{F/\mathbb{Q}}\, \mathbf{G}^{\mathrm{int}}(\mathbb{R}) ,$$

where for $z = x + \sqrt{-1}y \in \mathbb{C}^\times = \mathrm{Res}_{\mathbb{C}/\mathbb{R}}\, \mathbb{G}_m(\mathbb{R})$ we set $m(z) = \begin{bmatrix} x & y \\ -y & x \end{bmatrix}^{-1}$.

The reflex field is $\infty_1(F) \subset \mathbb{R} \subset \mathbb{C}$. Let X_∞ be the conjugacy class of h. Our identifications allow us to view X_∞ as $\mathcal{H} := \mathbb{C} \smallsetminus \mathbb{R}$. For a compact open subgroup $\widetilde{S} \subset G_{\mathrm{f}}^{\mathrm{int}}$, the corresponding Shimura variety is given complex analytically by

$$\widetilde{Y_{\widetilde{S}}^{\mathrm{int}}} = \left(X_\infty \times (\widetilde{S}\backslash G_{\mathrm{f}}^{\mathrm{int}})\right) / \, G^{\mathrm{int}} ,$$

where G^{int} acts on the product $X_\infty \times (\widetilde{S}\backslash G_{\mathrm{f}}^{\mathrm{int}})$ by the rule $(x, g)\gamma := (\gamma^{-1}(x), g\gamma)$. This variety is denoted by ${}_{\widetilde{S}}M_{\mathbb{C}}(\mathrm{Res}_{F/\mathbb{Q}}\, \mathbf{G}^{\mathrm{int}}, X_\infty)$ in [De1].

The complex manifold $\widetilde{Y_{\widetilde{S}}^{\mathrm{int}}}$ has a canonical algebraization $Y_{\widetilde{S}}^{\mathrm{int}}$ to a complex projective curve. In fact each $Y_{\widetilde{S}}^{\mathrm{int}}$ admits a canonical model over F, embedded into $\mathbb{C}$ via ∞_1, and the $Y_{\widetilde{S}}^{\mathrm{int}}$'s form a projective system. The result of [Va1], generalizing that of [Ch] (see [Va2, Sect. 5]) implies in particular that $Y^{\mathrm{int}} = \varprojlim_{\widetilde{S}} Y_{\widetilde{S}}^{\mathrm{int}}$ admits a $\mathcal{P}$-adic uniformization at each finite prime $\mathcal{P}$ of F dividing $\mathrm{Disc}\, B^{\mathrm{int}}$, i.e. at each finite prime in which B^{int} ramifies.

We shall now describe a special case of the result more precisely. This requires more notation.

Let B be a quaternion algebra over F split at $\mathcal{P}$, ramified at all infinite places, and with a fixed isomorphism

$$B^{\mathrm{int}} \otimes \mathbb{A}_{\mathrm{f}}^{\mathcal{P}} \cong B \otimes \mathbb{A}_{\mathrm{f}}^{\mathcal{P}} .$$

Let $\mathbf{G}$ be the algebraic group over F corresponding to $B^\times$, and let $\nu : \mathbf{G} \to \mathbb{G}_m$ be the F-morphism induced from the reduced norm from B to F. Set $\mathcal{G} = G_{\mathrm{f}}^{\mathcal{P}} = G_{\mathrm{f}}^{\mathrm{int},\mathcal{P}}$.

Fix a quaternion division algebra $\widetilde{B}_{\mathcal{P}}$ over $F_{\mathcal{P}}$. We then have that

$$G_{\mathrm{f}} \simeq \mathrm{GL}_2(F_{\mathcal{P}}) \times \mathcal{G} \quad \text{and} \quad G_{\mathrm{f}}^{\mathrm{int}} \simeq \widetilde{B}_{\mathcal{P}}^\times \times \mathcal{G} .$$

The ring of integers $\mathcal{O}_{\widetilde{B}_{\mathcal{P}}}$ is normalized by $\widetilde{B}_{\mathcal{P}}^\times$, and $\widetilde{B}_{\mathcal{P}}^\times / \mathcal{O}_{\widetilde{B}_{\mathcal{P}}}^\times$ is identified with $\mathbb{Z}$ via the valuation of the norm. Hence the group $G_{\mathrm{f}}^{\mathrm{int}}$ acts on $Y^{\mathrm{int},\mathcal{P}} := \mathcal{O}_{\widetilde{B}_{\mathcal{P}}}^\times \backslash Y^{\mathrm{int}}$ through its quotient

$$G_{\mathrm{f}}^{\mathrm{int}} / \mathcal{O}_{\widetilde{B}_{\mathcal{P}}}^\times \cong \mathcal{G} \times \mathbb{Z} .$$

Let $n \in \mathbb{Z}$ act on $\Omega_{F_{\mathcal{P}}}^{2,\mathrm{nr}}$ through the action of $\mathrm{Fr}_{F_{\mathcal{P}}}^{-n}$ on $F_{\mathcal{P}}^{\mathrm{nr}}$. This gives an $F_{\mathcal{P}}$-rational action of $\mathrm{GL}_2(F_{\mathcal{P}}) \times \mathbb{Z}$ on $\Omega_{F_{\mathcal{P}}}^{2,\mathrm{nr}}$. Let G act on $\Omega_{F_{\mathcal{P}}}^{2,\mathrm{nr}}$ via the embedding $G(F) \hookrightarrow \mathrm{GL}_2(F_{\mathcal{P}})$, and on $\mathcal{G}$ through the natural embedding.

For a compact open subgroup $S \subset \mathcal{G}$, the $F_{\mathcal{P}}$-analytic space $(\Omega^{2,\mathrm{nr}}_{F_{\mathcal{P}}} \times (S\backslash\mathcal{G}))/G(F)$ algebraizes canonically to a projective curve Y_S over $F_{\mathcal{P}}$. The inverse limit of Y_S over such S's is a scheme Y over $F_{\mathcal{P}}$ with an $F_{\mathcal{P}}$-rational action by $\mathcal{G} \times \mathbb{Z}$.

A special case of the main result of [Va1] (see [Va2, Sect. 5]) is the following

Theorem 3.1. *There exists a $\mathcal{G} \times \mathbb{Z}$-equivariant, $F_{\mathcal{P}}$-rational isomorphism*

$$Y^{\mathrm{int},\mathcal{P}} \otimes_F F_{\mathcal{P}} \cong Y\,.$$

4. Local points on Shimura curves

Choose a compact and open subgroup S of $\mathcal{G}$ and a geometrically connected component X of $S\backslash Y^{\mathrm{int},\mathcal{P}} \otimes_F F_{\mathcal{P}}$. By Theorem 3.1, there exists $a \in \mathcal{G}$ such that X is a projective curve X_Γ as considered in Section 2, with $K = F_{\mathcal{P}}, d = 2$ and $\Gamma = \Gamma(aSa^{-1}) = aSa^{-1} \cap G(F) \subset G(F_{\mathcal{P}}) = GL_2(F_{\mathcal{P}})$. This Γ certainly satisfies assumptions (A) and (B) of Section 2.

