ISRAEL JOURNAL OF MATHEMATICS 140 (2004), 319–332

DESCENT ON CERTAIN SHIMURA CURVES

BY

ALEXEI SKOROBOGATOV

Department of Mathematics, Imperial College London
South Kensington Campus, London SW7 2AZ, England
e-mail: a.skorobogatov@imperial.ac.uk

AND

ANDREI YAFAEV

Department of Mathematics, University College London
25 Gordon Street, London, WC1H OAH, England
e-mail: yafaev@math.ucl.ac.uk

ABSTRACT

We give an explicit procedure for constructing Shimura curves analogous to the modular curves $X_0(N)$ that are counterexamples to the Hasse principle over imaginary quadratic fields. These counterexamples are accounted for by the Manin obstruction.

Introduction

The aim of this note is to show that descent can be used to establish the non-existence of rational points on certain Shimura curves over number fields, in particular, in the case when rational points exist everywhere locally. Our result is an easy to implement algorithm which, when it applies, says that a particular Shimura curve gives a counterexample to the Hasse principle over many imaginary quadratic fields. All these counterexamples are automatically accounted for by the Manin obstruction.

We always consider Shimura curves attached to indefinite quaternion division algebras over $\mathbf{Q}$. Shimura proved that these curves have no real points [Sh]. Jordan and Livné determined the non-archimedian local fields over which a given

Received November 14, 2002 and in revised form May 15, 2003

Shimura curve without level structure has rational points [JL]. Little seems to be known about rational points on Shimura curves over global fields, though some interesting results were obtained by B. Jordan in [J]. In particular, he showed that the Hasse principle for such curves does not always hold: he gave an explicit example of a Shimura curve which has no point rational over $\mathbf{Q}(\sqrt{-13})$ but does have rational points over all completions of this field. Jordan and Livné consider only Shimura curves without level structure (the compact open subgroup in Deligne's definition of Shimura varieties is maximal at all places). In this paper we consider Shimura curves with level structure, more precisely, the Shimura curves analogous to the modular curves $X_0(N)$.

Let B be an indefinite quaternion algebra over $\mathbf{Q}$ of reduced discriminant $D \neq 1$. We fix once and for all a maximal order $O \subset B$. Let $O^1 \subset O$ be the group of elements of reduced norm 1. Let N be an odd prime not dividing D. Then $O \otimes \mathbf{Z}/N$ is isomorphic to the matrix algebra $M_2(\mathbf{Z}/N)$. Let $O_0^1 \subset O^1$ be the preimage of the subgroup

$$\left\{ \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \right\} \subset \mathrm{SL}_2(\mathbf{Z}/N)$$

under the reduction map $O^1 \to \mathrm{SL}_2(\mathbf{Z}/N)$. Similarly, let $O_1^1 \subset O^1$ be the preimage of the subgroup

$$\left\{ \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \right\} \subset \mathrm{SL}_2(\mathbf{Z}/N).$$

We view O^1, O_0^1 and O_1^1 as arithmetic subgroups of $\mathrm{SL}_2(\mathbf{R})$ under the identification $B \otimes \mathbf{R} \simeq M_2(\mathbf{R})$, and consider the compact Riemann surfaces that are obtained as the quotients of the upper half plane by these groups. Shimura showed that these Riemann surfaces have 'canonical models' which are smooth and projective algebraic curves over $\mathbf{Q}$. Let S (resp. Y, resp. X) be the curve corresponding to O^1 (resp. O_0^1, resp. O_1^1).

Let $f\colon X \to Y$ and $g\colon Y \to S$ be the natural maps. Since O_1^1 is normal in O_0^1, the map f is a Galois covering. The corresponding Galois group is $(\mathbf{Z}/N)^*/\pm 1 \simeq \mathbf{Z}/\frac{N-1}{2}$. Both maps are unramified provided we assume the following

CONDITION 1: *D is divisible by a prime congruent to 1 modulo 4, and a prime congruent to 1 modulo 3.*

Indeed, under this condition the action of $O^1/\pm 1$ on the upper half plane is free (there are no elliptic points; see [V], 3). Then $f\colon X \to Y$ is a Y-torsor under the group scheme $(\mathbf{Z}/N)^*/\pm 1$.

Let k be an imaginary quadratic field, $\Gamma_k = \mathrm{Gal}(\overline{k}/k)$, and let $\mathbf{A}_k$ be the ring of adèles of k. Our aim is to find examples when $Y(k) = \emptyset$ but $Y(\mathbf{A}_k) \neq \emptyset$. To show that $Y(k) = \emptyset$ we apply descent to the torsor $f\colon X \to Y$ (see [S] for a general introduction). The Galois cohomology group $H^1(k, (\mathbf{Z}/N)^*/\pm 1)$ is the group of characters of Γ_k with values in $(\mathbf{Z}/N)^*/\pm 1$. For $\sigma \in \mathrm{Hom}(\Gamma_k, (\mathbf{Z}/N)^*/\pm 1)$ we define X^σ as the twisted form of X with respect to the action of $(\mathbf{Z}/N)^*/\pm 1$ on X by automorphisms. The collection of natural maps $f^\sigma\colon X^\sigma \to Y$ is a 'covering family', in the sense that the set $Y(k)$ is the disjoint union of $f^\sigma(X^\sigma(k))$ for all characters σ. (A point $P \in Y(k)$ is in the image of $X^\sigma(k)$, where σ corresponds to the class of the k-torsor $f^{-1}(P)$ in $H^1(k, (\mathbf{Z}/N)^*/\pm 1)$.) If for every σ there is a place v of k such that $X^\sigma(k_v) = \emptyset$ we conclude that Y has no k-point. Moreover, by the descent theory (see, e.g., [S], 6.1.3 (1)), the counterexample to the Hasse principle provided by Y_k is then accounted for by the Manin obstruction.

