Canad. J. Math. Vol. **66** (4), 2014 pp. 924–960
http://dx.doi.org/10.4153/CJM-2013-023-8


# Twists of Shimura Curves

James Stankewicz

*Abstract.* Consider a Shimura curve $X_0^D(N)$ over the rational numbers. We determine criteria for the twist by an Atkin–Lenher involution to have points over a local field. As a corollary we give a new proof of the theorem of Jordan and Livné on $\mathbf{Q}_p$ points when $p \mid D$ and for the first time give criteria for $\mathbf{Q}_p$ points when $p \mid N$. We also give congruence conditions for roots modulo $p$ of Hilbert class polynomials.

Let $D$ be the squarefree product of an even number of primes and let $N$ be a squarefree integer coprime to $D$. The Shimura curves $X_0^D(N)_{/\mathbf{Q}}$ are natural generalizations of the classical modular curves $X_0(N)$, which we realize here as $X_0^1(N)_{/\mathbf{Q}}$. Shimura first defined these curves over $\mathbf{Q}$ [Shi71] and also showed that $X_0^D(N)(\mathbf{R})$ is nonempty if and only if $D = 1$. Later, conditions for $X_0^D(N)(\mathbf{Q}_p)$ to be nonempty were determined when $p \mid D$ first by Jordan and Livné [JL85, Theorem 5.6] in the case $N = 1$ and in the general case by Ogg [Ogg85, Théorème].

In this paper, we give comprehensive criteria for the presence of $\mathbf{Q}_p$-rational points on all Atkin–Lehner twists of $X_0^D(N)$ including the trivial twist, $X_0^D(N)$. Therefore as a consequence, we recover the theorem of Jordan and Livné and for the first time give criteria for $\mathbf{Q}_p$-points when $p \mid N$ and $D > 1$. We note that conjecturally, these twists and their combinations form *all* twists of $X_0^D(N)$ for all but finitely many pairs of $D$ and $N$ [KR08]. Let $C^D(N,d,m)$ denote the twist of $X_0^D(N)$ by $\mathbf{Q}(\sqrt{d})$ and the Atkin–Lehner involution $w_m$ as in Definition 2.2. Particular cases of interest are the twists by the full Atkin–Lehner involution $w_{DN}$. In that case we have the following.

***Corollary*** (3.17) *If $p \nmid DN$ is inert in $\mathbf{Q}(\sqrt{d})$, $C^D(N,d,DN)(\mathbf{Q}_p)$ is nonempty.*

***Theorem*** (4.1, partial) *Suppose that $p \nmid 2DN$ is a prime which is ramified in $\mathbf{Q}(\sqrt{d})$. Then $C^D(N,d,DN)(\mathbf{Q}_p) \neq \varnothing$ if and only if one of the following occurs:*

- $\left(\frac{-DN}{p}\right) = 1$ *and a certain Hilbert Class Polynomial has a root modulo* $p$.
- $\left(\frac{-DN}{p}\right) = -1$, $2 \nmid D$, $\left(\frac{-p}{q}\right) = -1$ *for all primes* $q \mid D$, *and* $\left(\frac{-p}{q}\right) = 1$ *for all primes* $q \mid N$ *such that* $q \neq 2$.
- $2 \mid D$, $\left(\frac{-DN}{p}\right) = -1$, $p \equiv \pm 3 \bmod 8$, $\left(\frac{-p}{q}\right) = -1$ *for all primes* $q \mid (D/2)$, *and* $\left(\frac{-p}{q}\right) = 1$ *for all primes* $q \mid N$.

***Corollary*** (5.2) *Let $p \mid D$ be a prime which is unramified in $\mathbf{Q}(\sqrt{d})$. Let $p_i$, $q_j$ be primes such that $D/p = \prod_i p_i$ and $N = \prod_j q_j$.*

Received by the editors November 28, 2012.
Published electronically September 4, 2013.
The author was partially supported by NSF VIGRE grant DMS-0738586 and the University of Georgia Dissertation completion award.
AMS subject classification: **11G18**, 14G35, 11G15, 11G10.
Keywords: Shimura curves, complex multiplication, modular curves, elliptic curves.

- *If $p$ is split in $\mathbf{Q}(\sqrt{d})$, then $C^D(N,d,DN) \cong X_0^D(N)$ over $\mathbf{Q}_p$ and $X_0^D(N)(\mathbf{Q}_p)$ is nonempty if and only if one of the following two cases occurs:*
  (1) $p = 2$, $p_i \equiv 3 \bmod 4$ *for all* $i$, *and* $q_j \equiv 1 \bmod 4$ *for all* $j$.
  (2) $p \equiv 1 \bmod 4$, $D = 2p$, *and* $N = 1$.
- *If $p$ is inert in $\mathbf{Q}(\sqrt{d})$ then $C^D(N,d,DN)(\mathbf{Q}_p)$ is nonempty.*

***Corollary*** (6.2) *Let $p$ be a prime dividing $N$ such that $p$ is unramified in $\mathbf{Q}(\sqrt{d})$. Then $C^D(N,d,DN)(\mathbf{Q}_p)$ is nonempty if and only if*

- *$p$ is split in $\mathbf{Q}(\sqrt{d})$ and either $D = 1$ or*
  - $p = 2$, $D = \prod_i p_i$ *with each* $p_i \equiv 3 \bmod 4$, *and* $N/p = \prod_j q_j$ *with each* $q_j \equiv 1 \bmod 4$, *or*
  - $p = 3$, $D = \prod_i p_i$ *with each* $p_i \equiv 2 \bmod 3$, *and* $N/p = \prod_j q_j$ *with each* $q_j \equiv 1 \bmod 3$, *or*
  - $TF'(D,N,1,p) > 0$ *where* $TF'$ *is as in Definition* 6.13.
- *$p$ is inert in $\mathbf{Q}(\sqrt{d})$ with $Dp = \prod_i p_i$, $N/p = \prod_j q_j$ such that one of the following holds:*
  - $p = 2$, *for all* $i$, $p_i \equiv 3 \bmod 4$ *and for all* $j$, $q_j \equiv 1 \bmod 4$;
  - $p \equiv 3 \bmod 4$, $D = 1$ *and* $N = p$ *or* $2p$.

We also give infinite families of examples of twists that have $\mathbf{Q}_v$-rational points for all places $v$ of $\mathbf{Q}$.

***Example*** (5.13) Suppose that $q$ is an odd prime and consider $X_0^{2q}(1)_{/\mathbf{Q}}$, a curve of genus $g$. Note that this curve is hyperelliptic over $\mathbf{Q}$ if and only if $q \in \{13,19,29,31,37,43,47,67,73,97,103\}$ [Ogg83, Theorem 7]. Let $p \equiv 3 \bmod 8$ be a prime such that $\left(\frac{-p}{q}\right) = -1$ and such that for all odd primes $\ell$ less than $4g^2$, $\left(\frac{-p}{\ell}\right) = -1$. Let the twist of $X_0^{2q}(1)$ by $\mathbf{Q}(\sqrt{-p})$ and $w_{2q}$ be denoted by $C^{2q}(1,-p,2q)_{/\mathbf{Q}}$. Then $C^{2q}(1,-p,2q)$ has $\mathbf{Q}_v$-rational points for all places $v$ of $\mathbf{Q}$.

If $q = 13$, then the genus of $X_0^{26}(1)$ is two. Therefore $X_0^{26}(1)$ is hyperelliptic and has the following explicit model, where $w_{2q}$ is identified with the hyperelliptic involution [GR04]:

$$y^2 = -2x^6 + 19x^4 - 24x^2 - 169.$$

Hence, an explicit model for $C^{26}(1,-p,2q)$ is given by the affine equation

$$y^2 = 2px^6 - 19px^4 + 24px^2 + 169p.$$

The primes less than 2000 satisfying the congruence conditions in the above example are $p = 67$, 163, and 1747. It can be checked that the explicit model of $C^{26}(1,-67,26)$ has at least the rational points $\left(\frac{\pm 9}{5}, \frac{\pm 10988}{125}\right)$, and that $C^{26}(1,-163,26)$ has at least the rational points $\left(\frac{\pm 67}{35}, \frac{\pm 5270116}{42875}\right)$. If $p = 1747$, a point search in `sage` [S+] failed to produce any rational points and the `TwoCoverDescent` command in `MAGMA` did not determine if $C^{26}(1,-1747,26)$ has no rational points.

https://doi.org/10.4153/CJM-2013-023-8 Published online by Cambridge University Press

***Example*** (6.16) Let $q \equiv 3 \bmod 4$ be a prime and consider the curve $X_0(q)_{/\mathbf{Q}}$. Let $p \equiv 1 \bmod 4$ be a prime such that $(\frac{p}{q}) = -1$ and let $C^1(q,p,q)_{/\mathbf{Q}}$ denote the twist of $X_0(q)$ by $\mathbf{Q}(\sqrt{p})$ and $w_q$. Then $C^1(q,p,q)$ has $\mathbf{Q}_v$-rational points for all places $v$ of $\mathbf{Q}$.

If $q = 23$, the least two primes satisfying the above are $p = 5$ and $p = 13$. Using a hyperelliptic model of the genus 2 curve $X_0(23)$ [GR91] as above, it can be verified that $C^1(23,5,23)(\mathbf{Q})$ is nonempty. Meanwhile, the `TwoCoverDescent` command in `MAGMA` determined that $C^1(23,13,23)(\mathbf{Q})$ is empty.

Finally if $\Delta < 0$ we recall the Hilbert Class Polynomial [Cox89, p. 285], which describes the unramified abelian extensions of $\mathbf{Q}(\sqrt{\Delta})$. Only for finitely many $\Delta$ is the splitting of $H_\Delta(X)$ modulo primes completely determined by congruence conditions [Cox89, Theorem 3.22]. The results of this paper allow us to find examples of primes $p$ in which congruence conditions determine the splitting of $H_\Delta(X)$ modulo $p$.

***Corollary*** (4.3) *Let $p \neq 2$ be a prime and let $N$ be a squarefree integer such that $(\frac{-N}{p}) = -1$. Let $H_\Delta(X) \in \mathbf{Z}[X]$ denote the Hilbert Class Polynomial of discriminant $\Delta$, supposing additionally that $p \nmid \operatorname{disc}(H_\Delta)$. It follows that $H_{-4N}(X)$ has a root modulo $p$ if and only if for all odd primes $q \mid N$, $(\frac{-p}{q}) = 1$.*

We proceed as follows. Always assuming a very solid background in quaternion algebras, Eichler's Embedding Theorem, Optimal Embeddings and others, we will give some theorems on embeddings of quadratic orders which may be of independent interest. Then after properly defining these Shimura curves and their Atkin–Lehner involutions, we will show how these embedding theorems can be applied to the problem of controlling *superspecial points* on Shimura curves over finite fields. The remaining sections deal with determination of $\mathbf{Q}_p$-rational points.

## 1 Simultaneous Embeddings into Eichler Orders

Let $B_D$ be the quaternion $\mathbf{Q}$-algebra of discriminant $D$ and let $B'$ be a definite quaternion $\mathbf{Q}$-algebra. Suppose that there exist $\omega_1, \omega_2 \in B'$ such that $\omega_1^2 = -q$ and $\omega_2^2 = -d$ for $q, d \in \mathbf{Z}$. Thus $\omega_1\omega_2 \in B'$ is of norm $qd$. Although $\omega_1$ and $\omega_2$ are integral, it may be the case that $\omega_1\omega_2$ is not integral. We only know that $\operatorname{tr}(\omega_1\omega_2) < 4qd$. In order for $\omega_1\omega_2$ to be integral it is necessary and sufficient that $\operatorname{tr}(\omega_1\omega_2) = \omega_1\omega_2 + \omega_2\omega_1 = s \in \mathbf{Z}$.

Now let us grant that $\operatorname{tr}(\omega_1\omega_2) \in \mathbf{Z}$. Since $\omega_1, \omega_2$, and $\omega_1\omega_2$ are integral, any order $\mathcal{O}'$ that contains $\omega_1$ and $\omega_2$ contains $\omega_1\omega_2$. Note that the $\mathbf{Z}$-module generated by $1$, $\omega_1$, $\omega_2$ and $\omega_1\omega_2$ is an order of $B'$ if and only if $\langle 1, \omega_1, \omega_2, \omega_1\omega_2\rangle$ is a basis for $B'$ over $\mathbf{Q}$. In the latter case, we can compute that the reduced discriminant of $\mathbf{Z}\oplus\mathbf{Z}\omega_1\oplus\mathbf{Z}\omega_2\oplus\mathbf{Z}\omega_1\omega_2$ is $4qd-s^2$. If $q \equiv 3 \bmod 4$, $\frac{1+\omega_1}{2}$ is integral and the reduced discriminant of $\mathbf{Z}\oplus\mathbf{Z}\frac{1+\omega_1}{2}\oplus\mathbf{Z}\omega_2\oplus\mathbf{Z}\frac{1+\omega_1}{2}\omega_2$ is $dq - (\frac{s}{2})^2$.

***Theorem 1.1*** *Fix square-free positive integers $D', N'$ such that $(D', N') = 1$ and $D'$ is the product of an odd number of primes. Fix also $m > 1$ such that $m \mid D'N'$. The following are equivalent.*

(1) *There is a definite quaternion algebra $B'$ over $\mathbf{Q}$ of discriminant $D'$, an Eichler order $\mathcal{O}'$ of level $N'$ in $B'$ and elements $\omega_1$ and $\omega_2$ contained in $\mathcal{O}'$ such that $\omega_1^2 = -1$ and $\omega_2^2 = -m$.*

(2) *There are factorizations $D' = \prod_i p_i$ and $N' = \prod_j q_j$ into distinct primes such that*
- *$m = D'N'$ or $2 \mid D'N'$ and $m = D'N'/2$;*
- *for all $i$ either $p_i = 2$ or $p_i \equiv 3 \bmod 4$;*
- *for all $j$ either $q_j = 2$ or $q_j \equiv 1 \bmod 4$.*

**Proof** If $\mathbf{Z}[\zeta_4] \hookrightarrow \mathcal{O}'$, then $p_i = 2$ or $p_i \equiv 3 \bmod 4$ and $q_j = 2$ or $q_j \equiv 1 \bmod 4$ by Eichler's Embedding Theorem.

Since $m > 1$, $\mathbf{Z}[\zeta_4] \not\hookrightarrow \mathbf{Z}[\sqrt{-m}]$ and vice versa. Therefore $\mathcal{O}' \supset \mathbf{Z} \oplus \mathbf{Z}\omega_1 \oplus \mathbf{Z}\omega_2 \oplus \mathbf{Z}\omega_1\omega_2$ and so $m \mid D'N' \mid 4m - s^2$. If $s = 0$, we have $m \mid D'N' \mid 2m$ since $D'N'$ is square-free.

If $s \neq 0$, $m \mid 4m - s^2$ implies that $m \mid s$ and $m \leq |s|$. Since $m^2 \leq s^2 < 4m$, we have $m < 4$. If $m = 2$ and $0 < s^2 < 4m = 8$ then $m \mid s$ implies that $|s| = 2$ and thus $2 \mid D'N' \mid 4$. Then since $D'N'$ square-free and $D' > 1$, $m = D' = D'N' = 2$. If $m = 3$ and $0 < s^2 < 4m = 12$ then $m \mid s$ implies that $|s| = 3$ and thus $3 \mid D'N' \mid 3$ so $m = D' = D'N' = 3$. We have thus shown $(1) \Rightarrow (2)$.

For $(2) \Rightarrow (1)$, it suffices to consider the quaternion algebra $A = \left(\frac{-1,-D'N'}{\mathbf{Q}}\right)$ with $\omega_1 = i$ and $\omega_2 = j$. It can be calculated that $A \cong B_{D'}$.

If $2 \mid D'N'$, $\left(\frac{1+\omega_1}{2}\right)\omega_2$ squares to $-D'N'/2$. Set $\omega_2' = \left(\frac{1+\omega_1}{2}\right)\omega_2$ so that the reduced discriminant of $\mathbf{Z} \oplus \mathbf{Z}\omega_1 \oplus \mathbf{Z}\omega_2' \oplus \mathbf{Z}\omega_1\omega_2'$ is $4D'N'/2 = 2D'N'$. An explicit order containing $\omega_1$ and $\omega_2$ is the "Hurwitz quaternions"

$$\mathbf{Z} \oplus \mathbf{Z}\omega_1 \oplus \mathbf{Z}\omega_2' \oplus \mathbf{Z}\frac{1 + \omega_1 + \omega_2' + \omega_1\omega_2'}{2}$$

which have reduced discriminant $D'N'$.

If $2 \nmid D'N'$ then $D'N' \equiv 3 \bmod 4$ and so $\frac{1+\omega_2}{2}$ is integral. Therefore $\mathbf{Z} \oplus \mathbf{Z}\omega_1 \oplus \mathbf{Z}\left(\frac{1+\omega_2}{2}\right) \oplus \mathbf{Z}\omega_1\left(\frac{1+\omega_2}{2}\right)$ is an order and has reduced discriminant $D'N'$. ■

***Corollary 1.2*** *Let $B'$ be a definite quaternion algebra of discriminant $D'$, and let $\mathcal{O}'$ be an Eichler order of $B'$ of squarefree level $N'$ such that $\mathbf{Z}[\zeta_4] \hookrightarrow \mathcal{O}'$. If $m \mid D'N'$ and $m \neq 1$, then $\mathbf{Z}[\sqrt{-m}] \hookrightarrow \mathcal{O}'$ if and only if $m = D'N'$ or $2 \mid D'N'$ and $m = D'N'/2$.*

We now turn our attention to simultaneous embeddings of $\mathbf{Z}[\zeta_6]$ and $\mathbf{Z}[\sqrt{-m}]$.

***Theorem 1.3*** *Fix squarefree positive integers $D', N'$ such that $(D', N') = 1$ and $D'$ is the product of an odd number of primes. Fix also $m \mid D'N'$ such that $m > 1$, $m \neq 3$. The following are equivalent.*

(1) *There is a definite quaternion algebra $B'$ of discriminant $D'$, an Eichler order $\mathcal{O}'$ of level $N'$ in $B'$ and $\frac{1+\omega_1}{2}, \omega_2 \in \mathcal{O}'$ such that $\omega_1^2 = -3$ and $\omega_2^2 = -m$.*

(2) *There are factorizations $D' = \prod_i p_i$, $N' = \prod_j q_j$ into distinct primes such that*
- *$m = D'N'$, or $3 \mid D'N'$ and $m = D'N'/3$;*
- *for all $i$ either $p_i = 3$ or $p_i \equiv 2 \bmod 3$;*
- *for all $j$ either $q_j = 3$ or $q_j \equiv 1 \bmod 3$.*

https://doi.org/10.4153/CJM-2013-023-8 Published online by Cambridge University Press

**Proof** This is proved with the same ideas as Theorem 1.1. ■

***Corollary 1.4*** *Let $B'$ be a definite quaternion algebra of discriminant $D'$ and let $\mathcal{O}'$ be an Eichler order of $B'$ of squarefree level $N'$ such that $\mathbf{Z}[\zeta_6] \hookrightarrow \mathcal{O}'$. If $m \mid D'N'$ and $m \neq 1, 3$, then $\mathbf{Z}[\sqrt{-m}] \hookrightarrow \mathcal{O}'$ if and only if $m = D'N'$ or $D'N'/3$.*

We state one final theorem on simultaneous embeddings without proof.