As in Section 2, Γ gives rise to positive integers k and k_+. Let us define them directly in terms of S. Put $T := S \cap Z_f^{\mathcal{P}} \subset (\mathbb{A}_f^{\mathcal{P}})^\times$, $T_+ := \mathrm{Nm}\, S \subset (\mathbb{A}_f^{\mathcal{P}})^\times$, $\widetilde{T} = T \times \mathcal{O}_{F_{\mathcal{P}}}^\times \subset \mathbb{A}_f^\times$ and $\widetilde{T}_+ = T_+ \times \mathcal{O}_{F_{\mathcal{P}}}^\times \subset \mathbb{A}_f^\times$. Finally set $\mathrm{Cl}_{\widetilde{T}} := \widetilde{T} F_\infty^\times \backslash \mathbb{A}^\times / F^\times$ and $\mathrm{Cl}^+_{\widetilde{T}} := \widetilde{T} F_\infty^+ \backslash \mathbb{A}^\times / F^\times$, and similarly for $\widetilde{T}_+$. Let $\pi_{\mathcal{P}}$ be any uniformizer of $F_{\mathcal{P}}$. Then we have the following

Lemma 4.1. *a) We have* $\mathrm{Nm}\,\Gamma = T_+ \cap F_+^\times$.
b) The integers k and k_+ are the orders of the image of $\pi_{\mathcal{P}}$ in $\mathrm{Cl}_{\widetilde{T}}$ *and in* $\mathrm{Cl}^+_{\widetilde{T}_+}$ *respectively.*

Proof. Notice first that for the proof of the statement we can replace aSa^{-1} by S, thus assuming that $a = 1$. Since $\Gamma = S \cap B^\times$ and B is definite, we get an inclusion $\mathrm{Nm}\,\Gamma \subseteq T \cap F_+^\times$. Conversely, take $t \in T \cap F_+^\times$ (viewed in $(\mathbb{A}_\mathrm{f}^{\mathcal{P}})^\times$). By the Hasse principle $t = \mathrm{Nm}\, b$ for some $b \in B^\times$, and also $t = \mathrm{Nm}\, s$ for some $s \in S$. Then $\mathrm{Nm}\, bs^{-1} = 1$ in $G_\mathrm{f}^{\mathcal{P}}$. By the Eichler-Kneser strong approximation theorem, $bs^{-1} = b_1 s_1$ for some $b_1 \in B$ and $s_1 \in S$, both of norm 1. Then $b_1^{-1} b = s_1 s$ is in Γ and has norm t, proving part a).

Part b) is a routine corollary of a) and the equality $Z\Gamma = T_+ \cap F^\times$, and is left to the reader. □

Finally, in order to assure that our Γ satisfies assumption (C) of Section 2, we assume that the subgroups T and T_+ of $(\mathbb{A}_f^{\mathcal{P}})^\times$ obtained from S satisfy

(*) $T_+ \subset T$.

Remark 4.2. Our restriction of the level at $\mathcal{P}$ means that the level (of G^{int}) at $\mathcal{P}$ is the maximal subgroup compact modulo the center. Some cases of larger level subgroups at $\mathcal{P}$ are discussed in [JL3], and a little bit is known about the simplest case of smaller level at $\mathcal{P}$ ([Tei]), but further information seems to be required to handle the general case. Assumption (*), on the other hand, is mainly for convenience. For example, all congruence subgroups satisfy it.

We can now apply the results of Section 2. As $d = 2$, we have two possibilities: either $k_+ = k$, in which case X is the quadratic unramified twist of $X' \otimes_{F_\mathcal{P}} F_\mathcal{P}^{(k_+)}$, or $k_+ = 2k$, in which case $X \simeq X' \otimes_{F_\mathcal{P}} F_\mathcal{P}^{(k_+)}$. In the latter case we will say that X is *Mumford uniformized*.

For a finite set W of finite primes $\neq \mathcal{P}$ of F, we denote by $K(W)$ the principal congruence subgroup of (squarefree) level $\prod_{\mathcal{Q} \in W} \mathcal{Q}$ in $G_\mathrm{f}^\mathcal{P}$. We will now show that for a "sufficiently small" S we have $k_+ = k$:

Proposition 4.3. *Let W_1 be a finite set of primes of F. Then there exists a finite set W_2 of finite primes of F, disjoint from $W_1 \cup \{\mathcal{P}\}$, such that $k_+ = k$ for any open subgroup $S \subset K(W_2)$ and any $a \in \mathcal{G}$.*

Proof. We view the center $Z\Gamma$ and $\mathrm{Nm}\,\Gamma$ as subgroups of $\mathcal{O}_{F,\mathcal{P}}^\times$, the units away from $\mathcal{P}$ of F. By the Unit Theorem, we have $\mathcal{O}_{F,\mathcal{P}}^\times \simeq (\mathbb{Z}/2\mathbb{Z}) \times \mathbb{Z}^g$. For $0 \le i \le g$, choose $\epsilon_i \in \mathcal{O}_{F,\mathcal{P}}^\times$ whose classes modulo squares are a basis for the $\mathbb{F}_2$-vector space $\mathcal{O}_{F,\mathcal{P}}^\times/(\mathcal{O}_{F,\mathcal{P}}^\times)^2$. A routine application of Chebotarev's Theorem shows that there are primes $\mathcal{Q}_i$, $0 \le i \le g$, not in $W_1 \cup \{\mathcal{P}\}$, such that ϵ_i has a non-square residue modulo $\mathcal{Q}_j$ if and only if $i = j$. Put $W_2 = \{\mathcal{Q}_i\}$. Then for any open subgroup $S \subset K(W_2)$ we have $Z\Gamma = aSa^{-1} \cap F^\times = S \cap F^\times \subset (\mathcal{O}_{F,\mathcal{P}}^\times)^2$, so a fortiori $Z\Gamma = \mathrm{Nm}\,\Gamma$. The Proposition follows. □

Remarks 4.4. 1. It follows from the proof that for $S \subset K(W_2)$ as above, the $\mathcal{P}$-adic valuation of each $x \in Z\Gamma$ is even, hence $k_+ = k$ is even.

