SHIMURA CURVES AND EXPLICIT DESCENT OBSTRUCTIONS VIA LEVEL STRUCTURE

JAMES STANKIEWICZ

Abstract. We give large families of Shimura curves defined by congruence conditions, all of whose twists lack $p$-adic points for some $p$. For each such curve we give analytically large families of counterexamples to the Hasse principle via the descent (or equivalently étale Brauer-Manin) obstruction to rational points applied to étale coverings coming from the level structure. More precisely, we find infinitely many quadratic fields defined using congruence conditions such that a twist of a related Shimura curve by each of those fields violates the Hasse principle. As a minimal example, we find the twist of the genus 11 Shimura curve $X_{143}^1$ by $\mathbb{Q}(\sqrt{-67})$ and its bi-elliptic involution to violate the Hasse principle.

1. Introduction

A central goal in modern number theory is to understand as much as possible about counterexamples to the Hasse principle. While many examples are known, systematic methods of finding them are few and far between. One such method \cite{5,3,9,10} depends on the idea that modular and Shimura curves have a plentiful supply of involutions $\iota$. If the quotient by $\iota$ has finitely many rational points and algebraic but not rational fixed points then only finitely many twists by $\iota$ have rational points. This follows from Faltings Theorem and is similarly ineffective: to explicitly determine the twists we would need to explicitly determine the rational points on the quotients, in this case quotients by Atkin-Lehner involutions. This is an interesting open problem. Moreover these counterexamples are not known to come from the étale Brauer-Manin/descent obstruction \cite{16} except in finitely many special cases \cite{9,6}. In this paper we prove an effective variant - we give infinite explicit families of counterexamples to the Hasse principle over $\mathbb{Q}$ given by the descent obstruction.

Theorem 1.1. For $D$ as in Theorem 1.2 let $\Sigma_D(X)$ be the set of negative integers $-X \leq d \leq -1$ such that the twist of $X^D$ by $w_D$ and $\mathbb{Q}(\sqrt{d})$ is a counterexample to the Hasse principle. Then $\Sigma_D(X)$ contains a subset $M_D(X)$ given by congruence conditions such that $\#M_D(X) \gg X/\log(X)$ and the associated twists have an empty descent (equivalently étale Brauer-Manin) obstruction set.

Here $X^D$ is the Shimura curve parameterizing abelian surfaces with an action by a maximal order in a quaternion algebra over $\mathbb{Q}$ of discriminant $D$ and $w_D$ is the main Atkin-Lehner involution of $X^D$. To the author’s knowledge the previous state of the art for $X^D_{193}$ was finding that a single twist of the genus 193 curve $X^{23(107)}$ is a counterexample to the Hasse principle \cite{13}. Moreover, this example comes...
from a modification of the descent obstruction via the Shimura covering [15]. The counterexamples of this paper come from étale coverings induced by the canonical level structure. To the author’s knowledge this is the first time such coverings have been used with the descent obstruction for any Shimura variety. The key to proving Theorem 1.1 is Theorem 1.2, which in turn depends crucially on previous work of the author [17]. The $D$ in Theorem 1.2 are also given by congruence conditions and the set of them is therefore similarly large, as we see in Lemma 5.5.

**Theorem 1.2.** Let $q_1 \equiv q_2 \equiv \cdots \equiv q_{2n} \equiv 1 \mod 12$ be an increasing sequence of primes such that $\left(\frac{q_i}{q_j}\right) = 1$ for all $i \neq j$. Suppose $p \equiv 1 \mod 4$ is a prime such that

- for all $s \in \{1, \ldots, \lfloor \sqrt{4p} \rfloor\}$, there is some $i$ such that $\left(\frac{s^2 - 4p}{q_i}\right) = 1$, and
- for all $i$, $q_{i+1} > 4pq_1 \ldots q_i$ including the case $q_1 > 4p$,
- $\left(\frac{D}{p}\right) = -1$ for $D = q_1 \ldots q_{2n}$.

Then every twist of $X_D^{(0)}(p)$ lacks $\mathbb{Q}_p$-rational points.

For such $D$ and $p$, we will say that $X_D^{(0)}(p)(\mathbb{Q}_p) = \emptyset$ palindromically in order to avoid referencing the cohomological theory of twists too frequently (we will eventually do so in Corollary 5.4). We choose this terminology to emphasize that in the same way a word is a palindrome if it is preserved under the reversing of letters, so too is the property of lacking $\mathbb{Q}_p$-points preserved by twisting. In any case, for such $D$, we can describe each twist of $X_D^{(0)}(p)$ and moreover know the map $X_D^{(0)}(p) \to X_D^{(0)}(p) \to X_D^{(0)}(1) = X_D$ forgetting level structure is a finite étale cover. Hasse principle violations are now obtained with the descent obstruction [14, Definition 5.3.1]. We verify this theorem by computing whether a given twist can have $p$-adic points in the cases of twisting by a split, inert, or ramified quadratic extension.

Finally, we note that our results can be adapted to cases besides the conditions of Theorem 1.2. For instance, it is not necessary to work with an odd prime $p$. Our lowest genus example is given by finding a $D$ where $X_D^{(0)}(2)$ lacks $\mathbb{Q}_2$ points palindromically. Moreover, in this case the quotient by $w_D$ is actually a positive rank elliptic curve, which is impossible with previous methods [5].

**Example 1.3.** Let $E$ denote the unique elliptic curve over $\mathbb{Q}$ with conductor 143. The twist of the Shimura curve $X_{143}^{(1)}$ by the involution giving the Shimura-modular parametrization $X_{143}^{(1)} \to E$ and the field $\mathbb{Q}(\sqrt{-67})$ is a counterexample to the Hasse principle.

This note is the result of a somewhat long investigation triggered by a question of Dino Lorenzini about whether it was possible to find curves over $\mathbb{Q}$ which palindromically lack $\mathbb{Q}$-rational points. It is my pleasure to acknowledge the helpful conversations about this work with Pete Clark, Lars Halle, and Ian Kiming. The author was partially supported by the Villum Fonden through the network for Experimental Mathematics in Number Theory, Operator Algebras and Topology.