In this note we show how to produce triples of positive integers (D, N, d) such that the Shimura curve Y, analogous to $X_0(N)$, attached to the indefinite quaternion algebra over $\mathbf{Q}$ of reduced discriminant D has the following property. Let $k = \mathbf{Q}(\sqrt{-d})$. For any character $\sigma \in \mathrm{Hom}(\Gamma_k, (\mathbf{Z}/N)^*/\pm 1)$ there is a place v of k such that $X^\sigma(k_v)$ is empty, while Y has k_w-points for any place w of k. Then $Y(k) = \emptyset$. For example, one can take $D = 35$, $N = 23$, $d = 127$ (or $d = 142$). When $Y(k) \neq \emptyset$ our method is obviously doomed to failure. When the method actually fails (e.g., for $D = 26$ or $D = 39$, and $N = 11$) it may or may not be because of possible k-points on Y.

Note that if the class number of $k = \mathbf{Q}(\sqrt{-d})$ is not 1, then a theorem of Jordan implies that for infinitely many values of D the curve S has no k-points ([J], Thm. 6.6). Then $Y(k)$ is also empty. However, Jordan's result does not seem to rule out the possibility that $Y(k_v) = \emptyset$ for some completion k_v. Earlier Shimura observed that if the class number of $k = \mathbf{Q}(\sqrt{-d})$ is 1, and every prime factor of D is inert or ramified in k, then a point of complex multiplication is a k-point on S, so that $S(k) \neq \emptyset$.

The methods of this paper do not allow us to treat Jordan's counterexample to the Hasse principle mentioned above. See [SS] for an elementary proof (based on the conjectured equation of this Shimura curve) that this counterexample is explained by the Manin obstruction.

Although we work with imaginary quadratic fields, our method can be implemented over more general number fields.

1. Good reduction

1.1. REDUCTION TO THE CASE WHEN σ IS A POWER OF THE CYCLOTOMIC CHARACTER. If K is a field, X_K a projective K-scheme acted on by a finite K-group scheme G_K, and P a (right) K-torsor under G_K, then the twist of X_K by P is defined as the quotient $X_K^P := (X_K \times_K P)/G_K$ by the simultaneous action of G_K on both factors. The following fact is well known. We sketch a proof here for the sake of completeness.

LEMMA 1.1: *Let R be a discrete valuation ring with field of fractions K. Let X be a smooth and projective R-scheme, and let G be a finite étale R-group scheme acting freely on X. Let P be a (right) K-torsor under G. If the twist X_K^P has a K-point, then P is unramified, that is, P becomes trivial over a maximal unramified extension of K.*

Proof: (See, e.g., [S], p. 106.) The morphism of R-schemes $X \to Z = X/G$ is a torsor under G. A K-point on X_K^P projects to a K-point on Z whose preimage in X is isomorphic to P. By the properness of Z any K-point extends to an R-point. Its preimage in X is an R-torsor under G whose generic fibre is P. Hence P is unramified. ∎

We apply this lemma to the following situation. Let $(\mathbf{Z}/N)^*/\pm 1$ be the obvious 'constant' étale group $\mathbf{Z}$-scheme, and let k be an imaginary quadratic field. The étale morphism of smooth, projective and geometrically irreducible k-curves $f\colon X \to Y$ endows X with the structure of a Y-torsor under $(\mathbf{Z}/N)^*/\pm 1$. The morphism f extends to a morphism of relative curves which are smooth and proper over $\mathbf{Z}[1/DN]$, with geometrically integral fibres (see [B]). This morphism defines a torsor under $(\mathbf{Z}/N)^*/\pm 1$.

The k-torsors of $(\mathbf{Z}/N)^*/\pm 1$ up to isomorphism are classified by the characters of the Galois group of k, that is,

$$\sigma \in H^1(k, (\mathbf{Z}/N)^*/\pm 1) = \mathrm{Hom}(\Gamma_k, (\mathbf{Z}/N)^*/\pm 1).$$

By Lemma 1.1 a necessary condition for a twist X^σ to have a point in the completion k_v of k at a place v not dividing DN is that σ must be unramified at v. This means that the restriction of σ to the inertia group at v is trivial. Therefore, while checking that $X^\sigma(\mathbf{A}_k) = \emptyset$ it is enough to consider characters unramified away from primes dividing DN.