***Theorem 1.5*** *Recall that $D$ is the squarefree product of an even number of primes, $N$ a squarefree integer coprime to $D$, and $p$ a prime not dividing $DN$. Let $B' = B_{Dp}$ and let $m \mid DN$ be an integer greater than one. We have the following equivalences.*

(1) *Suppose that $2 \nmid DNp$. There is an Eichler order $\mathcal{O}'$ of level $N$ in $B'$ and embeddings $\psi_1 \colon \mathbf{Z}[\sqrt{-p}] \hookrightarrow \mathcal{O}'$ and $\psi_2 \colon \mathbf{Z}[\sqrt{-m}] \hookrightarrow \mathcal{O}'$ if and only if $m = DN$, $(\frac{-p}{q}) = -1$ for all primes $q \mid D$, $(\frac{-p}{q}) = 1$ for all primes $q \mid N$, and $(\frac{-DN}{p}) = -1$.*
(2) *Suppose that $2 \mid N$. There is an Eichler order $\mathcal{O}'$ of level $N$ in $B'$ and embeddings $\psi_1 \colon \mathbf{Z}[\sqrt{-p}] \hookrightarrow \mathcal{O}'$ and $\psi_2 \colon \mathbf{Z}[\sqrt{-m}] \hookrightarrow \mathcal{O}'$ if and only if one of the following two cases occurs:*
   - *$m = DN$, $(\frac{-p}{q}) = -1$ for all primes $q \mid D$, $(\frac{-p}{q}) = 1$ for all primes $q \mid (N/2)$, and $(\frac{-DN}{p}) = -1$.*
   - *$m = DN/2$, $(\frac{-p}{q}) = -1$ for all primes $q \mid D$, $(\frac{-p}{q}) = 1$ for all primes $q \mid (N/2)$, and $(\frac{-DN/2}{p}) = -1$.*
(3) *Suppose $2 \mid D$ and $(\frac{-DN}{p}) = -1$. There is an Eichler order $\mathcal{O}'$ of level $N$ in $B'$ and embeddings $\psi_1 \colon \mathbf{Z}[\sqrt{-p}] \hookrightarrow \mathcal{O}'$ and $\psi_2 \colon \mathbf{Z}[\sqrt{-m}] \hookrightarrow \mathcal{O}'$ if and only if $m = DN$, $(\frac{-p}{q}) = -1$ for all primes $q \mid (D/2)$, $p \not\equiv 7 \bmod 8$, and $(\frac{-p}{q}) = 1$ for all primes $q \mid N$.*
(4) *Suppose $2 \mid D$ and $(\frac{-DN}{p}) = 1$. There is an Eichler order $\mathcal{O}'$ of level $N$ in $B'$ and embeddings $\psi_1 \colon \mathbf{Z}[\sqrt{-p}] \hookrightarrow \mathcal{O}'$ and $\psi_2 \colon \mathbf{Z}[\sqrt{-m}] \hookrightarrow \mathcal{O}'$ if and only if $m = DN/2$, $DN \equiv 2, 6$, or $10 \bmod 16$, $(\frac{-p}{q}) = -1$ for all primes $q \mid (D/2)$, $p \not\equiv 7 \bmod 8$, and $(\frac{-p}{q}) = 1$ for all primes $q \mid N$.*
(5) *Suppose that $p = 2$. There is an Eichler order $\mathcal{O}'$ of level $N$ in $B'$ and embeddings $\psi_1 \colon \mathbf{Z}[\sqrt{-p}] \hookrightarrow \mathcal{O}'$ and $\psi_2 \colon \mathbf{Z}[\sqrt{-m}] \hookrightarrow \mathcal{O}'$ if and only if $m = DN \equiv \pm 3 \bmod 8$, $(\frac{-2}{q}) = -1$ for all primes $q \mid D$, and $(\frac{-2}{q}) = 1$ for all primes $q \mid N$.*

Finally for convenience we record the following. Here $\{\frac{\cdot}{p}\}$ is the Eichler Symbol [Cla03, p. 25], while $h(\Delta)$, $f(\Delta)$, and $w(\Delta)$ are respectively the class number, the conductor and the number of units of the quadratic ring over $\mathbf{Z}$ of discriminant $\Delta$.

***Definition 1.6*** For square-free coprime integers $D$ and $N$ and some integer $\Delta \equiv 0, 1 \bmod 4$, we define the quantity

$$e_{D,N}(\Delta) := h(\Delta) \prod_{p \mid D} \Big(1 - \Big\{\frac{\Delta}{p}\Big\}\Big) \prod_{q \mid N} \Big(1 + \Big\{\frac{\Delta}{p}\Big\}\Big).$$

https://doi.org/10.4153/CJM-2013-023-8 Published online by Cambridge University Press

## 2 Shimura Curves

We begin with the definition of a Shimura curve as a coarse moduli scheme, presuming some familiarity with abelian schemes and moduli spaces. As always, we will assume that $D$ is the squarefree product of an even number of primes and that $N$ is squarefree and coprime to $D$.

***Definition 2.1*** Fix a scheme $S$ and an Eichler order $\mathcal{O}$ of level $N$ in $B_D$. By $X_0^D(N)_S$ we will denote the coarse moduli scheme parametrizing pairs $(A,\iota)$ over $S$-schemes $T$, where $A_{/T}$ is an abelian scheme and $\iota\colon \mathcal{O} \hookrightarrow \mathrm{End}_T(A)$ is an optimal embedding such that the pair $(A,\iota)$ is *mixed* in the sense of Ribet [Rib89].

It is well-known that this scheme is smooth if $p \nmid DN$ and $S$ is an $\mathbb{F}_p$-scheme.

***Definition 2.2*** Let $\beta_m$ denote a generator of the unique two-sided integral ideal of $\mathcal{O}$ of norm $m \mid DN$. There is an automorphism $w_m$ of $X_0^D(N)_S$ induced by the bijection $[(A,\iota)] \mapsto \big[\big(A, (\iota(\beta_m))^{-1}\iota(\cdot)\iota(\beta_m)\big)\big]$.

Note that the above makes sense because any generator of the unique two-sided integral ideal of $\mathcal{O}$ of norm $m$ is of the form $\beta_m u$ where $u$ is a unit of $\mathcal{O}$. Note that the group of all such $w_m$ is abelian because the group of two-sided integral ideals is abelian. We call the group of all such $w_m$ the *Atkin–Lehner group* $W$ and note there is an isomorphism $(\mathbf{Z}/2\mathbf{Z})^{\{p \mid DN \text{ prime}\}} \cong W$ by $m \mid DN \leftrightarrow \{p \mid m\} \mapsto w_m$.

***Definition 2.3*** We say that $(A,\iota)$ is fixed by $w_m$ if

$$[(A,\iota)] = \big[\big(A, (\iota(\beta_m))^{-1}\iota(\cdot)\iota(\beta_m)\big)\big],$$

where $\beta_m$ is a generator of the unique integral two-sided ideal of $\mathcal{O}$ of norm $m$.

***Definition 2.4*** Let $D, N$ be positive square-free integers and let $\mathcal{O}$ be an Eichler order of level $N$ in $B_D$. Define $\mathrm{Pic}(D,N)$ to be the set of isomorphism classes of right $\mathcal{O}$-ideals.

There exist formulas for the size of $\mathrm{Pic}(D,N)$ depending only on $D$ and $N$ [Vig80, Corollaire III.5.7(1)], [Piz76, Theorem 16]. Hence this definition makes sense even if $B_D$ is definite.

***Definition 2.5*** The *length* of an element $[I]$ of $\mathrm{Pic}(D,N)$ is

$$\ell([I]) := \#\big(\mathcal{O}_l(I)^\times/\pm 1\big),$$

where $\mathcal{O}_l(I)$ denotes the left order of the right ideal $I$.

We shall use this to make sense of the reduction $X_0^D(N)_{\mathbb{F}_p}$ when $p \mid D$. We say a normal, proper, flat relative curve $M_{/\mathbf{Z}_p}$ is a *Mumford curve* if each component of the special fiber is isomorphic over $\mathbb{F}_p$ to $\mathbb{P}^1_{\mathbb{F}_p}$ and the intersection points are all $\mathbb{F}_p$-rational double points.

***Definition 2.6*** Let $\mathbf{Z}_{p^2}$ denote the unique irreducible unramified degree two ring extension of $\mathbf{Z}_p$.

***Theorem 2.7*** ([Cla03, Corollary 78]) *Let $p \mid D$. There is a Mumford curve $M_{(D,N)/\mathbf{Z}_p}$ whose components over $\mathbb{F}_p$ are in bijection with two copies of $\operatorname{Pic}(D/p, N)$ interchanged by an involution $a_p$ of $M_{(D,N)}$, whose intersection points are in bijection with $\operatorname{Pic}(D/p, Np)$, and whose dual graph is bipartite. Moreover let $x$ be an intersection point between two components of $(M_{(D,N)})_{\mathbb{F}_p}$ corresponding to $[I] \in \operatorname{Pic}(D/p, Np)$. Then the following holds:*

$$\widehat{\mathcal{O}_{M_{(D,N)},x}} \cong \mathbf{Z}_p[[X, Y]]/(XY - p^{\ell([I])}).$$

*There is an isomorphism $\phi\colon X_0^D(N)_{\mathbf{Z}_{p^2}} \xrightarrow{\sim} (M_{(D,N)})_{\mathbf{Z}_{p^2}}$ such that $\phi w_p = a_p \phi$. If $\langle\sigma\rangle = \operatorname{Aut}_{\mathbf{Z}_p}(\mathbf{Z}_{p^2})$, this isomorphism realizes $X_0^D(N)_{\mathbf{Z}_p}$ as the étale quotient of $(M_{(D,N)})_{\mathbf{Z}_{p^2}}$ by the action of $\sigma a_p$.*

***Theorem 2.8*** *If $p \mid N$ and $T$ is an $\mathbb{F}_p$-scheme, then there exists a closed embedding $c\colon X_0^D(N/p)_T \to X_0^D(N)_T$ satisfying the following.*

*Let $S = \operatorname{Spec}(R)$ be a flat $\mathbf{Z}_{(p)}$-scheme. If $T$ is an $S$-scheme and if $\Phi\colon X_0^D(N)_T \to X_0^D(N/p)_T$ is the forgetful map $X_0^D(N/p) \times_{X_0^D(1)} X_0^D(p) \to X_0^D(N/p)$, then $\Phi c$ is the identity and $\Phi w_p c$ is the Frobenius map $(A, \iota) \mapsto (A^{(p)}, \mathrm{Frob}_{p,*}\,\iota)$ (see Definition 3.2). Moreover, $X_0^D(N)_T$ fits into the diagram*

$$\begin{tikzcd}
X_0^D(N/p)_T \arrow[dd, "\mathrm{id}"'] \arrow[dr, "c"] & & X_0^D(N/p)_T \arrow[dl, "w_p c"'] \arrow[dd, "\mathrm{id}"] \\
& X_0^D(N)_T \arrow[dl, "\Phi"'] \arrow[dr, "\Phi w_p"] & \\
X_0^D(N/p)_T & & X_0^D(N/p)_T.
\end{tikzcd}$$

*If $t$ is a closed point of $T$ such that $k(t) = \overline{k(t)}$, the intersection of $c(X_0^D(N/p)(k(t)))$ and $w_p c(X_0^D(N/p)(k(t)))$ is precisely the set of superspecial points (in the sense of Definition 2.12), which are in bijection with $\operatorname{Pic}(Dp, N/p)$. For each superspecial point $x$ over $t$ corresponding to $[I] \in \operatorname{Pic}(Dp, N/p)$, the completion of the strict henselization of the local ring of $X_0^D(N)$ at $x$ is isomorphic to $R \otimes W(\overline{\mathbb{F}}_p)[[X, Y]]/(XY - p^{\ell([I])})$.*

**Proof** The bijection between superspecial points and $\operatorname{Pic}(Dp, N/p)$ is from Theorem 2.16 below. The remainder of the result in the case of $\mathbf{Z}_{(p)}$ was first written down by Helm [Hel07, Theorem 10.3]. ■

***Lemma 2.9*** ([Mol12, Theorem 1.1]) *The components and singular points of the $\overline{\mathbb{F}}_p$ special fiber can be put into the following $W$-equivariant bijections.*

| | *Components* | *Intersection Points* |
|---|---|---|
| $p \mid D$ | $\mathrm{Pic}(D/p, N) \coprod \mathrm{Pic}(D/p, N)$ | $\mathrm{Pic}(D/p, Np)$ |
| $p \mid N$ | $\mathrm{Pic}(D, N/p) \coprod \mathrm{Pic}(D, N/p)$ | $\mathrm{Pic}(Dp, N/p)$ |

*If $p \mid D$, the bijection of a set of components with $\mathrm{Pic}(D/p, N)$ is $W/\langle w_p\rangle$-equivariant with $w_p$ interchanging each. If $p \nmid DN$, the superspecial points of $X_0^D(N)_{\overline{\mathbb{F}}_p}$ can be put into $W$-equivariant bijection with $\mathrm{Pic}(Dp, N)$ via the embedding $c\colon X_0^D(N)_{\overline{\mathbb{F}}_p} \to X_0^D(Np)_{\overline{\mathbb{F}}_p}$.*

## 2.1 Superspecial Surfaces

Fix a prime number $p$ and a maximal order $\mathcal{S}$ in the quaternion algebra $B_p$ over $\mathbf{Q}$ ramified precisely at $p$ and $\infty$. By a theorem of Deuring, there is a supersingular elliptic curve $E$ over the algebraic closure $\mathbb{F}$ of $\mathbb{F}_p$ such that $\mathrm{End}_{\mathbb{F}}(E) \cong \mathcal{S}$ [Rib89, p. 23].

***Definition 2.10*** Fix $E_{/\mathbb{F}}$, a *supersingular* elliptic curve with $\mathrm{End}_{\mathbb{F}}(E) \cong \mathcal{S}$. We say that an abelian variety $A_{/\mathbb{F}}$ is supersingular when there is an isogeny $A \to E^{\dim(A)}$.

***Lemma 2.11*** ([Cla03, Theorem 68], [Rib89, Lemma 4.1]) *If $A_{/\mathbb{F}_q}$ is an abelian surface over a finite field and $B_D \hookrightarrow \mathrm{End}^0_{\mathbb{F}_q}(A)$, $A$ is isogenous over $\mathbb{F}_q$ to the square of an elliptic curve $(E_0)_{\mathbb{F}_q}$. Moreover if $p \mid D$, this elliptic curve must be supersingular.*

***Definition 2.12*** We say that an abelian surface $A_{/\mathbb{F}}$ is *superspecial* if $A \cong E_i \times E_j$ with $E_i, E_j$ supersingular elliptic curves over $\mathbb{F}$.

***Lemma 2.13*** ([Rib89, p. 21–22]) *Suppose that $A$ is a supersingular abelian $\mathcal{O}$-surface over $\mathbb{F}$ with $p \nmid D$. Then $A$ is superspecial.*

***Theorem 2.14*** *If $(A_{/k}, \iota)$ is an ordinary QM-abelian surface over a finite field $k$, then there exist ordinary elliptic curves $E_0, E_0'$ over $k$ such that $A \cong E_0 \times E_0'$. If $m > 1$, then $(A, \iota)$ is $w_m$-fixed (see Definition 2.3) if and only if $\mathrm{End}_k(E_0) \cong_k \mathrm{End}_k(E_0')$ and $\mathrm{End}_k(E_0)$ is isomorphic to one of $\mathbf{Z}[\sqrt{-m}]$ or $\mathbf{Z}[\frac{1+\sqrt{-m}}{2}]$.*

**Proof** The first part of the statement is part of a more general theorem of Kani [Kan11, Theorem 2], who calls ordinary elliptic curves CM. For the second part, note that $(A_{/S}, \iota)$ is $w_m$-fixed if and only if $R = \mathbf{Z}[\sqrt{-m}]$ (or $\mathbf{Z}[\zeta_4]$ if $m = 2$) embeds into the commutant of $\iota(\mathcal{O})$ in $\mathrm{End}_S(A)$.

Let $k$ be a finite field, $A_{/k}$ be ordinary, and $(A, \iota)$ be $w_m$-fixed. Also let $W(k)$ denote the Witt vectors of $k$ [Neu99, Section II.4], which in this case are just a finite étale extension of $\mathbf{Z}_p$. Then there is a canonical choice of an abelian scheme $\mathcal{A}_{W(k)}$ with an isomorphism $f\colon \mathrm{End}_k(A) \xrightarrow{\sim} \mathrm{End}_{W(k)}(\mathcal{A})$ [Mes72, Theorem V.3.3]. Therefore the Serre–Tate canonical lift $(\mathcal{A}, f \circ \iota)$ is a QM-abelian surface. Therefore so is $\mathcal{A}_{\mathbf{C}}$ (the choice of embedding $W(k) \hookrightarrow \mathbf{C}$ does not change the isomorphism class of $\mathcal{A}_{\mathbf{C}}$ [Del69, 7. Théorème]), and there is an embedding of $R$ into $\mathrm{End}_{f(\iota(\mathcal{O}))}(\mathcal{A}_{\mathbf{C}})$. Then we can find both an optimal embedding $\varphi\colon R' \hookrightarrow \mathcal{O}$ for some imaginary quadratic

https://doi.org/10.4153/CJM-2013-023-8 Published online by Cambridge University Press

order $R' \supset R$ and an isomorphism $\mathcal{A}_{\mathbf{C}} \cong E_1 \times E_2$ where the $E_i$'s have CM by $R'$ and $f \circ \iota$ is given by $\varphi$ [Mol12, Section 2.2].

Now let $K := W(k) \otimes \mathbf{Q}$, which must therefore be a finite unramified extension of $\mathbf{Q}_p$. We can then show that $\mathcal{A}_K \cong E_1' \times E_2'$ where $E_i' \otimes \mathbf{C} \cong E_i$ [Kan11, Lemma 60]. Moreover, each $E_i'$ has CM by $R'$ since $\mathcal{O} \hookrightarrow \mathrm{End}_K(\mathcal{A}_K)$ and we have $\varphi\colon R' \hookrightarrow \mathcal{O}$. Now, if $V$ is an abelian variety over $K$, let $\mathfrak{N}(V)$ denote its Néron model over $W(k)$ [BLR90, Definition I.2.1]. It follows that since $\mathcal{A}$ is an abelian scheme, it is the Néron model of its generic fiber [BLR90, Proposition I.2.8], and thus

$$\mathcal{A} \cong \mathfrak{N}(\mathcal{A}_K) \cong \mathfrak{N}(E_1' \times E_2') \cong \mathfrak{N}(E_1') \times \mathfrak{N}(E_2'). \qquad \blacksquare$$

***Theorem 2.15*** ([Shi79, Theorem 3.5]) *Let $E_{/\mathbb{F}}$ be as in Definition 2.10 and let $A_{/\mathbb{F}}$ be an abelian surface isomorphic to the product of any two supersingular elliptic curves. Then $A \cong E \times E$.*

Recall that $\mathcal{S}$ is a maximal order in $B_p$ and $p \mid D$. Recall also that an $(\mathcal{O}, \mathcal{S})$-bimodule is a left $\mathcal{O}$-module $M$ which is also a right $\mathcal{S}$-module such that if $x \in \mathcal{O}$, $y \in \mathcal{S}$, and $m \in M$, then $(xm)y = x(my)$. This implies that we have homomorphisms $\mathcal{O} \to \mathrm{End}_{\mathcal{S}}(M)$ and $\mathcal{S}^{\mathrm{op}} \to \mathrm{End}_{\mathcal{O}}(M)$. If both of these homomorphisms are optimal embeddings we say that $M$ is an *optimal* $(\mathcal{O}, \mathcal{S})$ bimodule.

***Theorem 2.16*** ([Rib89, p. 38]) *Suppose that $\mathcal{O}$ is an Eichler order of square-free level $N$ in an indefinite quaternion algebra $B$ of discriminant $D$ with $(D, N) = 1$. There is a bijection between the following sets:*

- *superspecial $\mathcal{O}$-abelian surfaces $(A, \iota)_{/\mathbb{F}}$ up to isomorphism;*
- *$\mathbf{Z}$-rank 8 optimal $(\mathcal{O}, \mathcal{S})$ bimodules up to isomorphism.*

***Lemma 2.17*** *Let $q \mid DN$ and let $\mathfrak{Q}$ denote the unique two-sided integral ideal of norm $q$ in $\mathcal{O}$. Under the bijection in Theorem 2.16, the action of $w_q$ described in Definition 2.2 corresponds to the action $M \mapsto \mathfrak{Q} \otimes_{\mathcal{O}} M$.*

**Proof** The bimodule $\mathfrak{Q} \otimes_{\mathcal{O}} M$ is isomorphic to $\beta_q M$ as an $(\mathcal{O}, \mathcal{S})$-bimodule, since $\mathfrak{Q} = \beta_q \mathcal{O} = \mathcal{O} \beta_q$. Therefore to get an action of $\mathcal{O}$ on $\beta_q M$, we must pre-compose by $\beta_q^{-1}$ and post-compose by $\beta_q$. $\blacksquare$

***Definition 2.18*** Let $\mathcal{O}, \mathcal{S}$ be Eichler orders in a quaternion algebra over a number field $K$. We say that two $(\mathcal{O}, \mathcal{S})$-bimodules $M, N$ are *locally isomorphic* if for all places $v$ of $K$, $M_v \cong N_v$ as $(\mathcal{O}_v, \mathcal{S}_v)$-bimodules.

***Theorem 2.19*** *Let $\mathcal{O}, \mathcal{S}$ be as in Theorem 2.16 and fix an $(\mathcal{O}, \mathcal{S})$-bimodule $M$. Then $\Lambda := \mathrm{End}_{\mathcal{O},\mathcal{S}}(M)$ is an Eichler order in either $B_{Dp}$ if $p \nmid D$ or $B_{D/p}$ if $p \mid D$. Moreover, if we fix a bimodule $M$, there is a bijection between the following two sets*

- *$(\mathcal{O}, \mathcal{S})$-bimodules $N$ locally isomorphic to $M$ up to isomorphism, and*
- *rank one projective right $\Lambda$ modules up to isomorphism.*

*Let $q \neq p$ be prime. This bijection sends the action described in Lemma 2.17 to the action $[I] \mapsto [I\mathfrak{Q}_\Lambda]$, where $\mathfrak{Q}_\Lambda$ is the unique two-sided ideal of norm $q$ of $\Lambda$.*

**Proof** The bijection in the case where $\mathcal{O}$ is a maximal order is a theorem of Ribet [Rib89, Theorem 2.3]. The extension to Eichler orders is due to Molina [Mol12, Remark 4.11]. His proof depends on showing that $\mathrm{Hom}_{\mathcal{O},\mathcal{S}}(N, \mathfrak{Q}_{\mathcal{O}} \otimes N)$ is $\mathfrak{Q}_\Lambda$. ■

This allows us to compute dual graphs of special fibers using MAGMA code that can be found at http://stankewicz.net/SpecialFiber.html.

***Definition 2.20*** Retaining the notation of Theorem 2.19, the action $[I] \mapsto [I\mathfrak{Q}_\Lambda]$ will be referred to as $w_q$.

