Fake CM and the Stable Model of $X_0(Np^3)$

Robert Coleman[1] and Ken McMurdy

Received: September 11, 2005
Revised: October 5, 2006

Abstract. We complete the determination of the stable model of $X_0(Np^3)$, $p \geq 5$, $(N,p)=1$ begun in [CMc] and compute the inertial action on the stable reduction of $X_0(p^3)$.

2000 Mathematics Subject Classification: Primary 11G18; Secondary 14G22, 11G07
Keywords and Phrases: stable reduction, modular curve

1 Introduction

In [CMc] we found a stable model for the modular curve, $X_0(p^3)$, over the ring of integers in $\mathbb{C}_p$, for a prime $p \geq 13$. The stable models of $X_0(p)$ and $X_0(p^2)$ were previously known, due to work of Deligne-Rapoport and Edixhoven (see [CMc, §1] for a more complete list of relevant results). Finding a stable model for $X_0(p^n)$ for $n > 3$ remains an open problem, although a conjectural stable model for $X_0(p^4)$ is given in [M2, §5].

The results and main ideas of the argument used in [CMc] are summarized below in Section 2. Nevertheless, we still refer to [CMc] frequently, and do recommend that it be read first. Indeed, the purpose of this paper is to refine and extend those results. First, we prove results which enable us to define our model over an explicit finite extension of $\mathbb{Q}_p$, and to compute the inertia action on the stable reduction. More precisely, we show that a stable model for $X_0(p^3)$ can be defined over any field over which a stable model for $X_0(p^2)$ exists, and which contains the j-invariants of all elliptic curves whose formal groups have endomorphism rings isomorphic to $\mathbb{Z}_p[p\sqrt{-p}]$ or $\mathbb{Z}_p[p\sqrt{-Dp}]$ for D a non-square (mod p). Such elliptic curves, whose formal groups have endomorphism rings bigger than $\mathbb{Z}_p$, are said to have fake CM. In Section 4, we show that (real) CM points are dense in these fake CM points. Thus we are able to

[1]Supported by NSF grant DMS-0401594

apply the theory of CM elliptic curves when we determine, in Section 5, an explicit field of definition for our model. Once this is done, we compute the action of the inertia group on the stable reduction (in Section 6). This uses the results of Sections 3-5 and the fact (which we show) that the formal groups of elliptic curves with fake CM are relative Lubin-Tate groups as in [dS2]. As a consequence, we show that the extension of $\mathbb{Q}_p^{nr}$ found by Krir in [K], over which the Jacobian of $X_0(p^3)$ has semi-Abelian reduction, is minimal.

We also extend the results of [CMc] in two other ways. In order to do the explicit analysis in [CMc], it was necessary to have an approximation formula for the forgetful map, $\pi_f : X_0(p) \to X(1)$, over some supersingular annulus. Such a formula followed from a result of de Shalit (recalled in Section 2) for any region corresponding to a supersingular elliptic curve $A/\mathbb{F}_p$ whose j-invariant, $j(A)$, does not equal 0 or 1728. By a result of Everett Howe (see [CMc, §10]), one always has such an A as long as $p \geq 13$. So the only nontrivial cases which were left open were the three specific primes: $p = 5$, 7, and 11. This shortcoming of our construction could be resolved by either generalizing de Shalit's result or by adding level structure to the more symmetric deformation space of formal groups studied by Gross-Hopkins in [GH]. We handle the open cases here, however, by applying explicit known formulas (in Section 7). It is our hope that these calculations not only deal with the remaining open cases, but also serve to make the constructions of [CMc] more concrete and understandable. Finally, in Section 8 we extend the result of [CMc] by adding tame level, i.e. we compute the stable reduction of $X_0(Np^3)$ when $(N, p) = 1$. This is done by first viewing $X_0(Np^3)$ as the fiber product of $X_0(N)$ and $X_0(p^3)$ over $X(1)$. We construct semi-stable maps (as in [C2]) which extend both forgetful maps, and prove a lemma which implies that the product of semi-stable maps is semi-stable in this case. Then we compute the reductions of the components of $X_0(Np^3)$ by crossing pairs of components in $X_0(N)$ and $X_0(p^3)$ which have the same image in $X(1)$. Two specific examples are then worked out in some detail.

2 Stable Reduction of $X_0(p^3)$ for $p \geq 13$

In this section we summarize the content of [CMc] and in particular the construction of the stable model of $X_0(p^3)$ for $p \geq 13$. The goal will be to present the main ideas, along with the specific details which pertain directly to the results in this paper.

