ACTA ARITHMETICA
152.4 (2012)

Points on quadratic twists of $X_0(N)$

by

EKIN OZMAN (Austin, TX)

1. Introduction. Let $N = p_1 \cdots p_r$ be a positive, square-free integer. The modular curve $Y_0(N)$ is a moduli space of tuples (E, C), where E is an elliptic curve and C is a cyclic subgroup of order N in $E[N]$. Equivalently, any point of $Y_0(N)$ corresponds to (E, ϕ) where ϕ is a cyclic N-isogeny of E. A projective smooth curve $X_0(N)$ is obtained by adding 2^r cusps to $Y_0(N)$. Note that all the cusps are $\mathbb{Q}$-rational.

The Atkin–Lehner involution w_N of $Y_0(N)$ sends (E, C) to the pair $(E/C, E[N]/C)$. Equivalently, in terms of isogenies, $w_N : (E, \phi) \mapsto (E', \hat{\phi})$ where $\phi : E \to E'$ and $\hat{\phi}$ is the dual isogeny. The action of the rational map w_N extends to $X_0(N)$ and freely permutes the cusps.

A celebrated theorem of Mazur [17] and its extensions by Kenku and Momose give much more information about the rational points of $X_0(N)$.

THEOREM (Mazur, [17]). *For all $N > 163$, $X_0(N)(\mathbb{Q})$ consists of only cusps.*

This result was proved by Mazur for prime levels of N and generalized to square-free integers by Kenku and Momose.

Let d be a square-free integer, $\mathbb{K} := \mathbb{Q}(\sqrt{d})$, σ be the generator of $\mathrm{Gal}(\mathbb{K}/\mathbb{Q})$, and N a square-free integer. The twist $X^d(N)$ of $X_0(N)$ is constructed by Galois descent from $X_0(N)/\mathbb{K}$ (for a general reference to this process see [29, p. 102]). It is a smooth proper curve over $\mathbb{Q}$, isomorphic to $X_0(N)$ over $\mathbb{K}$ but not over $\mathbb{Q}$. The action of σ is 'twisted' on $X^d(N)$, meaning that $\mathbb{Q}$-rational points of $X^d(N)$ are naturally identified with the $\mathbb{K}$-rational points of $X_0(N)$ that are fixed by $\sigma \circ w_N$. We are interested in such points. However, the existence of rational points in this case is not immediate, as it is for $X_0(N)$. Since cusps are interchanged by w_N, they are not rational anymore.

2010 *Mathematics Subject Classification*: Primary 11G20; Secondary 14G05.
Key words and phrases: modular curves, quadratic twists, Brauer–Manin.

DOI: 10.4064/aa152-4-1

Like $X_0(N)$, the twisted curve $X^d(N)$ is a parameter space. A special class of elliptic curves, called *quadratic* $\mathbb{Q}$*-curves of degree* N, correspond to $\mathbb{Q}$-rational points on some $X^d(N)$. A quadratic $\mathbb{Q}$-curve of degree N is an elliptic curve defined over a quadratic number field $\mathbb{K} = \mathbb{Q}(\sqrt{d})$ which is isogenous to its Galois conjugate over $\mathbb{K}$ via an isogeny ϕ such that $\ker(\phi) \cong \mathbb{Z}/N\mathbb{Z}$. Therefore, if $X^d(N)(\mathbb{Q})$ is empty then there are no such quadratic $\mathbb{Q}$-curves of degree N defined over $\mathbb{Q}(\sqrt{d})$. $\mathbb{Q}$-curves appear in many interesting questions, such as those about 'twisted' Fermat equations. More details about these results and in general about $\mathbb{Q}$-curves, as well as related questions can be found in Ellenberg's survey article [7].

In general, there is no known algorithm to follow when trying to show existence or non-existence of a rational point on a variety. One of the first things to check is the existence of local points. If a curve over $\mathbb{Q}$ fails to have a $\mathbb{Q}_p$-point for some p, then there is no rational point on that curve. This gives rise to the main question of the paper, which was originally stated as Problem A by Ellenberg in [7]:

Question (Ellenberg, [7]). *For which d and N does $X^d(N)$ have rational points over every completion of $\mathbb{Q}$?*

In this paper we give an answer to this question under the assumption that no prime is simultaneously ramified in $\mathbb{K}$ and $\mathbb{Q}(\sqrt{-N})$.

Theorem 1.1. *Let p be a prime, N a square-free integer, and $\mathbb{K}$ a quadratic field. Then*

(1) $X^d(N)(\mathbb{Q}_p) \neq \emptyset$ *for all p that split in $\mathbb{K}$ and for* $\mathbb{Q}_\infty = \mathbb{R}$ (Proposition 1.2).
(2) $X^d(N)(\mathbb{Q}_p) \neq \emptyset$ *if p is inert in $\mathbb{K}$ and does not divide N* (Theorem 3.17).
(3) *For all odd p that are inert in $\mathbb{K}$ and divide N, $X^d(N)(\mathbb{Q}_p) \neq \emptyset$ if and only if either*
    (a) $N = p\prod_i q_i$ *where* $p \equiv 3 \bmod 4$ *and* $q_i \equiv 1 \bmod 4$ *for all i and* $\left(\frac{-\prod_i q_i}{p}\right) = -1$, *or*
    (b) $N = 2p\prod_i q_i$ *where* $p \equiv 3 \bmod 4$ *and* $q_i \equiv 1 \bmod 4$ *for all i and* $\left(\frac{-\prod_i q_i}{p}\right) = -1$ (Theorem 3.7).
(4) *If 2 is inert in $\mathbb{K}$ and divides N, $X^d(N)(\mathbb{Q}_p) \neq \emptyset$ if and only if* $N = 2\prod_i q_i$ *where* $q_i \equiv 1$ *modulo* 4 *for all i* (Theorem 3.8).
(5) *For all p that are ramified in $\mathbb{K}$ and unramified in $\mathbb{Q}(\sqrt{-N})$, $X^d(N)(\mathbb{Q}_p) \neq \emptyset$ if and only if p is in the set S_N defined in Proposition* 4.6 (Theorem 4.10).
(6) *For all p that are ramified in $\mathbb{K}$ and $\mathbb{Q}(\sqrt{-N})$, if $X^d(N)(\mathbb{Q}_p) \neq \emptyset$ then $p \in S_N$ (Proposition 4.5).*

The results about real points and $\mathbb{Q}_p$-points for primes p which split in $\mathbb{Q}(\sqrt{d})$ are rather elementary.

PROPOSITION 1.2. $X^d(N)(\mathbb{R}) \neq \emptyset$.

The proof of this fact for prime twists can be found, for instance, in [2], but the proof works in general.

If the prime p splits in $\mathbb{K}$ then a copy of $\mathbb{K}$ is in $\mathbb{Q}_p$. Since $X_0(N)$ and $X^d(N)$ are isomorphic over $\mathbb{K}$ and $X_0(N)(\mathbb{Q}_p)$ is non-empty, $X^d(N)(\mathbb{Q}_p)$ is also non-empty.

Therefore, $X^d(N)$ might fail to have p-adic points only for finite primes that are inert or ramified in $\mathbb{K}$.

Theorem 1.1 gives necessary and sufficient conditions to have $\mathbb{Q}_p$-points of a twist for every p under the assumption that there is no prime simultaneously ramified in $\mathbb{Q}(\sqrt{d})$ and $\mathbb{Q}(\sqrt{-N})$. If such twists fail to have rational points then they give a family of examples of curves that violate the Hasse principle. Combining this with a theorem of Serre and using the technique of Clark [1], we give the asymptotics of the number of twists that violate the Hasse principle. In several cases we show that this obstruction to the Hasse principle is explained by the Brauer–Manin obstruction.

Organization of the paper. In Section 2 we give an overview of the previous results and where our result fits in the general scheme. We prove, under the assumption that no prime is simultaneously ramified in $\mathbb{K}$ and $\mathbb{Q}(\sqrt{-N})$, that the previous results on this problem by Clark, González, Quer, and Shih follow from Theorem 1.1. We also answer a question of Clark raised in [1].

We draw on a number of different techniques to handle the various cases in Theorem 1.1. In Section 3, we handle the case when p is inert in $\mathbb{K}$. For instance, in this section we use Hensel's Lemma when $p \mid N$. On the other hand, in Section 4, we construct a $\mathbb{Q}_p$-point using the theory of CM elliptic curves. We give some examples that illustrate Theorem 1.1 and compare our result with previous results. Then in Section 5, we give the asymptotics of the number of twists which violate the Hasse principle. In Section 6, we give ideas about further directions, give examples of genus 2 curves that violate the Hasse principle, and show that these violations are explained by the Brauer–Manin obstruction.

2. Relation to previous work. In the case of conics there is a rational point if and only if there is a local point for every completion of $\mathbb{Q}$. Moreover if a conic has a rational point then it has many others, since it is isomorphic to $\mathbb{P}^1$. For the case of conics, i.e. when the genus of $X^d(N)$ is zero, we have a complete answer to our question due to the work of Shih [31] and González and Quer [24], based on the earlier work of Hasegawa [12]. The proof is based on a special parametrization of the j-invariants of these curves and some Hilbert symbol computations. Hence, González, Quer and Shih give the following complete list in the case of genus 0.

Theorem 2.1 (González, Quer, Shih, [24], [31]). *Using the notation above:*

- *When $N = 2, 3, 7$, $X^d(N)(\mathbb{Q})$ is infinite for any quadratic field $\mathbb{Q}(\sqrt{d})$.*
- *$X^d(5)(\mathbb{Q})$ is infinite if and only if d is of the form m or $5m$ where m is a square-free integer each of whose prime divisors is a quadratic residue modulo 5.*
- *$X^d(6)(\mathbb{Q})$ is infinite if and only if d is of the form m or $6m$ where m is a square-free integer such that 2 is a quadratic residue modulo each prime divisor of m.*
- *$X^d(10)(\mathbb{Q})$ is infinite if and only if d is of the form m or $10m$ where m is a square-free integer each of whose prime divisors is a quadratic residue modulo 5.*
- *$X^d(13)(\mathbb{Q})$ is infinite if and only if d is of the form m or $13m$ where m is a square-free integer each of whose prime divisors is a quadratic residue modulo 13.*

Note that since $X^d(N)$ and $X_0(N)$ are isomorphic over $\mathbb{K}$ they are geometrically the same; in particular, they have the same genus. Therefore the cases for which we know the answer completely correspond to the values $N = 2, 3, 5, 6, 7, 10$, 13.

For $N = 2, 3, 7$, since the class number of $\mathbb{Z}[\sqrt{-N}]$ is 1, any w_N-fixed point of $X_0(N)$ is defined over $\mathbb{Q}$, hence gives a point in $X^d(N)(\mathbb{Q})$ for any d. This is another way of stating the first part of Theorem 2.1. Now we derive the other parts of Theorem 2.1 using Theorem 1.1 for relatively prime N and d.

Corollary 2.2. *Let N and d be square-free integers such that there is no prime p that is simultaneously ramified in $\mathbb{Q}(\sqrt{-N})$ and $\mathbb{Q}(\sqrt{d})$. Then Theorem 2.1 can be derived from Theorem 1.1.*

Proof. Since we are dealing with the conics, having a $\mathbb{Q}$-rational point is equivalent to having $\mathbb{Q}_p$-points for every prime p. By Proposition 1.2, $X^d(N)(\mathbb{R}) \neq \emptyset$ for any N and d, hence we only need to check the finite primes. Let $d = \pm \prod_i p_i$ be the prime decomposition of d.