***Corollary 2.21*** *Let $m > 1$. A superspecial $\mathcal{O}$-abelian surface $(A, \iota)$ with corresponding bimodule $M$ is fixed under the action of $w_m$ if and only if there is an embedding of $\mathbf{Z}[\sqrt{-m}]$ (or $\mathbf{Z}[\zeta_4]$ if $m = 2$) into $\Lambda = \mathrm{End}_{\mathcal{O},\mathcal{S}}(M)$.*

**Proof** By Theorem 2.19, $(A, \iota)$ is fixed by the action of $w_m$ if and only if

$$[\textstyle\prod_{q\,|\,m} \mathfrak{Q}_\Lambda] = [1],$$

which is to say if and only if the unique two-sided ideal of norm $m$ is principal. Therefore, there is a fixed point if and only if there is an element $\gamma$ of $\mathrm{End}_{\mathcal{O},\mathcal{S}}(M)$ that can serve as the principal generator. That is, $\gamma^2\Lambda = m\Lambda$ so there is a unit $u$ of $\Lambda$ such that $\gamma^2 = um$. This now follows from work of Kurihara [Kur79, Proposition 4-4]. ■

***Lemma 2.22*** *If $(A, \iota)$ is a superspecial abelian $\mathcal{O}$-surface over $\mathbb{F}$, then $w_p(A, \iota)$ (in the sense of Theorem 2.19) is its $\mathbb{F}_{p^2}/\mathbb{F}_p$-Galois conjugate. Equivalently, if $P\colon \mathrm{Spec}(\mathbb{F}) \to X_0^D(N)$ corresponds to a superspecial abelian $\mathcal{O}$-surface $(A, \iota)$ over $\mathbb{F}$ and $\phi_1\colon \mathbb{F} \to \mathbb{F}$ is the $p$-th power map, the following diagram commutes.*

$$\begin{tikzcd} \mathrm{Spec}(\mathbb{F}) \arrow[r, "P"] \arrow[d, "\phi_1^*"] & X_0^D(N) \arrow[d, "w_p"] \\ \mathrm{Spec}(\mathbb{F}) \arrow[r, "P"] & X_0^D(N). \end{tikzcd}$$

**Proof** If $p\,|\,D$, then for *all* points $P\colon \mathrm{Spec}(\mathbb{F}) \to X_0^D(N)$, the square of this lemma commutes, by Theorem 2.7. If $p\,|\,N$ and $P\colon \mathrm{Spec}(\mathbb{F}) \to X_0^D(N)$ corresponds to an abelian $\mathcal{O}$-surface $(A_{\mathbb{F}}, \iota)$, then by Theorem 2.8, $w_pP$ corresponds to $(A^{(p)}, \mathrm{Frob}_{p,*}\,\iota)$. By Lemma 3.3, this corresponds to the point $P\phi_1^*$. If $p \nmid DN$, we can reduce to the case $p\,|\,N$ via the embedding $c\colon X_0^D(N)_{\mathbb{F}} \to X_0^D(Np)_{\mathbb{F}}$. ■

***Definition 2.23*** Let $(A, \iota)$ be a superspecial $\mathcal{O}$-abelian surface over $\mathbb{F}$ with corresponding bimodule $M$. The *length* of $(A, \iota)$ is $\#\big(\mathrm{End}_{(\mathcal{O},\mathcal{S})}(M)^\times/\pm 1\big)$.

Note that $\mathrm{End}_{(\mathcal{O},\mathcal{S})}(M) \cong \mathrm{End}_{\mathbb{F}}(A, \iota)$ [Mol12, equation 3.5]. Therefore if $(A, \iota)$ corresponds to a point of $X_0^D(N)(\mathbb{F})$ then this definition agrees with Definition 2.5.

***Corollary 2.24*** *Let $(A,\iota)$ be a mixed superspecial $\mathcal{O}$-abelian surface with corresponding bimodule $M$ and whose length is divisible by three. Let $N'$ be the level of $\mathcal{O}' = \mathrm{End}_{(\mathcal{O},\mathcal{S})}(M)$ and $D'$ the discriminant of $\mathcal{O}' \otimes \mathbf{Q}$. Then for all $p \mid D'$, $p = 3$ or $p \equiv 2 \bmod 3$, and for all $q \mid N'$, $q = 3$ or $q \equiv 1 \bmod 3$. Moreover, $(A,\iota)$ is fixed by $w_m$ if and only if $m = 1, 3, D'N'$, or $D'N'/3$ (if $3 \mid D'N'$).*

**Proof** Unless $D' = 2, 3$ and $N' = 1$, the only possible such length is three [Vig80, Proposition V.3.1]. In each of those cases, if $p \mid D'$ then $p = 2$ or $p = 3$. If $(D', N') \neq (2,1), (3,1)$, the length of $(A,\iota)$ is three if and only if $\mathbf{Z}[\zeta_6] \hookrightarrow \mathcal{O}'$, and the first part of our statement holds by Eichler's Embedding Theorem.

Recall now that any $(A,\iota)$ is fixed by $w_1$. If $\mathbf{Z}[\zeta_6]$ embeds into $\mathcal{O}'$, note that $\mathbf{Z}[\sqrt{-3}] \subset \mathbf{Z}[\zeta_6] \hookrightarrow \mathcal{O}'$, so $(A,\iota)$ is fixed by $w_3$ if $3 \mid D'N'$. Now suppose that $m \neq 3$, so $\mathbf{Z}[\zeta_6]$ does not contain $\mathbf{Z}[\sqrt{-m}]$ and vice versa. In that case we have simultaneous embeddings if and only if $m = D'N'$ or if $3 \mid D'N'$ and $m = D'N'/3$, by Theorem 1.3. ■

The proofs of the following are similar.

***Corollary 2.25*** *Let $(A,\iota)$ be a mixed superspecial $\mathcal{O}$-abelian surface with corresponding bimodule $M$ and whose length is even. Let $N'$ be the level of $\mathcal{O}' = \mathrm{End}_{(\mathcal{O},\mathcal{S})}(M)$ and $D'$ the discriminant of $\mathcal{O}' \otimes \mathbf{Q}$. Then for all $p \mid D'$, $p = 2$ or $p \equiv 3 \bmod 4$, and for all $q \mid N'$, $q = 2$ or $q \equiv 1 \bmod 4$. Moreover, $(A',\iota')$ is fixed by $w_m$ if and only if $m = 1, 2, D'N'$, or $D'N'/2$ (if $2 \mid D'N'$).*

***Corollary 2.26*** *Let $\mathcal{O}$ be an Eichler order of square-free level $N$ in $B_D$ where $D$ is the square-free product of an even number of primes and $N$ is coprime to $D$. Let $m \mid DN$ and let $p$ be a prime not dividing $DN$. If $p = 2$ there is a mixed superspecial abelian $\mathcal{O}$ surface $(A_{\mathbb{F}_p},\iota)$ fixed by $w_m$ if and only if one of the following occurs:*

(1) *$m = DN$, $q \equiv 3 \bmod 4$ for all $q \mid D$, and $q \equiv 1 \bmod 4$ for all $q \mid N$.*

(2) *$m = DN \equiv \pm 3 \bmod 8$, $\left(\frac{-2}{q}\right) = -1$ for all primes $q \mid D$, and $\left(\frac{-2}{q}\right) = 1$ for all primes $q \mid N$.*

*If $p \neq 2$, there is a mixed superspecial abelian $\mathcal{O}$ surface $(A_{\mathbb{F}_p},\iota)$ fixed by $w_m$ if and only if one of the following occurs:*

(3) *$2 \nmid D$, $m = DN$, $\left(\frac{-DN}{p}\right) = -1$, $\left(\frac{-p}{q}\right) = -1$ for all $q \mid D$, and $\left(\frac{-p}{q}\right) = 1$ for all $q \mid N$ such that $q \neq 2$.*

(4) *$2 \mid N$, $m = DN/2$, $\left(\frac{-DN/2}{p}\right) = -1$, $\left(\frac{-p}{q}\right) = -1$ for all $q \mid D$, and $\left(\frac{-p}{q}\right) = 1$ for all $q \mid N$ such that $q \neq 2$.*

(5) *$2 \mid D$, $m = DN$, $p \equiv \pm 3 \bmod 8$, $\left(\frac{-DN}{p}\right) = -1$, $\left(\frac{-p}{q}\right) = -1$ for all $q \mid (D/2)$, and $\left(\frac{-p}{q}\right) = 1$ for all $q \mid N$.*

(6) *$2 \mid D$, $m = DN/2$, $DN \equiv 2, 6, 10 \bmod 16$, $p \equiv \pm 3 \bmod 8$, $\left(\frac{-DN/2}{p}\right) = -1$, $\left(\frac{-p}{q}\right) = -1$ for all $q \mid D$, and $\left(\frac{-p}{q}\right) = 1$ for all $q \mid N$.*

## 3 Local Points at Good Primes

Throughout this section we will fix $D$ the discriminant of an indefinite quaternion $\mathbf{Q}$-algebra, $N$ a square-free integer coprime to $D$, an integer $m \mid DN$ and a prime $p \nmid DN$.

Recall that $X_0^D(N)_{/\mathbf{Z}_p}$ has a smooth special fiber by Theorem 2.8. Let $w_m$ be as in Definition 2.2. Let $\langle\sigma\rangle = \mathrm{Aut}_{\mathbf{Z}_p}(\mathbf{Z}_{p^2})$ and let $\mathcal{Z}_{/\mathbf{Z}_p}$ denote the quotient of $X_0^D(N)_{\mathbf{Z}_{p^2}}$ by the action of $w_m\sigma$.

If $p$ is split in $\mathbf{Q}(\sqrt{d})$, then $X_0^D(N)$ is isomorphic to $C^D(N,d,m)$ over $\mathbf{Q}_p$. We can then obtain results on local points without appealing to $\mathcal{Z}$.

If $p$ is inert in $\mathbf{Q}(\sqrt{d})$ and $C^D(N,d,m)_{/\mathbf{Q}}$ is the twist of $X_0^D(N)_{/\mathbf{Q}}$ by $w_m$ and $\mathbf{Q}(\sqrt{d})$ then $\mathcal{Z}$ is a $\mathbf{Z}_p$-model for $C^D(N,d,m)_{\mathbf{Q}_p}$. By étale base change [Liu02, Proposition 10.1.21(c)], $\mathcal{Z}_{\mathbb{F}_p}$ is also smooth.

***Theorem 3.1*** *Suppose that $p$ is unramified in $\mathbf{Q}(\sqrt{d})$ and $p > 4g^2$. It follows that $C^D(N,d,m)(\mathbf{Q}_p) \neq \varnothing$.*

**Proof** This is an easy application of Weil's Bounds and Hensel's Lemma. ∎

For $p < 4g^2$, we must use another technique. In the split case we use Shimura's construction of the zeta function of $X_0^D(N)_{\mathbb{F}_p}$ using Hecke operators to give an exact formula for the size of $X_0^D(N)(\mathbb{F}_p)$. In the inert case, we give a partial answer in terms of superspecial points. In the following we assume familiarity with the Frobenius and Verschiebung isogenies.

***Definition 3.2*** Let $S$ be an $\mathbb{F}_p$-scheme and let $(A,\iota)$ be an abelian $\mathcal{O}$-surface. By $\mathrm{Frob}_{p^r,*}\,\iota$ we denote the unique optimal embedding $\mathcal{O} \hookrightarrow \mathrm{End}_S(A^{(p^r)})$ such that for all $\alpha \in \mathcal{O}$ the following commutes.

$$\begin{tikzcd} A \arrow[r, "\iota(\alpha)"] \arrow[d, "\mathrm{Frob}_{p^r}"'] & A \arrow[d, "\mathrm{Frob}_{p^r}"] \\ A^{(p^r)} \arrow[r, "\mathrm{Frob}_{p^r,*}\,\iota(\alpha)"] & A^{(p^r)}. \end{tikzcd}$$

***Lemma 3.3*** *Let $S = \mathrm{Spec}(\overline{\mathbb{F}}_p)$ and $\phi_r\colon S \to S$ be the morphism given by the $p^r$-th power map. Let $(A_{/S},\iota)$ be a QM-abelian surface corresponding to a point $P\colon S \to X_0^D(N)_S$. Let $P \circ \phi_r\colon S \to S \to X_0^D(N)_S$ denote the Galois conjugate point. Then the QM-abelian surface corresponding to $P \circ \phi_r$ is $(A^{(p^r)}, \mathrm{Frob}_{p^r,*}\,\iota)$.*

**Proof** Since $\mathrm{Ver}_{p^r}$ itself is the pullback of $\phi_r$ along $A \to S$ [Liu02, p. 94], we have $(A^{(p^r)}, \mathrm{Frob}_{p^r,*}\,\iota) = (A^{(p^r)}, \mathrm{Ver}_{p^r}^*\,\iota)$, where $\mathrm{Ver}_{p^r}^*\,\iota$ is defined in the obvious way. ∎

### 3.1 Split Primes and the Eichler–Selberg Trace Formula

***Definition 3.4*** Let $S$ be a $\mathbf{Z}_p$-scheme with $p \nmid DN$. Let $X_0^D(N)$ be defined over $S$. If $(n, DN) = 1$, then $T_n$ is the correspondence

$$\begin{tikzcd} & X_0^D(Nn)_S \arrow[dl, "\Phi_1"'] \arrow[dr, "\Phi_2"] & \\ X_0^D(N)_S & & X_0^D(N)_S, \end{tikzcd}$$

where $\Phi_1$ is the modular forgetful map and $\Phi_2 = \Phi_1 \circ w_n$.

The correspondences $T_n$ are commonly known as *Hecke correspondences*. Let $s$ be a closed point of $S$ with $k(s) = \overline{k(s)}$ so that $X_0^D(N)_s$ has a $k(s)$-rational point and thus correspondences on $X_0^D(N)$ are in bijection with endomorphisms of $J_0^D(N)_s$ [Mil86, Corollary 6.3]. We may also use $T_n$ to denote the endomorphism of $J_0^D(N)_s \cong J\big(X_0^D(N)_s\big)$ induced by the map of sets $X_0^D(N)_s \to \mathrm{Div}\big(X_0^D(N)_s\big)$ $P \mapsto (\Phi_{2,*}\Phi_1^*)P$. This operator on $J_0^D(N)_s$ is commonly referred to as a *Hecke operator*. We will explore the case $(n, DN) > 1$ in Section 3.2.

***Theorem 3.5*** (Eichler–Shimura) *There is an equality of endomorphisms of $J_0^D(N)_s$ between $T_p$ and $\mathrm{Frob}_p + \mathrm{Ver}_p$.*

**Proof** The particularly simple proof given below was sketched by Stein in the case of the elliptic modular curve $X_0^1(N)$ [RS11, Theorem 12.6.4], and the same proof also works for Shimura Curves. ∎

***Definition 3.6*** If $C_{\mathbb{F}_p}$ is a smooth, projective curve, we can define the zeta function of $C$ as

$$Z(C, x) := \exp\Big(\sum_{r=1}^{\infty} \#C(\mathbb{F}_{p^r})\frac{x^r}{r}\Big).$$

Shimura [Shi67] proved the following explicit formula for the zeta function.

***Theorem 3.7*** *If $\Omega$ denotes the canonical sheaf on $X_0^D(N)$, then*

$$Z\big(X_0^D(N)_{\mathbb{F}_p}, x\big) = \frac{\det_{H^0(X_0^D(N),\Omega)}(I_g - T_p x + p x^2 I_g)}{(1-x)(1-px)}.$$

***Corollary 3.8*** ([JL85, Proposition 2.1]) *If $r > 1$ then*

$$\#X_0^D(N)(\mathbb{F}_{p^r}) = p^r + 1 - \mathrm{tr}(T_{p^r}) + p\,\mathrm{tr}(T_{p^{r-2}})$$

*and if $r = 1$,*

$$\#X_0^D(N)(\mathbb{F}_p) = p + 1 - \mathrm{tr}(T_p).$$

https://doi.org/10.4153/CJM-2013-023-8 Published online by Cambridge University Press

***Theorem 3.9*** (Eichler's Trace Formula, [Eic56, Section 4]) *Let $D$ be the discriminant of an indefinite rational quaternion algebra, $N$ a square-free integer coprime to $D$ and $\ell$ a prime not dividing $DN$. Let $\operatorname{tr}(T_n)$ denote the trace of $T_n$ on $H^0\big(X_0^D(N)_{\mathbf{C}}, \Omega\big)$ and let $\sigma_1$ as the usual divisor sum function.*

*If $n$ is not a square and $(n, DN) = 1$, then*

$$\operatorname{tr}(T_n) = \sigma_1(n) - \sum_{s=-\lfloor 2\sqrt{n}\rfloor}^{\lfloor 2\sqrt{n}\rfloor} \sum_{f \mid f(s^2-4n)} \frac{e_{D,N}\big(\frac{s^2-4n}{f^2}\big)}{w\big(\frac{s^2-4n}{f^2}\big)}.$$

***Corollary 3.10***

$$\#X_0^D(N)(\mathbb{F}_p) = \sum_{s=-\lfloor 2\sqrt{p}\rfloor}^{\lfloor 2\sqrt{p}\rfloor} \sum_{f \mid f(s^2-4p)} \frac{e_{D,N}\big(\frac{s^2-4p}{f^2}\big)}{w\big(\frac{s^2-4p}{f^2}\big)}.$$

## 3.2 Inert Primes and the Eichler–Selberg Trace Formula

We begin by extending the definition of the Hecke operators $T_n$.

Suppose that $(DN, \frac{n}{(n,DN)}) = 1$, $m = (n, DN) \mid DN$ and $n' = \frac{n}{(n,DN)}$. Let $S$ be a $\mathbf{Z}_p$-scheme and $\Phi_1 : X_0^D(Nn')_S \to X_0^D(N)_S$ be the forgetful map. By abuse of notation, let $w_m$ denote the Atkin–Lehner involution on either $X_0^D(Nn')_S$ or $X_0^D(N)_S$. Note that $\Phi_1 w_m = w_m \Phi_1$, so if $s$ is a closed point of $S$ with $k(s) = \overline{k(s)}$, then $T_{n'} w_m = w_m T_{n'} : X_0^D(N)_s \to \operatorname{Div}\big(X_0^D(N)_s\big)$.

***Definition 3.11*** If $(DN, \frac{n}{(n,DN)}) = 1$, $m = (n, DN) \mid DN$ and $n' = \frac{n}{(n,DN)}$, then $T_n = w_m T_{n'}$.

Let $m \mid DN$ and consider the quotient $\big(X_0^D(N)/w_m\big)_s$. Let $\Omega$ denote the canonical sheaf of $X_0^D(N)_s$. Since $w_m$ is an involution, $H^0\big(X_0^D(N)_s, \Omega\big)$ decomposes into the direct sum of the $+1$ and $-1$ eigenspaces under its action. Note that the $+1$ eigenspace is $H^0\big((X_0^D(N)/w_m)_s, \Omega\big)$.

Suppose that $v \in H^0\big(X_0^D(N)_s, \Omega\big)$ such that $w_m v = v$. Then $w_m T_p v = T_p w_m v = T_p v$ and therefore $T_p$ acts on $H^0\big((X_0^D(N)/w_m)_s, \Omega\big)$.

***Definition 3.12*** If $p \nmid DN$ and $m \mid DN$, then by $T_p^{(m)}$ we denote the restriction of $T_p$ to $H^0\big((X_0^D(N)/w_m)_s, \Omega\big)$.

Since $T_p^{(m)}$ is just $T_p$ on a smaller vector space, we have $T_p^{(m)} = \operatorname{Frob}_p + \operatorname{Ver}_p$ on $\operatorname{Jac}\big((X_0^D(N)/w_m)_s\big)$ by Theorem 3.5.

***Corollary 3.13*** *Let $g'$ be the genus of $\big(X_0^D(N)/w_m\big)_{\mathbb{F}_p}$. The zeta function of the quotient curve is*

$$Z_p\big(X_0^D(N)/w_m, x\big) = \frac{\det_{H^0(X_0^D(N)/w_m,\Omega)}(I_{g'} - T_p^{(m)}x + px^2 I_{g'})}{(1-x)(1-px)}.$$

**Proof** Since $T_p^{(m)} = \mathrm{Frob}_p + \mathrm{Ver}_p$ on $\mathrm{Jac}\big( (X_0^D(N)/w_m)_s\big)$, any modern proof of Theorem 3.7 using smooth and proper base change would carry over exactly to prove this theorem. ∎

We may thus see that if $r > 1$, then

$$\#\big( X_0^D(N)/w_m\big)(\mathbb{F}_{p^r}) = p^r + 1 - \mathrm{tr}(T_{p^r}^{(m)}) + p\,\mathrm{tr}(T_{p^{r-2}}^{(m)})$$

and

$$\#\big( X_0^D(N)/w_m\big)(\mathbb{F}_p) = p + 1 - \mathrm{tr}(T_p^{(m)}).$$

Similarly to Rotger–Skorobogatov–Yafaev [RSY05], we can compute that $\mathrm{tr}(T_{p^r}^{(m)})$ (on $(X_0^D(N)/w_m)$) is equal to $\frac{1}{2}(\mathrm{tr}(T_{p^r}) + \mathrm{tr}(T_{p^r m}))$ and we obtain the following.