2.1 Foundations

Over $\mathbb{C}_p$, we may think of points on the modular curve, $X_0(p^n)$, as corresponding to pairs (E, C) where $E/\mathbb{C}_p$ is an elliptic curve and C is a cyclic subgroup of order p^n. One way of studying the p-adic geometry of $X_0(p^n)$ is to study regions where the pair, (E, C), has prescribed properties. The most basic distinction which one can make is whether E has ordinary (including multiplicative) or supersingular reduction, and the geometry of the ordinary region of $X_0(p^n)$ is well understood. Indeed, if E is an elliptic curve with ordinary reduction, we define the canonical subgroup $K(E)$ to be the p-power torsion of $E(\mathbb{C}_p)$ in the kernel of reduction. For each $a, b \geq 0$ with $a + b = n$, we then have rigid subspaces of the ordinary locus of $X_0(p^n)$ given by

$$\mathbf{X}_{a\,b} := \{\ (E, C)\ :\ |C \cap K(E)| = p^a\ \}.$$

Then $\mathbf{X}_{a\,b}$ is an affinoid disk when $ab = 0$. Otherwise, it is shown in [C1, §1] that $\mathbf{X}_{a\,b}$ is the disjoint union of two irreducible affinoids, $\mathbf{X}^{\pm}_{a\,b}$, which reduce to the Igusa curve, $Ig(p^c)$, where $c = \min\{a, b\}$. This curve is studied in [Ig] and classifies pairs, (E, α), where $E/\overline{\mathbb{F}}_p$ is an elliptic curve and $\alpha : \mu_{p^c} \hookrightarrow E$ is an embedding.

The supersingular locus is not as well understood, but there are a number of tools which can provide a line of attack. One of the most important is the theory of the canonical subgroup for curves with supersingular reduction, for which we take [B, §3, §4] as our primary reference. When $E/\mathbb{C}_p$ has supersingular reduction, one can still define the canonical subgroup of order p^n, $H_n(E)$, to be the cyclic subgroup of order p^n which is (p-adically) closest to the origin. For each E with supersingular reduction, however, there is a largest n for which $H_n(E)$ exists, and we denote this subgroup by $K(E)$. The size of $K(E)$ is then completely determined by the valuation of the Hasse invariant of $\bar{E}$. Denoting this valuation by $h(E)$, from [B, Thm 3.3, Def 3.4] we have

$$|K(E)| > p^n \iff h(E) < p^{1-n}/(p+1).$$

The theory of canonical subgroups is intimately connected to the geometry of the supersingular region of $X_0(p)$. For a fixed supersingular elliptic curve, $A/\mathbb{F}_{p^2}$, we let $W_A(p^n)$ be the subspace of $X_0(p^n)$ consisting of pairs (E, C) where $\bar{E} \cong A$. It is well-known (from [DR, §VI 6.16], for example) that $W_A(p)$ is an annulus of width $i(A) = |\mathrm{Aut}(A)|/2$. Furthermore, one can choose a parameter x_A on this annulus, which identifies it with $0 < v(x_A) < i(A)$, and such that

$$v(x_A(E, C)) = \begin{cases} i(A)h(E), & \text{if } |C \cap K(E)| = p \\ i(A)(1 - h(E/C)), & \text{if } |C \cap K(E)| = 1. \end{cases}$$

Inside the annulus, $W_A(p)$, there are two circles of fundamental importance. The "too-supersingular circle," denoted $\mathbf{TS}_A$, is where

$$v(x_A(E, C)) = (p/(p+1))i(A)$$

or (equivalently) $K(E)$ is trivial. The self-dual circle, $\mathbf{SD}_A$, consists of all pairs (E, C) where C is potentially self-dual, equivalently those points where $v(x_A(E, C)) = i(A)/2$. When $A/\mathbb{F}_p$, this circle is fixed by the Atkin-Lehner involution, w_1 (recalled below), and hence can be called the "Atkin-Lehner circle."

Another tool for the analysis of the supersingular region of $X_0(p^n)$ is Woods Hole Theory [WH], which essentially says that lifting an elliptic curve is equivalent to lifting its formal group. More precisely, if $R_p \subseteq \mathbb{C}_p$ is the ring of integers, we have the following theorem.

Theorem 2.1. *The category of elliptic curves over R_p is equivalent to the category of triples (F, A, α), where F/R_p is a formal group, $A/\bar{\mathbb{F}}_p$ is an elliptic curve, and $\alpha : \bar{F} \to \hat{A}$ is an isomorphism. A morphism between two triples, (F, A, α) and (F', A', β), is either the* 0 *map or a pair (σ, τ), where $\sigma : F \to F'$ and $\tau : A \to A'$ are isogenies such that the following diagram commutes.*

$$\begin{array}{ccc} \bar{F} & \xrightarrow{\bar{\sigma}} & \bar{F'} \\ {\scriptstyle\alpha}\downarrow & & \downarrow{\scriptstyle\beta} \\ \hat{A} & \xrightarrow[\hat{\tau}]{} & \hat{A}' \end{array}$$