- $N = 5$: By Theorem 1.1(5), $X^d(5)(\mathbb{Q}_{p_i}) \neq \emptyset$ if and only if there is a prime of $\mathbb{Q}(j(\sqrt{-5}))$ lying over p_i with inertia degree 1. Note that the class number of $\mathbb{Z}[\sqrt{-5}]$ is 2 and it is the maximal order of $\mathbb{M} := \mathbb{Q}(\sqrt{-5})$. The Hilbert class field of $\mathbb{M}$ is $\mathbb{Q}(\sqrt{5}, i)$, hence $\mathbb{Q}(j(\sqrt{-5}))$ is $\mathbb{Q}(\sqrt{5})$, since $j(\sqrt{-5})$ is real. Therefore $X^d(5)(\mathbb{Q}_{p_i}) \neq \emptyset$ if and only if $\left(\frac{5}{p_i}\right) = \left(\frac{p_i}{5}\right) = 1$.

For all other primes q, $X^d(5)(\mathbb{Q}_q) \neq \emptyset$ by Theorem 1.1(1)&(2).
Hence, $X^d(5)(\mathbb{Q}) \neq \emptyset$ if and only if each prime divisor p_i of d is a quadratic residue modulo 5.
The case $N = 13$ is quite similar to $N = 5$, since the corresponding Hilbert class field is $\mathbb{Q}(\sqrt{13}, i)$, and they are both 1 mod 4.

- $N=6$: The Hilbert class field of $\mathbb{Q}(\sqrt{-6})$ is $\mathbb{Q}(\sqrt{-3}, \sqrt{2})$, and $\mathbb{Q}(j(\sqrt{-6}))$ is $\mathbb{Q}(\sqrt{2})$. Therefore by Theorem 1.1(5), $X^d(6)$ has $\mathbb{Q}_{p_i}$-rational points if and only if $(\frac{2}{p_i}) = 1$.
  If 3 is inert in $\mathbb{K}$ or splits in $\mathbb{K}$ then $X^d(6)(\mathbb{Q}_3) \neq \emptyset$ by Theorem 1.1(1)&(3).
  If 2 splits in $\mathbb{K}$ then $X^d(6)(\mathbb{Q}_2) \neq \emptyset$ by Theorem 1.1(1).
  Furthermore, 2 cannot be inert in $\mathbb{K}$, since $(\frac{2}{p_i}) = 1$ for all p_i.
  For all other primes q, $X^d(6)(\mathbb{Q}_q) \neq \emptyset$ by Theorem 1.1(1)&(2).
  The case $N = 10$ is quite similar to the previous cases. ■

Another result along these lines, which is a necessary condition for the existence of degree-N $\mathbb{Q}$-curves, was given in [24]:

THEOREM 2.3 (Quer, González, [24, Theorem 6.2]). *Assume that there exists a quadratic $\mathbb{Q}$-curve of degree N defined over some quadratic field K. Then every divisor $N_1 \mid N$ such that*

$$N_1 \equiv 1 \bmod 4 \quad \textit{or} \quad N_1 \textit{ is even and } N/N_1 \equiv 3 \bmod 4$$

is a norm of the field K.

The proof of this theorem is analytic, by constructing some functions on $X_0(N)$ with rational Fourier coefficients and studying the action of the involution w_N on them. We will take a more algebraic approach and given any square-free, relatively prime integers d and N show that Theorem 1.1 implies Theorem 2.3 in the following two corollaries.

Recall that saying that 'N_1 is a norm in $\mathbb{K}$' is equivalent to saying that $(N_1, d) = 1$, where $(-,-)$ denotes the Hilbert symbol. Moreover $(N_1, d) = 1$ if and only if the local Hilbert symbols $(N_1, d)_p$ are 1 for all primes p. Therefore, Theorem 2.3 gives a condition on the existence of local points.

The local Hilbert symbol is given by explicit formulas which can be found in [28].

These formulas imply that if $(N_1, d)_p = -1$ for some prime p then p divides N_1 or d. Since $\prod_p (a, b)_p = 1$, one can deduce that $(N_1, d)_p = -1$ for some odd prime p that divides N_1 or d.

COROLLARY 2.4. *Let N be an odd square-free integer such that there exists a divisor N_1 of N with $N_1 \equiv 1 \bmod 4$ and $(N_1, d)_p = -1$ for some p. Then $X^d(N)(\mathbb{Q}_p) = \emptyset$.*

Proof. Suppose $p \mid N_1$. Since $(N_1, d)_p = \left(\frac{d}{p}\right) = -1$, p is inert in $\mathbb{K}$. Since $N_1 \equiv 1 \bmod 4$, either $p \equiv 1 \bmod 4$ or $p \equiv 3 \bmod 4$ and there is another divisor p' of N_1 that is also congruent to 3 mod 4. If $p \equiv 1 \bmod 4$, then $X^d(N)(\mathbb{Q}_p) = \emptyset$, and if $p \equiv 3 \bmod 4$, then there are at least two primes dividing N_1 that are congruent to 3 mod 4, hence $X^d(N)(\mathbb{Q}_p) = \emptyset$, by Theorem 1.1(3).

Suppose $p \mid d$. Since $(N_1, d)_p = \left(\frac{N_1}{p}\right) = -1$, p is inert in $\mathbb{Q}(\sqrt{N_1})$. Let H denote the ring class field of the order $\mathbb{Z}[\sqrt{-N}]$. Then $H = \mathbb{Q}(\sqrt{-N}, j(\sqrt{-N}))$ and $H \cap \mathbb{R} = \mathbb{Q}(j(\sqrt{-N}))$ by class field theory. Since $N_1 \equiv 1 \bmod 4$, $\mathbb{Q}(\sqrt{N_1})$ lies in the genus field of $\mathbb{Q}(\sqrt{-N})$, hence $\mathbb{Q}(\sqrt{N_1}) \subset \mathbb{Q}(j(\sqrt{-N}))$. This shows that there is no prime of $\mathbb{Q}(j(\sqrt{-N}))$ lying above p with residue degree 1, thus $X^d(N)(\mathbb{Q}_p) = \emptyset$ by Theorem 1.1(5). ∎

COROLLARY 2.5. *Let N be an even square-free integer such that there exists an even divisor N_1 of N with $N/N_1 \equiv 1 \bmod 4$ and $(N_1, d)_p = -1$ for some p. Then $X^d(N)(\mathbb{Q}_p) = \emptyset$.*

Proof. Suppose $p \mid N_1$. Since $(N_1, d)_p = \left(\frac{d}{p}\right) = -1$, p is inert in $\mathbb{K}$, and since $\prod_\nu (a, b)_\nu = 1$, we can assume that p is odd. By Theorem 1.1(3), $X^d(N)(\mathbb{Q}_p) \neq \emptyset$ if and only if $N = 2p \prod_i q_i$ with $p \equiv 3 \bmod 4$ and all $q_i \equiv 1 \bmod 4$. Therefore $N_1 = 2p \prod_i q_i$ for some of the q_i's congruent to 1 mod 4, which contradicts the assumption that $N/N_1 \equiv 3 \bmod 4$, hence $X^d(N)(\mathbb{Q}_p) = \emptyset$.

The case where $p \mid d$ is similar to the corresponding case of Corollary 2.4. ∎

Corollaries 2.4 and 2.5 imply Theorem 2.3.

Another result about the existence of local points on $X^d(N)$ is given by Clark in [1]. Generalizing the techniques used in Clark's proof, we prove Theorem 1.1(3). As a result, the following theorem follows from Theorem 1.1(3).

THEOREM 2.6 (Clark, [2]). *Let N be a prime number congruent to 1 mod 4, and $p^* = (-1)^{(p-1)/2}p$ where p is a prime different from N and such that $\left(\frac{N}{p}\right) = -1$. Then $X^{p^*}(N)(\mathbb{Q}_N) = \emptyset$.*

In [1], it was asked whether or not p and N were the only primes for which $X^{p^*}(N)$ fails to have local points. We prove that the answer is 'yes' in Corollary 5.5.

3. Primes that are inert in $\mathbb{K}$.

We will keep the same notation as in the previous section. Given a square-free integer N, a quadratic number field $\mathbb{K} := \mathbb{Q}(\sqrt{d})$, and a prime p, we will study the set $X^d(N)(\mathbb{Q}_p)$, where $X^d(N)$ is the twist of $X_0(N)$ with w_N and $\langle\sigma\rangle := \mathrm{Gal}(\mathbb{Q}(\sqrt{d})/\mathbb{Q})$. Since we are dealing with local points, by abuse of notation we regard σ as the generator of the extension $\mathbb{K}_\nu$ over $\mathbb{Q}_p$, where ν is a prime of $\mathbb{K}$ lying over p. Let k be the residue field and R be the valuation ring of $\mathbb{K}_\nu$.

For the two main cases that we are dealing with—the inert case and the ramified case—we will be using different tools. For the inert case, since we have the notion of Galois descent for $X_0(N)_{/R}$, existence or non-existence of local points will be shown by checking the existence of points over the corresponding special fiber. For this, the following version of Hensel's Lemma will be used:

Lemma 3.1 (Lemma 1.1 in [13]). *Let K be a complete local ring, R its valuation ring, and k its residue field. Let X be a regular scheme over $S :=$ Spec(R) and $f : X \to S$ a proper flat morphism. Say $X_\eta := X \times_S$ Spec(K) is the generic fiber and $X_0 := X \times_S$ Spec(k) is the special fiber. Then the generic fiber has a K-rational point if and only if the special fiber has a* smooth *k-rational point.*

We will also use the following theorems of Deuring:

Theorem 3.2 (Deuring, [5]). *Let p be a rational prime, $\tilde{E}$ an elliptic curve that has CM by $\mathbb{Q}(\sqrt{-N})$ defined over a number field L, and β a prime of L lying over p such that $\tilde{E}$ has good reduction over β. Then E is supersingular if and only if p is ramified or inert in $\mathbb{Q}(\sqrt{-N})$.*

Theorem 3.3 (Deuring's Lifting Theorem, [5]). *Let E be an elliptic curve over a finite field k of characteristic p, and let α be an element of* End(E). *Then there exists an elliptic curve $\tilde{E}$ over a number field B, an endomorphism $\tilde{\alpha} \in$ End$(\tilde{E})$, and a place β of B lying over p such that the reductions of $\tilde{E}$ and $\tilde{\alpha}$ modulo β are E and α respectively. Moreover, $|k| = p^f$ where f is the inertia degree of β over p.*

Recall that σ is the generator of Gal$(\mathbb{Q}(\sqrt{d})/\mathbb{Q})$. When p is inert in $\mathbb{Q}(\sqrt{d})$, it induces the non-trivial map (Frobenius) on Gal$(k/\mathbb{F}_p)$, where $k = \mathbb{F}_{p^2}$. We have different cases according to whether $p \mid N$ or not.

3.1. p dividing the level. Say $p \mid N$, ν is the prime of $\mathbb{K}$ lying over p, and R is the ring of integers of the localization $\mathbb{K}_\nu$.

In Mazur [17] and Deligne–Rapaport [4] there is a model of $\mathcal{X}_0(N)_{/\mathbb{Z}_p}$ whose special fiber $X_0(N)_{/\mathbb{F}_p}$ is two copies of $X_0(N/p)_{/\mathbb{F}_p}$ glued along supersingular points twisted by the first power Frobenius. The Atkin–Lehner involution w_N interchanges the two branches and Frobenius stabilizes each branch (see Figure 1). A regular model $\tilde{\mathcal{X}}_0(N)$ can be obtained by blowing up $|\mathrm{Aut}(E,C)|/2 - 1$ times at each supersingular point. The actions of Frobenius and of w_N extend to regularization as well.

