AN "ANTI-HASSE PRINCIPLE" FOR PRIME TWISTS

PETE L. CLARK

ABSTRACT. Given an algebraic curve $C_{/\mathbb{Q}}$ having points everywhere locally and endowed with a suitable involution, we show that there exists a positive density family of prime quadratic twists of C violating the Hasse principle. The result applies in particular to w_N-Atkin-Lehner twists of most modular curves $X_0(N)$ and to w_p-Atkin-Lehner twists of certain Shimura curves X^{D+}.

1. INTRODUCTION

1.1. **Some motivation.** Let $C_{/\mathbb{Q}}$ be a (nonsingular, projective, geometrically integral) algebraic curve. We say C *violates the Hasse principle* if for all places $p \leq \infty$, $C(\mathbb{Q}_p) \neq \emptyset$, but $C(\mathbb{Q}) = \emptyset$. It is of interest to *construct* families of such curves in a systematic way, and also to *discover* naturally occurring families. Although one has various results showing that there are "many" curves violating the Hasse principle – e.g, infinitely many for every genus $g \geq 1$ [CM] – to the best of my knowledge the literature contains no "natural" infinite[1] family of curves $C_{/\mathbb{Q}}$ provably violating the Hasse principle, i.e., an infinite sequence of curves of prior arithmetic-geometric interest and not just constructed for this purpose.[2] Our primary goal in this note is to exhibit such a "natural" infinite family.

1.2. **Statements of the main results.**
Let N be a squarefree positive integer, $p \equiv 1 \pmod 4$ a prime with $p \neq N$, and let $C(N,p)_{/\mathbb{Q}}$ be the *quadratic twist* of $X_0(N)$ by the Atkin-Lehner involution w_N and the quadratic extension $\mathbb{Q}(\sqrt{p})/\mathbb{Q}$. (Precisely what this means will be reviewed shortly.) These curves are moduli spaces of elliptic $\mathbb{Q}$-curves (e.g. [Ell]): roughly speaking, $C(N,p)(\mathbb{Q})$ parameterizes elliptic curves defined over $\mathbb{Q}(\sqrt{p})$ which are cyclically N-isogenous to their Galois conjugates.

Theorem 1. *For $131 < N \neq 163$ a squarefree integer, the set of primes $p \equiv 1 \pmod 4$ such that $C(N,p)$ violates the Hasse principle over $\mathbb{Q}$ has positive density.*

Upon examining the proof of Theorem 1, it swiftly became clear that the properties of $X_0(N)$ and w_N needed for the argument could be axiomatized to yield a general criterion for prime quadratic twists violating the Hasse principle. This generalization costs nothing extra – indeed, it seems if anything to clarify matters – and it shall turn out to have (at least) one other interesting application.

The axiomatic version goes as follows: let $C_{/\mathbb{Q}}$ be a curve and $\iota : C \to C$ be a $\mathbb{Q}$-rational involution. Let $\mathbb{Q}(\sqrt{d})/\mathbb{Q}$ be a quadratic extension, with nontrivial automorphism σ_d. Then there is a curve $C_d = \mathcal{T}(C, \iota, \mathbb{Q}(\sqrt{d})/\mathbb{Q})$ called the *quadratic*

---

[1]For an interesting finite family constructed by a systematic method, see [RSY].
[2]The situation is different if one allows the possibility of a variable base extension: see [Cl2].

twist of C by ι and $\mathbb{Q}(\sqrt{d})/\mathbb{Q}$ (or just by d). The curve C_d is isomorphic to C over $\mathbb{Q}(\sqrt{d})$ but not, in general, over $\mathbb{Q}$: σ_d acts on $C_d(\mathbb{Q}(\sqrt{d}))$ by $P \mapsto \iota(\sigma_d(P))$. Its existence follows from the principle of Galois descent: the $\overline{\mathbb{Q}}/\mathbb{Q}$-twisted forms of C with respect to the automorphism group generated by ι are parameterized by

$$H^1(\overline{\mathbb{Q}}/\mathbb{Q}, \langle \sigma \rangle) = \mathrm{Hom}(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}), \pm 1) \cong \mathbb{Q}^\times/\mathbb{Q}^{\times 2}.$$

Theorem 2. *Let $C_{/\mathbb{Q}}$ be an algebraic curve. Suppose there is a $\mathbb{Q}$-rational involution ι on C such that:*
(i) $\{P \in C(\mathbb{Q}) \mid \iota(P) = P\} = \emptyset$.
(ii) There exists $P_0 \in C(\overline{\mathbb{Q}})$ such that $\iota(P_0) = P_0$.
(iii) For all $\ell \leq \infty$, $C(\mathbb{Q}_\ell) \neq \emptyset$, i.e., C has points everywhere locally.
(iv) The quotient C/ι has finitely many $\mathbb{Q}$-rational points.
Then the set of primes $p \equiv 1 \pmod 4$ for which the twist $C_p = \mathcal{T}(C, \iota, \mathbb{Q}(\sqrt{p})/\mathbb{Q})$ violates the Hasse principle has positive density.