The theorem is used in two specific ways in [CMc]. First of all, for any two supersingular elliptic curves, A and A', there is an isogeny $\phi : A \to A'$ whose degree is prime to p and which therefore passes to an isomorphism on formal groups. By taking (F, A, α) to $(F, A', \hat{\phi} \circ \alpha)$, we can define a surjection of $W_A(p^n)$ onto $W_{A'}(p^n)$ as long as $i(A) = 1$ (see [CMc, §4.1]). Note that here we have added level structure to Theorem 2.1 in the obvious way. So this implies that all of the supersingular regions are nearly isomorphic, which enables us to analyze $W_A(p^n)$ under the simplifying assumptions that $A/\mathbb{F}_p$ and $j(A) \neq 0, 1728$ (as long as $p \geq 13$, by the result of Howe). In particular, much of our explicit analysis depends on an approximation formula for the forgetful map from the annulus, $W_A(p)$, to the disk, $W_A(1)$. For $A/\mathbb{F}_p$ with $j(A) \neq 0, 1728$, such a formula was essentially found by de Shalit in [dS1, §3]. Let $\pi_f : W_A(p) \to W_A(1)$ denote the forgetful map, and $w_1 : W_A(p) \to W_A(p)$ the Atkin-Lehner involution, given by $\pi_f(E, C) = E$ and $w_1(E, C) = (E/C, E[p]/C)$ respectively. We reformulate de Shalit's result as the following theorem.

Theorem 2.2. *Let $R = W(\mathbb{F}_{p^2})$ and $A/\mathbb{F}_p$ be a supersingular curve with $j(A) \neq 0, 1728$. There are parameters s and t over R which identify $W_A(1)$ with the disk $B(0, 1)$ and $W_A(p)$ with the annulus $A(p^{-1}, 1)$, and series, $F(T), G(T) \in TR[[T]]$, such that*
(i) $w_1^*(t) = \kappa/t$ for some $\kappa \in R$ with $v(\kappa) = 1$.
(ii) $\pi_f^* s = F(t) + G(\kappa/t)$, where
(a) $F'(0) \equiv 1 \pmod{p}$, and
(b) $G(T) \equiv (F(T))^p \pmod{p}$.

The other way we use Woods Hole Theory is by letting $\mathrm{Aut}(\hat{A})$ act on $W_A(p^n)$ in the obvious way (here, as in Theorem 2.1, $\hat{A}$ denotes the formal group of A). From [T], we can identify $\mathrm{End}_{\bar{\mathbb{F}}_p}(\hat{A})$ with $B := \mathbb{Z}_p[i, j, k]$, where $i^2 = -r$ (a non-residue), $j^2 = -p$, and $ij = -ji = k$. When $A/\mathbb{F}_p$, j can also be identified with the Frobenius endomorphism. The action of $B^* \cong \mathrm{Aut}(\hat{A})$

on $W_A(1)$ commutes with the Gross-Hopkins period map, Φ, which can be viewed as a map from $W_A(1)$ to $\mathbf{P}^1$ whenever $j(A) \neq 0, 1728$. Furthermore, for $\alpha, \beta \in \mathbb{Z}_p[i]$ and $\rho = \alpha + j\beta \in B^*$, Gross-Hopkins show in [GH, §25] that the action of B^* on $\mathbf{P}^1$ is given explicitly by

$$\rho(t) = \frac{-p\bar{\beta} + \bar{\alpha}t}{\alpha + \beta t}.$$

It is important to note here that the action of B^* on $W_A(1)$ is then only completely determined by the explicit formula of Gross-Hopkins for B^*-invariant subspaces on which Φ is an injection. Fortunately, the Atkin-Lehner circle, or rather $\pi_f(\mathbf{SD}_A)$, is such a subspace and is identified with the circle described by $v(t) = 1/2$. So as an immediate consequence, the action of B^* induces a faithful action of

$$B^*/\mathbb{Z}_p^*(1 + jB) \cong \mu_{p^2-1}/\mu_{p-1}$$

on $\overline{\mathbf{SD}}_A$ (still when $j(A) \neq 0, 1728$). Also, on $\mathbf{SD}_A$ the involution w_1 can be identified with j in the above sense. We use this in [CMc, §4.2] to show that an involution on $\mathbf{SD}_A$ can be defined by $w_\rho := \rho \circ w_1$, for any $\rho = a + bi + dk \in B^*$ (this subset of B^* is called B').

Remark 2.3. *An affinoid* $\mathbf{X}$ *defined over a complete subfield of* $\mathbb{C}_p$ *has a canonical reduction over the ring of integers, which is what we mean by* $\overline{\mathbf{X}}$. *Later, we adopt the convention of un-bolding affinoid names to refer to associated components of the stable reduction. Thus, whenever both make sense,* $\overline{\mathbf{X}}$ *and* X *are birational but not isomorphic.*

2.2 Stable Model Construction

Our approach to constructing a stable model is purely rigid-analytic, in the sense that we actually construct a stable covering by wide open spaces. This equivalent notion is explained in detail in [CMc, §2]. Roughly, the wide open subspaces in a semi-stable covering intersect each other in disjoint annuli, and have underlying affinoids with (almost) good reduction. Each component in the stable reduction is (almost) the reduction of one of these underlying affinoids, and the annuli of intersection reduce to the ordinary double points where components intersect.