Since p is ramified in $\mathbb{Q}(\sqrt{-N})$, by Theorem 3.2, any w_N-fixed point is supersingular. Say x is a w_N-fixed supersingular (hence singular) point of $X_0(N)_{/\mathbb{F}_p}$. To have a regular model, we need to blow up at each supersingular

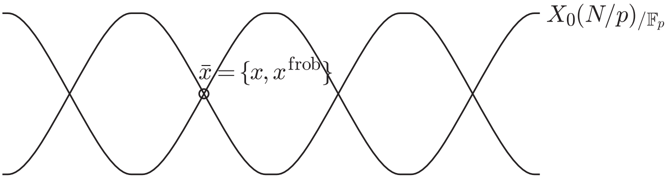

$X_0(N/p)_{/\mathbb{F}_p}$
$\bar{x} = \{x, x^{\mathrm{frob}}\}$

Fig. 1. Special fiber of $\mathcal{X}_0(N)_{/\mathbb{Z}_p}$

point $|\mathrm{Aut}(E,C)|/2-1$ times where (E,C) is on $X_0(N/p)_{/\mathbb{F}_p}$. To keep track of the different schemes, we need to introduce some notation. As introduced at the beginning, $\mathcal{X}_0(N)$ denotes the model of $X_0(N)$ over $\mathbb{Z}_p$ (not necessarily regular). Let $\tilde{\mathcal{X}}_0(N)$ denote the regularization of $\mathcal{X}_0(N)$ after blow-ups, and $\tilde{X}_0(N)_{/\mathbb{F}_p}$ be its special fiber.

We can define a model of $X^d(N)$ over $\mathbb{Z}_p$ as a descent to $\mathrm{Spec}(\mathbb{Z}_p)$ of $\mathcal{X}_0(N) \times_{\mathrm{Spec}(\mathbb{Z}_p)} \mathrm{Spec}(R)$ by a descent datum twisted by w_N. Note that the extension $R/\mathbb{Z}_p$ is Galois since p is inert in $\mathbb{K}$. This model will be denoted by $\mathcal{X}^d(N)_{/\mathbb{Z}_p}$. Our aim is to use Hensel's Lemma (Lemma 3.1) to make conclusions about $\mathbb{Q}_p$-rational points of the generic fiber of $\mathcal{X}^d(N)_{/\mathbb{Z}_p}$. In order to do this, we must first show that $\mathcal{X}^d(N)_{/\mathbb{Z}_p}$ is regular. This is because the minimal regular model commutes with etale base change. The next result recalls this fact.

Proposition 3.4 (Lemma 3.33 of [15]). *Let O_K be a discrete valuation ring with residue field k, and let O_L be a discrete valuation ring that dominates O_K, with field of fractions L algebraic over K. Suppose moreover that L is separable over K, the extension O_L/O_K is unramified, and its residue field is separable algebraic over k. Let C be a smooth projective curve over O_K. Then the formation of the minimal regular model and of the canonical model of C over O_K (if they exist) commutes with the base change* $\mathrm{Spec}(O_L) \to \mathrm{Spec}(O_K)$.

Now we will give a necessary condition for the existence of a smooth point on $X^d(N)(\mathbb{F}_p)$.

Proposition 3.5. *There exists a smooth point on $X^d(N)(\mathbb{F}_p)$ if and only if there is a $w_{N/p}$-fixed supersingular point on $X_0(N/p)(\mathbb{F}_{p^2})$ with an automorphism of order* 4.

Proof. As explained above, $X^d(N)$ is a generic fiber of $\mathcal{X}^d(N)_{/\mathbb{Z}_p}$ which is the Galois descent of $\mathcal{X}_0(N)_{/\mathbb{Z}_p}$ by $R/\mathbb{Z}_p$. Since w_N interchanges the branches of $X_0(N)_{/\mathbb{F}_p}$, $\mathbb{F}_p$-rational points on the special fiber $X^d(N)_{/\mathbb{F}_p}$ come from supersingular points of $X_0(N)_{/\mathbb{F}_p}$, which are all singular. In fact $X^d(N)_{/\mathbb{F}_p}$ consists of supersingular points of $X_0(N)_{/\mathbb{F}_p}$ fixed by $w_N \circ \sigma$. Since σ acts as w_p on supersingular points (see Chapter V, Section 1 of [4] or Proposition

3.8 in [25]), $w_N \circ \sigma$ acts as $w_{N/p}$ on supersingular points. Recall that at each singular (hence supersingular) point we have $|\mathrm{Aut}(E,C)|/2-1$ exceptional lines. The automorphism group of an elliptic curve over a field of characteristic ℓ is μ_2, μ_4 or μ_6 if ℓ is not 2 or 3, where μ_s denotes the group of primitive sth roots of unity. If $\ell = 2$ or 3 and E is the unique supersingular elliptic curve in characteristic ℓ then $\mathrm{Aut}(E)$ is $C_3 \rtimes \{\pm1, \pm i, \pm j, \pm k\}$ or $C_3 \rtimes C_4$ respectively, where C_m denotes the cyclic group of order m.

Therefore if $|\mathrm{Aut}(P)| = 4n$ for $n > 1$, there is an element of order 4 in $\mathrm{Aut}(P)$ and the number of blow-ups is $2n-1$, which is odd. Since we have an odd number of exceptional lines, there is one line $L_{/\mathbb{F}_p}$ that is fixed by the action of w_N (see the second column of Figure 2). On this line L the points A and B are singular and fixed by $w_N \circ \sigma$, but these are not the only fixed points. The action of $\sigma \circ w_N$ on the zeroth, first, and second cohomology of L has traces $1, 0$, and p respectively. Then by the Lefschetz fixed point theorem (Theorem 25.1 in [20]), there is a smooth $w_N \circ \sigma$-fixed point on this exceptional line L. Therefore if we have a supersingular point with an automorphism of order 4, then there is a smooth point on $X^d(N)(\mathbb{F}_p)$.

For the reverse direction, say there is no such supersingular point P with an automorphism of order 4. If $|\mathrm{Aut}(P)|$ is 2, then $\mathcal{X}_0(N)$ is already regular but all $\mathbb{F}_p$-rational points of $X^d(N)$ are singular.

If $|\mathrm{Aut}(P)| = 6$, then we replace this point by two exceptional lines over $\mathbb{F}_p$ and $\sigma \circ w_N$ interchanges these lines. Each of these exceptional lines cuts one of the branches and also the other exceptional line once. Denote the intersection point of these lines by x; then $\sigma(x) = x$ and it is the only point fixed by the action of σ on these lines. Furthermore, $w_N(x) = w_N(\sigma(x)) = \sigma(w_N(x))$, hence $w_N(x)$ is also fixed by σ, i.e. $w_N(x) = x = \sigma(x)$. Thus x induces an $\mathbb{F}_p$-rational point of $X^d(N)$. However, x is a singular point. For a picture of this situation we refer to the table at the end of this section. ■

Using Proposition 3.5 and Hensel's Lemma we get the following:

Corollary 3.6. *There exists a point on $X^d(N)(\mathbb{Q}_p)$ if and only if there is a $w_{N/p}$-fixed supersingular point with an automorphism of order* 4.

Theorem 3.7. *Let N be a square-free positive integer and p be an odd prime. If p is inert in $\mathbb{K}$ and divides N, then $X^d(N)(\mathbb{Q}_p) \neq \emptyset$ if and only if $p \equiv 3 \bmod 4$ and N is of the form either*

(1) $p\prod_i q_i$ *with all* $q_i \equiv 1 \bmod 4$ *and* $\left(\frac{-\prod_i q_i}{p}\right) = -1$, *or*

(2) $2p\prod_i q_i$ *with all* $q_i \equiv 1 \bmod 4$ *and* $\left(\frac{-\prod_i q_i}{p}\right) = -1$.

Proof. By Corollary 3.6, a local point exists if and only if there is a $w_{N/p}$-fixed supersingular point (E, C) on $X_0(N)_{/\mathbb{F}_p}$ with automorphism group divisible by 4.

Say N/p is different than 2. Then x is fixed by $w_{N/p}$ if and only if $\mathbb{Z}[\sqrt{-N/p}]$ embeds into the endomorphism ring of x. Note that $\operatorname{End}(x)$ is an Eichler order of level N/p in the quaternion algebra ramified at p. By Proposition 3.12 (Optimal Embedding Theorem), $\mathbb{Z}[\sqrt{-N/p}]$ embeds in $\operatorname{End}(x)$ if and only if $\big(\frac{-\prod_i q_i}{p}\big) = -1$. If N/p is 2 then since the elliptic curve over $\mathbb{Q}$ with CM by $\mathbb{Q}(i)$ is w_2-fixed and its reduction mod p is supersingular for every $p \equiv 3 \bmod 4$, we need no further conditions.

We also want the automorphism group of x to be divisible by 4. In particular we want $j = 1728$ to be a supersingular j-invariant in characteristic p. By Deuring's criterion this is equivalent to saying that $p \equiv 3 \bmod 4$ since p is assumed to be odd.

In order to have such a point, $\mathbb{Z}/4\mathbb{Z}$ must inject into $(\mathbb{Z}/q_i\mathbb{Z})^*$ for every odd prime divisor q_i of N that is not p. Therefore if N is odd, $N = p\prod_i q_i$ with $p \equiv 3 \bmod 4$ and all $q_i \equiv 1 \bmod 4$.

Since the automorphism $[i]$, which has order 4, sends a 2-torsion point $(x, 0)$ of $E_{1728} : y^2 = x^3 + x$ to $(-x, 0)$, $[i]$ fixes the cyclic-2 subgroup $\langle(0, 0)\rangle$ of $E_{1728}[2]$. Hence, if N is even and there is a supersingular point on $X_0(N)_{/\mathbb{F}_p}$ with automorphism group divisible by 4, then $N = 2p\prod_i q_i$ with $p \equiv 3 \bmod 4$ and all $q_i \equiv 1 \bmod 4$.

Conversely, if N is of the form (1) or (2) then there is a $w_{N/p}$-fixed supersingular point and 1728 is a supersingular j-invariant. Let E_{1728} be the elliptic curve over $\mathbb{F}_p$ having j-invariant 1728. Then $[i]$ is in $\operatorname{Aut}(E_{1728})$ and acts on $E_{1728}[\prod_i q_i]$. The automorphism $[i]$ stabilizes a cyclic-$\prod_i q_i$ subgroup if and only if $[i]$ stabilizes cyclic-q_i subgroups of $E_{1728}[q_i] = \mathbb{Z}/q_i\mathbb{Z} \times \mathbb{Z}/q_i\mathbb{Z}$ for all i. The automorphism $[i]$ can be seen as an element of $\mathrm{GL}_2(\mathbb{F}_{q_i})$ and it stabilizes a cyclic subgroup of order q_i if and only if $[i]$ has eigenvalues defined over $\mathbb{F}_p$. If q_i is odd then the minimal polynomial of $[i]$ is $x^2 + 1$, which is equivalent to saying that $q_i \equiv 1 \bmod 4$ for all i. If $q_i = 2$ then the minimal polynomial of $[i]$ is $x + 1$ and $[i]$ fixes the cyclic-2 subgroup $\langle(0, 0)\rangle$ of $E_{1728}[2]$. ∎

For $p = 2$ inert in $\mathbb{K}$ and N even, we get the following result:

THEOREM 3.8. *If* 2 *is inert in* $\mathbb{K}$ *and divides* N *then* $X^d(N)(\mathbb{Q}_2) \neq \emptyset$ *if and only if* $N = 2\prod_i q_i$ *with all* $q_i \equiv 1 \bmod 4$.