Remark 1.1: Each of the assumptions (i) and (ii) is necessary for the conclusion to hold: if (i) fails then every quadratic twist C_d has $\mathbb{Q}$-points; whereas if (ii) fails then the set of squarefree d for which C_d has points everywhere locally is finite [Sko′, Prop. 5.3.2]. One must assume at least (iii′): $C_{/\mathbb{Q}_\ell}$ has quadratic points for all $\ell \leq \infty$ (or, in the terminology of [Cl2], that $m_{\mathrm{loc}}(C) \leq 2$). It is probably not the case that (iii′) is *in general* sufficient for the existence of twists C_d (prime or otherwise) violating the Hasse principle, but it might be interesting to try to modify the argument so as to apply to some particular curves satisfying (iii′), e.g. certain Shimura curves $X_0^D(N)$. Finally, some additional hypothesis, like (iv), is needed to ensure that C is not the projective line!

Remark 1.2: A pair (C, ι) can satisfy the hypotheses of Theorem 2 only if C/ι has genus at least one and C has genus at least two. Indeed, since C has points everywhere locally, so does C/ι, so if it had genus zero it would – by the Hasse principle – be isomorphic to $\mathbb{P}^1$ and have infinitely many $\mathbb{Q}$-points. But C/ι would have genus zero if C had genus zero (clearly) or genus one (since ι has fixed points).

Remark 1.3: From the proof one can deduce an explicit lower bound on the density of the set $\mathcal{P} = \mathcal{P}(C, \iota)$ of primes such that C_p violates the Hasse principle in terms of the genera of C and C/ι. However, it does *not* give us an effective way to find any elements of $\mathcal{P}$ unless we can find all the $\mathbb{Q}$-points on C/ι. In the case of $X_0^+(N) = X_0(N)/w_N$, this is a notoriously difficult open problem, c.f. §3.3.

One may ask why in (iii) we do not just assume that C has a $\mathbb{Q}$-point: otherwise our curve *already* violates the Hasse principle, and twisting it to get further violations seems less interesting. The advantage of stating the result the way we have is that it applies *even if we don't know whether or not C has $\mathbb{Q}$-rational points*. This distinction is illustrated in the following additional application of Theorem 2.

Let $D = p_1 \cdots p_{2r}$ be a nontrivial squarefree product of an even number of primes, and consider the Shimura curve $X_{/\mathbb{Q}}^D$ (e.g. [Cl0, Chapter 0]). Unfortunately (iii) does not hold – e.g. $X^D(\mathbb{R}) = \emptyset$ [Og2] – so Theorem 2 does not apply. On the other hand, the full Atkin-Lehner group W consists of 2^{2r} commuting involutions w_d, one for each $1 \leq d \mid D$. It turns out that $X^{D+} := X^D/w_D$ has points everywhere locally

[Cl0, Main Theorem 2]. Since W is commutative of order at least 4, for a prime $q \mid D$, w_q induces a well-defined, nontrivial involution on X^{D+}, which we continue to denote by w_q. Let $C_p(D, w_q)$ be the twist of X^{D+} by w_q and $\mathbb{Q}(\sqrt{p})/\mathbb{Q}$.

Theorem 3. *There exists an integer D_0 with the following property: for pairwise distinct primes $q > 163$, $p_2, \ldots, p_{2r}$ such that:*
(a) $(\frac{q}{p_i}) \neq 1$ for all i; and
(b) $D := q \cdot p_2 \cdots p_{2r} > D_0$,
the set of primes p for which $C_p(D, w_q)$ violates the Hasse principle over $\mathbb{Q}$ has positive density.

Although this family is perhaps less "natural" than that of Theorem 1 – the modular interpretation of $C_p(D, w_q)$ is rather abstruse – it is interesting for other reasons, as we explain at the end.

The proofs are given in §2. In §3 we discuss certain complements, in particular a generalization of Theorem 2 to twists by automorphisms of prime degree p on curves defined over a number field containing the pth roots of unity.