CONDITION 2: *$(N-1)/2$ is coprime to $p(p^2-1)$, for all prime factors $p|D$.*

The inertia group at a prime v of k over $p|D$ is an extension of a group of order $p-1$ (if p is split or ramified in k) or p^2-1 (p inert) by a pro-p-group. The

assumption just made implies that σ is unramified at such primes of k. Thus σ can be ramified only at the prime(s) over N.

CONDITION 3: *The class number of k is coprime to $(N-1)/2$.*

CONDITION 4: *N is inert in k.*

These assumptions imply that σ is uniquely determined by its restriction to the Galois group of k_v, $v|N$. Indeed, if σ is unramified everywhere, then it comes from a character of the class group of k, and hence in our assumptions must be trivial.

Let ζ_N be a non-trivial N-th root of unity. Consider $L = \mathbf{Q}(\zeta_N)^+$, the maximal real subfield of the cyclotomic field $\mathbf{Q}(\zeta_N)$. This is a cyclic extension of $\mathbf{Q}$ with Galois group $(\mathbf{Z}/N)^*/\pm 1$, corresponding to (the image of) the cyclotomic character $c(p) = p \bmod N$. It is unramified away from N. Since $L \subset \mathbf{R}$ we have $L \cap k = \mathbf{Q}$, hence Lk is an extension of k with Galois group $(\mathbf{Z}/N)^*/\pm 1$, corresponding to the restriction of c to Γ_k. This restriction is a generator of the group of characters of Γ_k with values in $(\mathbf{Z}/N)^*/\pm 1$ that are unramified away from N. We have proved the following statement.

PROPOSITION 1.2: *Suppose that D, N and k satisfy Conditions 1, 2, 3 and 4. Then $X^\sigma(\mathbf{A}_k) = \emptyset$ unless σ is a power of the cyclotomic character corresponding to the field extension Lk/k.*

1.2. ZETA-FUNCTIONS. It is well known that X and Y have smooth and proper models over $\mathbf{Z}[1/DN]$ such that all the fibres are geometrically integral (see [B]). Abusing the notation we denote these models by X and Y, respectively. The same convention applies to S which has a model with the same properties over $\mathbf{Z}[1/D]$.

Let p be a prime number not dividing DN. The Eichler–Shimura relation leads to the following formula for the Zeta-function of $X_{\mathbf{F}_p}$:

$$Z(X_{\mathbf{F}_p}, t) = \frac{\det(1 - T_p t + \langle p \rangle p t^2)}{(1-t)(1-pt)}.$$

Here T_n, $(n, N) = 1$, is the Hecke operator acting on the space $S_2(\Gamma_1)$ of cusp forms of weight 2 (as defined in [M]); $\langle n \rangle$, $(n, N) = 1$, is the diamond operator defined via the natural action of $(\mathbf{Z}/N)^*/\pm 1$ on $S_2(\Gamma_1)$.

Following the approach of [JL] we deduce an explicit formula for $|X(\mathbf{F}_{p^r})|$. The identity $\log\det(A) = \operatorname{Tr}\log(A)$ implies the identity of formal power series

$$\frac{d}{dt}\log\det(1 - T_p t + \langle p \rangle p t^2) = \operatorname{Tr}((-T_p + 2\langle p \rangle p t)(1 - T_p t + \langle p \rangle p t^2)^{-1}).$$

Set $T_1 = Id$, $T_{p^{-1}} = 0$. Using the identity

$$T_{p^r} T_p = T_{p^{r+1}} + \langle p \rangle p T_{p^{r-1}}$$

for $r \geq 0$, one proves that

$$|X(\mathbf{F}_{p^r})| = 1 + p^r + \mathrm{Tr}(\langle p \rangle p T_{p^{r-2}} - T_{p^r}) \quad \text{for } r \geq 1.$$

Therefore, if l is a prime number that does not divide DNp, we have

$$\mathrm{Tr}((\mathrm{F}_p^*)^r | H^1_{\acute{e}t}(X_{\overline{\mathbf{F}}_p}, \mathbf{Q}_l)) = \mathrm{Tr}(T_{p^r} - \langle p \rangle p T_{p^{r-2}} | S_2(\Gamma_1)), \tag{1}$$

where F_p^* is the action of the Frobenius element F_p on the l-adic cohomology group $H^1_{\acute{e}t}(X_{\overline{\mathbf{F}}_p}, \mathbf{Q}_l)$.

Let σ be a character of Γ_k unramified away from the primes dividing DN. Let X^σ be the twist of $X_k = X \times k$ by σ, considered as a 1-cocycle of the Galois group Γ_k with coefficients in $(\mathbf{Z}/N)^*/\pm 1$. Then X^σ is a smooth and proper curve over k, with good reduction away from the primes dividing DN.

Let O_k be the ring of integers of k. We construct a model of X^σ over $O_k[1/DN]$ as follows. Let $\mathcal{P}$ be a $O_k[1/DN]$-torsor under $(\mathbf{Z}/N)^*/\pm 1$ defined by σ. Then the quotient $(X_{O_k} \times_{O_k[1/DN]} \mathcal{P})/G$ is smooth and proper over $O_k[1/DN]$, has geometrically integral closed fibres, and its generic fibre is X^σ. Abusing the notation we call X^σ this $O_k[1/DN]$-scheme.