2. The Split Case

Throughout this section, we will take $p$ to be an odd prime. We will also let $K = \mathbb{Q}(\sqrt{d})$ be a quadratic field in which $p$ splits. We will always let $D$ be the
Figure 1. $X^D_0(p)_{\mathbb{F}_p}$

(r) discriminant of an indefinite quaternion algebra, namely the squarefree product of an even number of primes. If $N$ is a positive integer such that $DN$ is squarefree and $m \mid DN$, we will let $C^D(N,d,m)$ be the twist of $X^D_0(N)$ by the Atkin-Lehner involution $w_m$ and $K$ [17]. We will be specifically interested in a certain class of discriminants $D$ which will guarantee good properties for our Shimura curves.

**Lemma 2.1.** The following are equivalent.

1. There are primes $q, q' \mid D$ (possibly equal) such that $q \equiv 1 \mod 4$ and $q' \equiv 1 \mod 3$.
2. For all primes $\ell \nmid D$, the natural map $X^D_0(\ell)_{\mathbb{Q}} \rightarrow X^D_{\mathbb{Q}}$ is étale.
3. For all primes $\ell \nmid D$, there are exactly two components of $X^D_0(\ell)_{\mathbb{F}_\ell}$.

**Proof.** The idea is that the natural map $X^D_0(\ell) \rightarrow X^D$ is étale over $\mathbb{Q}$ if and only if the base change to $\mathbb{C}$ is a covering space map of Riemann surfaces. For any $D$ and $\ell$, the branch locus lies inside the locus of cusps and elliptic points. If $D > 1$ there are no cusps and there can only be elliptic points of order 2 or 3. Respectively the number of these is

$$\prod_{q \mid D} \left(1 - \left(-\frac{4}{q}\right)\right) \prod_{q \mid D} \left(1 - \left(-\frac{3}{q}\right)\right).$$

Meanwhile, the exceptional components of $X^D_0(\ell)_{\mathbb{F}_\ell}$ come in chains of one or two copies of $\mathbb{P}^1_{\mathbb{F}_\ell}$ and the number of chains is respectively a nonzero constant times

$$\prod_{q \mid D\ell} \left(1 - \left(-\frac{4}{q}\right)\right) \prod_{q \mid D\ell} \left(1 - \left(-\frac{3}{q}\right)\right).$$

We note that if $D$ satisfies the conditions of Lemma 2.1 then the components of $X^D_0(p)_{\mathbb{F}_p}$ will be joined precisely at the supersingular points as in Figure 1.

**Lemma 2.2.** For $D$ as in Lemma 2.1, the only automorphisms of $X^D_0(N)$ for any $N$ such that $DN$ is squarefree are the Atkin-Lehner involutions.

**Proof.** [12 Theorem 2]
Theorem 2.3. If $D$ is an odd discriminant of a quaternion algebra satisfying the conditions of Lemma 2.1 coprime to $p$ and for all $s$ in $\{1, \ldots, \lfloor \sqrt{4p} \rfloor \}$ there exists a prime $q_s \mid D$ such that \( \left( \frac{s^2 - 4p}{q_s} \right) = 1 \) then $X_0^D(p)(\mathbb{Q}_p) = \emptyset$. Moreover, for all quadratic twists $X$ of $X_0^D(p)$ by $K$, $X(\mathbb{Q}_p) = \emptyset$.

The proof of this relies on the Eichler-Selberg trace formula [6]. We make this precise using the following definition.

Definition 2.4. Let $p$ be a prime and let $\Delta < 0$ such that $\Delta \mod 4 \in \{0, 1\}$. If we let $\left( \frac{\Delta}{p} \right)$ be the Kronecker symbol and $f(\Delta)$ the conductor of $\mathbb{Z}[\frac{\Delta + \sqrt{\Delta}}{2}]$ then we define the Eichler symbol as

\[
\{ \Delta \pmod{p} \} = \begin{cases} 1 & p \mid f(\Delta) \\ \left( \frac{\Delta}{p} \right) & \text{else.} \end{cases}
\]

Proof. If $p$ splits in $K$, we have an embedding $K \hookrightarrow \mathbb{Q}_p$. Since $X_K \cong X_0^D(p)_K$, we have $X_{\mathbb{Q}_p} \cong X_0^{D(N)}_{\mathbb{Q}_p}$. We can see that $X_{\mathbb{Q}_p}$ has no $p$-adic points if and only if a certain quantity $TF'(D, p, 1, p)$ vanishes [17, Theorem 6.1(a)].

The quantity $TF'(D, p, 1, p)$ can be explicitly realized as

\[
2 \sum_{s=1}^{\lfloor \sqrt{4p} \rfloor} \sum_{f \mid (s^2 - 4p)} H(s, f) \prod_{q \mid D} \left( 1 - \left\{ \frac{(s^2 - 4p)/f^2}{q} \right\} \right),
\]

where $H(s, f)$ is an explicit nonzero constant [6]. Therefore this sum vanishes if and only if for all $(s, f)$ in this range, there is a prime $q_s$ such that $\left( \frac{\Delta}{q_s} \right) = 1$. It suffices then to require that \( \left( \frac{s^2 - 4p}{q_s} \right) = 1 \) because if so, $q_s \nmid s^2 - 4p$ and thus $q_s \nmid f$ so $\left( \frac{f^2}{q_s} \right) = 1$ and thus

\[
\left( \frac{(s^2 - 4p)/f^2}{q_s} \right) = \left\{ \frac{(s^2 - 4p)/f^2}{q_s} \right\} = 1.
\]

\[ \Box \]

3. The Inert Case

Now let $p$ be inert in $K = \mathbb{Q}(\sqrt{d})$ and let $D$ be coprime to $p$, satisfying the conditions of Lemma 2.1. Here we vitally use Lemma 2.2 to say that each twist by $K$ is of the form $C^D(p, d, m)$ for some $m \mid Dp$. For $m \mid D$ we can mimic [2]. For all such $s, f, m$ there is an explicit nonzero constant $H = H(s, f, m)$ [13, Corollary 2.4], [17, Definition 6.13] such that if $\Delta = \Delta(s, f, m) = (s^2 - 4pm)/f^2$ then

\[
TF'(D, p, m, p) = 2 \sum_{s=1}^{\lfloor \sqrt{4pm} \rfloor} \sum_{f \mid (s^2 - 4pm)} H \prod_{q \mid D} \left( 1 - \left\{ \frac{\Delta}{q} \right\} \right).
\]

If we want to guarantee this quantity is zero for all $m$, we need to at least make sure that if $m = D$ and $q \mid D$ that $q \nmid s$ when $s^2 < 4pm$. If $q \mid s$ for some $q \mid D$ then
\[ \prod_{q \mid D} \left(1 - \frac{s^2 - 4pm}{q}\right) = 1, \] which we need to avoid. We do this by restricting the distance between the prime divisors of \( D = q_1 \ldots q_{2n} \).