1.3. **Connections with the Inverse Galois Problem for $PSL_2(\mathbb{F}_p)$.** Our motivation for considering Atkin-Lehner twists of $X_0(N)$ by *primes p* in particular comes from work of K.-y. Shih, who showed that if $(\frac{N}{p}) = -1$, then there is a covering of curves $Y \to C(N, p)$, Galois over $\mathbb{Q}$ with group $PSL_2(\mathbb{F}_p)$ [Shi, Thm. 8]. There is thus an ulterior motive for studying the locus $C(N, p)(\mathbb{Q})$: each such point P yields by specialization a homomorphism $\rho_P : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to PSL_2(\mathbb{F}_p)$. So if ρ_P is surjective for some P, we get a realization of $PSL_2(\mathbb{F}_p)$ as a Galois group over $\mathbb{Q}$ (an open problem, in general).

If we have such a surjective specialization, let us say that "Shih's strategy succeeds" for these values of N and p. Remarkably – more than 30 years after [Shi] – Shih's strategy remains the state of the art: with the single exception of a theorem of Malle [Mal] dealing with the case $(\frac{5}{p}) = -1$ – every realization of $PSL_2(\mathbb{F}_p)$ as a Galois group over $\mathbb{Q}$ is an instance of the success of Shih's strategy.

Shih himself gave a complete analysis of the cases where $C(N, p)$ has genus zero. Following up on a suggestion of Serre, some of the genus one cases were analyzed in [Cl1]. This paper closes with three questions about rational points on $C(N, p)$, the last being whether there are examples in which points exist eveywhere locally but not globally. An early draft of this paper billed Theorem 1 as an answer to this question, but it is not, really, since the primes constructed in the proof all satisfy $(\frac{N}{p}) = 1$. So there is now an Appendix to this paper in which the topic of local and global points on $C(N, p)$ under the hypothesis $(\frac{N}{p}) = -1$ is revisited. We make some further remarks on the genus one cases, and, especially, we modify the argument of Theorem 2 to give many Hasse principle violations when $(\frac{N}{p}) = -1$, showing that there are purely global obstructions to the success of Shih's method.

2. Proofs

Proof of Theorem 2: For a squarefree $d \neq 1$, there are natural set maps

$$\alpha_d : C_d(\mathbb{Q}) \hookrightarrow C(\mathbb{Q}(\sqrt{d}))$$

and

$$\beta_d : C(\mathbb{Q}(\sqrt{d})) \to (C/\iota)(\mathbb{Q}(\sqrt{d})).$$

Put

$$S_d = (\beta_d \circ \alpha_d)(C_d(\mathbb{Q})).$$

Then $S_d \subset (C/\iota)(\mathbb{Q})$. Moreover, $(C/\iota)(\mathbb{Q}) = \bigcup_d S_d \cup \iota(C(\mathbb{Q}))$, and for $d \neq d'$, $P \in S_d \cap S_{d'}$ implies that $P \in C(\mathbb{Q}(\sqrt{d})) \cap C(\mathbb{Q}(\sqrt{d'})) = C(\mathbb{Q})$. But $S_d \cap C(\mathbb{Q})$ consists of $\mathbb{Q}$-rational ι-fixed points, which we have assumed in (i) do not exist, so that for $d \neq d'$, $S_d \cap S_{d'} = \emptyset$. By (iv), $(C/\iota)(\mathbb{Q})$ is finite, and we conclude that the set of d for which $S_d \neq \emptyset$ is finite. In particular, for all sufficiently large primes p, the prime twists C_p have no $\mathbb{Q}$-rational points.

Thus it shall suffice to construct a set of primes $p \equiv 1 \pmod 4$ of positive density such that C_p has $\mathbb{Q}_\ell$-rational points for all $\ell \leq \infty$. A key observation is that if p is a square in $\mathbb{Q}_\ell$, then since $\mathbb{Q}_\ell$ contains $\mathbb{Q}(\sqrt{p})$, $C_p(\mathbb{Q}_\ell) = C(\mathbb{Q}_\ell)$, which is nonempty by (iii). In particular, since $p > 0$, $C_p(\mathbb{R}) \neq \emptyset$ for all p.