Proof. Over $\mathbb{F}_2$, 1728 is the only supersingular j-invariant and $|\operatorname{Aut}(E_{1728})| = 24$. Say q_i is a prime dividing $N/2$. Since N is square-free, q_i is odd.

By Corollary 3.6, a $\mathbb{Q}_2$-point exists if and only if there is a $w_{N/2}$-fixed supersingular point (E_{1728}, C) on $X_0(N)_{/\mathbb{F}_2}$ with automorphism group divisible by 4. In order to have a point with automorphism group divisible by 4, $\mathbb{Z}/4\mathbb{Z}$ must inject into $(\mathbb{Z}/q_i\mathbb{Z})^*$ for every odd prime divisor q_i of $N/2$, hence $N = 2\prod_i q_i$ with $q_i \equiv 1 \bmod 4$ for all i. This automatically implies that this point is $w_{N/2}$-fixed by Proposition 3.12 below.

For the converse, the argument is the same as in the corresponding part of Theorem 3.7. ■

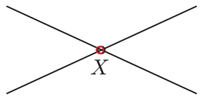
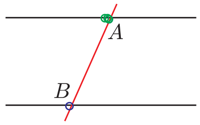
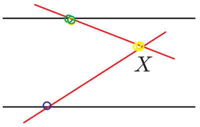
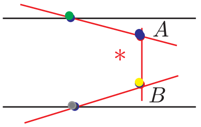
Over $\mathbb{Q}_p$ or $\mathbb{K}_\nu$ such that $\mathbb{K}_\nu/\mathbb{Q}_p$ is unramified		$\lvert\mathrm{Aut}(x)\rvert = h$ Singularity type is A_{k-1} where $k = h/2$	
 no smooth point	 There exists a point	 no smooth point	 There exists a point
$h = 2,\ A_0$	$h = 4,\ A_1$	$h = 6,\ A_2$	$(p = 2)\ h = 8,\ A_3$

Fig 2. Blow-ups

3.2. p **does not divide** N**.** In this section we will construct a point on the special fiber $X^d(N)(\mathbb{F}_p)$ and then by Hensel's Lemma we will be done. In order to construct such a point, our strategy is to prove that there is a supersingular point fixed by $w_N \circ \mathrm{frob}$, or equivalently, by $w_N \circ w_p = w_{Np}$. This is a known result of quaternion arithmetic (see [35, p. 152]. We will recall the necessary definitions and write the details of the proof in a slightly different way.

We will be using the notation introduced in the previous subsection, in particular $\mathcal{X}^d(N)_{/\mathbb{Z}_p}$ denotes the Galois descent $\mathcal{X}_0(N)$ from R to $\mathbb{Z}_p$. If p does not divide N then the following models are smooth, in particular regular:

- $\mathcal{X}_0(N)_{/\mathbb{Z}_p}$,
- $\mathcal{X}_0(N) \times_{\mathbb{Z}_p} R$ (since $R/\mathbb{Z}_p$ is unramified),
- $\mathcal{X}'^d(N)_{/R} := \mathcal{X}^d(N) \times_{\mathbb{Z}_p} R$ (as $\mathcal{X}'^d(N)_{/R}$ is isomorphic to $\mathcal{X}_0(N) \times_{\mathbb{Z}_p} R$).

By Proposition 3.4, $\mathcal{X}^d(N)_{/\mathbb{Z}_p}$ is also regular.

Let Σ_N be the set of tuples (E, C) such that E is a supersingular elliptic curve in characteristic p and C is cyclic group of order N. We start by studying the action of the involution $w_N \circ \sigma$ on Σ_N.

Definition 3.9. Let B be the unique quaternion algebra over $\mathbb{Q}$ that is ramified only at p and at infinity. An Eichler order O of B is of *level* N if

- $q \neq p$, $O_q = O \otimes_{\mathbb{Z}} \mathbb{Z}_q \cong \left(\begin{smallmatrix} \mathbb{Z}_q & \mathbb{Z}_q \\ N\mathbb{Z}_q & \mathbb{Z}_q \end{smallmatrix}\right)$,
- $O_p \cong \left\{\left(\begin{smallmatrix} \alpha & \beta \\ p\bar{\beta} & \bar{\alpha} \end{smallmatrix}\right) \;\middle|\; \alpha, \beta \in R\right\}$ where R is the ring of integers of the unique unramified quadratic extension of $\mathbb{Q}_p$.

Proposition 3.10. *Let $B := \mathrm{End}(E) \otimes_{\mathbb{Z}} \mathbb{Q}$, E a supersingular elliptic curve over $\mathbb{F}_{p^2}$, and C a cyclic subgroup of E of order N. Then B is the unique quaternion algebra over $\mathbb{Q}$ which is ramified only at p and ∞,* $\mathrm{End}(E)$ *is a maximal order in B, and* $\mathrm{End}(E,C)$ *is an Eichler order of level N.*

Proof. For B being the claimed quaternion algebra and $\mathrm{End}(E)$ its maximal order we refer to Silverman [32, Chapter 5] for the rest of the claim see for instance [25]. ■

Now we will focus on the orders lying inside certain Eichler orders. This will give us information about the elements in $\mathrm{End}(E,C)$.

Definition 3.11. Let L be an imaginary quadratic number field, O an order of L, and $\alpha : L \hookrightarrow B$ an algebra embedding such that $\alpha(L) \cap R = \alpha(O)$ where R is an Eichler order of level N in B as above. Then the pair (R,α) is called an *optimal embedding of O*.

The following theorem of Eichler states conditions for existence of an optimal embedding (see [35]):

Proposition 3.12. *Given R, B as above, and $L = \mathbb{Q}(\sqrt{M})$, an optimal embedding (R,α) of an order O of L exists if and only if*

- *$M < 0$, p is inert or ramified in L, and p is relatively prime to the conductor of O, and*
- *q splits or ramifies in O for every q dividing N.*

For any $q \mid N$ and $q' := N/q$, let w_q be the Atkin–Lehner operator that sends $(E,C) \mapsto (E/q'C, E[q] + C/q'C)$ where $E[q]$ is the kernel of multiplication by q. Each w_i is an involution and $w_i \circ w_j = w_j \circ w_i = w_{ij}$ for every coprime i,j. We have another operator, *Frobenius*, acting on the set Σ_N; remember that σ is acting as Frobenius in the inert case. The following result shows that Frobenius can also be seen as an Atkin–Lehner operator on Σ_N.

Theorem 3.13 (see Chapter V, Section 1 of [4] or Proposition 3.8 in [25]). *The involution w_p permutes the two components of $X_0(Np)_{/\mathbb{F}_p}$. It acts on the set of singular points of $X_0(Np)_{/\mathbb{F}_p}$ as the Frobenius morphism $x \mapsto x^p$.*

Let ψ be a map from $X_0(N)_{/\mathbb{F}_p}$ to $X_0(Np)_{/\mathbb{F}_p}$, an isomorphism onto one of the two components. The map ψ takes the supersingular locus of $X_0(N)_{/\mathbb{F}_p}$ to the supersingular locus of $X_0(Np)_{/\mathbb{F}_p}$. The set Σ_N defined at the beginning of the section is the supersingular locus of $X_0(N)_{/\mathbb{F}_p}$. The Atkin–Lehner operator w_{Np} acts on $X_0(Np)$, in particular acts on $\psi(\Sigma_N)$. When we speak of the action of w_{Np} on Σ_N, we actually mean the action of w_{Np} on $\psi(\Sigma_N)$.

In the following two corollaries we show that the Atkin–Lehner involution w_{Np} has a fixed point. This result can be seen as a classical fact of quaternion arithmetic, but we will state it in a slightly different way.

Corollary 3.14. *Given B there is an embedding of $\mathbb{Z}[\sqrt{-pN}]$ into some Eichler order R of level N.*

Proof. By Proposition 3.12 there is an optimal embedding (R,α) of order $\mathbb{Z}[\sqrt{-pN}]$ for an Eichler order R of level N. ■

Corollary 3.15. *If there is an embedding α of $\mathbb{Z}[\sqrt{-pN}]$ into R for some Eichler order $R = \mathrm{End}(E,C)$ of level N then there is a fixed point of w_{Np} in Σ_N.*

Proof. By assumption there exists an element whose square is $-pN$ in R, i.e. an endomorphism of degree Np of (E,C), in particular an endomorphism of degree Np, say f, of E. Using Deuring's Lifting Theorem (Theorem 3.3), this endomorphism and E can be lifted to characteristic 0, i.e. $(\tilde{E}, \ker(\tilde{f}))$ (E and f lifted to characteristic 0) is in $X_0(Np)(\bar{\mathbb{Q}})$ and is fixed by w_{Np}. The reduction of this point modulo p is a supersingular point on $X_0(Np)_{/\mathbb{F}_p}$ that is fixed by w_{Np}. Since E has no p-torsion, we have $|\ker(f)| = N$, and $(E,\ker(f))$ is identified with a point in Σ_N, i.e. is in $\psi(\Sigma_N)$. ■

Example 3.16. Let $p = 7$ and $N = 5$. Since $\left(\frac{-5}{7}\right) = 1$, by Theorem 3.2 reduction of any elliptic curve which has CM by $\mathbb{Q}(\sqrt{-5})$ over p is ordinary. Hence, there is no w_5-fixed point in Σ_5, i.e. there is no optimal embedding of $\mathbb{Z}[\sqrt{-5}]$ into any R where R is an Eichler order of level 5 in the quaternion algebra $\mathbb{Q}_{7,\infty}$. In fact, there is no embedding of $\mathbb{Q}(\sqrt{-5})$ into $\mathbb{Q}_{7,\infty}$ since 7 splits in $\mathbb{Q}(\sqrt{-5})$ and the localization of $\mathbb{Q}(\sqrt{-5})$ at the primes lying above 7 is not even a field.

Theorem 3.17. *If p is inert in $\mathbb{Q}(\sqrt{d})$ and $p \nmid N$ then $X^d(N)(\mathbb{Q}_p) \neq \emptyset$.*

Proof. By Corollaries 3.14 and 3.15, there is a point $x \in \Sigma_N$ such that $w_{Np}(x) = x$. Since $(p,N) = 1$ we have $w_N \circ w_p(x) = w_{Np}(x) = x$. By Theorem 3.13, w_p acts as frob_p on Σ_N, hence $w_N \circ \mathrm{frob}_p(x) = x$. By the theory of Galois descent this gives a point in $X^d(N)(\mathbb{F}_p)$ and since $p \nmid N$, we have a smooth model, and by Hensel's Lemma (Lemma 3.1) we are done. ■

4. Primes ramified in $\mathbb{K}$ and unramified in $\mathbb{Q}(\sqrt{-N})$.

Let p be a prime that is ramified in the quadratic field $\mathbb{K}$ but not in $\mathbb{Q}(\sqrt{-N})$. Let ν be the prime of $\mathbb{K}$ lying over p, and R be the ring of integers of $\mathbb{K}_\nu$. Note that we do not have a good model for $X^d(N)$ over R, since $R/\mathbb{Z}_p$ is not Galois. By assumption, $p \nmid N$. Then by a well-known theorem of Igusa (see for instance [6, Section 8.6]), $\mathcal{X}_0(N)$ is a smooth $\mathbb{Z}[1/N]$-scheme, hence for any $p \nmid N$ the special fiber of $\mathcal{X}_0(N) \to \mathrm{Spec}(R)$ is *smooth* over the residue field R/ν.