2. The Proposition can be strengthened in several ways. If $\epsilon_1, \ldots, \epsilon_h$ are in the subgroup $\mathcal{O}_{F,\mathcal{P}}^+$ of the totally positive elements of $\mathcal{O}_{F,\mathcal{P}}^\times$ and generate it modulo squares, it suffices to take $W_2 = \{\mathcal{Q}_i\}, h < i \le g$. It is also possible to choose W_2 in any set of positive density (with the obvious definition of positive density here), not merely to avoid $W_1 \cup \{\mathcal{P}\}$. In addition, if the primes of $W_1 \cup \{\mathcal{P}\}$ are all prime to 2, one can replace $K(W_2)$ by an open subgroup of $G_\mathrm{f}^\mathcal{P}$ whose level divides some power of 2. We shall not need these facts in the sequel.

We will need the following

Lemma 4.5. *Let $\gamma \in \mathrm{GL}_2(F_\mathcal{P})$ have finite order modulo the center and suppose that* $\mathrm{val}_\mathcal{P} \det \gamma$ *is odd. Then γ reverses a unique edge e_γ of the Bruhat-Tits tree.*

Proof. The subgroup of $\mathrm{PGL}_2(F_\mathcal{P})$ generated by γ is contained in a maximal compact subgroup, hence it fixes a vertex or an edge. Since γ moves each vertex to an odd distance, it cannot fix any vertex, hence must reverse a unique edge. □

Theorem 2.1 now says the following:

Theorem 4.6. *a) If $k_+ = 2k$, or if f is even, then $X(L) \neq \emptyset$.*
b) Suppose $k_+ = k$ and f odd. Then $X(L) \neq \emptyset$ if and only if there exists an element $\gamma \in \Gamma$, of finite order modulo the center, satisfying $\mathrm{val}_{\mathcal{P}} \det \gamma = k$*, such that either ek is even, or ek is odd and the stabilizer H of e_γ in $P\Gamma$ as an* oriented *edge has even order.*

Proof. Part a) is a particular case of part a) of Corollary 2.4. To deduce part b), suppose first $X(L) \neq \emptyset$. Then the subgroup $P\Delta$ of Theorem 2.1 contains an element γ as needed, and either ek is even or $P\Delta'$ has even order. But if ek is odd, then $P\Delta'$ is precisely the stabilizer of e_γ as an oriented edge. Conversely, if ek is even let Δ be the subgroup of $P\Gamma$ generated by γ; and if ek is odd let Δ be the stabilizer in Γ of the unoriented edge e_γ, defined in Lemma 4.5. Then it is immediate that Δ has the properties required in Theorem 2.1, so $X(L) \neq \emptyset$, since $d = 2$ is a prime. □

Corollary 4.7. *If M/L is a finite extension of odd degree, then $X(M) \neq \emptyset$ if and only if $X(L) \neq \emptyset$.*

If S is small enough, then $P\Gamma$ is torsion free. If S moreover satisfies the condition of Proposition 4.3, we shall say we are in the *asymptotic case*. It then follows from the Theorem that

(ASYMP) $\quad k_+ = k,$ and $X(L) \neq \emptyset$ if and only if f is even.

If we only assume that $P\Gamma'$ is torsion free, the Theorem has the following

Corollary 4.8. *If $P\Gamma'$ is torsion free, then $X(L) = \emptyset$ if and only if $k_+ = k$, f is odd, and either ek is also odd or $P\Gamma$ is torsion free.*

Proof. By the theorem, we may assume that $k_+ = k$, that f is odd and that $P\Gamma$ has torsion. It remains to show that $X(L) = \emptyset$ if and only if ek is odd. Assume first that ek is odd. As $P\Gamma'$ is torsion free, no non-trivial element of $P\Gamma$ stabilizes an oriented edge, so we get $X(L) = \emptyset$. Assume now that ek is even. Let $\gamma' \in \Gamma$ be any element of finite order modulo the center. Since $P\Gamma'$ is torsion free, $\mathrm{val}_{\mathcal{P}} \det \gamma' \equiv k \pmod{2k}$. Therefore, modifying γ by an element from $Z\Gamma$, we get an element γ with $\mathrm{val}_{\mathcal{P}} \det \gamma = k$, as claimed. □

At the other extreme, we can pin down the situation rather precisely when $X(L) \neq \emptyset$ and efk_+ is odd (so that $k = k_+$). This will require two lemmas, which we state in slightly more general form than necessary.

For an n^{th} root ζ of 1, let $\mathbb{Q}(\zeta)^+$ be the maximal totally real subfield of the field $\mathbb{Q}(\zeta)$ of n^{th} roots of 1. Then we have the following

Lemma 4.9. *Let ζ be a primitive n^{th} root of* 1*, with $n > 2$. Let $\mathcal{Q}^+$ be a prime ideal of $\mathbb{Q}(\zeta)^+$ of residue characteristic q. Then* $\mathrm{val}_{\mathcal{Q}^+}(1+\zeta)(1+\overline{\zeta}) = 1$ *if $n = 2q^r$ for $r \geq 1$. Otherwise this valuation is* 0.

Proof. Let A be the positive integer $\mathrm{Nm}_{\mathbb{Q}(\zeta)/\mathbb{Q}}(1+\zeta)$. We claim that $A = \ell$ if $n = 2\ell^r$ for a prime ℓ, and $A = 1$ otherwise. Indeed, write $n = 2^r t$ with t odd and $r \geq 0$. If $r = 0$ then $A = 1$ because $\mathrm{Nm}_{\mathbb{Q}(\zeta)/\mathbb{Q}}(1-\zeta) = \mathrm{Nm}_{\mathbb{Q}(\zeta)/\mathbb{Q}}(1-\zeta^2)$. For any u, let Φ_u denote the u^{th} cyclotomic polynomial. If $r = 1$ then $A = \prod_\eta(1-\eta)$, where η goes over all primitive t^{th} roots of 1, so $A = \Phi_t(1)$. Then if t is a power of a prime ℓ, we have $\Phi_t(x) = (x^t - 1)/(x^{t/\ell} - 1) = x^{(\ell-1)t/\ell} + \cdots + 1$, so $A = \ell$; else $t = t't''$ with t', t'' odd and relatively prime. Then $\Phi_t(x)$ divides $Q(x) = (x^{(t'-1)t''} + \cdots + 1)/(x^{t'-1} + \cdots + 1)$, so $A | Q(1) = 1$. Similarly, if $r \geq 2$, then $A = \Phi_n(1)$. Then if $t = 1$, we have $\Phi_n(x) = (x^{n/2} + 1)$, so $A = 2$, whereas if $t > 1$, then $\Phi_n(x)$ divides $Q(x) = \Phi_{2^r}(x^t)/\Phi_{2^r}(x) = (x^{n/2}+1)/(x^{2^{r-1}}+1)$, so $A | Q(1) = 1$. This proves our claim in all cases. The Lemma is now immediate if $n \neq 2q^r$, $r > 0$. Else, recall that $1+\zeta$ is a uniformizer for the (totally ramified) prime $\mathcal{Q}$ of $\mathbb{Q}(\zeta)$ above q and $\mathcal{Q}^+$. Then $\mathrm{val}_{\mathcal{Q}^+}(1+\zeta)(1+\overline{\zeta}) = \mathrm{val}_{\mathcal{Q}}(1+\zeta) = 1$, proving the Lemma. □