Let M_1 be a positive integer such that for $\ell > M_1$, C extends to a smooth relative curve $C_{/\mathbb{Z}_\ell}$. If $\ell > M_1$ is prime to p, then we claim that C_p also extends smoothly over $\mathbb{Z}_\ell$. Indeed, the extension $\mathbb{Q}_\ell(\sqrt{p})/\mathbb{Q}_\ell$ is unramified (note that we use $p \equiv 1 \pmod 4$ here), and after this base change C_p becomes isomorphic to C. As above, (iii) and (iv) imply that C (hence also C_p) has positive genus, so C admits a minimal regular $\mathbb{Z}_\ell$-model. But it is known that formation of the minimal regular model commutes with unramified base change, so the minimal model of $C_{/\mathbb{Z}_\ell}$ must already have been smooth.

Let g be the genus of C; notice that it is also the genus of C_p for all p. By the Weil bounds for curves over finite fields, there exists a number M_2 such that if $\ell > M_2$, every nonsingular curve $C_{/\mathbb{F}_\ell}$ of genus g has an $\mathbb{F}_\ell$-rational point. Thus, if $\ell > M = \max\{M_1, M_2\}$ and is different from p, then C_p admits a regular $\mathbb{Z}_\ell$ model whose special fiber has a smooth $\mathbb{F}_\ell$-rational point; by Hensel's Lemma this implies that $C_p(\mathbb{Q}_\ell) \neq \emptyset$.

It remains to choose p to take care of the primes $\ell \leq M$ and $\ell = p$. In the former case we may just assume that $p \equiv 1 \pmod 8$ and that p is a quadratic residue modulo every odd $\ell \leq M$, so that by the above observation we get that $C_p(\mathbb{Q}_\ell) = C(\mathbb{Q}_\ell) \neq \emptyset$. Finally, to get that $C_p(\mathbb{Q}_p) \neq \emptyset$, we use (ii) the existence of a geometric ι-fixed point P_0. If we choose p to split completely in $\mathbb{Q}(P_0)$, then P_0 is a $\mathbb{Q}_p$-rational fixed point of ι, so is an element of $C(\mathbb{Q}_p) \cap C_p(\mathbb{Q}_p)$. In all we have required p to split completely in a finite collection of number fields, so all primes splitting completely in the compositum will do. Cebotarev's theorem implies that this set of primes has positive density.

Proof of Theorem 1: We just check that the hypotheses of Theorem 2 apply with $C = X_0(N)$ and $\iota = w_N$. It is well-known that there are always w_N-fixed points – so (i) holds – and that

$$\min \{[\mathbb{Q}(P) : \mathbb{Q}] \mid P \in X_0(N)(\overline{\mathbb{Q}}), \ w_N(P) = P\} = h(\mathbb{Q}(\sqrt{-N})),$$

the class number of $\mathbb{Q}(\sqrt{-N})$ (e.g. [Og1, Prop. 3]). (We use here that N is square-free.) Thus (ii) holds unless $h(-N) = 1$, i.e., unless $N = 1$, 2, 3, 7, 11, 19, 43, 67 or 163. Using the genus formula for $X_0^+(N)$ (and the standard upper bound on the class numbers of imaginary quadratic fields), it is straightforward to compute the complete list of N for which $X_0^+(N)$ has genus at most one. We shall not give this list here, but the largest such N is 131 (compare with e.g. [Bar]), verifying (iii). Finally, the rationality of the cusps gives $X_0(N)(\mathbb{Q}) \neq \emptyset$ for all N, hence (iv) holds.

Proof of Theorem 3: Again we will verify the hypotheses of Theorem 2, now with $C = X^{D+}$ and ι the image of w_q. The congruence conditions in the statement of theorem ensure that w_q has fixed points on X^D (e.g. [Og2] or [Cl0, Prop. 48]); *a fortiori* its image on X^{D+} has fixed points, so (i) holds. The field of definition $\mathbb{Q}(P)$ of any w_q-fixed point P contains the Hilbert class field of $\mathbb{Q}(\sqrt{-q})$, so if $q > 163$, $[\mathbb{Q}(P) : \mathbb{Q}] > 2$. The degree of the field of definition of the image of P on the involutory quotient X^{D+} is at least $\frac{1}{2}[\mathbb{Q}(P) : \mathbb{Q}]$, so there are no $\mathbb{Q}$-rational ι-fixed points on X^{D+}.[3] Thus (ii) holds.

For (iv), it is enough to know that the genus of $X^D/\langle w_D, w_q\rangle$ is at least 2 for all sufficiently large D. But a routine calculation using the formulae for the genus of X^D and the number of fixed points of the w_d's shows that even the genus of the full Atkin-Lehner quotient X^D/W approaches ∞ with D (e.g. [Cl0, Corollary 50]).