Since p is ramified, the residue field R/ν is $\mathbb{F}_p$, and the induced action of σ on the residue field is trivial. In this setting, our approach will be to produce points on $X_0(N)(\mathbb{Q}_p)$ which are fixed by w_N and which are thus CM points. Note that such points are $\mathbb{Q}_p$-rational points of $X^d(N)$. The main tool is Deuring's Lifting Theorem (Theorem 3.3). It allows us to lift w_N-fixed points of $X_0(N)(\mathbb{F}_p)$ to w_N-fixed points of $X_0(N)(\mathbb{Q}_p)$, as Proposition 4.3 below demonstrates. Before stating the proposition we need to recall the following facts about CM elliptic curves.

If E corresponds to a fixed point of w_N on $X_0(N)(\bar{\mathbb{Q}})$ and $N > 2$ then E has an endomorphism whose square is $[-N]$, as stated in [22]. Hence, $\mathrm{End}(E)$ contains a copy of $\mathbb{Z}[\sqrt{-N}]$ and can be embedded in $\mathbb{Z}[(D + \sqrt{D})/2]$ where D is the discriminant of the CM field $\mathbb{M} := \mathbb{Q}(\sqrt{-N})$. If $N \equiv 1$ or $2 \bmod 4$ then these two orders are the same, hence $\mathrm{End}(E)$ is the maximal order of $\mathbb{M}$. Otherwise, $\mathrm{End}(E)$ is an order of conductor 2 in the maximal order.

Let O be $\mathbb{Z}[\sqrt{-N}]$, h the class number of O, E an elliptic curve such that $\mathrm{End}(E)$ contains $\mathbb{Z}[\sqrt{-N}]$, and $\mathbb{H}$ the ring class field of O. Recall that by the theory of CM, we have h elliptic curves which have CM by O, and their j-invariants are all conjugate.

PROPOSITION 4.1. *Let E be an elliptic curve over a number field $\mathbb{B}$ and suppose E has an endomorphism α_0 whose square is $[-N]$. Then $(E, \ker(\alpha_0))$ is a w_N-fixed point on $X_0(N)(\mathbb{B})$.*

Proof. By definition $(E, \ker(\alpha_0))$ is a w_N-fixed point of $X_0(N)(\bar{\mathbb{Q}})$ and E is defined over $\mathbb{B}$, while α_0 is defined over $\mathbb{B}(\sqrt{-N})$. Let ϕ be the generator of $\mathrm{Gal}(\mathbb{B}(\sqrt{-N})/\mathbb{B})$. Then $\ker(\alpha_0)^\phi = \ker(\pm\alpha_0) = \ker(\alpha_0)$ since the only endomorphisms of E whose square is $[-N]$ are $\pm\alpha_0$. Therefore $\ker(\alpha_0)$ is defined over $\mathbb{B}$ as well. ∎

REMARK 4.2. If $N = 2$ then a w_2-fixed point $X_0(N)(\bar{\mathbb{Q}})$ corresponds to an elliptic curve with CM by $\mathbb{Q}(i)$ or $\mathbb{Q}(\sqrt{-2})$. However, both of them have class number one, hence E is defined over $\mathbb{Q}$. The CM map α_0 is $1+i$ in the previous case (see [22]). Hence, as in Proposition 4.1, $\ker(1+i)^\phi = \ker(1+i)$ where ϕ is complex conjugation.

PROPOSITION 4.3. *Let p be an odd prime. Any w_N-fixed point on $X_0(N)(\mathbb{F}_p)$ is the reduction of a w_N-fixed $\mathbb{Q}_p$-rational point on the generic fiber of $X_0(N)$. Conversely, a w_N-fixed point on the generic fiber reduces to a w_N-fixed point on $X_0(\mathbb{F}_p)$.*

Proof. By Theorem 3.3, any w_N-fixed point on $X_0(N)(\mathbb{F}_p)$ can be lifted to a w_N-fixed point (E, α_0) such that E is defined over a number field $\mathbb{B}$

such that the inertia degree of p in $\mathbb{B}$ is 1. Since p is unramified in $\mathbb{B}$, $\mathbb{B}$ can be embedded in $\mathbb{Q}_p$, and by Proposition 4.1 we are done.

Conversely, since the fixed locus of w_N is proper, a w_N-fixed point on $X_0(N)(\mathbb{Q}_p)$ reduces to a w_N-fixed point on $X_0(N)(\mathbb{F}_p)$. ∎

Proposition 4.3 shows that if $X_0(N)(\mathbb{F}_p)$ contains a smooth w_N-fixed point, then $X^d(N)(\mathbb{Q}_p)$ is non-empty. We now show the converse.

Proposition 4.4. *Let x be a point of $X_0(N)(\mathbb{K}_\nu)$ such that $w_N(x^\sigma) = x$. Then x reduces to a w_N-fixed point on the special fiber of $\mathcal{X}_0(N)_{/R}$.*

Proof. Note that σ is not a morphism of $\mathrm{Spec}(R)$-schemes. We define the map $\hat{\sigma} : \mathcal{X}_0(N) \to \mathcal{X}_0(N)$ using the following diagram:

$$\begin{tikzcd}
\mathrm{Spec}(R) \arrow[r, "\sigma"] & \mathrm{Spec}(R) \\
\mathcal{X}_0(N) \arrow[u] \arrow[r, "\hat{\sigma}"] & \mathcal{X}_0(N) \arrow[u]
\end{tikzcd}$$

Since $\mathbb{K}_\nu/\mathbb{Q}_p$ is ramified, σ induces the trivial action on the residue field R/ν, and therefore also on the special fiber:

$$\begin{tikzcd}
\mathrm{Spec}(R) \arrow[r, "\sigma"] & \mathrm{Spec}(R) \\
\mathcal{X}_0(N) \arrow[u] \arrow[r, "\hat{\sigma}"] & \mathcal{X}_0(N) \arrow[u] \\
\mathcal{X}_0(N) \times_R \mathrm{Spec}(R/\nu) \arrow[u] \arrow[d] \arrow[r, "\mathrm{id}"] & \mathcal{X}_0(N) \times_R \mathrm{Spec}(R/\nu) \arrow[u] \arrow[d] \\
\mathrm{Spec}(R/\nu) \arrow[r, "\mathrm{id}"] \arrow[uuu, bend left=60] & \mathrm{Spec}(R/\nu) \arrow[uuu, bend right=60]
\end{tikzcd}$$

We now add to the picture the Atkin–Lehner involution w_N which is a morphism of $\mathrm{Spec}(R)$-schemes:

$$\begin{tikzcd}
 & \mathrm{Spec}(R) \arrow[r, "\sigma"] & \mathrm{Spec}(R) \\
\mathcal{X}_0(N) \arrow[ur] \arrow[r, "w_N"] & \mathcal{X}_0(N) \arrow[u] \arrow[r, "\hat{\sigma}"] & \mathcal{X}_0(N) \arrow[u] \\
\mathcal{X}_0(N) \times_R \mathrm{Spec}(R/\nu) \arrow[u] \arrow[r, "w_n"] & \mathcal{X}_0(N) \times_R \mathrm{Spec}(R/\nu) \arrow[u] \arrow[d] \arrow[r, "\hat{\sigma}\times\mathrm{id}"] & \mathcal{X}_0(N) \times_R \mathrm{Spec}(R/\nu) \arrow[u] \arrow[d] \\
 & \mathrm{Spec}(R/\nu) \arrow[r, "\mathrm{id}"] & \mathrm{Spec}(R/\nu)
\end{tikzcd}$$

Every point on $X_0(N)(\mathbb{K}_\nu)$ extends to a morphism $\phi : \operatorname{Spec}(R) \to \mathcal{X}_0(N)$ by properness, and if the point of $X_0(N)(\mathbb{K}_\nu)$ is fixed by $w_N \circ \sigma$ then the morphism ϕ is preserved under composition with $w_N \circ \hat{\sigma}$. To be more precise, let x be a point in $X_0(N)(\mathbb{K}_\nu)$ such that $w_N \circ \sigma(x) = x$. By properness, $x = \phi \circ i$ where i is the injection $i : \operatorname{Spec}(\mathbb{K}_\nu) \to \operatorname{Spec}(R)$, so $w_N \circ \hat{\sigma} \circ \phi \circ i = \phi \circ i$, hence $w_N \circ \hat{\sigma} \circ \phi = \phi$.

Moreover the diagram shows that the restriction of ϕ to the special fiber $\tilde{p} : \operatorname{Spec}(R/\nu) \to \mathcal{X}_0(N) \times_R \operatorname{Spec}(R/\nu)$ is a w_N-fixed point on $X_0(N)(\mathbb{F}_p)$. ■

In fact Proposition 4.4 is true even if p is ramified in $\mathbb{Q}(\sqrt{-N})$: in order to have a $\mathbb{K}_\nu$-rational $w_N \circ \sigma$-fixed point there must be a w_N-fixed $\mathbb{F}_p$-rational point of $X_0(N)$. However, the converse cannot be concluded using Proposition 4.3. Since if p is ramified in $\mathbb{Q}(\sqrt{-N})$, p is ramified in $\mathbb{H}/\mathbb{Q}$, it is not immediately clear how B ramifies at primes over p. Nonetheless, we have the following result for any prime p ramified in K, without any restriction on the decomposition of p in $\mathbb{Q}(\sqrt{-N})$:

Proposition 4.5. *Let p be a prime ramified in $\mathbb{K}$. If $X^d(N)(\mathbb{Q}_p) \neq \emptyset$ then there is a w_N-fixed point in $X_0(N)(\mathbb{F}_p)$.*

It remains to determine when there are w_N-fixed points of $X_0(N)(\mathbb{F}_p)$. Let S_N be the set of primes p such that there is a w_N-fixed, $\mathbb{F}_p$-rational point on the special fiber of $\mathcal{X}_0(N)_{/R}$. In Proposition 4.6, we describe the set S_N explicitly as a Chebotarev set. In addition to the notation introduced at the beginning of the section, $\mathbb{B}$ denotes $\mathbb{Q}(j(O))$ where $j(O)$ is the j-invariant of the order $O = \mathbb{Z}[\sqrt{-N}]$, and $\mathbb{M} := \mathbb{Q}(\sqrt{-N})$.

Proposition 4.6. *Let p be an odd prime and let $\mathcal{P}$ be a prime of $\mathbb{M}$ lying over p. Then p is in S_N if and only if there exists a prime ν of $\mathbb{B}$ lying over p such that $f(\nu|p) = 1$ and $\mathcal{P}$ totally splits in $\mathbb{H}/\mathbb{M}$.*

Proof. We know that $\mathbb{H}/\mathbb{M}$ is an abelian extension with Galois group G isomorphic to the ideal class group of $\mathbb{M}$, and $[\mathbb{H} : \mathbb{M}] = [\mathbb{B} : \mathbb{Q}]$. The extension $\mathbb{H}/\mathbb{Q}$ is Galois with Galois group $G \rtimes \mathbb{Z}/2\mathbb{Z}$ where $\mathbb{Z}/2\mathbb{Z}$ acts by inversion on G. The $\mathbb{Z}/2\mathbb{Z}$-fixed subfield of $\mathbb{H}$ is $\mathbb{B}$ as explained in Section 6 of [3].

We want to know for which primes there is a w_N-fixed point on $X_0(N)(\mathbb{F}_p)$. We have shown in Proposition 4.3 that this is equivalent to the presence of a w_N-fixed point on $X_0(N)(\mathbb{Q}_p)$.