Assume that $k_+ = k$, and let γ be as in Theorem 4.6. Then $F(\gamma)$ is a CM extension of F, since it splits the definite algebra B and is $\neq F$. Then $\mathrm{Nm}\,\gamma$ is a (totally positive) generator of $\mathcal{P}^k$. Writing Nm for $\mathrm{Nm}_{K/F}$ for a quadratic extension K of F is unambiguous, because $\mathrm{Nm}_{K/F}$ and the reduced norm of B agree for any F-embedding of K into B. Likewise we let $\overline{x}$ denote both the main involution of B and the (complex) conjugate of any element $x \in K \subset B$.

Lemma 4.10. *Let $F(\gamma)$ be a (quadratic) CM extension of F, such that some power γ^m is in F, with m (> 1) minimal. Suppose that* $\mathrm{Nm}\,\gamma$ *generates a power $\mathcal{P}^k$, $k > 0$, of a prime ideal $\mathcal{P}$ of F, of residue characteristic p. Set $\zeta = \gamma/\overline{\gamma}$. Then γ is an integer of $F(\gamma)$, ζ is a primitive m^{th} root of* 1*, and if m is even, then γ^m is totally negative. Moreover,*

(i) If $m = 2$ then $\gamma^2 = -u$, where $u \in F$ is a positive generator of $\mathcal{P}^k$.
(ii) If $m \neq 2$ then $F(\gamma) = F(\zeta)$, and $\gamma = s(1+\zeta)$ for some $s \in F^\times$.

Proof. γ is an algebraic integer since its power is. The order of ζ is the smallest positive integer n such that $\gamma^n = \overline{\gamma}^n$ or equivalently that $\gamma^n \in F$. Thus $n = m$, as claimed. If m is even, then $\zeta^{m/2} = -1$. Hence $\gamma^m = -\gamma^{m/2}\overline{\gamma}^{-m/2} = -\mathrm{Nm}\,\gamma^{m/2}$ is totally negative as asserted, and we also get (i). For (ii), define $s = \gamma\overline{\gamma}/(\gamma+\overline{\gamma})$, which makes sense since $\overline{\gamma} \neq -\gamma$. Then $\gamma = s(1+\zeta)$ as asserted. □

Remark 4.11. s need not belong to $\mathcal{O}_{F,\mathcal{P}}^\times$: take $F = \mathbb{Q}(\sqrt{6})$, $\mathcal{P} = (3, \sqrt{6})$, and $\gamma = \sqrt{6}(1+\sqrt{-1})/2$. Then $m = 4$, and $\gamma = \sqrt{3}\zeta_8$, but $\sqrt{6}/2$ is not in $\mathcal{O}_{F,\mathcal{P}}^\times$.

Let $t(F)$ be the maximal integer such that the maximal totally real subfield $\mathbb{Q}(\zeta_{2^{t(F)}})^+$ of $\mathbb{Q}(\zeta_{2^{t(F)}})$ is a subfield of F. Then $t(F) \geq 2$. Let τ be the unique prime of $\mathbb{Q}(\zeta_{2^{t(F)}})^+$ lying (and totally ramified) above 2. We now have the following

Proposition 4.12. *In the notation of Theorem 4.6, suppose that fek_+ is odd. Then $X(L) \neq \emptyset$ if and only if either of Conditions (a) or (b) below holds:*

(a) $\mathcal{P}$ lies above τ with odd ramification index $e(\mathcal{P}/\tau)$, and there exists an element γ' of Γ, of order $2^{t(F)}$ modulo the center, such that $\mathrm{val}_{\mathcal{P}} \mathrm{Nm}(\gamma') = k$.

(b) There exist elements α, γ' in Γ, of order 2 modulo the center, such that $\mathrm{val}_{\mathcal{P}} \mathrm{Nm}(\gamma') = k$, $\mathrm{val}_{\mathcal{P}} \mathrm{Nm}(\alpha) = 0$, *and* $\alpha\gamma = -\gamma\alpha$.

Proof. Suppose first that (a) or (b) hold. Lemma 4.1 and the fact that f is odd enable us to modify γ' by a central element in $Z\Gamma$ so as to replace it by an element γ with the same order modulo the center and such that $\mathrm{val}_{\mathcal{P}} \mathrm{Nm}(\gamma) = fk_+$. Since fk_+ is odd, γ reverses an edge. The stabilizer H of this edge contains $\overline{\gamma}^2$ in case (a), and $\overline{\alpha}$ in case (b). Hence its order $|H|$ is even in either case. By Theorem 4.6, $X(L) \neq \emptyset$.

Conversely, if $X(L) \neq \emptyset$ let γ be as in Theorem 4.6. Then an odd power of γ is of order 2^t, $t \geq 1$, modulo the center. Modifying this power by a central element of Γ we get an element γ_1, of order 2^t modulo the center, such that $\mathrm{val}_{\mathcal{P}} \mathrm{Nm}\, \gamma_1 = fk_+$. We now replace γ by γ_1. The new γ has the same fixed edge d' as before, and satisfies the properties of Theorem 4.6, and its order modulo the center is $m = 2^t$.