With this rigid analytic reformulation in mind, our strategy for constructing the stable model of $X_0(p^3)$ is basically to construct nontrivial components explicitly and then prove that nothing else interesting can happen (this is done, in part, with a total genus argument). In addition to the components in the ordinary region, we use the above tools to construct three distinct types of components in the supersingular region of $X_0(p^3)$ corresponding to any fixed supersingular elliptic curve, $A/\mathbb{F}_p$, with $j(A) \neq 0$ or 1728. First we consider the affinoid, $\mathbf{Y}_A := \pi_\nu^{-1}(\mathbf{TS}_A) \subseteq W_A(p^2)$, where $\pi_\nu : X_0(p^2) \to X_0(p)$ is given by

$\pi_\nu(E,C) = (E/C[p], C/C[p])$. We show in [CMc, §5] that $\mathbf{Y}_A$ can be identified with the rigid space,

$$T_A := \{\ (x,y) \in \mathbf{TS}_A \times \mathbf{TS}_A \mid x \neq y,\ \pi_f(x) = \pi_f(y)\ \}.$$

Then by applying Theorem 2.2 we compute the reduction of $\mathbf{Y}_A$ explicitly to be $y^2 = x^{p+1} + 1$. This affinoid, $\mathbf{Y}_A$, reduces to the supersingular component which Edixhoven found in [E1, Thm 2.1.1]. It can also be pulled back to $X_0(p^3)$ via π_f and π_ν (defined as above) to obtain nontrivial components of $W_A(p^3)$ (these pullbacks of $\mathbf{Y}_A$ are denoted by $\mathbf{E}_{1\,A}$ and $\mathbf{E}_{2\,A}$). However, there are other nontrivial components as well. Analogous to the above construction, let $\mathbf{Z}_A := \pi_{1\,1}^{-1}(\mathbf{SD}_A) \subseteq W_A(p^3)$, where $\pi_{1\,1} = \pi_f \circ \pi_\nu$. Then $\mathbf{Z}_A$ can be identified with

$$S_A := \{\ (x,y) \in \mathbf{C}_A \times \mathbf{C}_A \mid \tau_f(x) = w_1 \circ \tau_f(y)\ \}.$$

Here $\mathbf{C}_A \subseteq W_A(p)$ is the circle whose points correspond to pairs, (E,C), where $h(E) = 1/2$ and $C \neq H_1(E)$. Then $\tau_f : \mathbf{C}_A \to \mathbf{SD}_A$ is the degree p map which replaces C with $H_1(E)$. The above reformulation of de Shalit's analysis is again sufficient to explicitly compute the reduction of $\mathbf{Z}_A$ (in [CMc, §8]), which is given by

$$X^{p+1} + X^{-(p+1)} = Z^p.$$

Finally, we show that each of the $2(p+1)$ singular residue classes of $\mathbf{Z}_A$ contains an affinoid which reduces to the curve, $y^2 = x^p - x$. We do this by constructing a family of involutions on $\mathbf{Z}_A$, given by $\widetilde{w}_\rho(x,y) = (\rho y, \bar{\rho} x)$ (for $\rho \in B'$) and compatible with the w_ρ's in the sense that $\pi_{1\,1} \circ \widetilde{w}_\rho = w_\rho \circ \pi_{1\,1}$. Thus, fixed points of $\widetilde{w}_\rho$ lie over fixed points of w_ρ. Each singular residue class of $\mathbf{Z}_A$ is shown to be a connected wide open with one end, on which one of these involutions acts with p fixed points. To finish the argument, we show in [CMc, §8.2] that the quotient by $\widetilde{w}_\rho$ of such a residue class is a disk, in which the images of the p fixed points are permuted by an automorphism of order p (reducing to a translation). It is then straightforward analysis to prove that any such wide open is basic (as in [CMc, §2]), with an underlying affinoid that reduces to $y^2 = x^p - x$.

Remark 2.4. *We show in [CMc, Prop 4.9] that the fixed points of w_ρ correspond to pairs, (E,C), where E has fake CM by $\mathbb{Z}_p[\sqrt{-p}]$ or $\mathbb{Z}_p[\sqrt{-Dp}]$ (and $C = H_1(E)$). So this is where fake CM enters into the arithmetic of our stable model.*

The last step in our stable model construction is to form an admissible covering of $X_0(p^3)$ by wide open neighborhoods of the nontrivial affinoids that we know about. Once again, any supersingular region corresponding to $j(A) = 0$ or 1728, or for which $j(A) \notin \mathbb{F}_p$, is dealt with by applying an appropriate surjection from $W_{A'}(p^n)$ onto $W_A(p^n)$. We then total up our lower bounds for the genera of all of these wide opens (and the Betti number of the graph associated to our covering), and compare this with the genus of $X_0(p^3)$. Since the two are equal, we are able to conclude from [CMc, Proposition 2.5] that we haven't missed anything. Thus we have the following theorem.