As already mentioned, that (iii) holds for *all* squarefree D was shown in my (unpublished) Harvard thesis [Cl0, Main Theorem 2]. In the meantime, Rotger, Skorobogatov and Yafaev have proved a more general result [RSY, Theorem 3.1]. Both proofs use a result of Ogg for $\ell = \infty$; a trace formula for $(\ell, D) = 1$; and the Cerednik-Drinfeld uniformization for $\ell \mid D$; i.e., they are similar enough so that there seems to be no need to reproduce the details of my argument here.

3. Complements

3.1. **Variants of Theorem 2.**

Theorem 2 extends immediately to the case of (C, ι) defined over an arbitrary number field K, still twisting by the quadratic (for all but finitely many p) extensions $K(\sqrt{p})/K$. Of course, these need not be "prime" quadratic twists with respect to K, but this can be remedied.

Indeed, there is an analogue of Theorem 2 for a curve C over a number field $K \supset \mathbb{Q}(\mu_p)$ endowed with a K-rational automorphism φ of prime order p. Kummer theory gives:

$$K^\times/K^{\times p} = H^1(K, \langle\varphi\rangle).$$

By Galois descent, an element $x \in K^\times$ gives rise to a twist $C_x = \mathcal{T}(C, \varphi, K(x^{\frac{1}{p}})/K)$.

Theorem 4. *Let $K \supset \mathbb{Q}(\mu_p)$ be a number field, and let $C_{/K}$ be an algebraic curve. Suppose there is a K-rational automorphism $\varphi : C \to C$ of prime order p such that:*
(i) $\{P \in C(K) \mid \varphi(P) = P\} = \emptyset$.
(ii) There exists $P_0 \in C(\overline{K})$ such that $\varphi(P_0) = P_0$.
(iii) C has points everywhere locally.
(iv) The quotient C/φ has finitely many K-rational points.
Then there exists a modulus $\mathfrak{m}$ of K such that the prime ideals $\mathfrak{p}$ of $\mathfrak{o}_K$ which are generated by an element $\pi \equiv 1 \pmod{\mathfrak{m}}$ such that C_π violates the Hasse principle over K have positive density.

Here $\mathfrak{m}$ is chosen so that $\pi \equiv 1 \pmod{\mathfrak{m}}$ implies that π is totally positive and a perfect p-th power in the completion of K at any prime $\mathfrak{p}$ lying over p; e.g., when $K = \mathbb{Q}$ we take $\mathfrak{m} = 8 \cdot \infty$. The remainder of the proof is left to the reader.

---

[3]Note here the analogy between $X_0(N)$ and X^{D+}, rather than X^D.

3.2. **Rational points on Atkin-Lehner quotients of Shimura curves.** Let us end by calling attention to the sequence of curves X^{D+}: for me it is the example *par excellence* of a naturally occurring family of curves with points everywhere locally. In fact work of Jordan, Rotger and others shows that the modular interpretation of X^{D+} is in many respects more natural than that of X^D. Recall the "folk conjecture" that for sufficiently large squarefree N, $X_0^+(N)(\mathbb{Q})$ consists only of cusps and CM points. As alluded to above, this is an extremely difficult conjecture, since the favorable case for determining the $\mathbb{Q}$-points on $C_{/\mathbb{Q}}$ is when $\mathrm{Jac}(C)$ has a $\mathbb{Q}$-factor of rank less than its dimension. But analysis of the sign in the functional equations shows – assuming the conjecture of Birch and Swinnerton-Dyer (henceforth BSD) – that this *never* happens for $X_0^+(N)$.

By work of Jacquet-Langlands and Faltings, the same holds for X^{D+}, so that the study of $X^{D+}(\mathbb{Q})$ is again very difficult. The X^{D+} version of the above folk conjecture is that for sufficiently large D, $X^{D+}(\mathbb{Q})$ consists only of CM points. But the CM points are well understood, and one can see in particular that the set of D such that X^{D+} has a $\mathbb{Q}$-rational CM point has density zero.[4] Thus either (I) the curves X^{D+} violate the Hasse principle for a density one set of squarefree integers D; (II) there is some (as yet unknown) specific phenomenon which puts many $\mathbb{Q}$-rational points on Atkin-Lehner quotients of Shimura curves; or (III) our conventional wisdom about $\mathbb{Q}$-points on algebraic curves – i.e., that they are "typically" relatively sparse unless there is some good reason – is completely wrong. Each of three options is fascinating in its own way, but which is true?!?