Suppose first $t = 1$. Theorem 4.6 gives an element $\beta \in H$, of order 2 modulo the center. Let A be the subgroup of $P\Gamma$ generated by the images $\overline{\beta}$ and $\overline{\gamma}$ of β and γ. Since A acts discretely on the tree fixing the unoriented edge $\{d', \overline{d'}\}$, it is a finite group. Since A is generated by 2 involutions it is a dihedral group, and the cyclic subgroup A_0 generated by $\overline{\beta}\overline{\gamma}$ is of index 2. Also $\ell = |A_0|$ is even, because A has *another* subgroup $A_1 \neq A_0$ of index 2, namely the elements of A fixing d'. Hence the group generated by $\overline{\gamma}$ and $\overline{\alpha}$, where $\alpha = (\beta\gamma)^{\ell/2}$, is a non-cyclic group of order 4. Replacing α by $\alpha\gamma$ if necessary, we may assume that $\alpha d' = d'$. In $\Gamma \subset B^\times$ this implies that α^2 and γ^2 are in $F^\times$, that α is in Γ', and that $\gamma\alpha = u\alpha\gamma$ for some $u \in F^\times$. Taking norms (to F) we see that $\mathrm{Nm}_{B/F}\, u = u^2 = 1$, so that $u = \pm 1$. However $u = 1$ is impossible, since in this case α and γ would generate a commutative subgroup of $\mathrm{GL}_2(\mathbb{C})$, whose image modulo the center is finite and non-cyclic, which cannot happen. This gives case (b) of the Proposition.

Suppose next $t \geq 2$. By Lemma 4.10, $\gamma = s(1 + \zeta_{2^t})$ and $F(\gamma) = F(\zeta_{2^t})$, so that F must contain $F_0 = \mathbb{Q}(\zeta_{2^t})^+$. Then $\mathrm{Nm}\, \gamma = s^2\theta$, where $\theta = (1+\zeta_{2^t})(1+\overline{\zeta_{2^t}})$ generates the unique prime τ_0 of F_0 lying over 2. By Lemma 4.9 we get

$$fk_+ = \mathrm{val}_{\mathcal{P}}\, s^2\theta \equiv e(\mathcal{P}/\tau_0)\, \mathrm{val}_{\tau_0}\, \theta = e(\mathcal{P}/\tau_0) \pmod 2.$$

This shows that $e(\mathcal{P}/\tau_0)$ is odd.

Finally we check that $t = t(F)$. From its definition $t \leq t(F)$; but if $t(F) \geq t+1$ then $e(\mathcal{P}/\tau_0)$ would be divisible by the ramification index of τ_0 in $\mathbb{Q}(\zeta_{2^{t+1}})^+$, which is 2, contradicting the fact that $e(\mathcal{P}/\tau_0)$ is odd. Hence $t = t(F)$, concluding the proof of the Proposition. □

Remark 4.13. In case (b) above, the isomorphism type of the quaternion algebras B and B^{int} is almost forced. Indeed, for $a_1, a_2 \in F^\times$ let $B(a_1, a_2)$ denote the quaternion algebra over F with basis $1, \hat{\imath}, \hat{\jmath}, \hat{k}$ satisfying $\hat{\imath}^2 = a_1$, $\hat{\jmath}^2 = a_2$, and $\hat{k} = \hat{\imath}\hat{\jmath} = -\hat{\jmath}\hat{\imath}$. Then $B(a_1, a_2)$ is ramified at a place v of F if and only if the Hilbert symbol $(a_1, a_2)_{F_v}$ is -1. In case (b) we have $B \simeq B(-\operatorname{Nm}\gamma, -\operatorname{Nm}\alpha)$, so that B, in addition to being totally definite, is unramified away from primes above 2 (we know it is unramified at $\mathcal{P}$). For example, if $F = \mathbb{Q}$ we get that $B \simeq \mathbb{H} = B(-1, -1)$, the Hamilton quaternions over $\mathbb{Q}$; if F is (real) quadratic, then B is isomorphic to the base change of $\mathbb{H}$ to F, or is "the" totally definite algebra of discriminant 1 (or both). It is clear, however, that matters can get complicated when F has many primes above 2.

5. Relevant deficient local fields

Let $\widetilde{S}$ be an open and compact subgroup of $G_{\text{f}}^{\text{int}}$, and let X be a geometrically connected component of $\widetilde{S}\backslash Y^{\text{int}}$. Then under certain assumptions we will determine the *deficient* local fields for X in the sense of [JL1], namely those local fields L containing the field of definition of X for which $X(L) = \emptyset$. In fact, we will consider only those local fields which are either archimedean or are finite extensions of completions $F_{\mathcal{P}}$ for finite prime $\mathcal{P}$ of F dividing Disc B^{int}. (These local fields we will call *relevant*.)

The first our assumption is as follows.

(Max) $\widetilde{S}$ a maximal compact subgroup of $G_{\text{f}}^{\text{int}}$.

All such $\widetilde{S}$'s are conjugate in $G_{\text{f}}^{\text{int}}$. In fact they are the units of any maximal $\mathcal{O}_F$-order $\mathcal{M}^{\text{int}}$ of B^{int}.

Let $\mathcal{P}$ be a finite prime of F dividing Disc B^{int}. Then in the notation of Section 3, each such $\widetilde{S}$ decomposes as a product $S \times \mathcal{O}_{\widetilde{B}_{\mathcal{P}}}^\times$ for a certain maximal compact subgroup S of $\mathcal{G}$. Such an S is the group of units of $\mathcal{M} \otimes_{\mathcal{O}_F} \mathbb{O}_{\text{f}}^{\mathcal{P}}$ for a maximal $\mathcal{O}_F[1/\mathcal{P}]$-order $\mathcal{M}$ of B. Therefore it satisfies assumption (*) from Section 4.

The conjugacy classes of the $\mathcal{M}^{\text{int}}$'s in B^{int} and of the $\mathcal{M}$'s in B are classified by appropriate quotients of $\operatorname{Cl}(F)/2\operatorname{Cl}(F)$: (See e. g. [CF, Section 3] for the case of the $\mathcal{M}^{\text{int}}$'s). To avoid complications we shall therefore add the following assumption:

(Odd) The narrow class number $h^+(F)$ is odd.