If $r > 1$, then

$$\#\big( X_0^D(N)/w_m\big)(\mathbb{F}_{p^r}) = p^r + 1 - \frac{\mathrm{tr}(T_{p^r}) + \mathrm{tr}(T_{p^r m})}{2} + \frac{p\big(\mathrm{tr}(T_{p^{r-2}}) + \mathrm{tr}(T_{p^{r-2}m})\big)}{2}$$

and if $r = 1$, then

$$\#\big( X_0^D(N)/w_m\big)(\mathbb{F}_p) = p + 1 - \frac{\mathrm{tr}(T_p) + \mathrm{tr}(T_{pm})}{2}.$$

If $(\frac{d}{p}) = 1$, then $C^D(N,d,m) \cong_{\mathbf{Q}_p} X_0^D(N)$. If $(\frac{d}{p}) = -1$, then we can show that

$$2\#X_0^D(N)/w_m(\mathbb{F}_{p^r}) = \#X_0^D(N)(\mathbb{F}_{p^r}) + \#C^D(N,d,m)(\mathbb{F}_{p^r}).$$

***Theorem 3.14*** *Let $p$ be inert in $\mathbf{Q}(\sqrt{d})$ and let $m \mid DN$. If $r > 1$, then*

$$\#C^D(N,d,m)(\mathbb{F}_{p^r}) = p^r + 1 - \mathrm{tr}(T_{p^r m}) + p\,\mathrm{tr}(T_{p^{r-2}m}),$$

*and if $r = 1$, then*

$$\#C^D(N,d,m)(\mathbb{F}_p) = p + 1 - \mathrm{tr}(T_{pm}).$$

In light of Theorem 3.14, we make the following definition.

***Definition 3.15*** For squarefree coprime integers $D$ and $N$, for $m \mid DN$ and for $p \nmid DN$, let $TF(D,N,m,p) := p + 1 - \mathrm{tr}_{H^0(X_0^D(N),\Omega)}(T_{pm})$.

## 3.3 Inert Primes and Superspecial Points

We now use the theory of superspecial points to gain explicit criteria for the presence of rational points. Recall that the superspecial points of $X_0^D(N)(\overline{\mathbb{F}}_p)$ are in bijection with $\mathrm{Pic}(Dp,N)$ via the embedding $c: X_0^D(N)_{\mathbb{F}_p} \to X_0^D(Np)_{\mathbb{F}_p}$ by Lemma 2.9. Recall also that the action of $\mathrm{Frob}_p \in \mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$ on the superspecial points in $X_0^D(N)(\overline{\mathbb{F}}_p)$ is given by $w_p$ by Lemma 2.22.

***Theorem 3.16*** *If $p \nmid DN$ is inert in $\mathbf{Q}(\sqrt{d})$, then $C^D(N,d,m)(\mathbf{Q}_p)$ is nonempty if one of the following holds:*

- $mp \not\equiv 3 \bmod 4$ *and* $e_{Dp,N}(-4mp) \neq 0$*;*
- $mp \equiv 3 \bmod 4$ *and one of* $e_{Dp,N}(-4mp)$ *and* $e_{Dp,N}(-mp)$ *is nonzero;*
- $p = 2$*,* $m = 1$*, and one of* $e_{Dp,N}(-4)$ *and* $e_{Dp,N}(-8)$ *is nonzero.*

**Proof** We wish to determine if $\mathcal{Z}(\mathbb{F}_p)$ contains a superspecial point. This occurs if and only if there is a superspecial point $P \in X_0^D(N)(\overline{\mathbb{F}}_p)$ such that $P = w_{mp}P$. By Corollary 2.21, there is a superspecial $w_{mp}$-fixed point $P$ if and only if there is an embedding of $\mathbf{Z}[\sqrt{-mp}]$ into $\operatorname{End}_{\iota(\mathcal{O})}(A)$ where $(A,\iota)$ corresponds to $P$, or possibly $\mathbf{Z}[\zeta_4]$ if $mp = 2$.

If $mp = 2$, then both $\mathbf{Z}[\zeta_4]$ and $\mathbf{Z}[\sqrt{-2}]$ are maximal orders, of discriminants $-4$ and $-8$ respectively. If $mp \equiv 1 \bmod 4$, then $\mathbf{Z}[\sqrt{-mp}]$ is maximal and of discriminant $-4mp$. If $mp \equiv 3 \bmod 4$, then $\mathbf{Z}[\sqrt{-mp}]$ again has discriminant $-4mp$ but is no longer maximal. It is contained in $\mathbf{Z}[\frac{1+\sqrt{-mp}}{2}]$, which is maximal and has discriminant $-mp$. Since there are no intermediate orders, this completes the proof. ■

***Corollary 3.17*** *If $p \nmid DN$ is inert in $\mathbf{Q}(\sqrt{d})$, $C^D(N,d,m)(\mathbf{Q}_p)$ is nonempty when $m = DN$. Moreover, $\mathcal{Z}(\mathbb{F}_p)$ contains a point corresponding to a superspecial surface.*

## 4 Local Points at Ramified Primes

Throughout this section we will fix $D$ the discriminant of an indefinite quaternion $\mathbf{Q}$-algebra, $N$ a squarefree integer coprime to $D$, a squarefree integer $d$, an integer $m \mid DN$ and a prime $p \nmid DN$ ramified in $\mathbf{Q}(\sqrt{d})$. Let $X_0^D(N)_{/\mathbf{Q}}$ be given by Corollary 2.1. Let $w_m$ be as in Definition 2.2. Let $C^D(N,d,m)_{/\mathbf{Q}}$ be the twist of $X_0^D(N)$ by $\mathbf{Q}(\sqrt{d})$ and $w_m$. If $\Delta < 0$, let $H_\Delta(X) \in \mathbf{Z}[X]$ [Cox89, p. 285] denote the Hilbert Class Polynomial of discriminant $\Delta$, and recall that this is simply the polynomial whose roots are the $j$-invariants of elliptic curves with complex multiplication by $R_\Delta$.

***Theorem 4.1*** *Suppose that $p \nmid 2DN$ is a prime which is ramified in $\mathbf{Q}(\sqrt{d})$ and $m \mid DN$. Then $C^D(N,d,m)(\mathbf{Q}_p) \neq \varnothing$ if and only if one of the following occurs:*

(1) $\left(\frac{-m}{p}\right) = 1$, $e_{D,N}(-4m) \neq 0$, *and* $H_{-4m}(X) = 0$ *has a root modulo* $p$.

(2) $\left(\frac{-m}{p}\right) = 1$, $m \equiv 3 \bmod 4$, $e_{D,N}(-m) \neq 0$, *and* $H_{-m}(X) = 0$ *has a root modulo* $p$.

(3) $\left(\frac{-DN}{p}\right) = -1$, $m = DN$, $2 \nmid D$, $\left(\frac{-p}{q}\right) = -1$ *for all primes* $q \mid D$, *and* $\left(\frac{-p}{q}\right) = 1$ *for all primes* $q \mid N$ *such that* $q \neq 2$.

(4) $2 \mid N$, $\left(\frac{-DN/2}{p}\right) = -1$, $m = DN/2$, $\left(\frac{-p}{q}\right) = -1$ *for all primes* $q \mid D$, *and* $\left(\frac{-p}{q}\right) = 1$ *for all primes* $q \mid N$ *such that* $q \neq 2$.

(5) $2 \mid D$, $\left(\frac{-DN}{p}\right) = -1$, $m = DN$, $p \equiv \pm 3 \bmod 8$, $\left(\frac{-p}{q}\right) = -1$ *for all primes* $q \mid (D/2)$, *and* $\left(\frac{-p}{q}\right) = 1$ *for all primes* $q \mid N$.

(6) $2 \mid D$, $\left(\frac{-DN/2}{p}\right) = -1$, $m = DN/2$, $DN \equiv 2, 6,$ *or* $10 \bmod 16$, $p \equiv \pm 3 \bmod 8$, $\left(\frac{-p}{q}\right) = -1$ *for all primes* $q \mid D$, *and* $\left(\frac{-p}{q}\right) = 1$ *for all primes* $q \mid N$.

Compare this to the following theorem.

https://doi.org/10.4153/CJM-2013-023-8 Published online by Cambridge University Press

***Theorem 4.2*** *Let $p$ be a prime, $(p, 2N) = 1$, $D = 1$, and $m = N$. If $C^D(N, d, m)(\mathbf{Q}_p)$ is nonempty, then $H_{-4m}(X) = 0$ has a root modulo $p$. If $H_{-4m}(X)$ has a root modulo $p$ and additionally $p \nmid \operatorname{disc}\big(H_{-4m}(X)\big)$, then $C^D(N, d, m)(\mathbf{Q}_p)$ is nonempty.*

**Proof** Suppose that $p > 2$, $D = 1$ and $m = N$. By [Ozm12, Proposition 4.6], $C^D(N, d, m)(\mathbf{Q}_p)$ is nonempty if and only if there is a prime $\nu$ of $\mathbb{B} = \mathbf{Q}[X]/\big(H_{-4m}(X)\big)$ such that $f(\nu \mid p) = 1$. In fact, if $C^D(N, d, m)(\mathbf{Q}_p)$ is nonempty, then Ozman shows how to produce an elliptic curve over $\mathbf{Q}_p$ with good reduction and CM by $\mathbf{Z}[\sqrt{-m}]$. Therefore the $j$-invariant of its modulo $p$ reduction is a root modulo $p$ of $H_{-4m}(X) = 0$.

Conversely if $p \nmid \operatorname{disc}\big(H_{-4m}(X)\big)$, then $p$ does not divide the conductor of $\mathbf{Z}[\mathbf{X}]/H_{-4m}(X)$, and so if there is a linear factor modulo $p$ of $H_{-4m}(X)$, then there is a $\mathbf{Z}/p\mathbf{Z}$ factor of $\mathbf{Z}_{\mathbb{B}}/p\mathbf{Z}_{\mathbb{B}}$ [Neu99, I.8.3]. Therefore there is a prime $\nu$ of $\mathbf{Z}_{\mathbb{B}}$ such that $\nu \mid p\mathbf{Z}_{\mathbb{B}}$ and $f(\nu \mid p) = 1$. ∎

We note here that there are numerous counterexamples if $p \mid \operatorname{disc}(H_{-4m}(X))$, as pointed out to the author by Patrick Morton. Perhaps the easiest one is the case of $p = 13$, where $(\frac{-20}{13}) = (\frac{-13}{5}) = -1$ but $H_{-20}(X)$ factors as $(X + 8)^2$ modulo 13. Moreover, if $p \mid \operatorname{disc}(H_{-4m}(X))$ there is no guarantee of a root modulo $p$, as demonstrated by $m = 57$ and $p = 43$. In any case, we have unearthed a powerful tool for finding roots of Hilbert Class Polynomials modulo $p$ that may have useful applications in cryptography.

We can combine the results of Theorem 4.1(3) with those of Theorem 4.2 to yield the following.

***Corollary 4.3*** *Let $p \neq 2$ be a prime and let $N$ be a squarefree integer such that $p \nmid \operatorname{disc}(H_\Delta)$ and $(\frac{-N}{p}) = -1$. It follows that $H_{-4N}(X)$ has a root modulo $p$ if and only if, for all odd primes $q \mid N$, $(\frac{-p}{q}) = 1$.*

To establish Theorem 4.1 and Corollary 4.3, we determine a regular model over $\mathbf{Z}_p$ of $C^D(N, d, m)_{\mathbf{Q}_p}$. We shall indeed show the following.

***Theorem 4.4*** *There is a regular model $\mathcal{X}_{/\mathbf{Z}_p}$ of $C^D(N, d, m)_{\mathbf{Q}_p}$ with the following properties. There is an equality of divisors on $\mathcal{X}$,*

$$\mathcal{X}_{\mathbb{F}_p} = \sum_{i=0}^{b} d_i \Gamma_i,$$

*such that each $\Gamma_i$ is defined over $\mathbb{F}_p$ and is prime, $\Gamma_0 \cong (X_0^D(N)/w_m)_{\mathbb{F}_p}$, each $d_i \leq 2$, $d_0 = 2$, and for all $i > 0$, $p_a(\Gamma_i) = 0$.*

*Suppose additionally that $p \neq 2$. Then for all $i > 0$, $d_i = 1$ and $\Gamma_0$ intersects with $\Gamma_i$ in a unique point $Q_i$. These points $Q_i$ are such that $\sum_{i=1}^{b} Q_i$ is the branch divisor of $X_0^D(N)_{\mathbb{F}_p} \to (X_0^D(N)/w_m)_{\mathbb{F}_p}$.*

In fact, we shall show that if $p \neq 2$, then $\mathcal{X}$ is the blowup of a scheme $\mathcal{Z}_{/\mathbf{Z}_p}$ such that there is an equality of divisors $\mathcal{Z}_{\mathbb{F}_p} = 2\Gamma$ where $\Gamma \cong (X_0^D(N)/w_m)_{\mathbb{F}_p}$. Therefore there are smooth points of $\mathcal{X}(\mathbb{F}_p)$ if and only if $\mathbb{F}_p = \mathbb{F}_p(P_i) = \mathbb{F}_p(\Gamma_i)$, since $\Gamma_i \cong \mathbb{P}^1_{\mathbb{F}_p(Q_i)}$. After constructing $\mathcal{Z}$ and $\mathcal{X}$, we will describe $\mathbb{F}_p(Q_i)$, *i.e.*, the $\mathbb{F}_p$-rationality of $w_m$-fixed points.

### 4.1 The First Steps towards Forming a Model

Let us begin with a few foundational facts.

***Lemma 4.5*** *Let $X_{/K}$ be a curve with potentially semistable reduction realized by a cyclic totally ramified extension $L/K$ of local fields. Let $k$ be their common residue field and let $S/R$ be the corresponding extension of discrete valuation rings. Let $\mathcal{Y} \to \operatorname{Spec}(S)$ be a regular model of $X_L$, $\operatorname{Gal}(L/K) = \langle\sigma\rangle$, and assume that there exists some automorphism $\alpha$ of $\mathcal{Y}$ above $\sigma\colon \operatorname{Spec}(S) \to \operatorname{Spec}(S)$ extending the Galois action on $X_L$.*

(1) *The quotient $\mathcal{Z} = \mathcal{Y}/\langle\alpha\rangle$ is a scheme of relative dimension one over $\operatorname{Spec}(R)$ with generic fiber $X$.*

(2) *Let $\xi_1, \dots, \xi_n$ be the generic points of the irreducible components $C_1, \dots, C_n$ of $\mathcal{Y}_k$ lying above a component $C$ of $\mathcal{Z}_k$ with generic point $\xi$. Let $D_i = D(\xi_i \,|\, \xi)$, $I_i = I(\xi_i|\xi)$ denote the decomposition and inertia groups, respectively. Then the multiplicity of $\xi$ in $\mathcal{Z}_k$ is $|D_i|n/|I_i|$.*

**Proof** That $\mathcal{Z}$ is a $\operatorname{Spec}(R)$-scheme follows from the universal properties of the quotient as outlined in [Vie77, 3.6]. To obtain the multiplicities, we recall [Liu02, VIII.3.9] that the multiplicity of $\xi_i$ is $v_i(s)$, where $v_i$ is the discrete valuation of $\mathcal{O}_{\mathcal{Y},\xi_i}$ and $s$ is a uniformizer of $S$. As $\mathcal{Y}$ has semistable reduction, $v_i(s) = 1$ for all $i$. Likewise the multiplicity of $\xi$ is $v(r)$, where $v$ is the discrete valuation of $\mathcal{O}_{\mathcal{Z},\xi}$ and $r$ is a uniformizer of $R$. As $\mathcal{Y} \to \mathcal{Z}$ is Galois, there are positive integers $e, q$ such that $v_i\,|_R = ev$ and $q = |D_i/I_i|$ for all $i$ and $[L : K] = eqn$. As $L/K$ is totally ramified, $rS = s^{eqn}S$. It then follows that

$$ev(r) = v_i(r) = v_i(s^{eqn}) = eqnv_i(s)$$

and thus $v(r) = qnv_i(s) = qn = |D_i/I_i|n = |D_i|n/|I_i|$. ∎

***Lemma 4.6*** ([Lor11, 5.2]) *Under the hypotheses of Lemma 4.5, the non-regular points of $\mathcal{Z}$ are precisely the branch points $Q_1, \dots, Q_b$ of $\mathcal{Y}_k \to \mathcal{Z}_k$.*

If $K = \mathbf{Q}_p$ and $L = \mathbf{Q}_p(\sqrt{d})$ then $R = \mathbf{Z}_p$, $S = \mathbf{Z}_p[\sqrt{d}]$, $k = \mathbb{F}_p$, and $\sigma(\sqrt{d}) = -\sqrt{d}$. If additionally $X = X_0^D(N)_{\mathbf{Q}_p}$, then $\mathcal{Y}_{\mathbb{F}_p}$ is smooth and we can realize $\mathcal{Y} \cong X_0^D(N)_{/\mathbf{Z}_p[\sqrt{d}]}$ from Corollary 2.1. If we take $\alpha = w_m \circ \sigma$ and take $\mathcal{Z} = \mathcal{Y}/\langle\alpha\rangle$, then the following holds.

***Theorem 4.7*** *The scheme $\mathcal{Z}_{/\mathbf{Z}_p} = \mathcal{Y}/\langle\alpha\rangle$ has generic fiber $C^D(N,d,m)_{\mathbf{Q}_p}$, and there is an equality of divisors $\mathcal{Z}_{\mathbb{F}_p} = 2\Gamma$ where $\Gamma \cong \big(X_0^D(N)/w_m\big)_{\mathbb{F}_p}$.*

**Proof** Since there is a unique component of $\mathcal{Y}_{\mathbb{F}_p}$, $n = 1$. Let $\xi', \xi$ be the generic points of the components of $\mathcal{Y}_{\mathbb{F}_p}$ and $\mathcal{Z}_{\mathbb{F}_p}$ respectively. Then $D(\xi' \,|\, \xi) = \langle\alpha\rangle$ since $\alpha$ preserves $\mathcal{Y}_{\mathbb{F}_p}$. Since $w_m$ acts non-trivially on $\mathcal{Y}_{\mathbb{F}_p}$, $I(\xi' \,|\, \xi) = \{\mathrm{id}\}$. The multiplicity of the component corresponding to $\xi$ is thus 2.

To determine the $\Gamma$ such that $2\Gamma = \mathcal{Z}_{\mathbb{F}_p}$, recall that the pushforward under $f\colon \mathcal{Y} \to \mathcal{Z}$ of $\mathcal{Y}_{\mathbb{F}_p}$ forms a prime divisor of $\mathcal{Z}$ in $\mathcal{Z}_{\mathbb{F}_p}$ and must therefore be $\Gamma$. To determine this pushforward, note that the induced action of $\sigma$ on $\operatorname{Spec}(\mathbb{F}_p)$ is trivial and con-

https://doi.org/10.4153/CJM-2013-023-8 Published online by Cambridge University Press

sider the commutative square

$$\begin{tikzcd} \mathcal{Y} \arrow[r, "\alpha"] \arrow[d] & \mathcal{Y} \arrow[d] \\ \operatorname{Spec}(\mathbf{Z}_p[\sqrt{d}]) \arrow[r, "\sigma"] & \operatorname{Spec}(\mathbf{Z}_p[\sqrt{d}]). \end{tikzcd}$$

The fiber product of this square with $\operatorname{Spec}(\mathbb{F}_p) \to \operatorname{Spec}(\mathbf{Z}_p[\sqrt{d}])$ is simply the $\operatorname{Spec}(\mathbb{F}_p)$-involution $w_m$ on $\mathcal{Y}_{\mathbb{F}_p} = X_0^D(N)_{\mathbb{F}_p}$. It follows that $f$, when restricted to $\mathcal{Y}_{\mathbb{F}_p}$, becomes simply the quotient map $X_0^D(N)_{\mathbb{F}_p} \to \left(X_0^D(N)/w_m\right)_{\mathbb{F}_p}$, and therefore $\Gamma \cong \left(X_0^D(N)/w_m\right)_{\mathbb{F}_p}$. ■

We note by Lemma 4.6 that $\mathcal{Z}$ is not generally a regular scheme. To make the resolution of its singularities easier, we fix the following.

***Definition 4.8*** Fix an ordering $\{Q_i\}$ of the branch points of the quotient map $f\colon X_0^D(N)_{\mathbb{F}_p} \to \left(X_0^D(N)/w_m\right)_{\mathbb{F}_p}$. Let $P_i$ denote the unique preimage of $Q_i$ under $f$.

Note that by definition, the $P_i$ are exactly the points of $X_0^D(N)_{\mathbb{F}_p}$ fixed by $w_m$. When $p \neq 2$, we will explicitly describe a desingularization of $\mathcal{Z}$ in the strong sense [Liu02, Definition 8.3.39]. This will be a regular model of $C^D(N,d,m)_{\mathbf{Q}_p}$. We will first describe the branch points $\{Q_i\}$ and their $\mathbb{F}_p$-rationality.

## 4.2 Atkin–Lehner Fixed Points over Finite Fields

Throughout this section, we will keep the notation of Definition 4.8. Note that since $\mathbf{Q}_p[\sqrt{d}]$ is totally ramified over $\mathbf{Q}_p$, $\mathbb{F}_p(Q_i) \cong \mathbb{F}_p(P_i)$.