It seems to me that Theorems 2 and 3 provide some evidence against (III). But the curves X^{D+} are hardly "randomly chosen": the conjectured nonexistence of non-CM $\mathbb{Q}$-rational points implies the nonexistence of certain kinds of GL_2-type abelian surfaces $A_{/\mathbb{Q}}$ and (*a fortiori*, assuming Serre's conjecture) certain kinds of modular forms. Our current understanding of these associated objects is so limited that we certainly cannot dismiss the possibility of (II).

APPENDIX: ATKIN-LEHNER TWISTS WITH $\left(\frac{N}{p}\right) = -1$

This is essentially an addendum to [Cl1]. Although some of the results of *loc. cit.* will be revisited here with a slightly different emphasis, for more complete accounts the reader should consult [Cl1] as well as [Shi] and [Ser].

We will suppose throughout that $N > 1$ is a squarefree integer and p is an odd prime such that $\left(\frac{N}{p}\right) = -1$; by [Shi, Thm. 8] there is then a $\mathbb{Q}$-rational $PSL_2(\mathbb{F}_p)$-Galois cover $Y \to C(N, p)$.[5] We would like to know for which values of N and p there exists a point $P \in C(N, p)(\mathbb{Q})$ whose associated homomorphism $\rho_P : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{PSL}_2(\mathbb{F}_p)$ is surjective. In particular we would like to know whether $C(N, p)(\mathbb{Q}) \neq \emptyset$, and especially whether there are any non-CM points (since the specialization homomorphism at a CM point will have abelian image

---

[4]This uses the zero density of the set of integers with a bounded number of prime divisors; among discriminants $D = p_1 p_2$, the probability of rational CM point is $(1 - (1 - \frac{1}{4})^9) \approx .925$.

[5]In the body of the text we defined $C(N, p)$ only for $p \equiv 1 \pmod 4$; indeed the proof of Theorem 2 required $p \equiv 1 \pmod 8$. But Shih's theorem holds for $p \equiv -1 \pmod 4$ if we define $C(N, p)$ as the twist of $X_0(N)$ by w_N and $-p$ – i.e., in general as the twist by w_N and $p^* = p^{\frac{p-1}{2}}$.

upon restriction to the corresponding imaginary quadratic field, it will not be surjective for any odd p). Intuitively, one might expect ρ_P to be surjective for "most" non-CM points. Indeed, work of Hilbert, Faltings and Serre shows that whenever $C(N, p)(\mathbb{Q})$ is infinite, there are infinitely many irreducible specializations.

The cases in which $C(N, p)$ has genus zero ($N = 2$, 3, 5, 7, 10, 13) are decisively treated in [Shi], [Ser] and [Cl1]: in particular, when $N = 2$, 3 or 7 (class number 1!), Shih's strategy succeeds for all p (with $(\frac{N}{p}) = -1$). The genus one cases are $N = 11$, 14, 15, 17, 19, 21; for $N = 11$ and 19 (class number 1!) we will say only that Shih's strategy works when $p \equiv 1 \pmod 4$ conditionally on BSD and refer the reader to [Cl1] for more details. To deal with some of the other cases, the following result was used [Cl1, Theorem 11].[6]

Theorem 5. *For prime N, $C(N, p)(\mathbb{Q}_N) = \emptyset \iff N \equiv 1 \pmod 4$.*

This shows the failure of Shih's method when $N = 17$ (and also $N = 5$, 13; a similar argument shows that $C(10, p)(\mathbb{Q}_5) \neq \emptyset$ iff $(\frac{5}{p}) = 1$). The other cases ($N = 14$, 15, 21) were not analyzed in [Cl1] since they could not lead to any new Galois groups (nor even to the recovery of Malle's result).

Note the remarkable fact that in every case above, we either had an obvious $\mathbb{Q}$-rational point or a local obstruction at a prime $\ell \mid N$; in particular there were no violations of the Hasse principle.