Theorem 2.5. *The stable reduction of $X_0(p^3)$ for $p \geq 13$ consists of six ordinary components (reductions of the $\mathbf{X}^{\pm}_{a\,b}$) and a "necklace" of components, for each supersingular elliptic curve $A/\mathbb{F}_{p^2}$, whose graph is given below in Figure 1. The reductions of $\mathbf{E}_{1\,A}$ and $\mathbf{E}_{2\,A}$ are isomorphic to $y^2 = x^{(p+1)/i(A)} + 1$, and $\mathbf{Z}_A$ has $2(p+1)/i(A)$ singular residue classes with underlying affinoids that reduce to $y^2 = x^p - x$.*

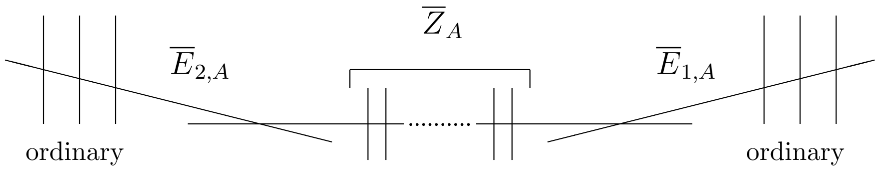

Figure 1: Partial Graph of the Stable Reduction of $X_0(p^3)$

3 Fake CM

Let K be a complete subfield of $\mathbb{C}_p$ with ring of integers R. Then we say that an elliptic curve, E/R, has fake CM if $\mathrm{End}_R(\hat{E}) \neq \mathbb{Z}_p$, and potential fake CM if this happens over $\mathbb{C}_p$. We showed in [CMc] that curves with certain types of fake CM can be used to understand the geometry of $X_0(p)$ and $X_0(p^3)$. In particular, let $\mathcal{R}$ be the set of rings of integers in quadratic extensions of $\mathbb{Q}_p$, and let $S \in \mathcal{R}$ be the ring of integers in a ramified extension. Then by [CMc, Prop 4.9], curves E with potential fake CM by S are precisely those for which $(E, H_1(E))$ is fixed by some involution w_ρ (for $\rho \in B'$, as in Section 2). Moreover, by [CMc, Prop 7.4], any fixed point of some involution, $\widetilde{w}_\rho$, is obtained from one of these by a non-canonical p-isogeny.

In this section we further investigate properties of curves which have fake CM by some $S \in \mathcal{R}$. In particular, we focus on the ways in which the fake endomorphism ring can embed into $B \cong \mathrm{End}(\hat{A})$ (via Woods-Hole theory), when A is supersingular and E corresponds to a point of $W_A(1)$. First we show that all subrings of B which are isomorphic to the same $S \in \mathcal{R}$ are B^* conjugate, and hence (using results from [G]) that all the curves in $W_A(1)$ with fake CM by the same ramified S make up a B^* orbit. Then we suppose that (E, C) is fixed by the involution w_ρ, for some $\rho \in B'$, and give alternative characterizations of the image of $\mathrm{End}(\hat{E})$ in B in terms of ρ.

3.1 Fake CM Curves and Orbits of B^*

With notation as in Section 2.1, we fix a supersingular elliptic curve $A/\mathbb{F}_{p^2}$ and an isomorphism between $\mathrm{End}(\hat{A})$ and $B = \mathbb{Z}_p[i,j,k]$. Then $B^* \cong \mathrm{Aut}(\hat{A})$ acts on $W_A(1)$ by $\rho(F,\alpha) = (F, \rho \circ \alpha)$. It is immediate that this restricts to an action of B^* on the subset of $W_A(1)$ corresponding to curves E with fake CM by a fixed $S \in \mathcal{R}$. We want to describe the orbits of this (restricted) action.

Lemma 3.1. *If S_1 and S_2 are subrings of B which are isomorphic to S, there is a $\rho \in B^*$ such that $S_2 = \rho^{-1} S_1 \rho$.*

Proof. We can assume without loss of generality that $S_1 = \mathbb{Z}_p[\iota]$, where $\iota = i$, j or k. Note that for each of these ι, and for any α, we have

$$Tr(\alpha\iota) = 0 \;\Rightarrow\; \iota\alpha = \bar{\alpha}\iota.$$

Suppose first that $S_1 = \mathbb{Z}_p[i]$. Since S_1 and S_2 are isomorphic, there must be an $\alpha \in S_2$ such that $\alpha^2 = -r$. Hence we have $N(\alpha) = r$ and $Tr(\alpha) = 0$. Now set $\gamma = \alpha/i \in B$, from which it follows that $N(\gamma) = 1$ (and therefore $\gamma^{-1} = \bar{\gamma}$). Finally, choose $\epsilon = \pm 1$ so that $\rho := 1 + \epsilon\gamma$ is a unit. Then using $Tr(\rho i) = 0$ we calculate:

$$\frac{\rho i \bar{\rho}}{N(\rho)} = (\bar{\rho})^{-1}\rho i = (\bar{\rho})^{-1}\rho\gamma^{-1}\alpha = (\bar{\rho})^{-1}(\epsilon + \gamma^{-1})\alpha = \epsilon\alpha.$$

In other words, $\rho i \rho^{-1} = \epsilon\alpha$, and therefore $\rho^{-1} S_2 \rho = \mathbb{Z}_p[i] = S_1$.