***Lemma 4.9*** *Let $\mathcal{Z}$ be non-regular and $\pi\colon \mathcal{X} \to \mathcal{Z}$ a desingularization in the strong sense and assume that for all $i$, $\pi^{-1}(Q_i)$ is a chain of rational curves such that at least one has multiplicity one. Then $C^D(N,d,m)(\mathbf{Q}_p)$ is nonempty if and only if either*

(1) $\left(\frac{-m}{p}\right) = 1$ *and one of the following holds:*
- $m = 2$,
- $H_{-4m}(X)$ *has a root modulo $p$,*
- $m \equiv 3 \bmod 4$ *and $H_{-m}(X)$ has a root modulo $p$,*

(2) $\left(\frac{-m}{p}\right) = -1$ *and one of the conditions of Corollary 2.26 is satisfied.*

**Proof** Note first that each component in $\pi^{-1}(Q_i)$ must be isomorphic to $\mathbb{P}^1_{\mathbb{F}_p(Q_i)}$. Therefore by our assumption on $\pi$, $\mathbb{F}_p = \mathbb{F}_p(Q_i)$ if and only if there is a reduced copy of $\mathbb{P}^1_{\mathbb{F}_p}$ in $\pi^{-1}(Q_i)$.

By Lemma 2.11, any QM-abelian surface over a finite field must be either ordinary or supersingular. Suppose first that $(A,\iota)$ is supersingular and fixed by $w_m$. By Lemma 2.13, if $(A,\iota)$ is a supersingular QM-abelian surface over a finite field

https://doi.org/10.4153/CJM-2013-023-8 Published online by Cambridge University Press

of characteristic $p$, then $(A,\iota)$ is superspecial. Therefore, one of the conditions of Corollary 2.26 holds if and only if there is a QM-abelian surface $(A,\iota)$ fixed by $w_m$ whose corresponding point $P_i$ is $\mathbb{F}_p$-rational.

Now suppose that $(A,\iota)$ is an ordinary QM-abelian surface over a finite field $k$ fixed by $w_m$. By Theorem 2.14, there are elliptic curves $E$ and $E'$ such that $\operatorname{End}_k(E) \cong \operatorname{End}_k(E') \cong R' = \mathbf{Z}[\sqrt{-m}]$ or $\mathbf{Z}[\frac{1+\sqrt{-m}}{2}]$ (or $\mathbf{Z}[\zeta_4]$ if $m = 2$) and $A \cong E \times E'$. Now note that the $j$-invariants of $E$ and $E'$ are roots of $H_{-4m}(X)$ mod $p$, $H_{-m}(X)$ mod $p$ if $m \equiv 3 \bmod 4$, or $H_{-4}(X)$ if $m = 2$. If $m = 2$, then $H_{-4}(X)$ and $H_{-8}(X)$ have degree one so for all $p$, $H_\Delta(X)$ has a root modulo $p$. Since the $j$-invariants of $E$ and $E'$ are defined over $\mathbb{F}_p$, $(A,\iota)$ is defined over $\mathbb{F}_p$. Therefore if $P_i$ corresponds to the surface $(A,\iota)$ then $\mathbb{F}_p(P_i) = \mathbb{F}_p$.

Recall now the classical theorem of Deuring that if $K$ is a number field, $\mathfrak{p} \mid p$ is a prime, and $E_{/K}$ is an elliptic curve with CM by $R_\Delta$, then $E$ mod $\mathfrak{p}$ is ordinary if and only if $(\frac{\Delta}{p}) = 1$ [Lan87, Theorem 13.12]. Therefore $(A,\iota)$ is ordinary if and only if $(\frac{-m}{p}) = 1$.

We have thus shown that either (1) or (2) holds if and only if there is a reduced copy of $\mathbb{P}^1_{\mathbb{F}_p}$ in some $\pi^{-1}(Q_i)$. Since the strict transform of $\Gamma$ in $\mathcal{X}$ has multiplicity two, the presence of a reduced copy of $\mathbb{P}^1_{\mathbb{F}_p}$ in some $\pi^{-1}(Q_i)$ is equivalent to the presence of a smooth point of $\mathcal{X}(\mathbb{F}_p)$. By Hensel's Lemma [JL85, Lemma 1.1], the presence of a smooth point in $\mathcal{X}(\mathbb{F}_p)$ is equivalent to $C^D(N,d,m)(\mathbf{Q}_p)$ being nonempty. ∎

### 4.3 Tame Potential Good Reduction

In this section we construct a regular model of $C^D(N,d,m)_{\mathbf{Q}_p}$. Let $\mathcal{X}_{\mathbf{Z}_p} := \operatorname{Bl}_{\{Q_i\}}(\mathcal{Z})$, the blowup of $\mathcal{Z}$ along the branch divisor of $\mathcal{Y}_{\mathbb{F}_p} \to \mathcal{Z}_{\mathbb{F}_p}$ [Liu02, Definition 8.1.1]. Since the blowup construction gives a map $\mathcal{X} \to \mathcal{Z}$ which is an isomorphism away from $\{Q_i\}$, $\mathcal{X}$ is a regular model if and only if $\mathcal{X} \to \mathcal{Z}$ is a desingularization in the strong sense if and only if $\mathcal{X}$ is a regular scheme.

To see that this is a regular scheme, let $\overline{R} = \mathbf{Z}_p^{nr}$, a strict henselization of $\mathbf{Z}_p$. We will construct in this section an auxiliary scheme $\mathcal{X}'_{/\overline{R}}$. If we can show that $\mathcal{X}_{\overline{R}} \cong \mathcal{X}'$, it will follow that $\mathcal{X}$ is regular [CES03, Lemma 2.1.1]. Thus, the hypotheses of Lemma 4.9 would be satisfied and thus Theorem 4.1 would be proved.

Also fix $\overline{S} = \overline{R}[\sqrt{d}]$, $k'$ the residue field of $\overline{S}$, $k$ the residue field of $\overline{R}$, and note that both $k$ and $k'$ must be isomorphic to $\overline{\mathbb{F}}_p$. We note the following.

***Lemma 4.10*** *Suppose that $p \neq 2$ and let $Q$ be a point of $Q_i \times_{\mathbf{Z}_p} \overline{R}$. Then $Q$ is a tame cyclic quotient singularity [CES03, Definition 2.3.6] with $n = 2$ and $r = 1$.*

**Proof** Let $\overline{\alpha}$ denote the extension of $\alpha$ from $\mathcal{Y}$ to $\mathcal{Y}_{\overline{S}}$. We wish to show that $\widehat{\mathcal{O}^{sh}_{\mathcal{Z},Q}}$ is the ring of invariants of a $\mu_2$ (or since $p \neq 2$, $\mathbf{Z}/2\mathbf{Z}$) action. Fix an isomorphism $\overline{S}[[X]] \cong \widehat{\mathcal{O}_{\mathcal{Y}_{\overline{S}},P}}$ where $P$ is the unique preimage of $Q$ under $\overline{f}\colon \mathcal{Y}_{\overline{S}} \to \mathcal{Z}_{\overline{R}}$. Since $w_m$ is always Galois-equivariant, $\overline{\alpha}(\sqrt{d}) = -\sqrt{d}$. Since $\overline{\alpha}$ induces an isomorphism $\overline{S}[[T]] \cong \overline{S}[[\overline{\alpha}(T)]]$, $\overline{\alpha}(T) = P_\alpha(T) = \sum_{j\ge 1} \alpha_j T^j$. Since $\overline{\alpha}$ is an involution, $\alpha_1 = -1$. Then $\overline{\alpha}(T) - T = -2T\big(1 + O(T)\big)$, *i.e.*, $\overline{\alpha}(T) - T \equiv -2T \bmod (T^2)$. Since $-2 \notin \mathfrak{m}_{\overline{S}}$,

$\overline{S}[[T]] \cong \overline{S}[[T']]$ where $T' := \overline{\alpha}(T) - T$. Note also that $\overline{\alpha}(T') = \overline{\alpha}\big(\overline{\alpha}(T) - T\big) = T - \overline{\alpha}(T) = -(T')$. Therefore $\sqrt{d}$ and $T'$ form a basis of uniformizers for the two-dimensional local ring $\widehat{\mathcal{O}_{\mathcal{Y}_{\overline{S}},P}}$ and $\overline{\alpha}$ acts as $-1$ on both $\sqrt{d}$ and $T'$.

Note now that $\widehat{\mathcal{O}_{\mathcal{Z}_{\overline{R}},Q}}$ is the ring of invariants of the $\mu_2$-action given by $\overline{\alpha}$ on $\overline{S}[[T']]$. Recall that since $p \neq 2$ is a uniformizer for $R$ and $p$ is ramified in $\mathbf{Q}(\sqrt{d})$ where $d$ is square-free, $d$ is also a uniformizer. Therefore

$$\overline{S}[[T']] \cong \overline{R}[[t_1, t_2]]/(t_1^{m_1} t_2^{m_2} - d)$$

where $m_1 = 2$, $t_2 = T'$, and $m_2 = 0$ in the notation of [CES03]. It follows that $Q$ is a tame cyclic quotient singularity with $n = 2$ and $r = 1$. ∎

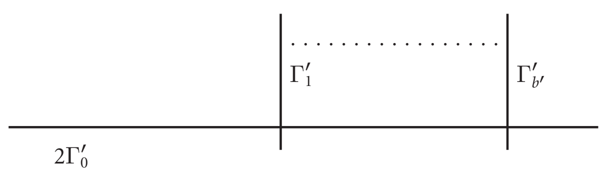
From here on, let $b'$ be such that $\sum_{i=1}^{b} Q_i \times_{\mathbf{Z}_p} \overline{R} = \sum_{i=1}^{b'} Q_i'$.

***Definition 4.11*** Let $R$ be a discrete valuation ring with algebraically closed residue field, $X_{/R}$ be a scheme, and $P$ a tame cyclic quotient singularity of $X$ of type $n, r$. Then [CES03, Theorem 2.4.1] we can inductively produce a chain of divisors $E_1, \dots, E_\lambda$ and a set of integers $b_1, \dots, b_\lambda$ such that

- There is a resolution $\tilde{X}_P \to X$ of the singularity at $P$ whose fiber over $P$ is the chain made up of the $E_i$s.
- $E_i \cdot E_j = \delta_{i,j\pm 1}$ if $i \neq j$, $E_j^2 = -b_j < -1$.
- $\frac{n}{r} = b_1 - \frac{1}{b_2 - \frac{1}{\dots - \frac{1}{b_\lambda}}}$.

This $\tilde{X}_P$ is called the Hirzebruch–Jung desingularization at $P$.

***Theorem 4.12*** *If $p \neq 2$ there is a desingularization of $\overline{R}$-schemes $\mathcal{X}' \to \mathcal{Z}_{\overline{R}}$ such that $\mathcal{X}_k'$ has the form*




*where $\Gamma_0'$ is the strict transform of $\Gamma_{\overline{R}}$ and for all $i > 0$, $\Gamma_i' \cong \mathbb{P}_k^1$. This is to say that there is an equality of divisors on $\mathcal{X}'$ between $\mathcal{X}_k'$ and $2\Gamma_0' + \sum_{i=1}^{b'} \Gamma_i'$, $\Gamma_0' \cap \Gamma_i' = Q_i' \in Q_i \times_{\mathbf{Z}_p} \overline{R}$, and all intersections are transverse. Moreover $\mathcal{X}_{\overline{R}} \cong \mathcal{X}'$, and since $\mathcal{X}'$ is a regular scheme, so is $\mathcal{X}$. It follows that $\mathcal{X}$ is a regular $\mathbf{Z}_p$ model for $C^D(N, d, m)_{\mathbf{Q}_p}$.*

**Proof** We construct $\mathcal{X}'$ by performing the Hirzebruch–Jung desingularization at $Q$ for all $Q$ in all $Q_i \times \overline{R}$. By Lemma 4.10, $n = 2$, $r = 1$ and thus $\lambda = 1$ and $b_1 = \frac{2}{1}$ in Definition 4.11. Therefore $\mathcal{X}_k'$ has the form above [CES03, Theorem 2.4.1].

Recall now that $\mathcal{X}' \to \mathcal{Z}_{\overline{R}}$, $\mathcal{X}_{\overline{R}} \to \mathcal{Z}_{\overline{R}}$ are birational morphisms and so there is a birational map $f\colon \mathcal{X}_{\overline{R}} \dashrightarrow \mathcal{X}'$ commuting with the maps down to $\mathcal{Z}_{\overline{R}}$.

Since $\overline{R}$ is Dedekind, $f^{-1}|_{\Gamma_0'}$ is the identity and $f$ can be extended so that the preimage of each divisor on either $\mathcal{X}_{\overline{R}}$ or $\mathcal{X}'$ is again a divisor. We thus find that $f$ is a morphism and thus an isomorphism [Liu02, Theorem 8.3.20]. It follows that $\mathcal{X}_{\overline{R}}$ is regular and therefore $\mathcal{X}$ is regular [CES03, Lemma 2.1.1]. ∎

**Proof of Theorem 4.1** By Theorem 4.12, the conditions of Lemma 4.9 hold. ∎

***Remark 4.13*** In the case that $X_0^D(N)/w_m \cong \mathbb{P}^1_{\mathbb{F}_p}$ we can deduce this theorem from work of Sadek [Sad10].

***Remark 4.14*** Retaining the notation of Lemma 4.6, if $p = 2$, we still have that $\mathcal{Z}_{/\mathbf{Z}_2}$ is a normal scheme, non-regular precisely at the fixed points on the special fiber of $w_m$. Moreover, these singularities are still $\mathbf{Z}/2\mathbf{Z}$-quotient singularities. Once more, we can resolve these singularities to give a regular model of $C^D(N,d,m)$. Unfortunately Lemma 4.10 no longer holds, as these singularities are *wild*, and it is not known under what circumstances a resolution will have non-reduced components.

## 5 Local Points when $p\,|\,D$

Fix a squarefree integer $d$, an integer $m\,|\,DN$, and a prime $p\,|\,D$ unramified in $\mathbf{Q}(\sqrt{d})$. Let $C^D(N,d,m)_{/\mathbf{Q}}$ be the twist of $X_0^D(N)_{/\mathbf{Q}}$ by $\mathbf{Q}(\sqrt{d})$ and $w_m$.

***Theorem 5.1*** *Suppose that $p\,|\,D$ is unramified in $\mathbf{Q}(\sqrt{d})$ and $m\,|\,DN$. Let $p_i$, $q_j$ be primes such that $D/p = \prod_i p_i$ and $N = \prod_j q_j$.*

- *Suppose $p$ is split in $\mathbf{Q}(\sqrt{d})$. Then $C^D(N,d,m)(\mathbf{Q}_p)$ is nonempty if and only if one of the following two cases occurs* [Theorem 5.11]*:*
  (1) *$p = 2$, $p_i \equiv 3 \bmod 4$ for all $i$, and $q_j \equiv 1 \bmod 4$ for all $j$.*
  (2) *$p \equiv 1 \bmod 4$, $D = 2p$, and $N = 1$.*
- *Suppose that $p$ is inert in $\mathbf{Q}(\sqrt{d})$.*
  - *If $p\,|\,m$, $C^D(N,d,m)(\mathbf{Q}_p)$ is nonempty if and only if one of the following four cases occurs:*
    (1) *$m = p$, $p_i \not\equiv 1 \bmod 3$ for all $i$, and $q_j \not\equiv 2 \bmod 3$ for all $j$* [Lemma 5.7].
    (2) *$m = 2p$ and one of $e_{D/p,N}(-4)$ or $e_{D/p,N}(-8)$ is nonzero* [Lemma 5.8].
    (3) *$m/p \not\equiv 3 \bmod 4$ and $e_{D/p,N}(-4m/p)$ is nonzero* [Lemma 5.8].
    (4) *$m/p \equiv 3 \bmod 4$ and one of $e_{D/p,N}(-4m/p)$ or $e_{D/p,N}(-m/p)$ is nonzero* [Lemma 5.8].
  - *If $p \nmid m$, $C^D(N,d,m)(\mathbf{Q}_p)$ is nonempty if and only if one of the following four cases occurs* [Theorem 5.11]*:*
    (1) *$p = 2$, $m = 1$, $p_i \equiv 3 \bmod 4$ for all $i$, and $q_j \equiv 1 \bmod 4$ for all $j$.*
    (2) *$p \equiv 1 \bmod 4$, $m = DN/(2p)$, for all $i$, $p_i \not\equiv 1 \bmod 4$, and for all $j$, $q_j \not\equiv 3 \bmod 4$.*
    (3) *$p = 2$, $m = DN/2$, $p_i \equiv 3 \bmod 4$ for all $i$, and $q_j \equiv 1 \bmod 4$ for all $i$.*
    (4) *$p \equiv 1 \bmod 4$, $m = DN/p$, for all $i$, $p_i \not\equiv 1 \bmod 4$, and for all $j$, $q_j \not\equiv 3 \bmod 4$.*

As opposed to the case where $p \mid N$, all conditions here are determined by congruences. For completeness, we record the following.

***Corollary 5.2*** *Let $p_i$, $q_j$ be primes such that $D/p = \prod_i p_i$ and $N = \prod_j q_j$.*

- *If $p$ is split in $\mathbf{Q}(\sqrt{d})$, then $C^D(N,d,DN) \cong X_0^D(N)$ over $\mathbf{Q}_p$ and $X_0^D(N)(\mathbf{Q}_p)$ is nonempty if and only if one of the following two cases occurs:*
  (1) $p = 2$, $p_i \equiv 3 \bmod 4$ *for all* $i$, *and* $q_j \equiv 1 \bmod 4$ *for all* $j$.
  (2) $p \equiv 1 \bmod 4$, $D = 2p$, *and* $N = 1$.
- *If $p$ is inert in $\mathbf{Q}(\sqrt{d})$ then $C^D(N,d,DN)(\mathbf{Q}_p)$ is nonempty.*

**Proof** Note that $e_{D/p,N}(-4DN/p)$ is always nonzero by Eichler's Embedding Theorem. ■

To prove Theorem 5.1, we shall need to work with regular models for $X_0^D(N)_{\mathbf{Q}_p}$ and $C^D(N,d,m)_{\mathbf{Q}_p}$.

***Definition 5.3*** Let $\pi\colon \mathcal{X} \to X_0^D(N)_{/\mathbf{Z}_p}$ denote a minimal desingularization. If $x$ is a superspecial point on $X_0^D(N)_{\overline{\mathbb{F}}_p}$ let $\ell = \ell(x)$ be as in Definition 2.5. If $\ell > 1$, $\pi^*\big(x(\operatorname{Spec}(\overline{\mathbb{F}}_p))\big) = \bigcup_{i=1}^{\ell-1} C_i$ where for all $i$, $C_i \cong \mathbb{P}^1_{\overline{\mathbb{F}}_p}$ and exactly two points of $C_i$ are singular in $\mathcal{X}_{\overline{\mathbb{F}}_p}$.

For $n \mid DN$, let $w_n$ denote the automorphism of Definition 2.2. Note that extending the automorphism $w_n$ from Definition 2.2 to $\mathcal{X}$ makes sense because $w_n\colon X_0^D(N) \to X_0^D(N)$ induces a birational morphism $\mathcal{X} \dashrightarrow \mathcal{X}$ permuting the components of $\mathcal{X}_{\mathbb{F}_p}$. Therefore $w_n$ on $X_0^D(N)$ induces an isomorphism $\mathcal{X} \to \mathcal{X}$ [Liu02, Remark 8.3.25].

We note also that the components of $X_0^D(N)_{\overline{\mathbb{F}}_p}$ are in $W$-equivariant bijection with $\operatorname{Pic}(D/p,N) \coprod \operatorname{Pic}(D/p,N)$ by Theorem 2.7. The intersection points, which can only link a component in one copy of $\operatorname{Pic}(D/p,N)$ to a component in the other copy of $\operatorname{Pic}(D/p,N)$, are in $W$-equivariant bijection with $\operatorname{Pic}(D/p,Np)$ as in Theorem 2.7. The bijection of the components with two copies of $\operatorname{Pic}(D/p,N)$ is $W/\langle w_p\rangle$-equivariant. As in Lemma 2.9, $w_p$ interchanges the two copies of $\operatorname{Pic}(D/p,N)$. We define the length of a component of $X_0^D(N)_{\overline{\mathbb{F}}_p}$ by the length of the associated element of $\operatorname{Pic}(D/p,N)$ as in Definition 2.5.

***Definition 5.4*** Let $\sigma$ be such that $\langle\sigma\rangle = \operatorname{Aut}_{\mathbf{Z}_p}(\mathbf{Z}_{p^2})$. We denote by $\mathcal{Z}_{/\mathbf{Z}_p}$ the regular model of $C^D(N,d,m)_{\mathbf{Q}_p}$ obtained as the étale quotient $\mathcal{Z}$ of $\mathcal{X}_{\mathbf{Z}_{p^2}}$ by the action of $w_m \circ \sigma$.

Note that if $p$ is inert in $\mathbf{Q}(\sqrt{d})$ then $\mathbf{Z}_p[\sqrt{d}] \cong \mathbf{Z}_{p^2}$ and thus the generic fiber of $\mathcal{Z}$ is $C^D(N,d,m)_{\mathbf{Q}_p}$. Therefore $\mathcal{Z}$ is a regular model of $C^D(N,d,m)_{\mathbf{Q}_p}$ if $p$ is inert in $\mathbf{Q}(\sqrt{d})$.