**Lemma 3.1.** If \( q_{i+1} > 4pq_i \ldots q_1 \) then for all \( m \mid D, m \neq 1, TF^*(D,p,m,p) = 0. \)

**Proof.** Let \( q \mid m \mid D \) be an odd prime and let \( q \mid s^2 - 4pm \) for some \( 0 < s^2 < 4pm \). Set \( \nu = (s^2 - 4pm)/q < 0 \) and \( \tau = s/q \). Thus \( q^2\tau^2 = q(\nu + 4pm/q) \) and so \( q \leq q^2\tau^2 = \nu + 4pm/q < 4pm/q \).

Suppose now \( q_{i+1} > 4pq_i \ldots q_1 \) and let \( j \) be the maximal \( i \) such that \( q_i \mid m \). It follows that \( q_j > 4pqj_{j-1} \ldots q_1 \geq 4pm/q_j \) and so \( q_j \nmid s^2 - 4pm \) for all \( s \) such that \( 0 < s^2 < 4pm \). For any fixed \( s \), let \( t_s = q_j - s \) and \( n_s = 2s - q_j - 4pm/q_j \). It follows that

\[
\frac{s^2 - 4pm}{q} = \frac{s^2 - 4pm}{q} = q_j(-4pm/q_j + q_j - 2s - 2s) = q_j^2 - 2sq_j + q_j(-4pm/q_j - q_j + 2s) = (q_j - s)^2 + q_j(2s - q_j - 4pm/q_j) = t_s^2 + q_jn_s. \]

We see that \( \frac{s^2 - 4pm}{q} = 1 \) for all \( s \) because there is an integer \( t \) such that \( q \nmid t \) and \( s^2 - 4pm \equiv t^2 \mod q \). To complete the proof, note that since \( q_j \nmid s^2 - 4pm \), \( q_j \nmid f \) and therefore there exists an integer \( f' \) such that \( ff' \equiv 1 \mod q_j \) and so \( (s^2 - 4pm)/f' \equiv (t_s f')^2 \mod q_j \). \( \square \)

**Theorem 3.2.** Suppose \( D \) satisfies the conditions of Theorem 1.2. Then all twists of \( X^D_0(p) \) by \( K \) have no \( \mathbb{Q}_p \)-points.

**Proof.** By Lemma 2.2, any such twist must be of the form \( C^D(p,d,m) \) for some \( m \mid Dp \). If \( m = 1 \) this is the trivial twist \( X^D_0(p) \) and [2] covers this case.

If \( p \mid m \) there are no smooth \( \mathbb{F}_p \)-rational points because the two branches of \( X^D_0(p)_{\mathbb{F}_p} \) are interchanged by the new action of Frobenius. If \( p \mid m \) then by Lemma 3.1 \( TF^*(D,p,m,p) = 0 \) and again there are no smooth \( \mathbb{F}_p \)-rational points. In either case, Hensel’s Lemma [2] Lemma 1.1] completes the proof. \( \square \)

**Remark 3.3.** We note a general framework here. Previous results [17, 4] show that we can always make a twist of \( X^D \) such that a supersingular point becomes \( \mathbb{F}_p \)-rational if \( p \nmid D \). Therefore our only choice to prevent \( \mathbb{Q}_p \) points is to make these points non-smooth on the special fiber [7, Lemma 1.1]. This is to say that we need to move from \( X^D \) to \( X^D_0(p) \), so that the supersingular points become singular as in Figure 1. Moving back from \( X^D_0(p) \) to \( X^D \), where our points become smooth again is essentially what lets us produce Counterexamples to the Hasse principle instead of just curves without rational points.

4. The Ramified Case

Finally we treat the case where \( p \) is ramified in \( K = \mathbb{Q}(\sqrt{d}) \) or rather that \( p \nmid d \) since \( p \) is odd. For general \( D \) and \( N \) this case can be rather complicated, but if we restrict to the \( D \) satisfying Lemma 2.1 and \( N = p \), this becomes more manageable. In particular the model whose special fiber has the two components depicted in Figure 4 is a regular model and the Atkin-Lehner involutions \( w_m \) for
m \mid D \text{ preserve the two components while } w_p \text{ interchanges them. We use this regular model to create regular models for twists as follows.}

4.1. A regular model when \( p \nmid m \). If \( m \mid D \) and \( p \mid d \), the twist of \( X_0^D(p) \) by \( w_m \) and \( Q(\sqrt{d}) \) has a normal model \( Z \) with a non-reduced special fiber [17, §4.1]. More precisely, as a divisor on \( Z \), \( Z_{\mathbb{F}_p} = 2(\Gamma + \Gamma') \) where \( \Gamma \cong \Gamma' \cong (X^D/w_m)_{\mathbb{F}_p} \), intersecting at the images of the supersingular points of \( X^D \). See Figure 2 for a depiction. We may locally compute that a simple blowup (at the images of the \( w_m \)-fixed points) resolves all singularities and thus gives a regular model.