Let v be a prime of k above p, and let $\mathbf{F}_q$ be the residue field at v, $q = p^f$. Since σ is unramified at v we can write $\gamma = \sigma(\mathrm{F}_q)$. The action of the Galois group of $\mathbf{F}_q$ on $X^\sigma_{\overline{\mathbf{F}}_q}$ is obtained from its action on $X_{\overline{\mathbf{F}}_q}$ by composing the Frobenius F_q with γ, hence we have

$$\mathrm{Tr}((\mathrm{F}_q^*)^s | H^1_{\acute{e}t}(X^\sigma_{\overline{\mathbf{F}}_q}, \mathbf{Q}_l)) = \mathrm{Tr}((\gamma^*)^s (\mathrm{F}_q^*)^s | H^1_{\acute{e}t}(X_{\overline{\mathbf{F}}_p}, \mathbf{Q}_l)),$$

using that $\mathrm{Tr}(AB) = \mathrm{Tr}(BA)$. The formula (1) now yields

$$\mathrm{Tr}((\mathrm{F}_q^*)^s | H^1_{\acute{e}t}(X^\sigma_{\overline{\mathbf{F}}_q}, \mathbf{Q}_l)) = \mathrm{Tr}(\langle \gamma^s \rangle T_{p^{fs}} - \langle \gamma^s p \rangle p T_{p^{fs-2}} | S_2(\Gamma_1)). \tag{2}$$

1.3. Application of the Eichler–Selberg trace formula. Let χ be a Dirichlet character modulo N such that $\chi(-1) = 1$. Let $S(\chi)$ be the subspace of $S_2(\Gamma_1)$ consisting of the cusp forms on which $(\mathbf{Z}/N)^*/\pm 1$ acts via the character χ.

Here is the list of notation for the Eichler–Selberg trace formula.

p is a prime, $(p, DN) = 1$;

r is a non-negative integer;

t is an integer such that $|t| < 2p^{r/2}$;

$d = \operatorname{discr} \mathbf{Q}(\sqrt{t^2 - 4p^r})$;

$h(d)$ is the class number of $\mathbf{Q}(\sqrt{d})$;

$w(d)$ is the number of roots of unity in $\mathbf{Q}(\sqrt{d})$;

$\mathcal{O}_f = \mathbf{Z} + fO_k$ is an order of conductor f in $\mathbf{Q}(\sqrt{d})$ containing the roots of $x^2 + tx + p^r = 0$ (note that if we write $t^2 - 4p^r = m^2 d$, then $f|m$);

$S(\mathcal{O}_f)$ is a non-negative rational number defined in ([JL], p. 239): $S(\mathcal{O}_f) = 0$ if $(D, f) \neq 1$, otherwise

$$S(\mathcal{O}_f) = 2\frac{h(d)}{w(d)} f \prod_{q_1 | f} \left(1 - \left(\frac{d}{q_1}\right) q_1^{-1}\right) \prod_{q_2 | D} \left(1 - \left(\frac{d}{q_2}\right)\right),$$

where q_1 (resp. q_2) runs over the prime factors of f (resp. of D);

$$c(t, f, \chi) = \begin{cases} \chi(\alpha) + \chi(\beta) & \text{if } (N, f) = 1 \text{ and } (*) \text{ has two roots } \alpha \neq \beta, \\ 0 & \text{if } (N, f) = 1 \text{ and } (*) \text{ has no roots}, \\ \chi(\alpha) & \text{if } (N, f) = 1, N|d, \text{ and } \alpha \text{ is the double root of } (*), \\ 2\chi(\alpha) & \text{if } N|f \text{ and } \alpha \text{ is the double root of } (*), \end{cases}$$

where $(*)$ is the equation

$$(*) \qquad X^2 + tX + p^r = 0 \bmod N.$$

When there is no level structure we set $c(t, f) = 1$. Note that if χ is trivial, then $c(t, f, \chi) = 1 + (\frac{d}{N})$ if N does not divide f; otherwise $c(t, f, \chi) = 2$.

Now we define $\Sigma_r(\chi)$ by the formula

$$\Sigma_r(\chi) = \frac{1}{2} \sum_{t \in \mathbf{Z}, |t| < 2p^{r/2}} \sum_{\mathcal{O}_f} S(\mathcal{O}_f) c(t, f, \chi).$$

Set $\Sigma_{-1}(\chi) = 0$. When χ is trivial, we shall write $c(t, f, N)$ for $c(t, f, \chi)$, and $\Sigma_r(N)$ for $\Sigma_r(\chi)$, to emphasize the dependence on N. If $(N, f) = 1$, then we have

$$c(t, f, N) = 1 + \left(\frac{d}{N}\right);$$

otherwise $c(t, f, N) = 2$. Note that the $\Sigma_r(N)$ are non-negative rational numbers which depend on r, p, D and N. We use the notation Σ_r when no level structure is involved.

Following [JL] we observe the following property of these numbers.