Here we want to point out that the cases $N = 14$ and $N = 21$ nevertheless give rise to some interesting Diophantine problems. The analysis of local points on $C(14, p)$ and $C(21, p)$ is complete except at the prime p: interestingly, computations suggest that there are points everywhere locally iff there are points at every place except p, which leads me to believe that there is a criterion for the emptiness of $C(N, p)(\mathbb{Q}_p)$ which is equally simple as that of $\mathbb{Q}_\ell$ for $\ell \mid N$ and "quaternionically linked to it." When (for instance) $N = 14$ and $p \equiv 17 \pmod{56}$, computations suggest that there are always points everywhere locally. Despite the fact that there are no "obvious" $\mathbb{Q}$-rational points here, for the first 101 such primes in this congruence class we do in fact get an elliptic curve, necessarily of odd analytic rank, so this gives 101 cases of the success of Shih's strategy. It would be surprising if this phenomenon persisted for all p in this congruence class. However, our lack of counterexamples is the "Selmer dual" of a phenomenon encountered in [Cl1]: let $J(14, p)$ be the Jacobian of $C(14, p)$, i.e., the quadratic twist of $X_0(14)$ by p^* in the usual sense. Since $J_0(14)[2] \cong X_0(14)[2] \cong \mathbb{Z}/2\mathbb{Z}$, and twists by primes $p \equiv 1 \pmod 4$ have odd analytic rank, then (assuming BSD) the curve $C(14, p)$ can only represent a nontrivial element of $\text{Ш}(\mathbb{Q}, J(14, p))[2]$ if the 2-Selmer rank of $J(14, p)$ is at least 3 (and in fact at least 4 because the contribution of $\text{Ш}[2]$ to the 2-Selmer rank will be even). Now recall that in [Cl1] we were unable to find prime twists of $X_0(11)$ or $X_0(19)$ of rank at least 3! It would be very interesting to have some conjectural asymptotics on the variation of 2-Selmer ranks in families of prime twists that would give us a hint as to how far we ought to look before being surprised by the lack of examples in each case.

---

[6] Let us note, as we did in [Cl1], that the implication $\Longleftarrow$ of Theorem 5 is a special case of a theorem of Gonzalez [Que, Thm 6.2].

I am not aware of a single example of the success of Shih's strategy when $C(N, p)$ has genus at least two. These would necessarily come from exceptional $\mathbb{Q}$-rational points on $X_0^+(N)$ with the additional condition that the quadratic field of the preimage is $\mathbb{Q}(\sqrt{p^*})$ for some prime p with $(\frac{N}{p}) = -1$ (for the associated ρ_P must be surjective, but this seems to be the least of our worries).[7] Note that the "folk conjecture" of §3.2 predicts that Shih's strategy succeeds for only finitely many pairs (N, p) with $g(C(N, p)) \geq 2$, so in particular that we will not be able to obtain all $PSL_2(\mathbb{F}_p)$'s as a Galois group over $\mathbb{Q}$ by this method.

We shall now show that there are plenty of curves $C(N, p)$ with $p \equiv 1 \pmod 4$, $(\frac{N}{p}) = -1$ violating the Hasse principle. Assume for simplicity that N is *prime*. Assume also that $N > 163$, so that $C(N, p)(\mathbb{Q}) = \emptyset$ for all but finitely many primes p. We will try to run through the argument of Theorem 2 except with the congruence condition $(\frac{N}{p}) = -1$, i.e., p is inert in $\mathbb{Q}(\sqrt{N})$. There are however two issues to be addressed: the first is that $C(N, p)$ need not have $\mathbb{Q}_N$-rational points; indeed by Theorem 5 we know that it will iff $N \equiv -1 \pmod 4$, so let us assume this condition on N. It is then indeed the case that for all but finitely many p satisfying the modified conditions, C_p violates the Hasse principle. However, there is a second issue: since one of our conditions on p is not a splitting condition, it is not *a priori* clear that our conditions on p are consistent, i.e., correspond to some nonvoid Cebotarev set.

Let us now carefully check the consistency. To be precise, we are imposing the following conditions on p: (a) p splits completely in $K_1 := \mathbb{Q}(\zeta_8)$ – i.e., $p \equiv 1 \pmod 8$; (b) p is inert in $\mathbb{Q}(\sqrt{N})$; (c) p splits in sufficiently many quadratic fields $\mathbb{Q}(\sqrt{\ell^*})$ for ℓ odd and different from p and N (namely, such that for the remaining primes ℓ, $C(N, p)$ has smooth reduction modulo ℓ and an $\mathbb{F}_\ell$-rational point on its special fiber); and (d) p splits completely in $\mathbb{Q}(P_0)$, where P_0 is a w_N-fixed point corresponding to the *maximal* order of $\mathbb{Q}(\sqrt{-N})$ (and not the one of conductor 2). Let K_2 be the compositum of $\mathbb{Q}(\sqrt{\ell^*})$ for the finite set of odd primes ℓ considered above, and let $K_3 := \mathbb{Q}(P_0, \sqrt{-N})$, the Hilbert class field of $\mathbb{Q}(\sqrt{-N})$. The fields K_i for $1 \leq i \leq 3$ are each Galois over $\mathbb{Q}$ and are mutually linearly disjoint, since their sets of ramified finite primes are pairwise disjoint. Put $K = K_1 \cdot K_2 \cdot K_3$, so that $\mathrm{Gal}(K/\mathbb{Q}) = \prod_{i=1}^{3} \mathrm{Gal}(K_i/\mathbb{Q})$. In G_3 there is a unique conjugacy class C consisting of elements σ with nontrivial restriction to $\mathbb{Q}(\sqrt{-N})$. So, by Cebotarev, the primes p which are unramified in K and with corresponding Frobenius automorphism lying in the conjugacy class $(1, 1, C)$ have positive density. We have shown:

Theorem 6. *Suppose $N > 163$ is prime and congruent to $-1 \pmod 4$. The set of primes $p \equiv 1 \pmod 4$, $(\frac{N}{p}) = -1$ such that $C(N, p)$ violates the Hasse principle over $\mathbb{Q}$ has positive density.*

Thus we get an affirmative answer to the question asked at the end of [Cl1]: there are "truly global" obstructions to the success of Shih's method.

---

[7]I have not, however, had the opportunity to read through all of the rapidly growing literature on $\mathbb{Q}$-curves in search of such examples. It would be very useful if there existed an online database containing all known exceptional rational points on $X_0^+(N)$.

Acknowledgements: Thanks to Jordan Ellenberg and Bjorn Poonen for useful comments. I am grateful to the authors of [RSY] for their citation of my unpublished thesis work. The title of this paper was chosen, in part, to please Siman Wong.

Postscript:　Recent (and recently remembered) correspondences with Nick Rogers and Noam Elkies suggest that the computationally observed phenomenon of 2-Selmer rank at most 2 in *prime* twist families of the elliptic curves $X_0(N)$ for $N = 11$, 19 (in [Cl1]) and $N = 14$ (here) may have a relatively simple explanation – and in particular, may persist for all primes in the given congruence classes – by means of a complete 2-descent. This suggests the possibility – quite surprising when compared to Theorem 1 – that when $X_0(N)$ has genus one there are *no* prime w_N-quadratic twists which violate the Hasse principle.

References

[Bar]　F. Bars, *Bielliptic modular curves*, J. Number Theory 76 (1999), 154-165.

[Cl0]　P.L. Clark, *Rational points on Atkin-Lehner quotients of Shimura curves*, 2003 Harvard thesis.

[Cl1]　P.L. Clark, *Galois groups via Atkin-Lehner twists*, to appear in Proc. AMS.

[Cl2]　P.L. Clark, *On the Hasse principle for Shimura curves*, to appear in Israel J. Math.

[CM]　D. Coray and C. Manoil, *On large Picard groups and the Hasse principle for curves and K3 surfaces*, Acta Arith. 76 (1996), 165-189.

[Ell]　J. Ellenberg, "$\mathbb{Q}$-curves and Galois representations," in *Modular Curves and Abelian Varieties*, J. Cremona, J.-C. Lario, J. Quer, K. Ribet, editors.

[Mal]　G. Malle, *Genus zero translates of three point ramified Galois extensions*, Manuscripta Math. 71 (1991), 97-111.

[Og1]　A. Ogg, *Hyperelliptic modular curves*, Bull. Math. Soc. France 102 (1974), 449-462.

[Og2]　A. Ogg, *Real points on Shimura curves*, Progress in Math. 35, Birkhauser, 1983, 277-307.

[Que]　J. Quer. $\mathbb{Q}$-*curves and abelian varieties of* GL_2-*type*, Proc. London Math. Soc. (3) 81 (2000), 285-317.

[RSY]　V. Rotger, A. Skorobogatov and A. Yafaev, *Failure of the Hasse principle for Atkin-Lehner quotients of Shimura curves over* $\mathbb{Q}$, Moscow Math. J. 5 (2005).

[Ser]　J.-P. Serre, *Topics in Galois Theory*, Research Notes in Mathematics 1, Jones and Bartlett, 1992.

[Shi]　K.-y. Shih, *p-torsion points on certain elliptic curves*, Comp. Math. 36 (1978), 113-129.

[Sko]　A. Skorobogatov, *Torsors and rational points*, Cambridge Tracts in Mathematics 144, 2001.

E-mail address: `pete@math.uga.edu`