If \( \left( \frac{-m}{p} \right) = 1 \) then we are in the ordinary case and we may localize away from one of the components of \( Z_{\mathbb{F}_p} \) before blowing up to see that this is the essentially the same regular model as in the case of good reduction [17, Theorem 4.1.1-2]. This is to say that we have smooth \( \mathbb{F}_p \)-rational points if and only if we have \( \mathbb{F}_p \)-rational \( w_m \)-fixed points on \( X^D_{\mathbb{F}_p} \). Over \( \mathbb{F}_p \) these correspond in a 2:1 fashion to the reduced components on the special fiber of the regular model of our twist if \( p \neq 2 \). A depiction of the regular model is given in Figure 3 where \( s \) denotes the strict transform under the blowup.

If \( \left( \frac{-m}{p} \right) = -1 \) then the \( w_m \)-fixed points are supersingular and hence lie on the intersection points of the two branches. In this case, the resulting blowup is different but again by considering only one of the branches, the conditions for existence and rationality of the \( w_m \)-fixed points remain the same as the case of good reduction [17, Theorem 4.1.3-6]. Again, the reduced components on the special fiber of the regular model of our twist if \( p \neq 2 \). A depiction of the regular model is given in Figure 4 where \( s \) denotes the strict transform under the blowup.

4.2. A regular model when \( p \mid m \). If on the other hand \( p \mid m \) then for the normal model \( Z \), \( Z_{\mathbb{F}_p} = 2\Gamma'' \) with \( \Gamma'' \cong X^D_{\mathbb{F}_p} \). A depiction of the regular model is given in Figure 5. An essential difference is that when \( p \mid m \) all fixed points are supersingular. Once more a simple blowup of the \( w_m \)-fixed points resolves all singularities and gives a regular model. Therefore the reduced components of the special fiber of the regular model are in bijection with the \( w_m \)-fixed points over \( \mathbb{F}_p \). We are left with previously explored cases [17, Theorem 4.1.3-6]. This is to say that the supersingular points on \( X^D_{\mathbb{F}_p} \) are in \( W = \text{Aut}(X^D) \)-equivariant bijection
with the fractional ideals of any maximal order in a definite quaternion algebra of discriminant $D_p$. We may then use a theorem on simultaneous embeddings into quaternion orders [17, Theorem 1.5] to determine when we have $\mathbb{F}_p$-rational $w_m$-fixed points.

4.3. **Rationality results.** We now use our newly-formed regular models to rule out rational points on ramified twists.

**Theorem 4.1.** Let $q_1, \ldots, q_{2n}, p$ be distinct primes such that
- for all $i$, $q_i \equiv 1 \mod 12$, $p \equiv 1 \mod 4$,
- $\left( \frac{q_i}{q_j} \right) = 1$ for all $i \neq j$, 

where $\mathbb{F}_p$.
Figure 6. A mnemonic for the configuration of the $q_i$ and $p$.

- there are an odd number of indices $i$ such that $\left( \frac{q_i}{p} \right) = -1$.

Then if $D = q_1 \ldots q_{2n}$ and $p \mid d$, any nontrivial twist of $X_0^D(p)$ by $\mathbb{Q}(\sqrt{d})$ has no $\mathbb{Q}_p$ points.

Proof. Note that $D$ satisfies Lemma $2.1$ and thus Lemma $2.2$. Let us first concentrate on the twists by $w_m$ and $\mathbb{Q}(\sqrt{d})$ where $m \mid D$. We note that if $m = D$ then $\left( \frac{-m}{p} \right) = -1$ and so we are in the case of supersingular reduction. We have no $\mathbb{F}_p$-rational $w_D$-fixed points on the twist because $[17$, Theorem 4.1.3$]$ there is a prime $q \mid D$ such that $\left( \frac{-p}{q} \right) = 1$.

If $m \mid D$, $m \neq D$ and $\left( \frac{-m}{p} \right) = -1$ then since neither $m$ nor $2m = D$, there are no $\mathbb{F}_p$-rational $w_m$-fixed points $[17$, Theorem 4.1$]$. If on the other hand $\left( \frac{-m}{p} \right) = 1$, there is a prime $q \mid (D/m)$ such that $\left( \frac{-m}{q} \right) = 1$. In fact all $q \mid (D/m)$ satisfy this. Thus there are no $w_m$-fixed points, $\mathbb{F}_p$-rational or not $[17$, Theorem 4.1.1-2$]$. Therefore if $p \nmid m$, there are no $\mathbb{Q}_p$ points on a twist of $X_0^D(p)$ by $w_m$ and $\mathbb{Q}(\sqrt{d})$.

Now we turn our attention to the case where $p \mid m$. Since $w_m$-fixed points are supersingular, we can only have $\mathbb{F}_p$-rational $w_m$-fixed points if $m = Dp$ $[14$, Theorem 4.1.3$]$. However, for our $D$ there are no fixed points since there is a prime $q \mid D$ such that $\left( \frac{-p}{q} \right) = 1$. $\square$

Remark 4.2. The conditions given by Theorem $4.1$ are by no means an exhaustive description of the conditions for a ramified twist to lack rational points. The methods we use here are rather robust, but generally require many Legendre conditions to be satisfied so we have tried to err on the side of being simple. We give a mnemonic for these conditions via the dictionary of Morishita $[8]$ between primes and knots, where for primes of the form $1 + 4n$, the Legendre symbol plays the role of the linking number between knots. In this case, no $q_i$ is linked to another $q_j$ and an odd number of the $q_i$ are linked to $p$ as depicted in Figure 6.
5. From Quadratic Twists to All Twists

The astute reader may note that we have thus far spoken only about quadratic twists of the curve $X_D^0(p)$. That is to say, curves $X$ over $\mathbb{Q}$ such that there is a quadratic extension $K$ of $\mathbb{Q}$ such that $X_K \cong X_D^0(p)K$. Consider the following definitions.

**Definition 5.1.** If $V_{/K}$ is a variety, we say that $V$ has property $\mathfrak{P}$ *palindromically* if for all twists $V_{/K}'$ of $V$, $V'$ has property $\mathfrak{P}$.