PROPOSITION 1.3: *For all $r \geq 1$ we have $\Sigma_r(N) \geq p\Sigma_{r-2}(N)$. The equality holds if and only if for any order $\mathcal{O}_f \subset \mathbf{Q}(\xi)$ containing a root ξ of $x^2 + tx + p^r = 0$, where $t \in \mathbf{Z}$, $|t| < 2p^{r/2}$, at least one of the following conditions is satisfied:*

(i) *at least one prime factor* $q|D$ *is split in* $\mathbf{Q}(\xi)$,
(ii) $p|t$ *and* p *splits in* $\mathbf{Q}(\xi)$,
(iii) $(f, D) \neq 1$,
(iv) $(N, f) = 1$ *and* N *is inert in* $\mathbf{Q}(\xi)$.

Proof: We note that $S(\mathcal{O}_f)c(t, f, N) = 0$ if and only if either some prime factor $q|D$ is split in $\mathbf{Q}(\xi)$, or $(D, f) \neq 1$, or $(N, f) = 1$ and N is inert in $\mathbf{Q}(\xi)$. When there is no level structure the proposition is proved in ([JL], Prop. 2.4). The same proof works for the case of general N, and gives the following formula:

$$2(\Sigma_r(N) - p\Sigma_{r-2}(N)) = \sum_{t,|t|<2p^{r/2},p|t} \sum_{\mathcal{O}_f,(p,f)=1} S(\mathcal{O}_f)\Big(1 - \Big(\frac{d}{p}\Big)\Big)c(t, f, N) + \sum_{t,|t|<2p^{r/2},(p,t)=1} \sum_{\mathcal{O}_f} S(\mathcal{O}_f)c(t, f, N).$$

The proposition follows. ∎

When no level structure is involved, Proposition 1.3 says that $\Sigma_r = p\Sigma_{r-2}$ for $r \geq 1$ if and only if for any quadratic integer ξ such that $N(\xi) = p^r$, $|\operatorname{Tr}(\xi)| < 2p^{r/2}$, at least one of the following conditions is satisfied:

(i) at least one prime factor $q|D$ is split in $\mathbf{Q}(\xi)$,
(ii) $p|\xi$ and p splits in $\mathbf{Q}(\xi)$ (this case does not occur for $r = 1$).

As an example let us compute $\Sigma_0(N)$. Here $r = 0$, $t \in \{-1, 0, 1\}$, and the relevant algebraic integers ξ are $\pm\sqrt{-1}$ and $\frac{1}{2}(\pm 1 \pm \sqrt{-3})$. Thus $\mathcal{O}_f$ is $\mathbf{Z}[\sqrt{-1}]$ or $\mathbf{Z}[\frac{1}{2}(1 + \sqrt{-3})]$. In the first case $d = -4$, $h(-4) = 1$, $w(-4) = 4$, and in the second case $d = -3$, $h(-3) = 1$, $w(-3) = 6$. Therefore we have

$$\Sigma_0(N) = \frac{1}{4}\Big(1 + \Big(\frac{-4}{N}\Big)\Big)\prod_{q|D}\Big(1 - \Big(\frac{-4}{q}\Big)\Big) + \frac{1}{3}\Big(1 + \Big(\frac{-3}{N}\Big)\Big)\prod_{q|D}\Big(1 - \Big(\frac{-3}{q}\Big)\Big).$$

Under Condition 1 we have $\Sigma_0(N) = \Sigma_0 = 0$. Obviously this need not always be the case: for instance, for the lowest possible $D = 6$ we have $\Sigma_0 = \frac{7}{6}$. If instead of Condition 1 we assume that N is a prime congruent to 11 modulo 12, then $\Sigma_0(N) = 0$.

We can now state the Eichler–Selberg trace formula. We use the convention that $\chi(\sqrt{n}) = 0$ if n is not a square.

PROPOSITION 1.4 (Eichler–Selberg trace formula): *In the above notation, if* χ *is not trivial, we have*

$$\operatorname{Tr}(T_{p^r}|S(\chi)) = \frac{1}{12}\chi(p^{r/2})(N + 1)\prod_{q|D}(q - 1) - \Sigma_r(\chi).$$

If χ is trivial then one has to add $1 + \cdots + p^r$ to this expression.

Proof: This is proved in [M], Thm 6.8.4, and Remark 6.8.1, p. 264. In the notation of [M] we have $S(\mathcal{O}_f) = 2a(t)b(t,f)$.* ∎

From this formula and the fact that $S_2(\Gamma_1)$ is the direct sum of the $S(\chi)$ taken over all characters of $(\mathbf{Z}/N)^*/\pm 1$, it follows that

$$\mathrm{Tr}(\langle\gamma^r p\rangle p T_{p^{r-2}} | S_2(\Gamma_1)) = p + \cdots + p^{r-1} + \frac{1}{12}p(N+1)\prod_{q|D}(q-1)\sum_{\chi}\chi(\gamma^r p^{r/2}) - p\sum_{\chi}\chi(\gamma^r p)\Sigma_{r-2}(\chi).$$