We list some consequences of assumption (Odd) in the following

Lemma 5.1. *(a) For every $1 \leq i \leq g(= [F : \mathbb{Q}])$ there exists a unit ϵ_i of F satisfying $\infty_i(\epsilon_i) > 0$ and $\infty_j(\epsilon_i) < 0$ for any $j \neq i$, $1 \leq j \leq g$.*
(b) Totally positive units in F are squares.
(c) All the $\mathcal{M}^{\text{int}}$'s are conjugate in B^{int} and all the $\mathcal{M}$'s are conjugate in B.
(d) All the geometrically connected components of $\widetilde{S}\backslash Y^{\text{int}}$ are isomorphic.
(e) The quotient of the normalizer of $\mathcal{M}^{\text{int}}$ in B^{int}_+ by $Z(B^{\text{int}})^\times(\mathcal{M}^{\text{int}})^\times$ is a finite group $(\mathbb{Z}/2\mathbb{Z})^r$, where r is the number of primes dividing Disc B^{int}*, and where by B^{int}_+ we denote the set of elements of B^{int} whose norm is totally positive.*

Proof. Though the proof is straightforward, we will sketch it for the convenience of the reader. Our assumption (Odd) is equivalent to the decomposition

$$\mathbb{A}^\times = (\mathbb{A}^\times)^2 \mathbb{O}_{\mathrm{f}}^\times F^\times. \tag{2}$$

Then $-\epsilon_i$ is any element of $F^\times$ appearing in the decomposition of the idèle -1 in $F^\times_{\infty_i} \subset \mathbb{A}^\times_F$, implying (a). (b) now follows from (a) together with the fact that $\{-\epsilon_1, \dots, -\epsilon_g\}$ form a basis of the $\mathbb{F}_2$-vector space $\mathcal{O}_F^\times/(\mathcal{O}_F^\times)^2$.

The decomposition (2) implies a decomposition $\mathbb{A}_{\mathrm{f}}^\times = (\mathbb{A}_{\mathrm{f}}^\times)^2\mathbb{O}_{\mathrm{f}}^\times F_+^\times$. Using the strong approximation theorem, we get that

$$\mathbf{G}^{\text{int}}(\mathbb{A}_{\mathrm{f}}) = \mathbf{Z}(\mathbf{G}^{\text{int}})(\mathbb{A}_{\mathrm{f}})\mathbf{G}^{\text{int}}(\mathbb{O}_{\mathrm{f}})\mathbf{G}^{\text{int}}(F)_+, \tag{3}$$

where $\mathbf{G}^{\text{int}}(F)_+ = B^{\text{int}}_+$, and similarly for $\mathbf{G}$ (compare the proof of Lemma 4.1). This decomposition immediately implies part (d) and reduces the remaining parts to the corresponding local statements, which are clear. □

Now we are ready to determine the relevant deficient local fields for X. Observe that assumption (Max) implies that the field of definition F' of X is a Hilbert class field of F. Furthermore, by assumption (Odd), F' is an abelian extension of F of odd degree. In particular, it is totally real.

The archimedean case had been settled in much greater generality by Shimura [Shi]. His results specialize in our case to the following

Proposition 5.2. *Let ∞ be a place of F' above ∞_i. Then $X(F'_\infty) \neq \emptyset$ if and only if $F(\sqrt{\epsilon_i})$ does not split at any prime where B^{int} ramifies, where ϵ_i is as in Lemma 5.1. (Equivalently, if no finite prime of F dividing* Disc B^{int} *splits in $F(\sqrt{\epsilon_i})$).*

Proof. For the convenience of the reader and for comparison with the non-archimedean case, we shall briefly sketch the proof.

The theorem on conjugation of Shimura varieties allows us to assume that B^{int} splits at ∞_i. By Lemma 5.1 (d), we get that $(X \otimes_{F'} \mathbb{C}_\infty)^{\text{an}} \simeq \Gamma\backslash\mathcal{H}$. Then

$$X(F'_\infty) \neq \emptyset \quad \Leftrightarrow \quad (\exists x \in \mathcal{H}, \exists \gamma \in \Gamma : \gamma(x) = \overline{x}).$$

In this case $\gamma^2(x) = x$, hence some power γ^k of γ is central. Also $\det \gamma < 0$, so γ is conjugate in $\mathrm{GL}_2(F'_\infty) = \mathrm{GL}_2(F_{\infty_i})$ to a matrix $\begin{bmatrix} \alpha & 0 \\ 0 & -\beta \end{bmatrix}$ with $\alpha, \beta > 0$. Then $(\alpha/\beta)^k = 1$ since γ^k is central, so that $\alpha = \beta$. It follows that $\epsilon := \gamma^2 = \alpha^2$ is in $\Gamma \cap F = \mathcal{O}_F^\times$. By Lemma 5.1 (b), we have $F(\sqrt{\epsilon_i}) = F(\sqrt{\epsilon})$, so that this field splits B^{int} and hence cannot be split (over F) at any prime dividing Disc B^{int}.

Conversely, assume that $F(\sqrt{\epsilon_i})$ is not split at any prime dividing Disc B^{int}. Then $F(\sqrt{\epsilon_i})$ embeds into B^{int}, and the image γ of $\sqrt{\epsilon_i}$ must belong to some maximal order of B^{int}. By Lemma 5.1 (c), we may assume that $\gamma \in \Gamma$. Moreover, γ is conjugate in $\mathrm{GL}_2(F_{\infty_i})$ to a matrix $\begin{bmatrix} \alpha & 0 \\ 0 & -\alpha \end{bmatrix}$, since $\gamma^2 = \epsilon_i$ is a scalar negative at ∞_i. Hence there exists $x \in \mathcal{H}$ such that $\gamma(x) = \overline{x}$, therefore $X(F'_\infty) \neq \emptyset$. □

Finally, fix a finite prime $\mathcal{P}$ dividing Disc B^{int}, and let S and B be as in the beginning of the section. Then we get $\widetilde{S}\backslash Y^{\mathrm{int}} = S\backslash Y^{\mathrm{int},\mathcal{P}}$. Hence to determine rational points of X over finite extensions of $F_{\mathcal{P}}$ we may replace X by the corresponding component of $S\backslash Y^{\mathrm{int},\mathcal{P}} \otimes_F F_{\mathcal{P}}$. In particular, we can apply the notation and the results of Section 4.

Let π be a totally positive generator of the principal ideal $\mathcal{P}^{k_+}$, and let L be a finite extension of $F_{\mathcal{P}}^{(k_+)}$.

Proposition 5.3. *Assume that assumptions (Odd) and (Max) hold and that the degree $[L : F_{\mathcal{P}}] = efk_+$ is odd. Then in the notation of Proposition 4.12, we have that $X(L) \neq \emptyset$ if and only if either of conditions (a) or (b) below holds:*

(a) In the notation of Proposition 4.21 $f(\zeta_{2^{t(F)}})$ splits B, and $\mathcal{P}$ lies above τ with odd ramification index.
(b) B is isomorphic to $B(-1, -\pi)$.

Proof. We will check that our conditions (a) and (b) are equivalent to the corresponding conditions of Proposition 4.12. The equivalence of conditions (b) follows from Remark 4.13 and Lemma 5.1 (b). Since $t(F) \geq 2$, Lemma 4.10 (ii) implies that our condition (a) follows from that of Proposition 4.12.