**Definition 5.2.** Let $q_1 \equiv q_2 \equiv \cdots \equiv q_{2n} \equiv 1 \mod 12$ be an increasing sequence of primes such that $\left( \frac{q_i}{q_j} \right) = 1$ for all $i \neq j$. If $p \equiv 1 \mod 4$ is a prime we let $S_p$ be the set of $D = q_1 \ldots q_{2n}$ such that

- for all $s \in \{1, \ldots, \lfloor \sqrt{4p} \rfloor \}$, there is some $i$ such that $\left( \frac{s^2 - 4p}{q_i} \right) = 1$, and
- for all $i$, $q_{i+1} > 4pq_1 \ldots q_i$, $q_1 > 4p$, and
- $\left( \frac{D}{p} \right) = -1$.

By Theorem 2.3, Theorem 3.2, and Theorem 4.1 we have moreover shown the following.

**Theorem 5.3.** For $\sigma \in \text{Gal}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p)$ and $X/\mathbb{Q}_p$ the base change of $X_D^0(p)$ to $\mathbb{Q}_p$, let $\sigma$ also denote the corresponding automorphism of $X(\bar{\mathbb{Q}}_p)$. Suppose that $D \in S_p$ and let $\{1, u, p, up\}$ denote representatives for the square classes of $\mathbb{Q}_p^\times$, $u = d_1$, $p = d_2$, $up = d_3$, and $\tau_1, \tau_2 \in \text{Gal}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p)$ such that $\tau_i(\sqrt{d_j}) = (-1)^{d_j}d_j^{1/2}$ with $\delta$ denoting the Kronecker delta function. Then for all $\sigma \in \{\tau_1, \tau_2, \tau_1 \tau_2\}$, for all $m \mid Dp$ and for all $P \in X(\bar{\mathbb{Q}}_p)$, $\sigma w_m P \neq P$.

If we state our results in this way, it is easy to show in this case that lacking points on all quadratic twists implies lacking points on all twists.

**Corollary 5.4.** If $D \in S_p$ then $X_D^0(p)(\mathbb{Q}_p) = \emptyset$ palindromically. That is to say, for all $[\xi] \in H^1(\text{Gal}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p), \text{Aut}(X_D^0(p)))$, and any twist $X_D^0(p)_{\xi}$ corresponding to $[\xi]$, $X_D^0(p)_{\xi}(\mathbb{Q}_p) = \emptyset$.

**Proof.** First we base change to $\mathbb{Q}_p$, where we have only a finite number of square classes. Consider that the isomorphism class of a twist $V'$ of a variety $V_{/\mathbb{Q}_p}$ corresponds bijectively to a cohomology class $[\xi] \in H^1(\text{Gal}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p), \text{Aut}(X_{\mathbb{Q}_p}))$. If $V = X$ then for all $\sigma \in \text{Gal}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p)$, there is some $m \mid Dp$ such that $\xi^\sigma = w_m$, and this depends only on the residue class of $\sigma$ in $\text{Gal}(\mathbb{Q}_p(\sqrt{u}, \sqrt{p})/\mathbb{Q}_p)$. If this residue is nontrivial then by the theorem, $\sigma \xi^\sigma P = \sigma w_m P \neq P$. Therefore any twist of $X$ corresponding to the class of $\xi$ has no $Q_p$ points and thus the same is true for $X_D^0(p)_{\xi}$. \qed

**Lemma 5.5.** For any $X \in \mathbb{Z}_{>0}$ and prime $p \equiv 1 \mod 4$, $\# S_p \cap \{1, \ldots, X\} \gg X/\log(X)$.

**Proof.** If we fix $p$, find some $q_1 > 4p$ such that $q_1 \equiv 1 \mod 12$, $\left( \frac{q_1}{p} \right) = -1$ and for all $1 \leq s < \sqrt{4p}$, $\left( \frac{s^2 - 4p}{q_1} \right) = 1$. Fix $q_1$. Then the number of primes $q_3$ such that
For all $D \in S$, and for all $[\xi] \in H^1(\text{Gal}_Q, \text{Aut}(X_D^0(p)))$, we have $X_D^0(p)[\xi](\mathbb{Q}_p) = \emptyset$. Recall now that $X_D^0(p)$ is an intermediate étale cover in the étale torsor $X_D^0(p) \to X^D$ under $G$ where $G(\mathbb{Q}) = \text{GL}_2(\mathbb{F}_p)$. We shall use this torsor to show that certain twists of $X_D$ form counterexamples to the Hasse principle.

Lemma 6.1. Let $V$ be a smooth, proper variety over $\mathbb{Q}$. Then we have a bijection of sets between $\prod_{p \leq \infty} V(\mathbb{Q}_p)$ and $V(\mathbb{A})$ where $\mathbb{A}$ denotes the adeles of $\mathbb{Q}$. Note that by the diagonal embedding we have $V(\mathbb{Q}) \subset V(\mathbb{A})$.

Proof. [13] pp.98-99

Definition 6.2. We say that a smooth, proper variety $V/Q$ is a counterexample to the Hasse principle if $V(\mathbb{Q}) = \emptyset$ but $V(\mathbb{A}) \neq \emptyset$.

Recall now that the Galois twists of the torsor $X_D^0(p) \to X^D$ are given by the cohomology set $H^1(\text{Gal}_Q, \text{GL}_2(\mathbb{F}_p))$. Likewise, if we construct a twist $X$ of $X_D^0$ (in this case, such that $X(\mathbb{A}) \neq \emptyset$) then there is a twist $Y$ of $X_D^0(p)$ such that the twisted map $f : Y \to X$ is a torsor. Once more there is a twist $Z$ of $X_D^0(p)$ through which the torsor $f$ factors. We therefore have the following diagram of étale morphisms of schemes.

\[
\begin{array}{c}
Y \\
\downarrow f \\
Z \\
\downarrow \\
X
\end{array}
\]

Likewise we note that for all $[\xi] \in H^1(\text{Gal}_Q, \text{GL}_2(\mathbb{F}_p))$, we have the twisted diagram

\[
\begin{array}{c}
Y_\xi \\
\downarrow f_\xi \\
Z_\xi \\
\downarrow \\
X
\end{array}
\]