Let P be a w_N-fixed point of $X_0(N)$, defined over $\mathbb{B}$. Then P reduces to an $\mathbb{F}_p$-point on the special fiber if and only if it is fixed by Frobenius. Recall that since $\mathbb{B}/\mathbb{Q}$ is unramified at p, Frobenius acts on $\mathbb{B}$. Hence, we should find for which p there exists a prime ν of $\mathbb{B}$ such that $f(\nu|p) = 1$.

Let π_p be the Frobenius at p. The map π_p gives a conjugacy class in $\operatorname{Gal}(\mathbb{H}/\mathbb{Q})$ via Artin symbol.

The conjugacy classes of $G \rtimes \mathbb{Z}/2\mathbb{Z}$ are as follows:

(1) $\{(g,0)\}$, one for each $g \in G[2]$.
(2) $\{(g,0),(-g,0)\}$, one for each g in $G - G[2]$.
(3) $\{(g+2x,1) \mid x \in G\}$, one for each representative g of $G/2G$.

A prime ν of $\mathbb{B}$ over p has $f(\nu|p) = 1$ if and only if the conjugacy class π_p contains an element of the form $(0,y)$ for some y in $\mathbb{Z}/2\mathbb{Z}$. Hence, the only allowed conjugacy classes are the trivial class and one of the classes of type (3).

Hence, p is in S_N if and only if π_p contains an automorphism which fixes $\mathbb{B}$, equivalently, $\mathcal{P}$ totally splits in $\mathbb{H}/\mathbb{M}$. ∎

Remark 4.7. Note that if p splits in $\mathbb{M}/\mathbb{Q}$ then there are two primes of $\mathbb{M}$ lying over p. If a prime $\mathcal{P}$ of $\mathbb{M}$ lying over p splits totally in $\mathbb{H}/\mathbb{M}$ then p splits totally in $\mathbb{H}/\mathbb{Q}$, hence it does not matter which prime of $\mathbb{M}$ lying over p we take.

Remark 4.8. Proposition 4.6 determines for which p the field of definition of an elliptic curve whose endomorphism ring contains $\mathbb{Z}[\sqrt{-N}]$ embeds into $\mathbb{Q}_p$. Then using Proposition 4.1, we get a w_N-fixed $\mathbb{Q}_p$-rational point of $X_0(N)$.

We have thus established a complete criterion for the non-emptiness of $X^d(N)(\mathbb{Q}_p)$, where p is an odd prime ramified in $\mathbb{K}$ but not in $\mathbb{Q}(\sqrt{-N})$.

For $\mathbb{Q}_2$-points, the argument is as follows. Let d and N be square-free integers such that $d \equiv 2,3$ and $-N \equiv 1 \bmod 4$. Over $\mathbb{F}_2$ there are two elliptic curves: the ordinary one, with endomorphism ring $\mathbb{Z}[(1+\sqrt{-7})/2]$, and the supersingular one whose endomorphism ring is the Hurwitz quaternions, $B(\mathbb{Z}) := \mathbb{Z} + i\mathbb{Z} + j\mathbb{Z} + \frac{1+i+j+k}{2}\mathbb{Z}$. It is a maximal order in the quaternion algebra ramified only at 2 and at infinity. Hence, if a w_N-fixed point (E,C) of $X_0(N)(\mathbb{F}_2)$ is ordinary—in particular $N = 7$—then E can be lifted to an elliptic curve over a number field $\mathbb{B}$ that has complex multiplication by the maximal order of $\mathbb{Q}(\sqrt{-7})$ by Theorem 3.3. If (E,C) is supersingular, then the maximal order of $\mathbb{Q}(\sqrt{-N})$ embeds in $\mathrm{End}(E)$ since the local order $B(\mathbb{Z}) \otimes_{\mathbb{Z}} \mathbb{Z}_2$ contains all elements of $B(\mathbb{Q}) \otimes \mathbb{Q}_2$ with norm in $\mathbb{Z}_2$. Therefore by Theorem 3.3, E can be lifted to an elliptic curve over a number field $\mathbb{B}$ that has complex multiplication by the maximal order of $\mathbb{Q}(\sqrt{-N})$. Hence, we proved the following lemma:

Lemma 4.9. *Let (E,C) be a w_N-fixed point of $X_0(N)(\mathbb{F}_2)$. Then E can be lifted to an elliptic curve $\tilde{E}$ over a number field $\mathbb{B}$ such that $\tilde{E}$ has complex multiplication by the maximal order of $\mathbb{Q}(\sqrt{-N})$.*

Suppose $\tilde{E}$ has CM by the maximal order of $\mathbb{Q}(\sqrt{-N})$. Since 2 is unramified in $\mathbb{Q}(\sqrt{-N})$ and the Hilbert class field is an unramified extension of

$\mathbb{Q}(\sqrt{-N})$, 2 is unramified in $\mathbb{B}/\mathbb{Q}$. This implies that $\mathbb{B}_\nu$ embeds in $\mathbb{Q}_2$, where ν is a prime of $\mathbb{B}$ lying over 2. Therefore $\tilde{E}$ induces a point in $X^d(N)(\mathbb{Q}_2)$. Hence, we conclude that $X^d(N)(\mathbb{Q}_2) \neq \emptyset$ if and only if there is a w_N-fixed point on $X_0(N)(\mathbb{F}_2)$, if and only if p is in the set S_N defined above, exactly as in the case of odd primes. This yields

Theorem 4.10. *Let p be a prime ramified in $\mathbb{Q}(\sqrt{d})$ and N a square-free integer such that p is unramified in $\mathbb{Q}(\sqrt{-N})$. Then $X^d(N)(\mathbb{Q}_p) \neq \emptyset$ if and only if p is in the set S_N defined in Proposition* 4.6.

Example 4.11. Let $d = 5$ and $N = 29$. According to Theorem 2.3, since $(5, 29) = 1$, the necessary condition for the existence of a $\mathbb{Q}$-curve of degree 29 over $\mathbb{K} = \mathbb{Q}(\sqrt{5})$ is satisfied, but the existence is not guaranteed. Note that this case is not covered by Theorem 2.6.

If we use Theorem 4.10 for the ramified prime 5, we see that $X^5(29)(\mathbb{Q}_5)$ is empty, hence there is no $\mathbb{Q}$-curve of degree 29 over $\mathbb{K}$. For $X^5(29)(\mathbb{Q}_5)$ to be non-empty, 5 should split in $\mathbb{H}/\mathbb{Q}(\sqrt{-29})$, where $\mathbb{H}$ is the Hilbert class field of $\mathbb{Q}(\sqrt{-29})$. However, the prime $P \mid 5$ of $\mathbb{Q}(\sqrt{-29})$, decomposes as P_1P_2 where the inertia degree of P_i is 3, hence $X^5(29)(\mathbb{Q}_5) = \emptyset$. Note that $X^5(29)(\mathbb{Q}_p) \neq \emptyset$ for any other prime p different from 5 using Theorem 1.1. It is interesting that this curve fails to have local points at exactly one place, unlike the examples of Shih, Quer and Clark.

5. Violations of the Hasse principle. We now give a more precise statement of the density result stated in the introduction and prove it.

Definition 5.1. If $L/\mathbb{Q}$ is a finite normal extension of $\mathbb{Q}$ and $c \subset \mathrm{Gal}(L/\mathbb{Q})$ is a subset closed under conjugacy, then the set of primes p whose Artin symbol in $\mathrm{Gal}(L/\mathbb{Q})$ lies in c is called a *Chebotarev set.*

The density of a Chebotarev set is well-defined by the Chebotarev density theorem, and the set S_N of primes defined in Proposition 4.6 is a Chebotarev set with density $(|2G| + 1)/(2|G|)$ where G is the Galois group of $\mathbb{H}$ over $\mathbb{M}$ as introduced in the previous section.

Theorem 5.2 (Serre, Theorem 2.8 in [30]). *Let $0 < \alpha < 1$ be the Frobenius density of a set of primes S, and $N_S(X)$ the number of square-free integers in $[1, \ldots, X]$ all of whose prime factors lie in S. Then*

$$N_S(X) = c_S \frac{X}{\log^{1-\alpha} X} + O\left(\frac{X}{\log^{2-\alpha} X}\right) \quad \textit{for some positive constant } c_S.$$

Using this result we obtain a density result for the twists which have local points at every prime p. One can write down a curve $X_0(N)$ and compute an explicit asymptotics for the set of quadratic twists of $X_0(N)$ violating the Hasse principle using Faltings' finiteness results as in the proof of Theorem 2 in [1]. We will detail the case of N prime and congruent to 1 modulo 4 below.

The other cases are similar. Note that for a given N, the set S_N, defined in the previous section, is fixed.

PROPOSITION 5.3. *Given a prime number $N \equiv 1 \bmod 4$ and a positive integer X, let A' be the set of positive square-free integers $d \le X$ such that $X^d(N)(\mathbb{Q}_p)$ is non-empty for all p and there is no prime simultaneously ramified in $\mathbb{Q}(\sqrt{d})$ and $\mathbb{Q}(\sqrt{-N})$. Then*

$$|A'| = \frac{1}{2} M_{S_N} \frac{X}{\log^{1-\alpha} X} + O\biggl(\frac{X}{\log^{2-\alpha} X}\biggr)$$

where $\alpha = (|2G|+1)/(2|G|)$ is the density of S_N.

Proof. By Theorem 5.2 the set $A = \{d \in \mathbb{Z} \mid d \le X$, square-free, $(d,N)=1$, $d = \prod_i p_i$, $p_i \in S_N\}$ has density

$$M_{S_N} \frac{X}{\log^{1-\alpha} X} + O\biggl(\frac{X}{\log^{2-\alpha} X}\biggr) \quad \text{where} \quad \alpha = \frac{|2G|+1}{2|G|}$$

is the density of S_N.

We will examine $\mathbb{Q}_p$-points for each p separately, starting with $p=2$. If $N \equiv 1 \bmod 4$ then 2 is ramified in $\mathbb{Q}(\sqrt{-N})$, hence it cannot be ramified in $\mathbb{Q}(\sqrt{d})$ when $d \equiv 1 \bmod 4$ and 2 is not in S_N. Therefore, in order to have $\mathbb{Q}_2$-points we should consider the d's in A which are congruent to 1 mod 4.

By Theorem 1.1, the only primes p such that $X^d(N)$ may fail to have $\mathbb{Q}_p$-points are the primes ramified in $\mathbb{Q}(\sqrt{d})$ and unramified in $\mathbb{Q}(\sqrt{-N})$ and the primes that are inert in $\mathbb{Q}(\sqrt{d})$, dividing N. We start by showing that N splits in $\mathbb{Q}(\sqrt{d})$, hence $X^d(N)(\mathbb{Q}_N) \neq \emptyset$.