We also note that if $p$ is split in $\mathbf{Q}(\sqrt{d})$, or if $p$ is inert and $m = 1$, then we have $C^D(N,d,m)_{\mathbf{Q}_p} \cong X_0^D(N)_{\mathbf{Q}_p}$. If $p$ is split in $\mathbf{Q}(\sqrt{d})$, we can consider $d'$ to be any square-free integer such that $p$ is inert in $\mathbf{Q}(\sqrt{d'})$ and $\mathcal{Z}'$ to be the regular model of

$C^D(N,d',1)_{\mathbf{Q}_p} \cong X_0^D(N)_{\mathbf{Q}_p}$. Therefore, we shall obtain our results when $p$ is split as a corollary to our results when $p \nmid m$.

## 5.1 The Proof when $p \mid m$

***Lemma 5.5*** *Let $p \mid D$ be unramified in $\mathbf{Q}(\sqrt{d})$ and $p \mid m$. Then $C^D(N,d,m)(\mathbf{Q}_p)$ is nonempty if and only if one of the following occurs:*

(1) *$p = m$ and there is some component of $X_0^D(N)_{\overline{\mathbb{F}}_p}$ with length greater than one.*

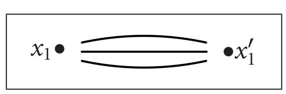
(2) *$p \neq m$ and there is a component of $X_0^D(N)_{\overline{\mathbb{F}}_p}$ fixed by $w_{m/p}$.*

**Proof** If $p = m$, this is an extension of a result of Rotger–Skorobogatov–Yafaev, [RSY05, Proposition 3.4].

Now suppose that $p \mid m$ but $p \neq m$ and recall the curve $M_{/\mathbf{Z}_p}$ of Theorem 2.7. Let $\pi' \colon N \to M$ be a minimal desingularization, so that $N_{\mathbb{F}_p}$ is the twist of $\mathcal{Z}_{\mathbb{F}_p}$ by $\mathbb{F}_{p^2}$ and $w_{m/p}$. Since $m \neq p$, $w_{m/p}$ is not the identity. Recall that a non-identity involution of $\mathbb{P}^1$ fixes exactly two points of $\mathbb{P}^1(\overline{\mathbb{F}}_p)$. Suppose that a component of $N_{\overline{\mathbb{F}}_p}$ is fixed by $w_{m/p}$ (under the isomorphism $N_{\overline{\mathbb{F}}_p} \cong \mathcal{Z}_{\overline{\mathbb{F}}_p} \cong \mathcal{X}_{\overline{\mathbb{F}}_p}$). Therefore there is a component $y \cong \mathbb{P}^1_{\mathbb{F}_p}$ of $\mathcal{Z}_{\mathbb{F}_p}$. Since all intersection points are rational and at most two singular intersection points stayed $\mathbb{F}_p$-rational, $y$ contains the image of a smooth $\mathbb{F}_p$ rational point. Since there is a smooth point of $\mathcal{Z}(\mathbb{F}_p)$, $C^D(N,d,m)(\mathbf{Q}_p)$ is nonempty by Hensel's Lemma.

Finally we note that if a component $C$ of $\mathcal{X}_{\overline{\mathbb{F}}_p}$ is fixed by $w_{m/p}$, then so is its image $\pi(C)$. If $\pi(C)$ is a component of $X_0^D(N)_{\overline{\mathbb{F}}_p}$, we are done. If $\pi(C)$ is not a component, then it is an intersection point of two components $C_1, C_2$ of $X_0^D(N)_{\overline{\mathbb{F}}_p}$. It follows that $w_{m/p}$ either fixes both of them or interchanges them. However, Theorem 2.7 tells us that under the bijection between components of $X_0^D(N)_{\overline{\mathbb{F}}_p}$ and $\operatorname{Pic}(D/p,N) \coprod \operatorname{Pic}(D/p,N)$, $C_1$ must lie in one copy and $C_2$ in the other. Since these bijections are $W/\langle w_p\rangle$-equivariant, $w_{m/p}$ cannot interchange $C_1$ and $C_2$ and must therefore fix them. ■

***Example 5.6*** Let $\mathcal{X} = X_0^{26}(1)_{/\mathbf{Z}_2}$, which is regular over $\mathbf{Z}_2$. Depicted below is the dual graph of $\mathcal{X}_{\overline{\mathbb{F}}_2}$. This tells us that $\mathcal{X}_{\overline{\mathbb{F}}_2}$ is simply two copies of $\mathbb{P}^1_{\overline{\mathbb{F}}_2}$ glued along the $\mathbb{F}_2$-rational points of each.




Since the action of $w_2 \operatorname{Frob}_2$ fixes each component and intersection point, the only fixed points are non-smooth, and thus $C^{26}(1,d,2)(\mathbf{Q}_2)$ is empty for all $d \equiv \pm 3 \bmod 8$. On the other hand, since the action of $w_{26} \operatorname{Frob}_2$ cannot interchange $x_1$ and $x_1'$, it must act non-trivially on each component, and thus there must be a smooth fixed point of $w_{26} \operatorname{Frob}_2$. It follows that $C^{26}(1,d,26)(\mathbf{Q}_2)$ is nonempty for all $d \equiv \pm 3 \bmod 8$.

***Lemma 5.7*** *If $p = m$ and $p$ is inert in $\mathbf{Q}(\sqrt{d})$, then $C^D(N,d,m)(\mathbf{Q}_p) \neq \varnothing$ if and only if one of the following occurs:*

(1) *For all primes $q \mid (D/p)$, $q \not\equiv 1 \bmod 4$, and for all primes $q \mid N$, $q \not\equiv 3 \bmod 4$.*
(2) *For all primes $q \mid (D/p)$, $q \not\equiv 1 \bmod 3$, and for all primes $q \mid N$, $q \not\equiv 2 \bmod 3$.*

**Proof** Eichler's Embedding Theorem shows that condition (1) is equivalent to $e_{D/p,N}(-4) \neq 0$ and condition (2) is equivalent to $e_{D/p,N}(-3) \neq 0$. We know that $e_{D/p,N}(-4) \neq 0$ if and only if there is a component of $X_0^D(N)_{\overline{\mathbb{F}}_p}$ with length divisible by two and $e_{D/p,N}(-3) \neq 0$ if and only if there is a component of $X_0^D(N)_{\overline{\mathbb{F}}_p}$ with length divisible by three. This is to say that one of the two conditions of the lemma occurs if and only if there is a component $y$ of $X_0^D(N)_{\overline{\mathbb{F}}_p}$ such that $\ell(y) > 1$. But then by Lemma 5.5 there is such a component if and only if $C^D(N,d,m)(\mathbf{Q}_p)$ is nonempty. ■

***Lemma 5.8*** *If $p \mid m$ and $p \neq m$, then $C^D(N,d,m)(\mathbf{Q}_p)$ is nonempty if and only if one of the following occurs:*

- *$m = 2p$ and one of $e_{D/p,N}(-4), e_{D/p,N}(-8)$ is nonzero.*
- *$m/p \not\equiv 3 \bmod 4$ and $e_{D/p,N}(-4m/p)$ is nonzero.*
- *$m/p \equiv 3 \bmod 4$ and one of $e_{D/p,N}(-4m/p)$ or $e_{D/p,N}(-m/p)$ is nonzero.*

**Proof** Suppose that $p \mid m$ and $p \neq m$. In view of Lemma 5.5, $C^D(N,d,m)(\mathbf{Q}_p)$ is nonempty if and only if a component of $X_0^D(N)_{\overline{\mathbb{F}}_p}$ is fixed by $w_{m/p}$. After Lemma 2.9, such a component corresponds to an element of $\mathrm{Pic}(D/p,N)$. After Lemma 2.21, such a component is fixed by $w_{m/p}$ if and only if there is an embedding of $\mathbf{Z}[\sqrt{-m/p}]$ (or $\mathbf{Z}[\zeta_4]$ if $m/p = 2$) into the QM endomorphisms of $(A,\iota)$. Such an embedding of an order $R$ exists if and only if there is an optimal embedding of an order $R' \supset R$. In this case, the only orders which contain $\mathbf{Z}[\sqrt{-m/p}]$ are itself or $\mathbf{Z}[\frac{1+\sqrt{-m/p}}{2}]$ if $m/p \equiv 3 \bmod 4$. Respectively, their discriminants are $-4m/p$ and $-m/p$, so the result follows from Eichler's Embedding Theorem. ■

## 5.2 The Proof when $p \nmid m$

If $p \nmid m$ then the action of $\mathrm{Frob}_p$ on the components and intersection points of $\mathcal{Z}_{\overline{\mathbb{F}}_p} \cong \mathcal{X}_{\overline{\mathbb{F}}_p}$ coincides with the action of $w_{mp}$. However, by Lemma 2.9, the action of $w_{mp}$ on $X_0^D(N)_{\overline{\mathbb{F}}_p}$ fixes no component. In fact, we conclude the following.

***Lemma 5.9*** *Suppose that $p \nmid m$ is unramified in $\mathbf{Q}(\sqrt{d})$. Then $C^D(N,d,m)(\mathbf{Q}_p)$ is nonempty if and only if there is a superspecial $w_{mp}$-fixed intersection point $x$ of even length in $X_0^D(N)_{\overline{\mathbb{F}}_p}$.*

**Proof** If $C^D(N,d,m)(\mathbf{Q}_p)$ is nonempty, then by Hensel's Lemma there is a smooth point of $\mathcal{Z}(\mathbb{F}_p)$. Therefore, there is a smooth point $P$ of $\mathcal{X}(\overline{\mathbb{F}}_p)$ fixed by $P \mapsto w_m P\,\mathrm{Frob}_p = w_{mp}P$. By Lemma 2.9, the action of $w_{mp}$ on $X_0^D(N)_{\overline{\mathbb{F}}_p}$ fixes no component. Therefore, $\pi(P) = x$ is the intersection point of two components. Since $P$ is smooth, $\pi^*(x(\mathrm{Spec}(\overline{\mathbb{F}}_p))) \neq P(\mathrm{Spec}(\overline{\mathbb{F}}_p))$. Therefore $\ell = \ell(x) > 1$ and thus

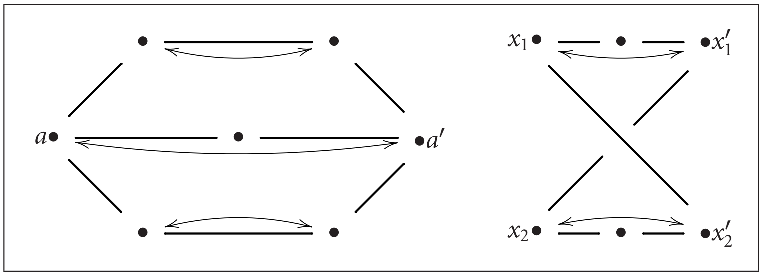



*Figure 1*: The dual graphs of $\mathcal{X}_{\overline{\mathbb{F}}_{13}}$ and $\mathcal{Y}_{\overline{\mathbb{F}}_2}$.

$\pi^*(x(\mathrm{Spec}(\overline{\mathbb{F}}_p))) = \bigcup_{i=1}^{\ell-1} C_i$ with $C_i \cong \mathbb{P}^1_{\overline{\mathbb{F}}_p}$ as in Definition 5.3. Since $w_{mp}(x) = x$, $w_{mp}C_i = C_{\ell-i}$. Therefore, the only component that could be fixed by $w_{mp}$ is $C_{\ell/2}$. If such a component exists, then $\ell$ must be even.

Conversely, if there is a superspecial $w_{mp}$-fixed intersection point $x$ of even length then $w_{mp}C_{\ell/2} = C_{\ell/2}$. There is thus a component of $\mathcal{Z}_{\overline{\mathbb{F}}_p}$ which is defined over $\mathbb{F}_p$. It follows that there is a smooth point in $\mathcal{Z}(\mathbb{F}_p)$ and therefore $C^D(N,d,m)(\mathbf{Q}_p)$ is nonempty. ∎

***Example 5.10*** Let $\mathcal{X}$ denote the regular $\mathbf{Z}_{13}$ model of $X_0^{26}(1)$ and let $\mathcal{Y}$ denote the regular $\mathbf{Z}_2$ model of $X_0^6(5)$. Depicted in Figure 1 are the dual graphs of $\mathcal{X}_{\overline{\mathbb{F}}_{13}}$ (on the left) and $\mathcal{Y}_{\overline{\mathbb{F}}_2}$ (on the right). Respectively the arrows denote the action of $w_2\,\mathrm{Frob}_{13}$ and $\mathrm{Frob}_2$.

Even though the intersection points of length 3 on $X_0^{26}(1)_{\overline{\mathbb{F}}_{13}}$ are fixed by the action of $w_2\,\mathrm{Frob}_{13}$, they can not yield smooth rational points, as the action exchanges $a$ with $a'$. The rational points here can only come from a fixed intersection point of length 2. Since there is such an intersection point on $X_0^{26}(1)_{\overline{\mathbb{F}}_2}$, there is a component of $\mathcal{X}_{\overline{\mathbb{F}}_2}$ fixed by the action of $w_2\,\mathrm{Frob}_{13}$. Thus $C^{26}(1,d,2)(\mathbf{Q}_{13})$ is nonempty for all $d$ such that $\left(\frac{d}{13}\right) = -1$. Similarly, because the two intersection points of length 2 on $X_0^6(5)_{\overline{\mathbb{F}}_2}$ are not interchanged by the action of $\mathrm{Frob}_2$, there are components of $\mathcal{Y}_{\overline{\mathbb{F}}_2}$ fixed by the action of $\mathrm{Frob}_2$. Therefore $X_0^6(5)(\mathbf{Q}_2)$ is nonempty.

***Theorem 5.11*** *If $p \nmid m$, $C^D(N,d,m)(\mathbf{Q}_p)$ is nonempty if and only if one of the following occurs:*

(1) $p = 2$, $m = 1$, $q \equiv 3 \bmod 4$ *for all* $q \mid (D/2)$, *and* $q \equiv 1 \bmod 4$ *for all* $q \mid N$.
(2) $p \equiv 1 \bmod 4$, $m = DN/(2p)$, $q \not\equiv 1 \bmod 4$ *for all* $q \mid (D/p)$, *and* $q \not\equiv 3 \bmod 4$ *for all* $q \mid N$.
(3) $p = 2$, $m = DN/2$, $q \equiv 3 \bmod 4$ *for all* $q \mid (D/2)$ *and* $q \equiv 1 \bmod 4$ *for all* $q \mid N$.
(4) $p \equiv 1 \bmod 4$, $m = DN/p$, $q \not\equiv 1 \bmod 4$ *for all* $q \mid (D/p)$, *and* $q \not\equiv 3 \bmod 4$ *for all* $q \mid N$.

**Proof** By Lemma 5.9, $C^D(N,d,m)(\mathbf{Q}_p)$ is nonempty if and only if there is a superspecial $w_{mp}$-fixed intersection point of even length. By Corollary 2.25, this can occur if and only if $mp \in \{1, 2, DN/2, DN\}$, and for all $q \mid (D/p)$, either $q = 2$ or

$q \equiv 3 \bmod 4$, and for all $q \mid Np$, either $q = 2$ or $q \equiv 1 \bmod 4$. ∎

We show how this gives a new proof of the Theorem of Jordan, Livné, and Ogg.

***Corollary 5.12*** *Let $D$ be the discriminant of an indefinite $\mathbf{Q}$-quaternion algebra, $N$ a square-free integer coprime to $D$ and $p \mid D$. Then $X_0^D(N)(\mathbf{Q}_p)$ is nonempty if and only if one of the following occurs:*

- $p = 2$, $q \equiv 3 \bmod 4$ *for all* $q \mid (D/2)$ *and* $q \equiv 1 \bmod 4$ *for all* $q \mid N$.
- $p \equiv 1 \bmod 4$, $D = 2p$ *and* $N = 1$.

**Proof** If $p = 2$, we are in case (1) of Theorem 5.11. We cannot have $p = DN$ for any $p$ since $p \mid D$ and thus $D$ is divisible by at least two primes, so Theorem 5.11 (3) or (4) cannot occur. If $DN = 2p$ with $p \equiv 1 \bmod 4$ then we must at least have $(2p) \mid D$, but then $D = 2p$ and $N = 1$. ∎

Finally we give a family of examples of twists of $X_0^D(N)$ which have points everywhere locally.

***Example 5.13*** Let $q$ be an odd prime and $g$ the genus of $X_0^{2q}(1)$. Let $p \equiv 3 \bmod 8$ such that $(\frac{-p}{q}) = -1$ and for all odd primes $\ell$ less than $4g^2$, $(\frac{-p}{\ell}) = -1$. Consider the twist $C^{2q}(1, -p.2q)$ of $X_0^{2q}(1)$.

Note that since $p \equiv 3 \bmod 8$ and $(\frac{-p}{q}) = -1$, both 2 and $q$ are inert in $\mathbf{Q}(\sqrt{-p})$. Therefore $C^{2q}(1, -p, 2q)(\mathbf{Q}_2)$ and $C^{2q}(1, -p, 2q)(\mathbf{Q}_q)$ are both nonempty by Corollary 5.2.

Since $(\frac{-p}{q}) = -1$ and $p \equiv 3 \bmod 4$, $(\frac{q}{p}) = -1$. Since $p \equiv 3 \bmod 8$, $(\frac{-1}{p}) = -1$ and $(\frac{2}{p}) = -1$. Therefore $(\frac{-2q}{p}) = -1$ and $(\frac{-p}{2}) = (\frac{p}{2}) = -1$. Since we already had $(\frac{-p}{q}) = -1$, we can apply Theorem 4.1 to say $C^{2q}(1, -p, 2q)(\mathbf{Q}_p) \neq \varnothing$.

Let $\ell \nmid 2pq$ be a prime. If $\ell > 4g^2$ then we can apply Theorem 3.1 to see that $C^{2q}(1, -p.2q)(\mathbf{Q}_\ell)$ is nonempty. If $\ell < 4g^2$ then we can apply Corollary 3.17 to see that $C^{2q}(1, -p, 2q)(\mathbf{Q}_\ell)$ is nonempty.

Finally, since $-p < 0$, $C^{2q}(1, -p, 2q) \ncong_{\mathbf{R}} X_0^{2q}(1)$, the latter of which does not have real points [Cla03, Theorem 55]. Therefore $\big(X_0^{2q}(1)/w_{2q}\big)(\mathbf{R}) \neq \varnothing$ if and only if $C^{2q}(1, -p, 2q)(\mathbf{R})$ is nonempty. By Eichler's Embedding Theorem, there is an embedding of $\mathbf{Z}[\sqrt{-2q}]$ into any maximal order in $B_{2q}$ and thus $X_0^{2q}(1)/w_{2q}$ has real points [Ogg83, Theorem 3].

## 6 Local Points when $p \mid N$

Fix a square-free integer $d$, an integer $m \mid DN$, and a prime $p \mid N$ unramified in $\mathbf{Q}(\sqrt{d})$. Let $C^D(N, d, m)_{/\mathbf{Q}}$ be the twist of $X_0^D(N)_{/\mathbf{Q}}$ by $\mathbf{Q}(\sqrt{d})$ and $w_m$.

***Theorem 6.1*** *Let $p \mid N$ be unramified in $\mathbf{Q}(\sqrt{d})$ and $m \mid DN$. Then $C^D(N, d, m)(\mathbf{Q}_p)$ is nonempty if and only if (1) or (2) holds.*

(1) *$p$ is split in $\mathbf{Q}(\sqrt{d})$ and one of the following conditions holds:*

- $D = 1$ [Lemma 6.8].

https://doi.org/10.4153/CJM-2013-023-8 Published online by Cambridge University Press

- $p = 2$, $D = \prod_i p_i$ *with each* $p_i \equiv 3 \bmod 4$, *and* $N/p = \prod_j q_j$ *with each* $q_j \equiv 1 \bmod 4$ [Lemma 6.11].
- $p = 3$, $D = \prod_i p_i$ *with each* $p_i \equiv 2 \bmod 3$, *and* $N/p = \prod_j q_j$ *with each* $q_j \equiv 1 \bmod 3$ [Lemma 6.12].
- $TF'(D, N, 1, p) > 0$ [Definition 6.13, Lemma 6.14].

(2) *$p$ is inert in $\mathbf{Q}(\sqrt{d})$, and there are prime factorizations $Dp = \prod_i p_i$, $N/p = \prod_j q_j$ such that one of the following two conditions holds:*

(i) *$p \mid m$ and one of the following two conditions holds* [Theorem 6.7].