Finally assume our assumption (a) and choose an embedding of $F(\zeta_{2^{t(F)}})$ into B. Observe that $\gamma := 1 + \zeta_{2^{t(F)}}$ is an algebraic integer such that $\mathrm{Nm}\,\gamma \in \mathcal{O}_{F,\mathcal{P}}^\times$. Lemma 5.1 (c) implies that some conjugate γ'' of γ belongs to Γ. By Lemma 4.10, γ'' is of order $2^{t(F)}$ modulo the center, and by Lemma 4.9,

$$\mathrm{val}_{\mathcal{P}}\,\mathrm{Nm}(\gamma'') = e(\mathcal{P}/\tau)\,\mathrm{val}_\tau(1 + \zeta_{2^{t(F)}})(1 + \overline{\zeta}_{2^{t(F)}}) = e(\mathcal{P}/\tau)$$

is odd. Hence using Lemma 4.1 we can modify γ'' by an element of $Z\Gamma$ to get an element γ' satisfying $\mathrm{val}_{\mathcal{P}}\,\mathrm{Nm}(\gamma') = k$. □

6. Evenness of jacobians of Shimura curves

In [PS] Poonen and Stoll defined a dichotomy of principally polarized abelian varieties over a global field E into even and odd cases. When the abelian variety is a jacobian of a curve C/E they gave the following criterion for the evenness in terms of C.

Let $g(C)$ be the genus of C. We will call a (finite or infinite) prime v of E *PS-deficient* (that is deficient in the sense of [PS]) if C has no E_v-rational divisor of degree $g(C) - 1$. As it was explained in [JL2, Prop. 1.1], a prime v of E is not PS-deficient for X if v is a finite prime of E in which C has good reduction. In particular, the number of PS-deficient primes is always finite. The criterion of Poonen-Stoll [PS, Cor. 10] asserts that the Jacobian of C/E is even if and only if the number of PS-deficient primes of C is even.

We will apply this criterion to certain Shimura curves X, considered in Section 5, generalizing [PS, Thm. 23].

Theorem 6.1. *Assume that F is a quadratic extension of $\mathbb{Q}$ and that assumptions (Max) and (Odd) hold. For technical reasons assume also that F is not isomorphic to $\mathbb{Q}(\sqrt{2}\,)$ and that* Disc B^{int} *is not a prime of residual characteristic* 2*. Then the Jacobian of X/F' is even.*

Before starting the proof we will need certain preparations. Similarly to Section 5, we will call a prime of F' *relevant* if it is either infinite of divides Disc B^{int}. The following result is a straighforward generalization of [JL2, Thm. 2 a)].

Proposition 6.2. *A prime v of F' is PS-deficient for X if and only if it is a relevant deficient prime for X, and the genus of X is even.*

Proof. Assume first that v is relevant and deficient for X. Then we claim that X has a rational point over a certain quadratic extension of F'_v, but it does not have rational points over all extensions of F'_v of odd degree. Indeed, if v is infinite, then $F'_v = \mathbb{R}$, in which case the statement is clear. Assume now that v is finite. Then Theorem 4.6 a) implies that X has a rational point over $F'^{(2)}_v$. This shows the first statement, while the second one follows from Corollary 4.7.

It follows from the claim that X has a F'_v-rational divisor of degree 2 (hence of arbitrary even degree), but does not have F'_v-rational divisors of odd degree. Thus a relevant deficient prime of X is PS-deficient if and only if the genus of X is even.

Conversely, suppose that v is PS-deficient. Then it is clearly deficient. On the other hand, [JL2, Prop. 1.1] implies that v is either infinite or a finite prime of bad reduction of X. Since Morita proved in [Mo] that all finite primes of bad reduction of X divide Disc B^{int}, v is relevant, as claimed. □

Also we shall need the following

Proposition 6.3. *Let* $F = \mathbb{Q}(\sqrt{m})$ *for a prime* $m \equiv 1 \mod 4$. *Suppose that* Disc B^{int} *is an odd prime* $\mathcal{P}$ *of* F. *Let* k_+ *be the order of* $\mathcal{P}$ *in* $\text{Cl}^+(F)$, *and let* π *be a totally positive generator of* $\mathcal{P}^{k_+}$. *Then*

(i) The number of infinite deficient primes of X *is even if and only if* $(-1, -\pi)_{F_\mathcal{P}} = 1$.
(ii) The number of finite relevant deficient primes of X *is even if and only if* $(-1, -\pi)_{F_\mathcal{Q}} = 1$ *for* $\mathcal{Q} = \mathcal{P}$ *and for all* $\mathcal{Q}$ *of residue characteristic* 2.

Proof. As F' is an abelian extension of F of odd degree, the number of primes of F' above each of ∞_1, ∞_2, and $\mathcal{P}$ is odd and they are deficient simultaneously. For the infinite primes, the fields $F(\sqrt{\epsilon_i})$ are unramified at $\mathcal{P}$ since $\mathcal{P}$ is odd. By Proposition 5.2, the number of deficient infinite primes is even if and only if $\mathcal{P}$ is split in both or inert in both these fields. This happens if and only if $\left(\frac{-1}{\mathcal{P}}\right) = \left(\frac{\epsilon_1}{\mathcal{P}}\right)\left(\frac{\epsilon_2}{\mathcal{P}}\right) = 1$, which is equivalent to $(-1, -\pi)_{F_\mathcal{P}} = 1$, as k_+ and $\mathcal{P}$ are odd.

For (ii) notice as before that only case (b) of Proposition 5.3 can happen since $\mathcal{P}$ is odd. Thus the number of finite relevant deficient primes of X is even if and only if the quaternion algebra $B(-1, -\pi)$ splits at all the finite places of F. The assertion now follows from Remark 4.13. □

Corollary 6.4. *(a) If* $m \equiv 5 \mod 8$ *then the number of relevant deficient primes for* X *is even.*
(b) If $m \equiv 1 \mod 8$ *and* $\mathcal{P} = p\mathcal{O}_F$ *with* p *a rational prime (inert in* F, *i. e.* $\left(\frac{m}{p}\right) = -1$*) which is* $\equiv 1 \mod 4$, *then the number of relevant deficient primes for* X *is odd.*

Proof. (a) The condition on m means that the rational prime 2 is inert in F. By the product formula, $(-1, -\pi)_{F_\mathcal{P}} = (-1, -\pi)_{F_2}$, so the assertion follows.
(b) Since p is inert in F then without loss of generality $\pi = p^{k_+}$. Also -1 is a square in $F_p = F_\mathcal{P}$, so $(-1, -\pi)_{F_\mathcal{P}} = 1$. By the proposition, the number of infinite deficient primes is even. Now let λ be a prime of F above 2. As 2 splits in F and k_+ is odd, we get

$$(-1, -\pi)_{F_\lambda} = (-1, -p)_{\mathbb{Q}_2} = (-1, -p)_\mathbb{R}(-1, -p)_{\mathbb{Q}_p} = -1,$$

and the claim follows from the Proposition.