By Theorem 6.1 in [3], the genus field of $\mathbb{Q}(\sqrt{-N})$ is $\mathbb{Q}(\sqrt{N}, \sqrt{-N})$. Recall that the ring class field of $\mathbb{Z}[\sqrt{-N}]$ is $\mathbb{Q}(\sqrt{-N}, j(\sqrt{-N}))$ and $j(\sqrt{-N})$ is real ([3, p. 220]). Therefore $\mathbb{Q}(\sqrt{N})$ lies inside $\mathbb{Q}(j(\sqrt{-N}))$. Let p be a prime divisor of d. Note that p has to be odd. Since p is in S_N, there is a prime $\mathcal{P}$ of $\mathbb{Q}(j(\sqrt{-N}))$ lying over p with inertia degree 1. Consequently, $\bigl(\frac{N}{p}\bigr) = \bigl(\frac{p}{N}\bigr) = 1$, hence $\bigl(\frac{d}{N}\bigr) = 1$, and N splits in $\mathbb{Q}(\sqrt{d})$. Therefore if N is prime congruent to 1 mod 4, then for any d in A and $d \equiv 1 \bmod 4$, $X^d(N)(\mathbb{Q}_p) \neq \emptyset$ for all p. Since A consists of only odd numbers, the set A' has density $\frac{1}{2}|A|$. ■

In [1, Theorem 2] Clark proved that there are only finitely many d's such that $X^d(N)(\mathbb{Q})$ is non-empty, when $N > 131$ and $N \neq 163$. Therefore, excluding this finite set of N, Proposition 5.3 gives the asymptotics for the number of twists $X^d(N)$ which violate the Hasse principle when N is a prime congruent to 1 mod 4 and there is no prime simultaneously ramified in $\mathbb{Q}(\sqrt{d})$ and $\mathbb{Q}(\sqrt{-N})$. Hence one gets the following result:

THEOREM 5.4. *Let N be a prime greater than* 131 *and congruent to* 1 *mod* 4. *Then the number of twists $X^d(N)$ which violate the Hasse principle* *when there is no prime simultaneously ramified in* $\mathbb{Q}(\sqrt{d})$ *and* $\mathbb{Q}(\sqrt{-N})$, *is asymptotically* $\frac{1}{2}M_{S_N}\frac{X}{\log^{1-\alpha} X}$.

The following corollary gives an answer to a question of Clark [1].

Corollary 5.5. *Let* N *be a prime congruent to* 1 *mod* 4, *and* p *be an odd prime such that* $(N/p) = -1$. *Then*

(1) $X^{p^*}(N)(\mathbb{Q}_N) = \emptyset$.
(2) $X^{p^*}(N)(\mathbb{Q}_p) = \emptyset$.
(3) $X^{p^*}(N)(\mathbb{Q}_\ell) \neq \emptyset$ *for any other prime* ℓ *different than* p *and* N.

Proof. The first conclusion was also given in [1] and can be seen as a consequence of Theorem 3.7. The second conclusion can also be derived from a theorem of González [1, Theorem 9] but we give a slightly different approach below.

Let $\mathbb{M} := \mathbb{Q}(\sqrt{-N})$. Since $N \equiv 1 \bmod 4$, the genus field of $\mathbb{M}$ is $\mathbb{Q}(i, \sqrt{N})$. Note that since $-N \equiv 3 \bmod 4$, the ring class field of $\mathbb{Z}[\sqrt{-N}]$ is the Hilbert class field. Let $\mathbb{B} := \mathbb{Q}(j(\mathbb{Z}[\sqrt{-N}]))$. Since $j(\mathbb{Z}[\sqrt{-N}])$ is real, $\mathbb{B} \cap \mathbb{Q}(i, \sqrt{N})$ is $\mathbb{Q}$ or $\mathbb{Q}(\sqrt{N})$. If it is $\mathbb{Q}$, the class number of $\mathbb{Z}[\sqrt{-N}]$ is 1, a contradiction.

By Theorem 4.10 and Lemma 4.6, $X^d(N)(\mathbb{Q}_p) = \emptyset$ if and only if $p \notin S_N$. Since $(N/p) = -1$ this is equivalent to saying that for all primes ν of $\mathbb{B}$ lying over p, $f(\nu|p) > 1$.

The third conclusion can be derived from Theorem 3.17. ∎

6. Further directions.

We have seen that there are lots of curves over $\mathbb{Q}$ which have local points everywhere (Proposition 5.3). As stated by Clark [1], one natural follow-up question would be asking about the $\mathbb{Q}$-rational points. We know by Theorem 5.4 that there are many quadratic twists which have local points everywhere but no $\mathbb{Q}$-rational points. In this section we will give examples of such twists and show that this violation of the Hasse principle can be explained by the Brauer–Manin obstruction.

In the case of imaginary quadratic fields $\mathbb{K}$ and when N is inert in $\mathbb{K}$, we have an answer to the question of Clark mentioned above, implied by the following theorem of Mazur:

Theorem 6.1 (Mazur, [18]). *If* $\mathbb{K}$ *is a quadratic imaginary field and* N *is a sufficiently large prime which is inert in* $\mathbb{K}$, *then* $X_0(N)(\mathbb{K})$ *is empty. In particular, there are no* $\mathbb{Q}$*-curves over* $\mathbb{K}$ *of degree* N.

When N splits in $\mathbb{K}$ and $\mathbb{K}$ is imaginary quadratic, or N is inert in $\mathbb{K}$ and $\mathbb{K}$ is real quadratic, using the formula of Weil given in [14], every cuspform associated with a quotient of the Jacobian of $X^d(N)$ has odd functional equation. Thus, conjecturally none of these quotients has Mordell–Weil rank 0 and we cannot hope to apply Mazur's techniques. The future plan is to prove a result about existence of rational points on $X^d(N)$ where $\mathbb{K}$ is a real quadratic field and N splits in $\mathbb{K}$ using Mazur's techniques.

Another direction to go is understanding the reasons of violations of the Hasse principle. Say for some d and N, $X^d(N)$ has local points for every p but no global points, hence it violates the Hasse principle. What is the reason for that? One natural guess would be the Brauer–Manin obstruction.

Let C be a smooth, projective, geometrically integral curve over $\mathbb{Q}$ of genus greater than or equal to 2 with a rational degree one divisor D. Then we can embed C into its Jacobian J via the map $P \mapsto [P] - D$. The aim is to obtain information on the set $C(\mathbb{Q})$, in particular we would like to prove that $C(\mathbb{Q})$ is empty. Using the technique that is explained below, which first appeared in Scharaschkin's thesis [26], one may prove that $C(\mathbb{Q})$ is empty.

Let S be a finite set of primes at which C has good reduction and assume that we know the generators of the Mordell–Weil group, $J(\mathbb{Q})$. Then for every p in S we can compute the finite abelian group $J(\mathbb{F}_p)$ and the set $C(\mathbb{F}_p)$. Let inj_p denote the injection from $C(\mathbb{F}_p)$ to $J(\mathbb{F}_p)$, and red_p be the reduction map from $J(\mathbb{Q})$ to $J(\mathbb{F}_p)$. Then we obtain the following diagram:

$$\begin{tikzcd}
C(\mathbb{Q}) \arrow[r, "P\mapsto[P]-D"] \arrow[d] & J(\mathbb{Q}) \arrow[d, "\mathrm{red}=\prod_{p\in S}\mathrm{red}_p"] \\
\prod_{p\in S} C(\mathbb{F}_p) \arrow[r, "\mathrm{inj}=\prod_{p\in S}\mathrm{inj}_p"] & \prod_{p\in S} J(\mathbb{F}_p)
\end{tikzcd}$$

If there is a P in $C(\mathbb{Q})$ then $\mathrm{red}_p([P]-D)$ is in $\mathrm{inj}_p(C(\mathbb{F}_p))$ for any p in S. In particular if the images of red and inj do not intersect then $C(\mathbb{Q}) = \emptyset$. This technique is called *Mordell–Weil sieve.*

The Brauer–Manin obstruction is checking if a certain subset C^B, where B is a subset of the Brauer group of C, is empty or not. This method was introduced by Manin in [16] and says that if C^B is empty then $C(\mathbb{Q})$ is empty. Note that C^B is a subset of adeles $\prod_\nu C(\mathbb{Q}_p)$, containing $C(\mathbb{Q})$. What Scharaschkin proved in his thesis is that in the case of curves (and under the assumption that the Tate–Shafarevich group of J is finite and C has a rational degree one divisor), Mordell–Weil sieve is equivalent to the Brauer–Manin obstruction ([26], [27]).

Given a smooth, projective, geometrically integral curve over $\mathbb{Q}$ with local points for every $\mathbb{Q}_p$, it is an open question whether the Brauer–Manin obstruction is the only obstruction to the Hasse principle [33]. However, in the cases below, this is known.

Theorem 6.2 (Manin, [33]). *Let C be a proper, smooth curve of genus* 1 *with Jacobian J. If* Sha(J) *is finite then the Brauer–Manin obstruction is the only obstruction to the Hasse principle.*

Theorem 6.3 (Scharaschkin, [26]). *Let C be a proper, smooth curve with Jacobian J. If C has a rational divisor class of degree* 1, *and $J(\mathbb{Q})$ and* Sha(J) *are finite, then the Brauer–Manin obstruction is the only obstruction to the Hasse principle.*

In order to apply Scharaschkin's technique, one needs an equation of the curve C, generators of $J(\mathbb{Q})$ and also existence of a $\mathbb{Q}$-rational degree one divisor class. In the case of quadratic twists of $X_0(N)$, if the curve is hyperelliptic and w_N is the hyperelliptic involution then finding the equation of the twist is easy. According to [22] there are 18 values of N such that $X_0(N)$ is hyperelliptic. Moreover there exist relatively simple equations of $X_0(N)$ given by Galbraith in [9] that make the computations feasible. Such equations for hyperelliptic modular curves were first given by González [10] (see also the works of Murabayashi [21] and Hasegawa [11]). It is a result of Ogg [22] that $X_0(N)$ is hyperelliptic with automorphism group $\{1, w_N\}$ for $N = 23, 26, 29, 31, 35, 39, 41, 47, 50, 59, 71$. Then the equation of the twist $X^d(N)$ is $dy^2 = f_{2g+2}(x)$ where g is the genus of the curve and f_m is a degree m polynomial.

Since for genus 1 the claim is already proved, we will restrict to the cases $g \geq 2$ and we want a hyperelliptic curve with $w_N = -1$. The smallest such N is 23 and $X_0(23)$ is given by $(x^3 - x + 1)(x^3 - 8x^2 + 3x - 7)$ in [9]. The following computations were done using the computer package MAGMA.

Example 6.4. Let $N = 23$. We will study the twists of $X_0(23)$ for all primes d between -300 and 300. There are 124 such primes. The twist is given by the equation $y^2 = d(x^3 - x + 1)(x^3 - 8x^2 + 3x - 7)$. Let a_1, a_2, a_3 be the roots of $x^3 - x + 1$, and $P_i = (a_i, 0)$ be the corresponding points on $X^d(N)$. Then $D = [P_1 + P_2 + P_3 - \infty_1 - \infty_2]$ is a rational divisor of degree one on $X^d(N)$. A similar construction can be found in [8].

(1) Let $|d|$ be prime different from 23 and between -300 and 300. Then $X^d(N)$ has local points everywhere for 39 values of d. For 10 among these 39 values, $X^d(N)$ has points with small height. When we eliminate these, we are left with a set with 29 elements.

(2) In order to apply Scharaschkin's technique, we need the generators of $J^d(\mathbb{Q})$ where J^d is the Jacobian of $X^d(N)$. This seems to be the hardest thing to do. First let us consider the only case where we were able to apply Scharaschkin's technique.

Say $d = 17$: Let C be $X^{17}(23)$ and J^{17} be its Jacobian. It can be computed that J^{17} has no non-trivial torsion and the rank of $J^{17}(\mathbb{Q})$ is less than or equal to 2. After a short search we come up with the generators of $J^{17}(\mathbb{Q})$: $D_1 = \langle x^2+3, 17x-34, 2\rangle$ and $D_2 = \langle x^2 - 3/4x + 5/8, 153/16x - 17/32, 2\rangle$. The notation means that $D_1 = [P_1 + \bar{P}_1 - \infty_1 - \infty_2]$ with $P_1 = (a, 17a-34)$ where a is one of the roots of x^2+3 and $\bar{P}_1 = (\bar{a}, 17\bar{a}-34)$. Similarly for D_2.