Now suppose that $S_1 = \mathbb{Z}_p[j]$. In this case there must be an $\alpha \in S_2$ such that $\alpha^2 = -p$, and hence $\alpha = bi + cj + dk$, for some $b, c, d \in \mathbb{Z}_p$ such that

$$-b^2 r - c^2 p - d^2 rp = -p.$$

Thus, we see that $p|b$. So $b = (ej)j$ for some $e \in \mathbb{Z}_p$, and $\alpha = \gamma j$ where $\gamma := ek + c + di \in B$. Again take $\rho = 1 \pm \gamma$. The remaining case, when $S_1 = \mathbb{Z}_p[k]$, is similar. $\square$

Corollary 3.2. *When S is ramified, any two formal S-module structures,*

$$\sigma_1, \sigma_2 : S \to B = End(\hat{A}),$$

are conjugate in the sense that there is a $\rho \in B^*$ with

$$\rho^{-1}\sigma_1(s)\rho = \sigma_2(s) \qquad \forall s \in S.$$

Proof. From Lemma 3.1, there exist $\gamma_1, \gamma_2 \in B^*$ such that $\gamma_i^{-1}\sigma_i(S)\gamma_i = \mathbb{Z}_p[\iota]$ where $\iota = j$ or k. Note that $i\iota i^{-1} = -\iota$ in either case. Therefore we obtain two distinct automorphisms of S (over $\mathbb{Q}_p$) by taking

$$s \to \sigma_2^{-1}(\rho^{-1}\sigma_1(s)\rho),$$

where ρ is either $\gamma_1\gamma_2^{-1}$ or $\gamma_1 i^{-1}\gamma_2^{-1}$. One of these automorphisms must be the identity, which proves the corollary. $\square$

THEOREM 3.3. *Suppose that $a := (E, C)$ and $b := (E', C')$ are points in $W_A(p)$ such that E and E' have (potential) fake CM by S (ramified), and such that C and C' are either both canonical or both not. Then $a = \rho b$ for some $\rho \in B^*$.*

Proof. Let $E = (F, \alpha)$ and $E' = (F', \beta)$. By the lemma, there is a $\rho \in B^*$ such that

$$\alpha\overline{\mathrm{End}(F)}\alpha^{-1} = (\rho\beta)\overline{\mathrm{End}(F')}(\rho\beta)^{-1}.$$

Moreover, by the corollary, we can choose ρ so that (F, α) and $(F', \rho \circ \beta)$ are two liftings of the same formal S-module structure on $\hat{A}$ (in the sense of [G]). Hence by [G, Prop 2.1], we have $\rho(E') = E$.

Now, if C and C' are canonical, it is immediate that $a = \rho b$ for this same ρ. So suppose that C and C' are both non-canonical. Then the isomorphism between $(F', \rho\circ\beta)$ and (F, α) at least takes C' to some non-canonical subgroup $D \subseteq F$. But $\mathrm{Aut}(F)$ transitively permutes the non-canonical subgroups by Remark 4.11 of [CMc]. Therefore we may choose an automorphism σ with $\sigma(D) = C$, and thus we have $a = \rho_1 b$ for $\rho_1 = (\alpha \circ \sigma \circ \alpha^{-1})\rho$. □

REMARK 3.4. *If E is defined over $W(\mathbb{F}_{p^2})$, and $\bar{E} \cong A$ for some supersingular A with A defined over $\mathbb{F}_p$ or with $j(A) \neq 0$ or 1728, then E has fake CM. Indeed, the Frobenius endomorphism of $\bar{E}$ over $\mathbb{F}_{p^2}$ is $[\pm p]_{\bar{E}}$. Since this endomorphism lifts to E, $\hat{E}$ is a Lubin-Tate formal group.*

For example, suppose that $p = 2$ and E is given by $y^2 + 2xy - Ay = x^3$, where $A^3 = 1$. Then in characteristic 2, we have $[2](x, y) = (Ax^4, y^4)$. So if $A \neq 1$, we don't know if E has fake CM 2-adically.