- *$p = 2$, $m = p$ or $DN$, for all $i$, $p_i \equiv 3 \bmod 4$, and for all $j$, $q_j \equiv 1 \bmod 4$.*
- *$p \equiv 3 \bmod 4$, $m = p$ or $2p$, for all $i$, $p_i \not\equiv 1 \bmod 4$, and for all $j$, $q_j \not\equiv 3 \bmod 4$.*

(ii) *$p \nmid m$ and one of the following nine conditions holds:*

- $m = D = 1$ [Lemma 6.8].
- *$p = 2$, $m = 1$, for all $i$, $p_i \equiv 3 \bmod 4$, and for all $j$, $q_j \equiv 1 \bmod 4$* [Lemma 6.11].
- *$p = 3$, $m = 1$, for all $i$, $p_i \equiv 2 \bmod 3$, and for all $j$, $q_j \equiv 1 \bmod 3$* [Lemma 6.12].
- *$p \equiv 3 \bmod 4$, $m = DN/2p$, $p_i \not\equiv 1 \bmod 4$ for all $i$, and $q_j \not\equiv 3 \bmod 4$ for all $j$* [Lemma 6.11].
- *$p \equiv 2 \bmod 3$, $m = DN/3p$, $p_i \not\equiv 1 \bmod 3$ for all $i$, and $q_j \not\equiv 2 \bmod 3$ for all $j$* [Lemma 6.12].
- *$m = DN/p$, $p_i \not\equiv 1 \bmod 4$ for all $i$, and $q_j \not\equiv 3 \bmod 4$ for all $j$* [Lemma 6.11].
- *$m = DN/p$, $p_i \not\equiv 1 \bmod 3$ for all $i$, and $q_j \not\equiv 2 \bmod 3$ for all $j$* [Lemma 6.12].
- $TF'(D, N, m, p) > 0$ [Definition 6.13, Lemma 6.14].

***Corollary 6.2*** *Let $p$ be a prime dividing $N$ such that $p$ is unramified in $\mathbf{Q}(\sqrt{d})$. Then $C^D(N, d, DN)(\mathbf{Q}_p)$ is nonempty if and only if either*

- *$p$ is split in $\mathbf{Q}(\sqrt{d})$ and one of the following conditions holds:*
  - $D = 1$.
  - *$p = 2$, $D = \prod_i p_i$ with each $p_i \equiv 3 \bmod 4$, and $N/p = \prod_j q_j$ with each $q_j \equiv 1 \bmod 4$.*
  - *$p = 3$, $D = \prod_i p_i$ with each $p_i \equiv 2 \bmod 3$, and $N/p = \prod_j q_j$ with each $q_j \equiv 1 \bmod 3$.*
  - $TF'(D, N, 1, p) > 0$.

*or*

- *$p$ is inert in $\mathbf{Q}(\sqrt{d})$ with $Dp = \prod_i p_i$, $N/p = \prod_j q_j$ such that one of the following holds:*
  - *$p = 2$, for all $i$, $p_i \equiv 3 \bmod 4$ and for all $j$, $q_j \equiv 1 \bmod 4$.*
  - *$p \equiv 3 \bmod 4$, $D = 1$ and $N = p$ or $2p$.*

***Definition 6.3*** Assume that $p \mid N$. Let $X_0^D(N)_{/\mathbf{Z}_p}$ be as in Theorem 2.8 and let $\pi\colon \mathcal{X} \to X_0^D(N)$ be a minimal desingularization, so that $\mathcal{X}_{\mathbf{Z}_p}$ is a regular model for

https://doi.org/10.4153/CJM-2013-023-8 Published online by Cambridge University Press

$X_0^D(N)_{\mathbf{Q}_p}$.

The model $\mathcal{X}$ is equipped with a closed embedding $c' : X_0^D(N/p)_{/\mathbb{F}_p} \to \mathcal{X}$ such that $\pi c' = c$, the embedding defined in Theorem 2.8. Let $\sigma$ be such that $\langle \sigma \rangle = \mathrm{Aut}_{\mathbf{Z}_p}(\mathbf{Z}_{p^2})$.

***Definition 6.4*** Let $\mathcal{Z}$ be the étale quotient of $\mathcal{X}_{\mathbf{Z}_{p^2}}$ by the action of $w_m \circ \sigma$.

Note that if $p$ is inert in $\mathbf{Q}(\sqrt{d})$ then $\mathbf{Z}_p[\sqrt{d}] \cong \mathbf{Z}_{p^2}$ and thus the generic fiber of $\mathcal{Z}$ is $C^D(N,d,m)_{\mathbf{Q}_p}$. Therefore $\mathcal{Z}$ is a regular model of $C^D(N,d,m)_{\mathbf{Q}_p}$ if $p$ is inert in $\mathbf{Q}(\sqrt{d})$.

We also note that if $p$ is split in $\mathbf{Q}(\sqrt{d})$, or if $p$ is inert and $m = 1$, then

$$C^D(N,d,m)_{\mathbf{Q}_p} \cong X_0^D(N)_{\mathbf{Q}_p}.$$

Therefore, if $p$ is split in $\mathbf{Q}(\sqrt{d})$, we can consider $d'$ to be any square-free integer such that $p$ is inert in $\mathbf{Q}(\sqrt{d'})$ and $\mathcal{Z}'$ to be the regular model of $C^D(N,d',1)_{\mathbf{Q}_p} \cong X_0^D(N)_{\mathbf{Q}_p}$. Therefore, we shall obtain our results when $p$ is split as a corollary to our results when $p \nmid m$.

We shall organize our results into two sections. In the first, we will consider the case when $p \mid m$. In that case, $w_m$ and thus the twisted action of Galois will permute $c'\big(X_0^D(N/p)_{\mathbb{F}_p}\big)$ and $w_p c'\big(X_0^D(N/p)_{\mathbb{F}_p}\big)$ on the special fiber. In the second, we will consider the case when $p \nmid m$, and we may have to additionally allow for points on $c'\big(X_0^D(N/p)_{\mathbb{F}_p}\big)$. Note also that if $X^o$ denotes the complement of the superspecial points in $X$, $X_0^D(N)^o_{\mathbb{F}_p} = c'\big(X_0^D(N/p)^o_{\mathbb{F}_p}\big) \coprod w_p c'\big(X_0^D(N/p)^o_{\mathbb{F}_p}\big)$.

## 6.1 The Proof when $p \mid m$ is Inert

Suppose that $D$ is the discriminant of an indefinite quaternion $\mathbf{Q}$-algebra, $N, d$ are square-free integers with $(D,N) = 1$, $m \mid DN$, and $p \mid m$ is inert in $\mathbf{Q}(\sqrt{d})$. Fix $\mathcal{X}$ and $\mathcal{Z}$ as in Definition 6.3. If $p \mid m$, the action of $w_m$ on the regular model $\mathcal{X}$ interchanges $c'(X_0^D(N/p)_{\mathbb{F}_p})$ and $w_p c'(X_0^D(N)_{\mathbb{F}_p})$. Therefore if $P$ denotes an element of $\mathcal{Z}(\mathbb{F}_p)$, then $\pi(P(\mathrm{Spec}(\mathbb{F}_p)))$ must lie on both copies of $X_0^D(N/p)_{\mathbb{F}_p}$. This is to say that the base change to $\overline{\mathbb{F}}_p$ of $\pi P$ is a superspecial point, say $x$.

***Lemma 6.5*** *If $D,N,d,m,p$ are as described in the beginning of this chapter and $p \mid m$ is inert in $\mathbf{Q}(\sqrt{d})$, then $C^D(N,d,m)(\mathbf{Q}_p) \neq \varnothing$ if and only if there is a superspecial $w_{m/p}$-fixed point $x \in X_0^D(N)(\overline{\mathbb{F}}_p)$ of even length.*

**Proof** By abuse of notation, let $\mathrm{Frob}_p = \phi_1^* : \mathrm{Spec}(\overline{\mathbb{F}}_p) \to \mathrm{Spec}(\overline{\mathbb{F}}_p)$ where $\phi_1 : \overline{\mathbb{F}}_p \to \overline{\mathbb{F}}_p$. Note that under the bijection from $\mathcal{Z}(\overline{\mathbb{F}}_p)$ to $\mathcal{X}(\overline{\mathbb{F}}_p)$, the Galois action $P \mapsto P\,\mathrm{Frob}_p$ on $\mathcal{Z}(\overline{\mathbb{F}}_p)$ translates to the action of $P \mapsto w_m P\,\mathrm{Frob}_p$ on $\mathcal{X}(\overline{\mathbb{F}}_p)$.

Suppose that $C^D(N,d,m)(\mathbf{Q}_p)$ is nonempty. Then by Hensel's Lemma [JL85, Lemma 1.1] there must be an element of $\mathcal{Z}^{sm}(\mathbb{F}_p)$, or rather a smooth point, such that $P = w_m P\,\mathrm{Frob}_p$ in $\mathcal{X}(\overline{\mathbb{F}}_p)$. Since $p \mid m$, $w_m$ interchanges $c\big(X_0^D(N/p)_{\overline{\mathbb{F}}_p}\big)$ with $w_p c\big(X_0^D(N/p)_{\overline{\mathbb{F}}_p}\big)$. A smooth fixed point $P$ of $w_m \circ \mathrm{Frob}_p$ must therefore map to a superspecial point under $\pi$.

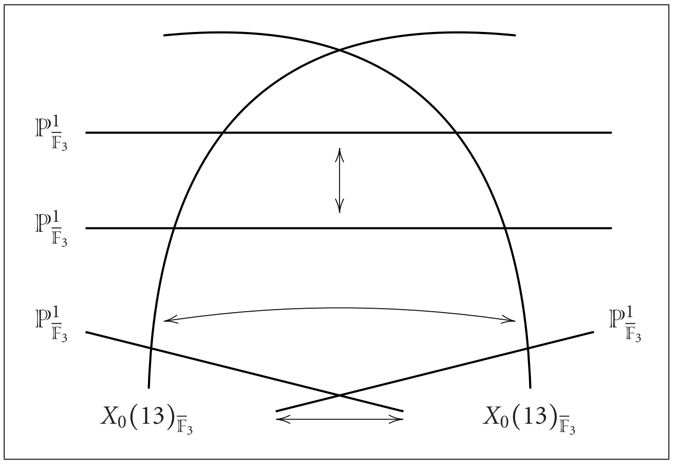



*Figure 2*: The $\overline{\mathbb{F}}_3$ special fiber of $\mathcal{X}$.

Suppose that there is such a smooth fixed point $P$. Let $\ell = \ell(x)$, so that smoothness implies $\ell > 1$. We have $\pi^* x\big(\operatorname{Spec}(\overline{\mathbb{F}}_p)\big) = \bigcup_{i=1}^{\ell-1} C_i$ with $C_i \cong \mathbb{P}^1_{\overline{\mathbb{F}}_p}$ and if $i < j$,

$$C_i \cdot C_j = \begin{cases} 1 & \text{if } j = i+1, 1 \le i < \ell, \\ 0 & \text{otherwise.} \end{cases}$$

By Lemma 2.22 $x\,\mathrm{Frob}_p = w_p(x)$, so we have $w_m \circ \mathrm{Frob}_p(x) = w_m w_p(x) = w_{m/p}(x)$. Therefore by continuity, $w_{m/p}$ fixes each $C_i$ and for each $i$, $w_p C_i = C_{\ell-i}$. Therefore, unless $\ell$ is even we arrive at a contradiction.

Conversely suppose that there is a superspecial point $x$ such that $\ell = \ell(x)$ is even and $w_{m/p}(x) = x$. Then we have $C_1, \dots, C_{\ell-1}$ fixed by $w_{m/p}$ by assumption. Since $w_p$ fixes $C_{\ell/2}$, it follows that $C_{\ell/2}$ is defined over $\mathbb{F}_p$. Therefore by Hensel's Lemma, $C^D(N,d,m)(\mathbf{Q}_p) \neq \varnothing$. ∎

***Example 6.6*** The diagram in Figure 2 depicts the special fiber of $\mathcal{X}$ over $\overline{\mathbb{F}}_3$ where $\mathcal{X}$ denotes the regular $\mathbf{Z}_3$-model of $X_0^1(39) = X_0(39)$ with the action $w_{39}\,\mathrm{Frob}_3$ given by the arrows.

Note the resolutions of the four superspecial points of $X_0(39)_{\overline{\mathbb{F}}_3}$: 1 of length 1, 2 of length 2 and 1 of length 3. Note also that while there are superspecial points of length 2 and there are some superspecial points fixed by the action of $w_{39}\,\mathrm{Frob}_3$, there are no superspecial points of length 2 fixed by the action of $w_{13}$. As a consequence, if 3 is inert in $\mathbf{Q}(\sqrt{d})$ then $C^1(39,d,39)(\mathbf{Q}_3)$ is empty, because there are no smooth fixed points of $w_{39}\,\mathrm{Frob}_3$ on $\mathcal{X}_{\overline{\mathbb{F}}_3}$.

This example illustrates an error in the criterion of Theorem 1.1(3) in the recent paper of Ozman [Ozm12]. The correct numerical criterion is properly given by Corollary 6.2, via the following theorem.

https://doi.org/10.4153/CJM-2013-023-8 Published online by Cambridge University Press

***Theorem 6.7*** *Suppose that $D, N, d, m$ and $p$ are as in Theorem 6.1 and $p \mid m$ is inert in $\mathbf{Q}(\sqrt{d})$. Then $C^D(N,d,m)(\mathbf{Q}_p) \neq \varnothing$ if and only if*

- *$p = 2$, $m = p$ or $DN$, for all $q \mid D$, $q \equiv 3 \bmod 4$, and for all $q \mid (N/2)$, $q \equiv 1 \bmod 4$, or*
- *$p \equiv 3 \bmod 4$, $m = p$ or $2p$, for all $q \mid D$ $q \not\equiv 1 \bmod 4$, and for all $q \mid (N/p)$, $q \not\equiv 3 \bmod 4$.*

**Proof** By Lemma 6.5, $C^D(N,d,m)(\mathbf{Q}_p)$ is nonempty if and only if there is a superspecial $w_{m/p}$-fixed point of even length in $X_0^D(N)(\overline{\mathbb{F}}_p)$. By Lemma 2.9, the QM endomorphism ring of a superspecial point on $X_0^D(N)(\overline{\mathbb{F}}_p)$ has discriminant $D' = Dp$ and level $N' = N/p$. Note that $D'N' = DN$. By Lemma 2.25, there is a superspecial $w_{m/p}$-fixed point of even length if and only if $m/p \in \{1, 2, DN/2, DN\}$, and for all $q \mid Dp$, $q = 2$ or $q \equiv 3 \bmod 4$, and for all $q \mid (N/p)$, $q = 2$ or $q \equiv 1 \bmod 4$. ∎

## 6.2 The Proof When $p \nmid m$ is Split or Inert

We begin with the following observation regarding cusps, which are points that can only exist if $D = 1$.

***Lemma 6.8*** ([Ogg74, Proposition 3]) *If $N$ is square-free and $m \mid N$, then $w_m$ fixes a cusp of $X_0^1(N)$ if and only if $m = 1$.*

Therefore in our setting, $C^1(N,d,m)(\mathbf{Q}_p)$ contains a cusp if and only if either $p$ is split in $\mathbf{Q}(\sqrt{d})$ or $m = 1$. We now illustrate the three ways in which $C^D(N,d,m)(\mathbf{Q}_p)$ could be nonempty.

***Example 6.9*** Let $D = 6, N = p = 11$, $m = 1$ and $d$ any integer such that 11 is inert in $\mathbf{Q}(\sqrt{d})$, say $-1$ for instance. Note that $C^6(11,-1,1) \cong_{\mathbf{Q}_{11}} X_0^6(11)$. Let $\mathcal{X}$ denote the regular $\mathbf{Z}_{11}$-model of $X_0^6(11)$. Then the diagram in Figure 3 depicts $\mathcal{X}_{\overline{\mathbb{F}}_{11}}$ where the arrows describe the action of $w_1 \operatorname{Frob}_{11} = \operatorname{Frob}_{11}$.

We check to see if $X_0^6(11)(\mathbf{Q}_{11})$ is nonempty as follows. Although there are intersection points of length 2 and 3 on $X_0^6(11)_{\overline{\mathbb{F}}_{11}}$, none are fixed by the action of $\operatorname{Frob}_{11}$. Therefore the only way that $X_0^6(11)(\mathbf{Q}_{11})$ could be nonempty would be if there were a nonsuperspecial point in $X_0^6(1)(\mathbb{F}_{11})$. Using the trace formula, or the fact that there are only four superspecial points on $X_0^6(1)_{\mathbb{F}_{11}} \cong \mathbb{P}^1_{\mathbb{F}_{11}}$, we conclude that $X_0^6(11)(\mathbf{Q}_{11})$ is nonempty.

***Lemma 6.10*** *Let $D, N, d, m, p$ be as in Theorem 6.1 and suppose $p \nmid m$ is unramified in $\mathbf{Q}(\sqrt{d})$. Suppose that $C^D(N,d,m)(\mathbf{Q}_p)$ does not contain a cusp. Then $C^D(N,d,m)(\mathbf{Q}_p) \neq \varnothing$ if and only if one of the following occurs:*

- *There is a superspecial $w_{mp}$-fixed point of even length on $X_0^D(N)(\overline{\mathbb{F}}_p)$.*
- *There is a superspecial $w_{mp}$-fixed point of length divisible by three on $X_0^D(N)(\overline{\mathbb{F}}_p)$.*
- *There is a non-superspecial point of $C^D(N/p,d,m)(\mathbb{F}_p)$.*

**Proof** Recall that there is a bijection from $\mathcal{Z}(\overline{\mathbb{F}}_p)$ to $\mathcal{X}(\overline{\mathbb{F}}_p)$, under which the Galois action $P \mapsto P \operatorname{Frob}_p$ on $\mathcal{Z}(\overline{\mathbb{F}}_p)$ translates to the action $P \mapsto w_m P \operatorname{Frob}_p$ on $\mathcal{X}(\overline{\mathbb{F}}_p)$.

https://doi.org/10.4153/CJM-2013-023-8 Published online by Cambridge University Press

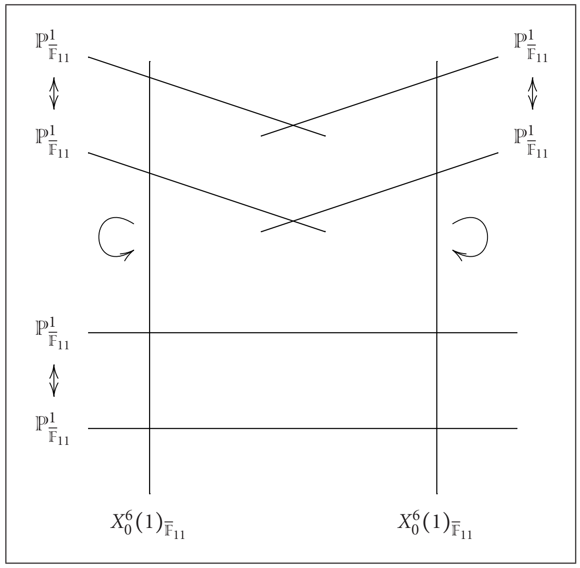



*Figure 3*: The $\overline{\mathbb{F}}_{11}$ special fiber of $\mathcal{X}$.

By Lemma 2.22, the action of $\mathrm{Frob}_p$ on the superspecial points of $X_0^D(N)_{\overline{\mathbb{F}}_p}$ is the action of $w_p$. Therefore a superspecial $\mathbb{F}_p$-rational point of $\mathcal{Z}$ corresponds to a superspecial $w_{mp}$-fixed point of $X_0^D(N)_{\overline{\mathbb{F}}_p}$.

Suppose now that $C^D(N,d,m)(\mathbf{Q}_p)$ is nonempty, or equivalently, by Hensel's Lemma, that $\mathcal{Z}^{sm}(\mathbb{F}_p)$ is nonempty. Suppose further that there are no superspecial $w_{mp}$-fixed points of length divisible by 2 or 3, that is, all superspecial points fixed by $w_{mp}$ have length 1. It follows that if $P$ is a smooth fixed point of $w_{mp}$ in $\mathcal{X}(\overline{\mathbb{F}}_p)$, then $\pi(P) = x$ is not superspecial.

Conversely, suppose first that there is an $\mathbb{F}_p$-rational point of $\mathcal{Z}$ which is not superspecial. By the embedding $c\colon X_0^D(N/p)_{\mathbb{F}_p} \to X_0^D(N)_{\mathbb{F}_p}$, there is a non-superspecial $\mathbb{F}_p$-rational point of $\mathcal{Z}$. Since $X_0^D(N)_{\overline{\mathbb{F}}_p}$ is smooth away from superspecial points, $C^D(N,d,m)(\mathbf{Q}_p)$ is nonempty by Hensel's lemma.

Let $x$ be a superspecial $w_{mp}$-fixed point with $\ell = \ell(x) > 1$. Then

$$\pi^*(x(\mathrm{Spec}(\overline{\mathbb{F}}_p))) = \bigcup_{i=1}^{\ell-1} C_i,$$

with $C_i \cong \mathbb{P}^1_{\overline{\mathbb{F}}_p}$ and at most two singular points in $\mathcal{X}_{\overline{\mathbb{F}}_p}$ on each $C_i$. Since $w_m x\,\mathrm{Frob}_p = w_{mp}(x) = x$, for all $i$, $w_m\,\mathrm{Frob}_p\,C_i = w_{mp}C_i = C_i$ by continuity of $\pi$. Therefore $C_i$ defines an $\mathbb{F}_p$-rational component of $\mathcal{Z}_{\overline{\mathbb{F}}_p}$ with at most two singular points. Therefore $\mathcal{Z}^{sm}(\mathbb{F}_p)$ is nonempty, and by Hensel's Lemma, $\mathcal{Z}(\mathbf{Q}_p)$ is nonempty. ■

***Lemma 6.11*** *There is a superspecial $w_{mp}$-fixed point of even length on $X_0^D(N)_{\overline{\mathbb{F}}_p}$ if and only if one of the following occurs:*

https://doi.org/10.4153/CJM-2013-023-8 Published online by Cambridge University Press

(1) $p = 2$, $m = 1$, $q \equiv 3 \bmod 4$ *for all primes* $q \mid D$, *and* $q \equiv 1 \bmod 4$ *for all primes* $q \mid (N/2)$.
(2) $p \equiv 3 \bmod 4$, $2 \mid DN/p$, $m = DN/2p$, $q \not\equiv 1 \bmod 4$ *for all primes* $q \mid D$, *and* $q \not\equiv 3 \bmod 4$ *for all primes* $q \mid (N/p)$.
(3) $m = DN/p$, $p \not\equiv 1 \bmod 4$, $q \not\equiv 1 \bmod 4$ *for all primes* $q \mid D$, *and* $q \not\equiv 3 \bmod 4$ *for all primes* $q \mid (N/p)$.