Let us mention why such a diagram exists. Let $f : Y \to X$ be an étale morphism of schemes over a field $K \subset L$ so that we have the étale morphism $F : Y_L \to X_L$. If $X_\xi$ is a twist of $X$ resolving over $L$, then we have an isomorphism $\phi_\xi : (X_\xi)_L \to X_L$ of Spec$(L)$-schemes. Therefore we have a fiber product diagram over Spec$(L)$.
Theorem 6.5. If all \( S \) \( X \) \( D \) sets

\[
\begin{align*}
(Y_{\xi})_L &\xrightarrow{F_{\xi}} (X_{\xi})_L \\
\psi_{\xi} &\downarrow \quad \phi_{\xi} \\
Y_L &\overset{F}{\rightarrow} X_L.
\end{align*}
\]

As suggested by the notation, even though a priori \((Y_{\xi})_L\) is just a fibered product, it is easy to deduce that \( F_{\xi} \) is étale and thus that \( \psi_{\xi} \) is an isomorphism. Therefore, the descent datum on \( Y_L \) given by \( \{ \rho'_\xi : Y_L \rightarrow Y_L \} \) translates over \((Y_{\xi})_L\) to \( \psi_{\xi}^{-1}\rho'_\xi\psi_{\xi} \) and thus there is a corresponding twist \( Y_{\xi} \) of \( Y \) over \( \text{Spec}(K) \) \([11] \, \text{§6.6} \).

Here \( Y_{\xi} \) and \( Z_{\xi} \) are respectively twists of \( Y \) and \( Z \). Now from any particular torsor we can produce an obstruction to rational points.

**Definition 6.3.** \([14] \, \text{Definition 5.3.1} \) Let \( G \) be a linear algebraic group (e.g., a finite group scheme) over \( Q \) and let \( f : Y \rightarrow X \) be a torsor under \( G \). It follows that we have an intermediate set \( X(Q) \subset D(f) \subset X(A) \) defined as

\[
D(f) = \bigcup_{[\xi] \in H^1(\text{Gal}(Q), GL_2(F_p))} f_{\xi}(Y_{\xi}(A)).
\]

We call this set the descent obstruction associated to the torsor \( f \).

**Conjecture 6.4.** If \( X \) is a curve then the intersection over all \( X \)-torsors \( f \) of the sets \( D(f) \) is empty.

This conjecture is known in certain special cases \([14] \, \text{§6.2} \). Let \( S \) be the union of all \( S_p \).

**Theorem 6.5.** If \( X \) is a twist of \( X^D \) with \( D \in S \) such that \( X(A) \neq \emptyset \) then \( X \) is a counterexample to the Hasse principle.

**Proof.** If \( X \) is such a twist then for all \([\xi] \in H^1(\text{Gal}(Q), GL_2(F_p))\) the twist \( Z_{\xi} \) of \( Z \) is a twist of \( X^D(p) \) for some \( p \). By Theorem \([12] \) all such twists have \( Z_{\xi}(Q_p) = \emptyset \) and so \( Y_{\xi}(Q_p) = \emptyset \). It follows that \( Y_{\xi}(A) = \emptyset \) and thus \( D(f) = \emptyset \). Since \( X(Q) \subset D(f) \) \([14] \, \text{§5.3} \), \( X \) is a counterexample to the Hasse principle. \( \square \)

Now let us show how to find twists of \( X^D \) which have adelic points. First we note that if \( n > 630 \) is an integer then \( \phi(n) \geq 6\sqrt{n} \). For \( D \) satisfying Lemma \([2.1] \)

\[
g = g(X^D) = 1 + \phi(D)/12.
\]

Therefore for all \( q \mid D \),

\[
4g^2 = \frac{(\phi(D) + 12)^2}{36} \geq (\sqrt{D} + 2)^2 > D > q.
\]

For \( D < 630 \) satisfying Lemma \([2.1] \) we may check by hand that \( 4g^2 > q \) for all \( q \mid D \). In any case \([17] \, \text{Corollary 3.17, Corollary 5.2} \), if \( d < 0 \) is a squarefree integer such that \( \left( \frac{d}{\ell} \right) = -1 \) for all primes \( \ell < 4g^2 \), then \( C^D(1,d,D)(Q_\ell) \neq \emptyset \) for all primes \( \ell \mid d \) including \( \infty \). If \( r \mid d \), then we can guarantee \( Q_r \) points by letting \( r \equiv 3 \mod 4 \) and requiring \( \left( \frac{-r}{q} \right) = -1 \) for all \( q \mid D \). Since there are an even number of divisors of \( D \) and \( \left( \frac{-r}{q} \right) = \left( \frac{q}{r} \right) \), we additionally have \( \left( \frac{-D}{r} \right) = -1 \). Understanding how to create counterexamples we repurpose \( X \) to be a positive integer and make the following definition.
Definition 6.6. Let $\Sigma_D$ be the collection of $d < 0$ such that $C^D(1,d,D)(A) \neq \emptyset$ and let $M_D$ be the collection of $d < 0$ squarefree with an odd number of prime divisors $r$ such that $r \equiv 3 \mod 4$ and for all $\ell < 4g(X^D)^2$, $\left( \frac{-r}{\ell} \right) = -1$. Moreover if $\Sigma$ is a set of negative integers, let $\Sigma(X) = \Sigma \cap \{-X, \ldots, -1\}$.

We note that the primes $r$ which are divisors of elements of $M_D(X)$ are given by the congruence conditions implied by the conditions $\left( \frac{-r}{\ell} \right) = -1$. In particular the density of these primes in the set of all primes less than $X$ is approximately $(1/2)^{2g^2/\log(2g)}$, a positive constant depending only on $D$. We could also loosen the conditions away from $q \mid D$ to say simply that $\left( \frac{d}{\ell} \right) = -1$, but this makes little difference for our purposes. We now complete the proof of Theorem 1.1.

Lemma 6.7. We have $M_D \subset \Sigma_D$ and $\# M_D(X) \gg X/\log(X)$.