3.2 EMBEDDINGS OF FAKE ENDOMORPHISM RINGS

Now suppose that A is defined over $\mathbb{F}_p$ and that $j(A) \neq 0, 1728$. Recall (from [CMc, §4.2]) that for any $\rho \in B'$, the involution of $\mathbf{SD}_A$ given by $w_\rho = \rho \circ w_1$ has two fixed points. Let $x = (E, C) = (F, \alpha, C)$ be one of the them. As in the previous section, Woods Hole theory gives us an embedding of $\mathrm{End}(F)$ into B:

$$\alpha_*\mathrm{End}(F) := \alpha^{-1}\overline{\mathrm{End}(F)}\alpha \subseteq \mathrm{End}(\hat{A}) = B.$$

In this section, we use the embedding to reprove the result that E has fake CM by the ring of integers in a ramified quadratic extension of $\mathbb{Q}_p$. We also give alternate descriptions of the embedding which depend only on ρ, in particular showing that the fake endomorphism rings of both fixed points embed onto the same subring of B.

DEFINITION 3.5. *For $\rho = a + bi + cj + dk \in B$, we let $\rho' = a - bi + cj - dk$.*

LEMMA 3.6. *(i) For all $\rho \in B$, $\rho j = j\rho'$.*
(ii) $B' = \{ \rho \in B^* \mid \rho\rho' \in \mathbb{Z}_p^* \}$
(iii) If $\rho_1, \rho_2 \in B^*$, $(\rho_1\rho_2)' = \rho_1'\rho_2'$.
(iv) If $\rho \in B'$, $\rho\rho' = \rho'\rho$.

Proposition 3.7. *Let $\rho \in B'$, and let $x := (E, C) = (F, \alpha, C)$ be fixed by w_ρ. Then $\alpha_* End(F) = \mathbb{Z}_p[\gamma]$, where $\gamma = \rho j$ and hence $\gamma^2 \in p\mathbb{Z}_p^*$.*

Proof. This is basically proven in [CMc, Prop 4.9], although we repeat the argument here. By Theorem 2.1 (and the fact that the only degree p endomorphisms of A are $\pm j$) we can choose isogenies,

$$\beta : \overline{F/C} \xrightarrow{\sim} \hat{A} \qquad \iota_C : F \to F/C,$$

such that $E/C = (F/C, \beta)$, and such that (ι_C, j) represents the natural isogeny from E to E/C. In fact, ι_C can be taken to be the natural map.

Now, the fact that $\rho(E/C) = E$ implies that there is an isomorphism, $\sigma : F/C \to F$, such that $\rho \circ \beta = \alpha \circ \bar{\sigma}$. So let $\pi_0 = \sigma \circ \iota_C \in \mathrm{End}(F)$, and then take $\gamma = \alpha \overline{\pi}_0 \alpha^{-1}$. Then $\gamma \in \alpha_* \mathrm{End}(F)$ by definition, $\gamma = \rho j$ by commutativity, and from Lemma 3.6 we have

$$\gamma^2 = \rho j \rho j = -p\rho\rho' \in -p\mathbb{Z}_p^*.$$

Furthermore, since this implies that $\mathbb{Z}_p[\gamma]$ is a maximal order, it must be all of $\alpha_* \mathrm{End}(F)$. □

Corollary 3.8. *Let $x = (F, \alpha, C)$ be fixed by w_ρ for $\rho \in B'$, and let $K = \mathbb{Q}_p(\sqrt{-p}, \sqrt{-Dp})$ for D a quadratic non-residue (mod p). Then x is defined over K, and*

$$End(F) = End_K(F) \cong \mathbb{Z}_p\left[\sqrt{-\rho\rho' p}\right].$$

Proof. The fixed points of w_ρ are defined over K, by the explicit formula for w_ρ (given in [CMc, Eq 3]). Therefore, F/C and the natural map, $\iota_C : F \to F/C$, are defined over K. Hence, the endomorphism, π_0 (as in Proposition 3.7), is defined over K. □

Proposition 3.9. *If $\rho \in B'$ and $x := (F, \alpha, C)$ is fixed by w_ρ, then*

$$\alpha_* End(F) = S_\rho := \{\tau \in B \colon \rho\tau' = \tau\rho\}.$$

Proof. One direction is easy. In particular, from the previous proposition, everything in $\alpha_* \mathrm{End}(F)$ can be written as $a + b\gamma$. This is in S_ρ since

$$\rho(a + b\rho j)' = a\rho + b\rho\rho' j = (a + b\rho j)\rho.$$

For the other direction, Lemma 3.6 implies that S_ρ is at least a ring. We want to show that $S_\rho \subseteq \alpha_* \mathrm{End}(F)$. So first choose a $\tau \in S_\rho^*$. From the fact that $\rho \circ w_1 = w_1 \circ \rho'$ on $\mathbf{SD}_A$ (basically just $\rho j = j\rho'$, see [CMc, Cor 4.6]), we have

$$w_\rho(\tau x) = \rho\tau' w_1 x = \tau\rho w_1 x = \tau x,$$

which means that τx is one of the two fixed points of w_ρ. Suppose first that $\tau x = x$, i.e., $(F, \alpha) \cong (F, \tau \circ \alpha)$. Then by Theorem 2.1, there is a $\sigma \in \mathrm{End}(F)$ such that