To apply Scharaschkin's idea, we need a finite set S of primes. In our case S will be $\{3, 19\}$. Now we explain how we came up with this S. The first thing to do is reduce the generators D_1, D_2 of the Mordell–Weil group modulo several primes such that J^{17} has good reduction. Let $\tilde{C}, \tilde{J}^{17}, \tilde{D_1}, \tilde{D_2}$ be the reductions of C, J^{17}, D_1, D_2 modulo p. We did this for primes in $[3, 25]$ and we got Table 1.

Table 1

Prime	Order of $\tilde{D_1}$ and $\tilde{D_2}$	k such that $D_2 = kD_1$
3	$[11, 11]$	4
5	$[10, 10]$	-
7	$[38, 38]$	-
11	$[38, 38]$	-
13	$[11, 11]$	4
19	$[11, 11]$	4

Since the strategy is to compare the linear combinations of reductions of D_1 and D_2 modulo p with the image of inj_p, we would like to have primes which will give fewer linear combinations, i.e. primes p for which D_1 and D_2 have smaller orders modulo p. Another thing that might be useful is having the extra relation $\tilde{D_2} = k\tilde{D_1}$. We see that there are three primes $3, 13, 19$ for which this happens. We remark that, in fact, the set $\{13\}$ would also work to show the non-existence of any point on C, but we think that the set consisting of two primes gives a better understanding of the technique. We should also mention that none of the primes $3, 19$ (or 5) would work alone.

Say there exists a point P in $C(\mathbb{Q})$. Then its image D under the injection map is in $J(\mathbb{Q})$, hence $D = n_1D_1 + n_2D_2$ for some integers n_1, n_2.

Let $p = 3$. The reduction of D is $\tilde{D} = n_1\tilde{D_1} + n_2\tilde{D_2}$. Since $\tilde{D_2} = 4\tilde{D_1}$, for any linear combination we have $n_1\tilde{D_1} + n_2\tilde{D_2} = (n_1 + 4n_2)\tilde{D_1}$. The image of the map inj_3 is $k\tilde{D_1}$ with $k \in \{1, 5, 6, 10\}$. This shows that $n_1 + 4n_2 \equiv 1, 5, 6$ or $10 \bmod 11$.

Now let $p = 19$. Again we have $\tilde{D_2} = 4\tilde{D_1}$ so any linear combination $n_1\tilde{D_1} + n_2\tilde{D_2}$ reduces to $(n_1 + 4n_2)\tilde{D_1}$. However, the image of inj_{19} is $k\tilde{D_1}$ with $k \in \{2, 3, 8, 9\}$. This yields $n_1 + 4n_2 \equiv 2, 3, 8$ or $9 \bmod 11$. Contradiction.

This example shows that the twisted modular curve $X^{17}(23)$ has local points everywhere but no global points, hence it violates the Hasse principle, and this violation can be explained by the Brauer–Manin obstruction.

This example is also interesting in the sense that 23 is inert in the quadratic field $\mathbb{Q}(\sqrt{17})$. Then, using the formula of Weil given in [14], every cuspform associated with a quotient of the Jacobian of $X^{17}(23)$ has odd functional equation. Thus, conjecturally none of these quotients has Mordell–Weil rank 0 and Mazur's methods cannot be applied. In fact, the Jacobian of $X^{17}(23)$ is simple since $J^{17}(23)$ is an abelian surface with rank 2 and therefore its only non-trivial quotients are the elliptic ones. However, the q-expansion of the corresponding newforms of level 23 has conjugate coefficients in $\mathbb{Q}(\sqrt{-5})$ (see [34]), hence there is only one isogeny class, therefore $J^{17}(23)$ is simple.

If we continue our search for the same level, $N = 23$, we get some more d values such that the corresponding twists fail to have rational points.

Example 6.5 (continuation of the above). For $d = 173, -211, 101, -59, -223$ the rank of $J(\mathbb{Q})$ is 0 since the 2-Selmer group is trivial. Moreover, the torsion part of $J(\mathbb{Q})$ is also trivial in all these cases. Say there exists $P \in C(\mathbb{Q})$ where C is the twist $X^d(23)$; then $[P] - D$, where D is as above, is in $J(\mathbb{Q})$. By Lemma 6.6 below, D is not equivalent to $[P]$ for any point P, hence $[P] - D$ is non-zero, contradiction. Therefore $X^d(23)(\mathbb{Q}) = \emptyset$ for $d = 173, -211, 101, -59, -223$.

Lemma 6.6. *Let C be a hyperelliptic curve of genus at least 2. Let P_1, P_2, P_3 be fixed points of the hyperelliptic involution, and let I_1, I_2 be a pair of points interchanged by the hyperelliptic involution. Let $D = P_1 + P_2 + P_3 - I_1 - I_2$. Then D is not linearly equivalent to a point.*

Proof. Since $2P_3$ and (I_1+I_2) are fibers of the hyperelliptic map $C \to \mathbb{P}^1$, the divisor $2P_3 - I_1 - I_2$ is principal. Hence, D can also be written as $P_1 + P_2 - P_3$. If D is equivalent to some point Q, then $P_1 + P_2 - P_3 - Q$ is a principal divisor $\operatorname{div}(f)$. But then $f : C \to \mathbb{P}^1$ would have degree 2, and in particular would give another hyperelliptic map and another hyperelliptic involution. It must be different from the hyperelliptic involution we already know, because it interchanges P_1 and P_2. Since the hyperelliptic involution is unique in genus greater than one, this gives us a contradiction. ∎

In [2] Clark proves that the density of twists that violate the Hasse principle is positive. Hence, we know they exist. However, the examples stated so far are the first explicit examples of this family of twists that violate the Hasse principle. Moreover, this violation is explained by the Brauer–Manin obstruction.

Acknowledgements. This paper is part of my Ph.D. thesis. I would like to thank my advisor, Jordan Ellenberg, for suggesting the main problem of the paper, and for advice about technical matters and about the presentation. I would also like to thank Pete Clark for several conversations on the topic, Jim Stankewicz for letting me know a mistake in the earlier version of the paper as well as Robert Rhoades and Steven Galbraith for useful comments on the paper. Some parts of this paper were completed during my stay in Centre de Recerca Matemàtica with EPDI fellowship. I would like to thank both CRM and EPDI network for their hospitality and financial support.

References

[1] P. L. Clark, *An "anti-Hasse principle" for prime twists*, Int. J. Number Theory 4 (2008), 627–637.

[2] —, *Galois groups via Atkin–Lehner twists*, Proc. Amer. Math. Soc. 135 (2007), 617–624.

[3] D. Cox, *Primes of the Form $x^2 + ny^2$*, Wiley, 1989.

[4] P. Deligne et M. Rapoport, *Les schémas de modules de courbes elliptiques*, in: Modular Functions of One Variable, II (Antwerp, 1972), Lecture Notes in Math. 349, Springer, Berlin, 1973, 143–316.

[5] M. Deuring, *Die Typen der Multiplikatorenringe elliptischer Funktionenkörper*, Abh. Math. Sem. Hansischen Univ. 14 (1941), 197–272.

[6] F. Diamond and J. Shurman, *A First Course in Modular Forms*, Grad. Texts in Math. 228, Springer, New York, 2005.

[7] J. S. Ellenberg, *$\mathbb{Q}$-curves and Galois representations*, in: Modular Curves and Abelian Varieties, J. Cremona et al. (eds.), Birkhäuser, 2004, 93–103.

[8] E. V. Flynn, *The Hasse principle and the Brauer–Manin obstruction for curves*, Manuscripta Math. 115 (2004), 437–466.

[9] S. Galbraith, *Equations for modular curves*, Doctoral Thesis, Oxford, 1996, http://www.isg.rhul.ac.uk/~sdg/thesis.html.

[10] J. González, *Equations of hyperelliptic modular curves*, Ann. Inst. Fourier (Grenoble) 41 (1991), 779–795.

[11] Y. Hasegawa, *Table of quotient curves of modular curves $X_0(N)$ with genus 2*, Proc. Japan Acad. Ser. A Math. Sci. 71 (1995), 235–239.

[12] —, *Q-curves over quadratic fields*, Manuscripta Math. 94 (1997), 347–364.

[13] B. W. Jordan and R. A. Livné, *Local Diophantine properties of Shimura curves*, Math. Ann. 270 (1985), 235–248.

[14] W. C. W. Li, *Newforms and functional equations*, ibid. 212 (1975), 285–315.

[15] Q. Liu, *Algebraic Geometry and Arithmetic Curves*, Oxford Univ. Press, 2002.

[16] Y. I. Manin, *Le groupe de Brauer–Grothendieck en géométrie diophantienne*, in: Actes du Congrès International des Mathématiciens (Nice, 1970), 1, 1970, 401–411.

[17] B. Mazur, *Modular curves and the Eisenstein ideal*, Inst. Hautes Études Sci. Publ. Math. 47 (1977), 33–186.

[18] —, *Rational isogenies of prime degree*, Invent. Math. 44 (1978), 129–162.

[19] J.-F. Mestre, *La méthode des graphes. Exemples et applications*, in: Proc. Int. Conf. on Class Numbers and Fundamental Units of Algebraic Number Fields (Katata, 1986), Nagoya Univ., Nagoya, 1986, 217–242.

[20] J. S. Milne, *Lectures on Etale Cohomology*, http://www.jmilne.org.

[21] N. Murabayashi, *On normal forms of modular curves of genus 2*, Osaka J. Math. 29 (1992), 405–462.

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

[23] K. Ono, *Nonvanishing of quadratic twists of modular L-functions and applications to elliptic curves*, J. Reine Angew. Math. 533 (2001), 81–97.

[24] J. Quer, *Q-curves and abelian varieties of GL_2-type*, Proc. London Math. Soc. (3) 81 (2000), 285–317.

[25] K. A. Ribet, *On modular representations of* $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ *arising from modular forms*, Invent. Math. 100 (1990), 431–476.

[26] V. Scharaschkin, *Local global problems and the Brauer–Manin obstruction*, PhD Thesis, Univ. of Michigan, 1999.

[27] —, *The Brauer Manin obstruction for curves*, http://www.jmilne.org/math/Students/b.pdf.

[28] J.-P. Serre, *A Course in Arithmetic*, Springer, 1973.

[29] —, *Algebraic Groups and Class Fields*, Springer, 1975.

[30] —, *Divisibilité de certaines fonctions arithmétiques*, Enseign. Math. 22 (1976), 227–260.

[31] K. Shih, *On the construction of Galois extensions of function fields and number fields*, Math. Ann. 207 (1974), 99–120.

[32] J. Silverman, *The Arithmetic of Elliptic Curves*, 2nd ed., Springer, 2009.

[33] A. N. Skorobogatov, *Torsors and Rational Points*, Cambridge Tracts in Math. 144, Cambridge Univ. Press, 2001.

[34] W. Stein, http://modular.math.washington.edu/Tables.

[35] M. Vignéras, *Arithmétique des Algèbres de Quaternions*, Springer, New York, 1980.

Ekin Ozman
Department of Mathematics
University of Texas-Austin
Austin, TX 78712, U.S.A.
E-mail: ozman@math.utexas.edu

Received on 21.12.2010
and in revised form on 29.7.2011 (6581)