**Proof** By Lemma 2.25, there is a superspecial $w_{mp}$-fixed point of even length if and only if $mp \in \{1, 2, DN/2, DN\}$, and for all primes $q \mid Dp$, $q = 2$ or $q \equiv 3 \bmod 4$, and for all primes $q \mid (N/p)$, $q = 2$ or $q \equiv 1 \bmod 4$. ∎

***Lemma 6.12*** *There is a superspecial point of length divisible by three in* $X_0^D(N)(\overline{\mathbb{F}}_p)$ *fixed by* $w_{mp}$ *if and only if one of the following occurs:*

(1) $p = 3$, $m = 1$, $q \equiv 2 \bmod 3$ *for all primes* $q \mid D$, *and* $q \equiv 1 \bmod 3$ *for all primes* $q \mid (N/3)$.
(2) $p \equiv 2 \bmod 3$, $3 \mid DN/p$, $m = DN/3p$, $q \not\equiv 1 \bmod 3$ *for all primes* $q \mid D$, *and* $q \not\equiv 2 \bmod 3$ *for all primes* $q \mid (N/p)$.
(3) $m = DN/p$, $p \not\equiv 1 \bmod 3$, $q \not\equiv 1 \bmod 3$ *for all primes* $q \mid D$, *and* $q \not\equiv 2 \bmod 3$ *for all primes* $q \mid (N/p)$.

**Proof** The proof is similar to that of Lemma 6.11. ∎

We note that since $p \nmid (DN/p)$ and $m \mid (DN/p)$, we may recall that

$$TF(D, N/p, m, p) = (p + 1) - \operatorname{tr}(T_{pm}),$$

as in Definition 3.15. With this in mind we make the following definition.

***Definition 6.13*** If $p \mid N$ and $m \mid (DN/p)$, we let

$$TF'(D, N, m, p)$$
$$:= \begin{cases} TF(D, N/p, m, p) - \left( \frac{e_{Dp,N/p}(-4)}{w(-4)} + \frac{e_{Dp,N/p}(-8)}{w(-8)} \right) & mp = 2, \\ TF(D, N/p, m, p) - \left( \frac{e_{Dp,N/p}(-4mp)}{w(-4mp)} + \frac{e_{Dp,N/p}(-mp)}{w(-mp)} \right) & mp \neq 2, mp \not\equiv 3 \bmod 4, \\ TF(D, N/p, m, p) - \frac{e_{Dp,N/p}(-4mp)}{w(-4mp)} & mp \equiv 3 \bmod 4. \end{cases}$$

***Lemma 6.14*** *There is a non-superspecial* $\mathbb{F}_p$*-rational point of* $\mathcal{Z}$ *if and only if* $TF'(D, N, m, p) > 0$.

**Proof** Let $\mathcal{Y}_{/\mathbf{Z}_p}$ denote the smooth model of $C^D(N/p, d, m)$. By Theorem 3.14, $\#\mathcal{Y}(\mathbb{F}_p) = (p + 1) - \operatorname{tr}(T_{pm}) = TF(D, N/p, m, p)$. By Lemma 2.22, there is a superspecial point in $\mathcal{Y}(\mathbb{F}_p)$ if and only if there is a superspecial point fixed by $w_{mp}$ in $X_0^D(N)(\overline{\mathbb{F}}_p)$. By Corollary 2.21, there is a superspecial point $x$ in $X_0^D(N/p)(\overline{\mathbb{F}}_p)$ fixed by $w_{mp}$ if and only if $\mathbf{Z}[\sqrt{-mp}]$ (or $\mathbf{Z}[\zeta_4]$ if $mp = 2$) embeds into $\operatorname{End}_{\iota(\mathcal{O})}(A)$ where $(A, \iota)$ corresponds to $x$.

We now count the number $n_{mp}$ of $w_{mp}$-fixed superspecial points, so that we can subtract them off. Suppose that $\mathcal{O}'$ is an Eichler order $\mathcal{O}'$ of level $N/p$ in $B_{Dp}$, $\wp_m$ is the unique two-sided ideal of norm $mp$ in $\mathcal{O}'$, and $M_1, \dots, M_h$ are right ideals of $\mathcal{O}'$ which form a complete set of representatives of $\mathrm{Pic}(D/p, Np)$. Under Lemma 2.9, $n_{mp}$ is the number of indices $i$ such that $M_i \cong M_i \otimes \wp_m$. Thus [Vig80, p. 152], the number of such superspecial fixed points is the number of embeddings of $\mathbf{Z}[\sqrt{-mp}]$ (or $\mathbf{Z}[\zeta_4]$ if $mp = 2$) into any left order of an $M_i$. If $mp = 2$, then the number of these is

$$\frac{e_{Dp,N/p}(-4)}{w(-4)} + \frac{e_{Dp,N/p}(-8)}{w(-8)}.$$

If $mp \neq 2$ and $mp \not\equiv 3 \bmod 4$, then the number of these is

$$\frac{e_{Dp,N/p}(-4mp)}{w(-4mp)}.$$

If $mp \equiv 3 \bmod 4$, then the number of these is

$$\frac{e_{Dp,N/p}(-mp)}{w(-mp)} + \frac{e_{Dp,N/p}(-4mp)}{w(-4mp)}. \qquad \blacksquare$$

Unlike the case $p \mid D$, the conditions under which $X_0^D(N)(\mathbf{Q}_p)$ is nonempty were not previously known when $p \mid N$ and $D > 1$. In the following, we eschew the $TF'$ notation to show how it is possible to directly compute on the special fiber of this Shimura curve. Note that condition (4) is simply the inequality $TF'(D, N, 1, p) > 0$.

***Theorem 6.15*** *Let $D$ be the discriminant of an indefinite $\mathbf{Q}$-quaternion algebra, $N$ a square-free integer coprime to $D$, and $p \mid N$. Then $X_0^D(N)(\mathbf{Q}_p)$ is nonempty if and only if one of the following occurs:*

(1) $D = 1$.

(2) $p = 2$, *for all* $q \mid D$, $q \equiv 3 \bmod 4$, *and for all* $q \mid (N/2)$, $q \equiv 1 \bmod 4$.

(3) $p = 3$, $m = 1$, *for all* $q \mid D$, $q \equiv 2 \bmod 3$, *and for all* $q \mid (N/3)$, $q \equiv 1 \bmod 3$.

(4) *The following inequality holds:*

$$\sum_{\substack{s=-\lfloor 2\sqrt{p}\rfloor \\ s\neq 0}}^{\lfloor 2\sqrt{p}\rfloor} \left( \sum_{f \mid f(s^2-4p)} \frac{e_{D,N/p}\left(\frac{s^2-4p}{f^2}\right)}{w\left(\frac{s^2-4p}{f^2}\right)} \right) > 0.$$

**Proof** First we note that if $D = 1$, then there is a $\mathbf{Q}$-rational cusp by Lemma 6.8. Set $m = 1$ and assume $D \neq 1$. By Lemma 6.10, $X_0^D(N)(\mathbf{Q}_p)$ is non-empty if and only if one of the following occurs:

- There is a superspecial $w_p$-fixed point of even length in $X_0^D(N)(\overline{\mathbb{F}}_p)$.
- There is a superspecial $w_p$-fixed point of length divisible by three in $X_0^D(N)(\overline{\mathbb{F}}_p)$.
- There is a non-superspecial $\mathbb{F}_p$-rational point.

By Lemma 6.11, there is a $w_p$ fixed point of even length if and only if one of the following occurs:

- $p = 2$, for all $q \mid D$, $q \equiv 3 \bmod 4$ and for all $q \mid (N/2)$, $q \equiv 1 \bmod 4$.
- $p \equiv 3 \bmod 4$ and $DN = 2p$.

https://doi.org/10.4153/CJM-2013-023-8 Published online by Cambridge University Press

- $DN = p$ and $p = 2$ or $p \equiv 3 \bmod 4$.

However, if either of the latter two occurs, then $D = 1$, in contradiction to our assumption.

By Lemma 6.12, there is a $w_p$ fixed point whose length is divisible by three if and only if one of the following occurs:

- $p = 3$, for all $q \mid D$, $q \equiv 2 \bmod 3$ and for all $q \mid (N/3)$, $q \equiv 1 \bmod 3$.
- $p \equiv 2 \bmod 3$ and $DN = 3p$.
- $DN = p$ and $p = 3$ or $p \equiv 2 \bmod 3$.

Once again, if either of the latter two occurs, $D = 1$. Suppose now that in addition to $D \neq 1$, all superspecial points have length 1, so the number of non-superspecial $\mathbb{F}_p$-rational points on $X_0^D(N/p)$ can be written as

$$(p+1) - \operatorname{tr}(T_p) - \sum_{f \mid f(-4p)} \frac{e_{Dp,N/p}(\frac{-4p}{f^2})}{w(\frac{-4p}{f^2})}.$$

Recall now Theorem 3.9, the Eichler–Selberg trace formula on $H^0\big(X_0^D(N/p)_{\overline{\mathbb{F}}_p}, \Omega\big)$:

$$\operatorname{tr}(T_p) = (p+1) - \sum_{s=-\lfloor 2\sqrt{p}\rfloor}^{\lfloor 2\sqrt{p}\rfloor} \Bigg( \sum_{f \mid f(s^2-4p)} \frac{e_{D,N/p}(\frac{s^2-4p}{f^2})}{w(\frac{s^2-4p}{f^2})} \Bigg).$$

Therefore, if $p \neq 2$ there is a non-superspecial $\mathbb{F}_p$-rational point of $X_0^D(N/p)$ if and only if the following quantity is nonzero:

$$\begin{aligned}
(p+1) - \Bigg( (p+1) - \sum_{s=-\lfloor 2\sqrt{p}\rfloor}^{\lfloor 2\sqrt{p}\rfloor} \Big( \sum_{f \mid f(s^2-4p)} \frac{e_{D,N/p}(\frac{s^2-4p}{f^2})}{w(\frac{s^2-4p}{f^2})} \Big) \Bigg) - \sum_{f \mid f(-4p)} \frac{e_{Dp,N/p}(\frac{-4p}{f^2})}{w(\frac{-4p}{f^2})} \\
= \Bigg( \sum_{\substack{s=-\lfloor 2\sqrt{p}\rfloor \\ s\neq 0}}^{\lfloor 2\sqrt{p}\rfloor} \Big( \sum_{f \mid f(s^2-4p)} \frac{e_{D,N/p}(\frac{s^2-4p}{f^2})}{w(\frac{s^2-4p}{f^2})} \Big) \Bigg) + \sum_{f \mid f(-4p)} \frac{e_{D,N/p}(\frac{-4p}{f^2}) - e_{Dp,N/p}(\frac{-4p}{f^2})}{w(\frac{-4p}{f^2})}.
\end{aligned}$$

Now recall that

$$e_{D,N}(\Delta) = h(\Delta) \prod_{p \mid D} \big(1 - \{\frac{\Delta}{p}\}\big) \prod_{q \mid N} \big(1 + \{\frac{\Delta}{p}\}\big)$$

and $f(\Delta)$ is the conductor of $R_\Delta$. Therefore $e_{Dp,N/p}(\Delta) = (1 - \{\frac{\Delta}{p}\}) e_{D,N/p}(\Delta)$, and thus $e_{D,N/p}(\Delta) - e_{Dp,N/p}(\Delta) = \{\frac{\Delta}{p}\} e_{D,N/p}(\Delta)$. However, consider that $f(-4p) = 1$ or 2, depending on $p \bmod 4$. Moreover, if $p = 2$, then $f(-8) = 1$. Therefore, since $p \mid \frac{-4p}{f^2}$ for all $f \mid f(-4p)$, we have

$$\left\{ \frac{\frac{-4p}{f^2}}{p} \right\} = 0.$$

Finally, if $p = 2$ and (2) does not hold, then $e_{Dp,N/p}(-4) = 0$, and the formula of (4) still suffices. ■

https://doi.org/10.4153/CJM-2013-023-8 Published online by Cambridge University Press

We now find, for infinitely many pairs of integers $D$ and $N$, infinitely many non-trivial twists of $X_0^D(N)$ that have points everywhere locally.

***Example 6.16*** Let $q$ be a prime that is 3 mod 4 and consider the curve $X_0^1(q)$. We will show that if $p \equiv 1 \bmod 4$ is a prime such that $(\frac{q}{p}) = -1$ then $C^1(q,p,q)(\mathbf{Q}_v)$ is nonempty for all places $v$ of $\mathbf{Q}$. Since $p > 0$, $C^1(q,p,q) \cong_{\mathbf{R}} X_0^1(q)$ and thus $C^1(q,p,q)(\mathbf{R}) \neq \varnothing$. We note that since $p \equiv 1 \bmod 4$, $\mathbf{Q}(\sqrt{p})$ is ramified precisely at $p$. Therefore if $\ell \nmid pq$ is a prime, then $\ell$ is unramified in $\mathbf{Q}(\sqrt{p})$. If $\ell$ splits in $\mathbf{Q}(\sqrt{p})$, then $C^1(q,p,q) \cong_{\mathbf{Q}_\ell} X_0^1(q)$ and thus $C^1(q,p,q)(\mathbf{Q}_\ell) \neq \varnothing$. If $\ell$ is inert in $\mathbf{Q}(\sqrt{p})$, then $C^1(q,p,q)(\mathbf{Q}_\ell) \neq \varnothing$ by Corollary 3.17.

Since $p \equiv 1 \bmod 4$, $(\frac{p}{q}) = (\frac{q}{p}) = -1$, and thus $q$ is inert in $\mathbf{Q}(\sqrt{p})$. Therefore by Theorem 6.1(b), $C^1(q,p,q)(\mathbf{Q}_q)$ is nonempty. Moreover, $(\frac{-q}{p}) = (\frac{q}{p}) = -1$ and so by Theorem 4.1, $C^1(q,p,q)(\mathbf{Q}_p) \neq \varnothing$.

**Acknowledgements** The work in this paper formed a part of the author's Ph.D. thesis under Pete L. Clark and Dino Lorenzini. The author would also like to thank Patrick Morton and John Voight for helpful conversations.

## References

[BLR90] Siegfried Bosch, Werner Lütkebohmert, and Michel Raynaud, *Néron models.* Ergeb. Math. Grenzgeb. **21**, Springer-Verlag, Berlin, 1990.

[CES03] Brian Conrad, Bas Edixhoven, and William Stein, *$J_1(p)$ has connected fibers.* Doc. Math. **8**(2003), 331–408 (electronic).

[Cla03] Pete L. Clark, *Rational Points on Atkin–Lehner Quotients of Shimura Curves.* Ph.D. thesis, Harvard, 2003.

[Cox89] David A. Cox, *Primes of the form $x^2 + ny^2$.* A Wiley-Interscience Publication, John Wiley & Sons, Inc., New York, 1989.

[Del69] Pierre Deligne, *Variétés abéliennes ordinaires sur un corps fini.* Invent. Math. **8**(1969), 238–243. http://dx.doi.org/10.1007/BF01406076

[Eic56] Martin Eichler, *Modular correspondences and their representations.* J. Indian Math. Soc. (N.S.) **20**(1956), 163–206.

[GR91] Josep Gonzàlez Rovira, *Equations of hyperelliptic modular curves.* Ann. Inst. Fourier (Grenoble) **41**(1991), 779–795. http://dx.doi.org/10.5802/aif.1273

[GR04] Josep González and Victor Rotger, *Equations of Shimura curves of genus two.* Int. Math. Res. Not. **14**(2004), 661–674.

[Hel07] David Helm, *On maps between modular Jacobians and Jacobians of Shimura curves.* Israel J. Math. **160**(2007), 61–117. http://dx.doi.org/10.1007/s11856-007-0056-0

[JL85] Bruce W. Jordan and Ron A. Livné, *Local Diophantine properties of Shimura curves.* Math. Ann. **270**(1985), 235–248. http://dx.doi.org/10.1007/BF01456184

[Kan11] Ernst Kani, *Products of CM elliptic curves.* Collect. Math. **62**(2011), 297–339. http://dx.doi.org/10.1007/s13348-010-0029-1

[KR08] Aristides Kontogeorgis and Victor Rotger, *On the non-existence of exceptional automorphisms on Shimura curves.* Bull. London Math. Soc. **40**(2008), 363–374. http://dx.doi.org/10.1112/blms/bdn012

[Kur79] Akira Kurihara, *On some examples of equations defining Shimura curves and the Mumford uniformization.* J. Fac. Sci. Univ. Tokyo Sect. IA Math. **25**(1979), 277–300.

[Lan87] Serge Lang, *Elliptic functions.* Second edition, Graduate Texts in Math. **112**, Springer-Verlag, New York, 1987.

[Liu02] Qing Liu, *Algebraic geometry and arithmetic curves.* Oxford Graduate Texts in Math. **6**, Oxford University Press, Oxford, 2002.

[Lor11] Dino J. Lorenzini, *Wild Models of Curves.* http://www.math.uga.edu/~lorenz/Paper2.pdf

[Mes72] William Messing, *The crystals associated to Barsotti–Tate groups: with applications to abelian schemes.* Lecture Notes in Math. **264**, Springer-Verlag, Berlin, 1972.

[Mil86] James S. Milne, *Jacobian varieties.* In: Arithmetic geometry (Storrs, Conn., 1984), Springer, New York, 1986, 167–212.

[Mol12] Santiago Molina, *Ribet bimodules and the specialization of Heegner points.* Israel J. Math. **189**(2012), 1–38. http://dx.doi.org/10.1007/s11856-011-0172-8

[Neu99] Jürgen Neukirch, *Algebraic number theory.* Grundlehren Math. Wiss. **322**, Springer-Verlag, Berlin, 1999.

[Ogg74] Andrew P. Ogg, *Hyperelliptic modular curves.* Bull. Soc. Math. France **102**(1974), 449–462.

[Ogg83] ———, *Real points on Shimura curves.* In: Arithmetic and geometry, Vol. I, Progr. Math. **35**(1983), 277–307.

[Ogg85] ———, *Mauvaise réduction des courbes de Shimura.* In: Séminaire de théorie des nombres (Paris 1983–84), Progr. Math. **59**(1985), 199–217.

[Ozm12] Ekin Ozman, *Local Points on Quadratic Twists of $X_0(N)$.* Acta Arith. **152**(2012), 323–348. http://dx.doi.org/10.4064/aa152-4-1

[Piz76] Arnold Pizer, *On the arithmetic of quaternion algebras.* Acta Arith. **31**(1976), 61–89.

[Rib89] Kenneth A. Ribet, *Bimodules and abelian surfaces.* In: Algebraic number theory, Adv. Stud. Pure Math. **17**(1989), 359–407.

[RS11] Ken Ribet and William Stein, *Lectures on Modular Forms and Hecke Operators.* http://wstein.org/books/ribet-stein/main.pdf, 2011.

[RSY05] Victor Rotger, Alexei Skorobogatov, and Andrei Yafaev, *Failure of the Hasse principle for Atkin–Lehner quotients of Shimura curves over $\mathbb{Q}$.* Mosc. Math. J. **5**(2005), 463–476, 495.

[S$^+$] W. A. Stein *et al.*, *Sage Mathematics Software (Version 4.8).* The Sage Development Team, 2012. http://www.sagemath.org

[Sad10] Mohammad Sadek, *On Quadratic Twists of Hyperelliptic Curves.* arxiv:http://arxiv.org/abs/1010.0732, 2010.

[Shi67] Goro Shimura, *Construction of class fields and zeta functions of algebraic curves.* Ann. of Math. (2) **85**(1967), 58–159. http://dx.doi.org/10.2307/1970526

[Shi71] ———, *Introduction to the arithmetic theory of automorphic functions.* Kanô Memorial Lectures, No. 1, Publications of the Mathematical Society of Japan **11**, Iwanami Shoten, Publishers, Tokyo, 1971.

[Shi79] Tetsuji Shioda, *Supersingular K3 surfaces.* In: Algebraic geometry (Proc. Summer Meeting, Univ. Copenhagen, Copenhagen, 1978), Lecture Notes in Math. **732**(1979), 564–591.

[Vie77] Eckart Viehweg, *Invarianten der degenerierten Fasern in lokalen Familien von Kurven.* J. Reine Angew. Math. **293/294**(1977), 284–308.

[Vig80] Marie-France Vignéras, *Arithmétique des algèbres de quaternions.* Lecture Notes in Math. **800**, Springer, Berlin, 1980.

*Mathematics and Computer Science, Wesleyan University, Middletown, CT, USA*
*e-mail*: stankewicz@gmail.com