We have used that $\langle n\rangle$ acts as multiplication by $\chi(n)$ on $S(\chi)$. We also have

$$\mathrm{Tr}(\langle\gamma^r\rangle T_{p^r} | S_2(\Gamma_1)) = 1 + p + \cdots + p^r + \frac{1}{12}(N+1)\prod_{q|D}(q-1)\sum_{\chi}\chi(\gamma^r p^{r/2}) - \sum_{\chi}\chi(\gamma^r)\Sigma_r(\chi).$$

Now let us assume that p is split or ramified in k. We obtain from (2)

$$-\mathrm{Tr}((\mathrm{F}_p^*)^r | H^1_{\acute{e}t}(X^{\sigma}_{\overline{\mathbf{F}}_p}, \mathbf{Q}_l)) = \Phi_r - (1+p^r) + \frac{1}{12}(p-1)(N+1)\prod_{q|D}(q-1)\sum_{\chi}\chi(\gamma^r p^{r/2}),$$

where $\Phi_r = \sum_{\chi}\chi(\gamma^r)(\Sigma_r(\chi) - p\chi(p)\Sigma_{r-2}(\chi))$. We finally obtain

$$|X^{\sigma}(\mathbf{F}_{p^r})| = \Phi_r + \frac{1}{12}(N+1)(p-1)\prod_{q|D}(q-1)\sum_{\chi}\chi(\gamma^r p^{r/2}). \tag{3}$$

In particular, we have

$$|X^{\sigma}(\mathbf{F}_p)| = \Phi_1 = \sum_{\chi}\chi(\gamma)\Sigma_1(\chi). \tag{4}$$

The space of cusp forms $S_2(\Gamma_0)$ with respect to Γ_0 is identified with the subspace of $S_2(\Gamma_1)$ on which $(\mathbf{Z}/N)^*/\pm 1$ acts trivially. Therefore, if in all the

* It appears that the definition of $a(t)$ in [M] should be corrected: $a(t) = 0$ if there is a prime factor $p|D$ such that p is split in $\mathbf{Q}(\sqrt{d})$ or divides f; see [JL], p. 239. In particular, $a(t)$ actually depends on f as well as on t.

calculations of this and the previous subsection we consider only the trivial character χ, we obtain the following formula for the number of points on Y:

$$(5)\quad |Y(\mathbf{F}_{p^r})| = \Sigma_r(N) - p\Sigma_{r-2}(N) + \frac{1}{24}(1+(-1)^r)(N+1)(p-1)\prod_{q|D}(q-1).$$

We quote a similar formula for S from [JL], Prop. 2.3:

$$(6)\qquad |S(\mathbf{F}_{p^r})| = \Sigma_r - p\Sigma_{r-2} + \frac{1}{24}(1+(-1)^r)(p-1)\prod_{q|D}(q-1).$$

One can use the Eichler–Selberg trace formula in the case $T_1 = Id$ to deduce a formula for the genus of the relevant Shimura curve. However, we just quote ([V], p. 120) which says that the genus of Y is

$$g_Y = 1 - \Sigma_0(N) + \frac{1}{12}(N+1)\prod_{q|D}(q-1),$$

and the genus of S is

$$g_S = 1 - \Sigma_0 + \frac{1}{12}\prod_{q|D}(q-1).$$

1.4. LOCAL POINTS IN THE CASE OF GOOD REDUCTION.

PROPOSITION 1.5: *Let v be a prime of k of residual characteristic p not dividing DN. If p is inert in k, then $Y(k_v) \neq \emptyset$. If p is split or ramified in k, then $Y(k_v) \neq \emptyset$ if and only if $\Sigma_1(N) \neq 0$.*

Proof: Formula (5) and the first statement of Proposition 1.3 imply that Y always has $\mathbf{F}_{p^2}$-points. Since we are in the good reduction case, the proposition now follows from Hensel's lemma. ∎

Proposition 1.3 gives an explicit criterion for $\Sigma_1(N) \neq 0$.

PROPOSITION 1.6: *If for any $m \in \{0, 1, \ldots, (N-3)/2\}$ there exists a prime p not dividing DN, split or ramified in k, and such that $p^{2m} + tp^m + p \neq 0 \bmod N$ for all integers t satisfying $|t| < 2\sqrt{p}$, then $X^\sigma(\mathbf{A}_k) = \emptyset$ for all twists X^σ.*

Proof: By Proposition 1.2, $X^\sigma(\mathbf{A}_k) = \emptyset$ unless σ is a power of c, the restriction to Γ_k of the cyclotomic character at N, that is, for $p \neq N$ we have $c(\mathrm{F}_p) = p \bmod N$. The target group being $(\mathbf{Z}/N)^*/\pm 1$ we can assume without loss

of generality that $\sigma = c^{-m}$, where $m \in \{0, 1, \ldots, (N-3)/2\}$. We have $\gamma = c^{-m}(\mathrm{F}_p) = p^{-m} \bmod N$. Thus (4) yields

$$|X^{c^{-m}}(\mathbf{F}_p)| = \sum_{\chi} \chi(p^{-m})\Sigma_1(\chi) = \frac{1}{2} \sum_{t \in \mathbf{Z}, |t| < 2\sqrt{p}} \sum_{\mathcal{O}_f} S(\mathcal{O}_f) \sum_{\chi} \chi(p^{-m}) c(t, f, \chi).$$