Proof. By the above discussion, $C^D(1,d,D)(A) \neq \emptyset$ [17, §4] for all $d \in M_D$. Consider the elements $d \in M_D(X)$ such that $|d|$ is prime. This is simply the set of $-r \equiv 1 \mod 4$ where $r \leq X$ is a prime such that $\left( \frac{-r}{\ell} \right) = -1$ for all primes $\ell < 4g^2$. This is a set whose size is asymptotically a positive constant times $X/\log(X)$. \hfill \Box

7. The Minimal Example

We note that the examples in Theorem 6.5 are not going to be possible to write down in a conventional paper. The smallest $D$ in $S_5$ (see Definition 5.2) for example is 8473 and $g(X^D) = 685$. In this case, $4g(X^D)^2 = 1876900$ and all possible $d < 0$ must have $\left( \frac{d}{7} \right) = -1$ for the first 140429 primes. Such $d$ will thus lie in congruence classes for a modulus of about 1.8 million digits. Factoring such numbers is not feasible with current technology or perhaps ever. It may be possible to find an example of a prime $d$ as primality testing is easier than factoring, but all known primes with more than 1 million digits are Mersenne primes [2] and if $d$ is prime, then simply checking at the prime 2 reveals that a Mersenne prime will not work.

Instead, we will minimize the genus. It is possible to find $D$ outside of $S_5$ but satisfying Lemma 2.1 such that $X^D_0(5)(\mathbb{Q}_5) = \emptyset$ palindromically. A low-genus example of this phenomenon is $D = 770$ with genus 21. If we use this as a base case, we can find the lowest-genus example of an $X^D$ such that there exists some prime $p$ such that $X^D_0(p)(\mathbb{Q}_p) = \emptyset$ palindromically. There are finitely many Shimura curves $X^D$ of genus $g \leq 20$ and all of them are divisible by at most 4 primes. The Weil bounds of course imply that a smooth genus $g$ curve over $\mathbb{F}_p$ has a rational point if $p > 4g^2$. We meanwhile require that for all $m \mid D$ that $TF'(D,p,m,p) = 0$ in order for $X^D_0(p)(\mathbb{Q}_p) = \emptyset$ palindromically. We therefore want to ensure that $X^D(\mathbb{F}_p)$ has a non-supersingular rational point. If $n$ is the number of prime divisors of $D$ then the number of supersingular points is at most $2^{n+1}h(K)/w(K)$ where $K = \mathbb{Q}(\sqrt{-p})$. The analytic class number formula thus gives us an upper bound on $h(K)$ and tells us that we need only verify the inequality $\#X^D(\mathbb{F}_p) - 2^{n+1}\sqrt{p}\log(p) > 0$. Finally we can use the Weil bounds to see that for instance if $D$ is the product of two primes that we need only check $p < 4g^2 + 24\log(g) + 9\log^2(g)$. A similar inequality holds for four primes.
The lowest-genus pair that we found was \( D = 143 \) and \( p = 2 \). We note that extra care is required when working with the prime 2. Due to wild ramification issues, the conditions for a twist of \( X^D \) by a ramified quadratic extension to have \( \mathbb{Q}_2 \)-rational points are not known \([17]\) Remark 4.14). That said, we can in special cases prevent the existence of \( \mathbb{Q}_2 \) points.

We note first that since \( TF'(143, 2, m, 2) = 0 \) for all \( m \mid D \) and since \( X^D_{\mathbb{F}_2} \) has no supersingular components, \( C^D(2, d, m)(\mathbb{Q}_2) = \emptyset \) for all \( m \mid 2D \) and for all \( d \) such that \( \mathbb{Q}(\sqrt{d}) \) is unramified at 2 \([17]\) Theorem 6.1]. If \( \mathbb{Q}(\sqrt{d}) \) is ramified at 2, note that the only \( m \mid 2D \) where \( w_m \neq \text{id} \) has ordinary fixed points is \( m = D = 143 \). As they are ordinary, they correspond exactly to the CM points for quadratic rings of discriminant \(-143 \) and \(-4(143)\). Note however that if \( H_\Delta(X) \) denotes the Hilbert Class Polynomial of discriminant \( \Delta \), \( Q[X]/H_{-4(143)}(X) \equiv Q[X]/H_{-143}(X) \). By reducing the latter Hilbert Class Polynomial modulo 2 and finding it to be an irreducible degree 10 polynomial over \( \mathbb{F}_2 \), we see that there are no \( \mathbb{F}_2 \)-rational \( w_{143} \)-fixed points.

Now suppose that \( m \mid 2D = 286 \) and \( m \neq 1, 143 \). Then we see that all \( w_m \)-fixed points are supersingular. We therefore appeal to a previously proved theorem on supersingular fixed points on \( X_{\mathbb{F}_2}^{143} \) \([17]\) Corollary 2.26] and thus on \( X_{\mathbb{Q}}^{143}(2) \). There cannot possibly be supersingular \( \mathbb{F}_2 \)-rational \( w_m \)-fixed points on \( X_{\mathbb{Q}}^{143}(2) \) unless \( m = 286 \). Even if \( m = 286 \) there are no \( \mathbb{F}_2 \)-rational \( w_m \)-fixed points because \( 13 \mid D \) and \( 13 \equiv 1 \mod 4 \([17]\) Corollary 2.26.1] and \( 143 \equiv \pm 3 \mod 8 \([17]\) Corollary 2.26.2]. We have therefore shown that all quadratic twists of \( X_{\mathbb{Q}}^{143}(2) \) have no \( \mathbb{Q}_2 \)-rational points.

Finally, we note that there are 7 quadratic extensions of \( \mathbb{Q}_2 \) as opposed to 3 quadratic extensions of \( \mathbb{Q}_p \) for odd \( p \), essentially because there are more unramified quadratic extensions of \( \mathbb{Q}_2 \). Still, our methods for denying points on quadratic twists come down to finding an appropriate integral model and then applying Hensel’s Lemma to the reduction. Since there is still a unique quadratic extension of \( \mathbb{F}_2 \), we can just as well say that for all \( \sigma \in \text{Gal}(\mathbb{Q}_2/\mathbb{Q}) \) and for all cocycles \( \xi : \text{Gal}(\mathbb{Q}_2/\mathbb{Q}_2) \to \text{Aut}(X_{\mathbb{Q}}^{143}(2)) \), there is no point \( P \) such that \( P = \sigma \xi[P] \) since \( \xi = w_m \) for some \( m \mid 286 \) depending on \( \sigma \). We therefore have our example.