□

Proof of Theorem 6.1. The discriminant of B^{int} is a product of an odd number r of finite primes of F. By Lemma 5.1 (e), the group $W \simeq (\mathbb{Z}/2\mathbb{Z})^r$ acts naturally on X. The stabilizer of a point $x \in \mathcal{H}$ in W must be cyclic, hence trivial or of order 2. Let n be the number of non-free W-orbits in X. Then the genera $g(X)$ and $g(X/W)$ of X and of X/W are related by

$$2 - 2g(X) = |W|(2 - 2g(X/W)) - n\ |W|/2.$$

Hence if $r \geq 3$ it follows that $4|2 - 2g(X)$ so that $g(X)$ is odd and the jacobian $\mathrm{Jac}(X)$ is certainly even. Now assume $r = 1$, so that Disc $B^{\mathrm{int}} = \mathcal{P}$ for a prime $\mathcal{P}$ of F of residual characteristic p. By genus theory ([BSh, Ch. 3.8, Cor.]), assumption (Odd) forces $F = \mathbb{Q}(\sqrt{m})$ for a prime m which is either 2 or $\equiv 1 \mod 4$. The case $m = 2$ is excluded by our assumption. If $g(x)$ is odd, there is nothing to prove. Else we must be in either case 1.(a) or 1.(b)(i) of [Sad, Theorem 1.1].

In the first of these cases $m \equiv 5 \mod 12$ so that 3 is inert in F and $\mathcal{P} = 3\mathcal{O}_F$. Then $(-1, -3)_{F_p} = 1$, so that the number of deficient infinite primes is even. We need therefore to show that the number of relevant deficient finite primes is even as well; equivalently, by Proposition 6.3, that $(-1, -3)_{F_\mathcal{Q}} = 1$ for all finite primes $\mathcal{Q}$ of residue characteristic 2. Set $(-1, -3)_{F_2} = \prod_\mathcal{Q}(-1, -3)_{F_\mathcal{Q}}$, where the product is over $\mathcal{Q}$ of residue characteristic 2. By the product formula $(-1, -3)_{F_2} = 1$, so that if 2 is inert we are done. If 2 is split (the only case left), then for a prime $\mathcal{Q}$ above 2 we have $F_\mathcal{Q} = \mathbb{Q}_2$, so that

$$(-1, -3)_{F_\mathcal{Q}} = (-1, -3)_{\mathbb{Q}_2} = (-1)^{\frac{(-1-1)}{2}\frac{(-3-1)}{2}} = 1,$$

proving again what we need.

In the other case, $m \equiv 5 \mod 8$, so Corollary 6.4(a) shows that the number of relevant deficient primes is even, concluding the proof of the Theorem. □

References

[Ber] Berkovich, V.G.: Spectral Theory and Analytic Geometry over non-Archimedean Fields. Mathematical Surveys and Monographs 33, American Mathematical Society, Providence, 1990

[BSh] Borevich, A.I., Shafarevich, I.R.: Number Theory. Academic Press, New York-London, 1966

[Ch] Cherednik, I.V.: Uniformization of algebraic curves by discrete arithmetic subgroups of $\mathbf{PGL_2}(K_w)$ with compact quotients. Math. USSR Sb. **29**, 55–85 (1976)

[CF] Chinburg, T., Friedman, E.: An embedding theorem for quaternion algebras. J. London Math. Soc. **60**, 33–44 (1999)

[De1] Deligne, P.: Variétés de Shimura : Interprétation modulaire, et techniques de construction de modèles canoniques. Proc. Symposia in Pure Math. **33**, 247–290 (1979)

[De2] Deligne, P.: Travaux de Shimura , Sém. Bourbaki. Fév. 1971, Exposé 389, Lecture Notes Math. 244, Springer, Heidelberg, 1971

[JL1] Jordan, B.W., Livné, R.: Local diophantine properties of Shimura curves. Math. Ann. **270**, 235–248 (1985)

[JL2] Jordan, B.W., Livné, R.: Divisor classes on Shimura curves rational over local fields. J. reine angew. Math. **378**, 46–52 (1985)

[JL3] Jordan, B.W., Livné, R.: On Atkin-Lehner quotients of Shimura curves. Bull. London Math. Soc. **31**, 681–685 (1999)

[Kur] Kurihara, A.: On some examples of equations defining Shimura curves and the Mumford uniformization. J. Fac. Sci. Univ. Tokyo, Sec. 1A **25**, 277–301 (1979)

[Mil] Milne, J.: Canonical models of (mixed) Shimura varieties and automorphic vector bundles. In: L. Clozel and J. S. Milne, Automorphic Forms, Shimura Varieties, and L-functions, Perspectives in Mathematics 10, Academic Press, San Diego, 1990

[Mo] Morita, Y.: Reduction modulo $\mathcal{P}$ of Shimura curves. Hokkaido Math. J. **10**, 209–238 (1981)

[Mum] Mumford, D.: An analytic construction of degenerating curves over complete local rings. Compositio Math. **24**, 129–174 (1972)

[Mus] Mustafin, G.A.: Nonarchimedean uniformization. Math. USSR Sb. **34**, 187–214 (1978)

[PS] Poonen, B., Stoll, M.: The Cassels-Tate pairing on polarized abelian varieties. Ann. Math. **150**, 1109–1149 (1999)

[Sad] Sadykov, M.: Parity of genera of Shimura curves over a real quadratic field. Preprint 336 at the Algebraic Number Theory Archives, available at http://www.math.uiuc.edu/Algebraic-Number-Theory, 2/14/02

[Shi] Shimura, G.: On the real points of an arithmetic quotient of a bounded symmetric domain. Math. Ann. **215**, 135–164 (1975)

[Tei] Teitelbaum, J.: On Drinfeld's universal formal group on the p -adic upper half plane. Math. Ann. **284**, 647–674 (1989)

[Va1] Varshavsky, Y.: p-adic uniformization of unitary Shimura varieties. Publ. Math. IHES **87**, 57–119 (1998)

[Va2] Varshavsky, Y.: P-adic uniformization of unitary Shimura varieties, II. J. Diff. Geom. **49**, 75–113 (1998)