By definition, $c(t, f, \chi)$ is a weighted sum of $\chi(\alpha)$, where $\alpha \in \mathbf{Z}/N$ is a root of $x^2 + tx + p = 0 \bmod N$, $t \in \mathbf{Z}$, $|t| < 2\sqrt{p}$. It is clear that for $x \in \mathbf{Z}/N$ we have

$$\sum_{\chi} \chi(x) = 0 \quad \text{if } x \neq \pm 1,$$

where the sum is over all characters of $(\mathbf{Z}/N)^*$ such that $\chi(-1) = 1$. Thus $\sum_{\chi} \chi(p^{-m}\alpha) = 0$ as long as $\alpha \neq \pm p^m \bmod N$. Thus $|X^{c^{-m}}(\mathbf{F}_p)| = 0$ as long as $p^m \bmod N$ is not a root of such a quadratic equation. ∎

2. Bad reduction

2.1. BAD REDUCTION OF Y AT N. Recall that S has good reduction away from primes dividing D. An integral model of Y over $\operatorname{Spec} \mathbf{Z}_N$ can be obtained using the results of [B], by first choosing some level structure at a prime not dividing DN, and then passing to the quotient by the action of the corresponding finite group. The structure of this model is very similar to the model of the classical modular curves $X_0(N)$ studied by Deligne and Rapoport.

The curve Y has a flat and proper model $\mathcal{Y}/\operatorname{Spec} \mathbf{Z}_N$ such that the scheme $\mathcal{Y}^h$ obtained by deleting the supersingular points in the closed fibre $\mathcal{Y}_{\mathbf{F}_N}$ is smooth over $\operatorname{Spec} \mathbf{Z}_N$. The closed fibre $\mathcal{Y}_{\mathbf{F}_N}$ is isomorphic to the union of two copies of $S_{\mathbf{F}_N}$ intersecting transversally at supersingular points.

PROPOSITION 2.1: *Suppose that D satisfies Condition 1. If N is inert in k, and v is the place of k over N, then $Y(k_v) \neq \emptyset$ if and only if there exists a quadratic integer ξ of norm $N(\xi) = N^2$ and trace $|\operatorname{Tr}(\xi)| < 2N$, such that the following condition holds:*

(a) *if $(N, \operatorname{Tr}(\xi)) = 1$, then every prime factor of D is inert or ramified in $\mathbf{Q}(\xi)$,*

(b) *if $\operatorname{Tr}(\xi) \in \{-N, 0, N\}$, then every prime factor of DN is inert or ramified in $\mathbf{Q}(\xi)$.*

Proof: Using the constancy of the arithmetic genus in a flat projective family we find the number of supersingular $\overline{\mathbf{F}}_N$-points in $\mathcal{Y}_{\mathbf{F}_N}$ as $s = g_Y - 2g_S + 1$. It is known that all supersingular points are defined over $\mathbf{F}_{N^2}$. Now (6) and the

formulae for g_Y and g_S imply that $|S(\mathbf{F}_{N^2})| - s = \Sigma_2 - (N+2)\Sigma_0 + \Sigma_0(N) = \Sigma_2$. Now Prop. 2.4 of [JL] gives a necessary and sufficient condition for $\Sigma_2 > 0$, equivalent to the condition in the proposition. An ordinary $\mathbf{F}_{N^2}$-point is smooth on $\mathcal{Y}_{F_N}$. Hence, by Hensel's lemma, it can be lifted to a k_v-point on Y. ∎

2.2. BAD REDUCTION OF Y AT THE PRIMES DIVIDING D. When p divides D, then Y has bad reduction at p. This problem is studied in [JLV] via p-adic uniformization of the curve. Theorem 5.5 of [JLV] implies that if the place p is inert in k, then Y has a point rational over k_v (in their notation $f = 2$).

We now summarize the results obtained so far regarding the local points on Y.

THEOREM 2.2: *Suppose that D satisfies Condition 1. Let k be an imaginary quadratic field such that*

(1) *all the prime divisors of D are inert in k;*

(2) *N is inert in k, and there exists a quadratic integer ξ with $N(\xi) = N^2$, $|\operatorname{Tr}(\xi)| < 2N$, such that if $\operatorname{Tr}(\xi) \notin \{-N, 0, N\}$, then every prime factor of D is inert or ramified in $\mathbf{Q}(\xi)$, and if $\operatorname{Tr}(\xi) \in \{-N, 0, N\}$, then every prime factor of DN is inert or ramified in $\mathbf{Q}(\xi)$;*

(3) *the primes not dividing DN and such that $\Sigma_1(N) = 0$ are inert in k;*

then Y has points over all completions of k.

(Note that the archimedian places are not a problem since k is imaginary.) The curve Y has $\mathbf{F}_p$-points when p is large enough ($p > 4g_Y$ is clearly enough), therefore the set of primes mentioned in (3) is finite. In particular, conditions (1) and (3) are satisfied as long as finitely many 'small' primes are inert in k.