**Example 7.1.** For \( D = 143 \), \( X_{\mathbb{Q}}^{143}(2)/\mathbb{Q}_2 = \emptyset \) palindromically. In particular if \( X/\mathbb{Q} \) is a twist of \( X^D \) such that \( X(\mathbb{A}) \neq \emptyset \) then the genus 11 curve \( X \) is a counterexample to the Hasse principle.

In the case of \( X^{143} \), taking the quotient by the involution \( w_{143} \) produces \( E_{143} \), the unique (up to isomorphism) elliptic curve of conductor 143 over the rational numbers. In fact, taking the quotient of \( X^{143} \) by \( w_{143} \) is actually the Shimura-Modular parametrization of \( E_{143} \) and so if we twist \( X^{143} \) by \( w_{143} \) we obtain a twist of the Shimura-Modular parametrization map. We note that \( E_{143}(\mathbb{Q}) \cong \mathbb{Z} \) so these infinitely many twists of \( X^{143} \) are bi-elliptic onto a positive-rank elliptic curve.

While a priori our construction asks to twist \( X^{143} \) by \( w_{143} \) and an imaginary quadratic field \( \mathbb{Q}(\sqrt{d}) \) such that \( \left( \frac{d}{\ell} \right) = -1 \) for all primes \( \ell < 484 \), we can deal only with the primes \( \ell = 11, 13 \) and the primes \( \ell \nmid 143 \) such that \( X^{143}(\mathbb{F}_\ell) = \emptyset \). The only such primes are 2 and 7 so we will twist \( X^{143} \) by \( w_{143} \) and a discriminant \( d \) such that \( \left( \frac{d}{\ell} \right) = -1 \) for \( \ell \in \{2, 7, 11, 13\} \) such that for all primes \( r \mid d \) we have
\[
\left(\frac{-143}{r}\right) = \left(\frac{-r}{11}\right) = \left(\frac{-r}{13}\right) = -1 \quad \text{[17, Theorem 4.1.3].}
\]
Although we may use a similar argument to the proof of Theorem [1.1] to show that the number of such \(d\) with \(|d| < X\) is \(\gg X/\log(X)\), it may be helpful to be explicit here and that if we restrict \(d\) to the case \(-r\) where \(r\) is prime, then our congruence conditions say precisely that we are considering the primes \(r \equiv 3 \mod 8\) such that
\[
\left(\frac{-r}{7}\right) = \left(\frac{-r}{11}\right) = \left(\frac{-r}{13}\right) = -1.
\]
The number of primes \(r < X\) satisfying this condition is asymptotically equal to \(\left(\frac{X}{32\log(X)}\right)\). In particular, \(r = 67\) is the smallest such prime.

**Remark 7.2.** It has also been asked at various times that since \(\mathbb{Q}_p\) points are being ruled out on all twists of \(X^D(p)\), it is natural to wonder if these techniques could be applied to the modular curves \(X(p)\), or perhaps even \(Y(p)\) to avoid cusps. Unfortunately not, and we give a rough argument as follows. Following earlier work [11, §4.5], we can give a twist \(Y_E(p)\) with a rational point [11, Lemma 4.4].

**References**

1. Siegfried Bosch, Werner Lütkebohmert, and Michel Raynaud, *Néron models*, Ergebnisse der Mathematik und ihrer Grenzgebiete (3), vol. 21, Springer-Verlag, Berlin, 1990.
2. Chris Caldwell, *The largest known primes*, http://primes.utm.edu/largest.html, May 2014.
3. Pete L. Clark, *Curves over global fields violating the Hasse principle*, Preprint.
4. _____, *Rational points on Atkin-Lehner quotients of Shimura curves*, ProQuest LLC, Ann Arbor, MI, 2003, Thesis (Ph.D.)–Harvard University.
5. _____, *An “anti-Hasse principle” for prime twists*, Int. J. Number Theory 4 (2008), no. 4, 627–637.
6. Martin Eichler, *Modular correspondences and their representations*, J. Indian Math. Soc. (N.S.) 20 (1956), 163–206.
7. Bruce W. Jordan and Ron A. Livné, *Local Diophantine properties of Shimura curves*, Math. Ann. 270 (1985), no. 2, 235–248.
8. Masanori Morishita, *Knots and primes*, Universitext, Springer, London, 2012.
9. Ekin Ozman, *Points on quadratic twists of \(X_0(N)\)*, Acta Arith. 152 (2012), no. 4, 323–348.
10. _____, *On polyquadratic twists of \(X_0(N)\)*, J. Number Theory 133 (2013), no. 10, 3325–3338.
11. Bjorn Poonen, Edward F. Schaefer, and Michael Stoll, *Twists of \(X(7)\) and primitive solutions to \(x^2 + y^3 = z^7\)*, Duke Math. J. 137 (2007), no. 1, 103–158.
12. Victor Rotger, *On the group of automorphisms of Shimura curves and applications*, Compositio Math. 132 (2002), no. 2, 229–241.
13. Victor Rotger, Alexei Skorobogatov, and Andrei Yafaev, *Failure of the Hasse principle for Atkin-Lehner quotients of Shimura curves over \(\mathbb{Q}\)*, Mosc. Math. J. 5 (2005), no. 2, 463–476.
14. Alexei Skorobogatov, *Torsors and rational points*, Cambridge Tracts in Mathematics, vol. 144, Cambridge University Press, Cambridge, 2001.
15. _____, *Shimura coverings of Shimura curves and the Manin obstruction*, Math. Res. Lett. 12 (2005), no. 5-6, 779–788.
16. _____, *Descent obstruction is equivalent to étale Brauer-Manin obstruction*, Math. Ann. 344 (2009), no. 3, 501–510.
17. James Stankewicz, *Twists of Shimura curves*, Canad. Jour. Math. 66 (2014), no. 4, 924–960.