3. Numerical examples

3.1. ALGORITHM.

1. Set $D = q_1 q_2$ with primes q_1 and q_2 satisfying Condition 1.

2. Choose a prime N satisfying Condition 2, then check condition (2) of Theorem 2.2.

3. Make a list of primes not dividing $q_1 q_2 N$ such that $\Sigma_1(N) = 0$. We actually make a somewhat larger list of 'bad' primes. A prime not dividing $q_1 q_2 N$ is called **good** if there exists $t \in \mathbf{Z}$, $|t| < 2\sqrt{p}$, such that *all* of the following conditions are satisfied: neither q_1 nor q_2 is split in $\mathbf{Q}(\sqrt{t^2 - 4p})$; p does not divide t, or p is not split in $\mathbf{Q}(\sqrt{t^2 - 4p})$; N is not inert in $\mathbf{Q}(\sqrt{t^2 - 4p})$. These conditions guarantee that $\Sigma_1(N) \neq 0$ (see Proposition 1.3), hence $Y(\mathbf{Q}_p) \neq \emptyset$ by (5).

4. For each $m \in \{0, 1, \ldots, (N-3)/2\}$ find a good prime p such that $p^{2m}+tp^m+p \neq 0 \bmod N$ for all integers t satisfying $|t| < 2\sqrt{p}$. Call these primes **auxiliary**.
5. Choose an imaginary quadratic field k where q_1, q_2, N, and the (finitely many) bad primes are inert (Condition 4 is now fulfilled), whereas the auxiliary primes are split or ramified. Verify Condition 3, that the class number of k is coprime to $(N-1)/2$.

3.2. A WORKED-OUT EXAMPLE. We choose $D = 35$, $N = 23$. Then Conditions 1 and 2 are satisfied. Condition (2) of Theorem 2.2 is also satisfied (for many values of $\mathrm{Tr}(\xi)$, e.g., 1 or 43). We check that the following primes are good: $p = 2, 11, 13, 17, 19$ (for respective values $t = 1, 4, 3, 5, 4$). In fact, a computation using `pari` reveals that the only bad prime is 3. We check that $p = 2$ is an auxiliary prime for all m, $0 \leq m \leq 10$, except for $m = 5$ and $m = 7$, when $p = 13$ is an auxiliary prime. Now let $k = \mathbf{Q}(\sqrt{-127})$. We check that 3, 5, 7 and 23 are inert in k, and 2 and 13 are split in k. Moreover, k has class number 5, which is coprime to $(23-1)/2 = 11$. Hence Conditions 3 and 4 are satisfied. (Another k that works is $k = \mathbf{Q}(\sqrt{-142})$. The only difference with the previous case is that 2 is now ramified, and the class number is 7.)

CONCLUSION: For $D = 35$ and $N = 23$, the curve Y_k over the field $k = \mathbf{Q}(\sqrt{-127})$ or $k = \mathbf{Q}(\sqrt{-142})$ has points everywhere locally but not globally. Our method of proof used the unramified cyclic covering $X \to Y$ of degree 11.

Another case when the algorithm works is $D = 26$ (or $D = 39$) and $N = 23$. A case when the algorithm does not work is $D = 26$ (or $D = 39$) and $N = 11$ (no auxiliary primes were found for $m = 2, 3, 4$).

It would be interesting to know whether our algorithm can produce infinitely many triples (D, N, d) such that the curve Y_k over the field $k = \mathbf{Q}(\sqrt{-d})$ has points everywhere locally but not globally. One could try to fix D and N and vary d. It would be enough to know that a certain arithmetic progression (one that ensures that k satisfies the conditions of step 5 of the algorithm) contains infinitely many positive integers d such that the class number of $\mathbf{Q}(\sqrt{-d})$ is coprime to a given number. This seems to be an open problem.

ACKNOWLEDGEMENT: Our deepest thanks are extended to Kevin Buzzard for infallibly answering our many questions regarding modular curves. We thank Ron Livné for the timely sending of the preprint [JLV]. The second author thanks EPSRC for financial support.

References

[B] K. Buzzard, *Integral models of certain Shimura curves,* Duke Mathematical Journal **87** (1997), 591–612.

[J] B. Jordan, *Points on Shimura curves rational over number fields,* Journal für die reine und angewandte Mathematik **371** (1986), 92–114.

[JL] B. Jordan and R. Livné, *Local Diophantine properties of Shimura curves,* Mathematische Annalen **270** (1985), 235–248.

[JLV] B. Jordan, R. Livné and Y. Varshavsky, *Local points on p-adically uniformized Shimura varieties,* Preprint, March 2002.

[M] T. Miyake, *Modular Forms,* Springer-Verlag, Berlin, 1989.

[Sh] G. Shimura, *On the real points of an arithmetic quotient of a bounded symmetric domain,* Mathematische Annalen **215** (1975), 135–164.

[SS] S. Siksek and A. N. Skorobogatov, *On a Shimura curve that is a counterexample to the Hasse principle,* The Bulletin of the London Mathematical Society **35** (2003), 409–414.

[S] A. N. Skorobogatov, *Torsors and Rational Points,* Cambridge University Press, 2001.

[V] M.-F. Vignéras, *Arithmétique des algèbres de quaternions,* Lecture Notes in Mathematics **800**, Springer-Verlag, Berlin, 1980.