$$\alpha \circ \bar{\sigma} = \tau \circ \alpha,$$

and hence $\tau \in \alpha_*\mathrm{End}(F)$. We conclude that if $\tau \in S_\rho^*$, at least $\tau^2 \in \alpha_*\mathrm{End}(F)$. But then, since $(1 \pm \tau)^2 = 1 \pm 2\tau + \tau^2$, it follows that $\tau \in \alpha_*\mathrm{End}(F)$. Finally, if $c \in S_\rho$, one of either $1+c$ or $1-c$ must be in S_ρ^*. Thus, $S_\rho \subseteq \alpha_*\mathrm{End}(F)$. □

Corollary 3.10. *If F and G are formal groups corresponding to the two fixed points of w_ρ, End(F) is canonically isomorphic to End(G).*

Proof. Let $x = (F, \alpha, C)$ and $y = (G, \beta, C')$ be the two fixed points of w_ρ. Then from either proposition, we have

$$\alpha_*\mathrm{End}(F) = \beta_*\mathrm{End}(G).$$

So α_* and β_* identify End(F) and End(G) with the same subring of B. □

Remark 3.11. *Let $x = (F, \alpha, C)$ and $y = (G, \beta, C')$ be the two fixed points of w_ρ, for $\rho \in B'$ (as above). Let S be the ring of integers in the ramified quadratic extension of $\mathbb{Q}_p$ for which End(F) $\cong$ End(G) $\cong S$. Then by [G, Prop 2.1], x and y are the two canonical liftings of the two S-module structures on $\hat{A}$ with image α_*End(F) $= \beta_*$End(G).*

4 Real CM

In this section, we shift our focus to elliptic curves E/R which have real CM, i.e. for which $\mathrm{End}_R(E) \neq \mathbb{Z}$. Our main result is that, inside $\mathbf{SD}_A$, real CM points are dense in the set of fake CM points. The strategy is to use Woods Hole theory and the fact that End(A) is dense in End($\hat{A}$). First we make B into a topological ring in the usual way, by defining

$$||\rho|| = \max\{|h(\rho)|\colon h \in \mathrm{Hom}_{\mathbb{Z}_p}(B, \mathbb{Z}_p)\}.$$

Then from the explicit formula of Gross-Hopkins (see [CMc, §4.2] or Section 2.1), the action,

$$B^* \times \mathbf{SD}_A \to \mathbf{SD}_A,$$

is continuous with respect to both variables.

Now assume that $A/\mathbb{F}_p$, and let $K = \mathbb{Q}_p(\sqrt{-p}, \sqrt{-Dp})$ and $R = \mathcal{O}_K$. Thus the fake CM curves corresponding to points of $\mathbf{SD}_A$ are all defined and have fake CM over R by Corollary 3.8. Then real CM points are dense in these fake CM points in the following sense.

Theorem 4.1. *Choose $S \in \mathcal{R}$ ramified. Then points of $\mathbf{SD}_A$ corresponding to elliptic curves, E/R, for which $\mathrm{End}_R(E) \otimes \mathbb{Z}_p \cong S$ are dense in those for which $\mathrm{End}_R(\hat{E}) \cong S$. In fact, if (F, α) has fake CM and $\epsilon \in \mathbb{R}^+$, there exist $\rho \in B^*$ such that $||\rho - 1|| < \epsilon$ and $(F, \rho\alpha) \neq (F, \alpha)$ has real CM.*

Proof. In general, when $E = (F, \alpha)$ is defined over R with residue field k, E has CM over R if and only if $\alpha_*\mathrm{End}_R(F) \cap \mathrm{End}_k(A) \neq \mathbb{Z}$ in $\mathrm{End}_k\hat{A}$. In fact,

$$\mathrm{End}_R(F, \alpha) \cong \alpha_*\mathrm{End}_R F \cap \mathrm{End}_k A.$$

This follows from Theorem 2.1 if $R = R_p$, and an argument for more general R can be made via crystalline cohomology. In our case, $k = \mathbb{F}_{p^2}$, and since $A/\mathbb{F}_p$ is supersingular, this guarantees that $\mathrm{End}_k(A)$ is dense in $\mathrm{End}_k(\hat{A}) = \mathrm{End}(\hat{A})$.

So suppose (F, α) is defined over R (as above) and has fake CM by $S \in \mathcal{R}$ (ramified) and $\alpha_* S = \mathbb{Z}_p[\gamma]$. Fix an $\epsilon > 0$. Then there exists $\delta > 0$ such that for all $g \in \mathrm{End}(\hat{A})$ with $||g - \gamma|| < \delta$, there exists $\rho \in B^*$ with $||\rho - 1|| < \epsilon$ and

$$\rho S \rho^{-1} = \mathbb{Z}_p[g].$$

This follows from the construction of Theorem 3.3, since δ can be chosen so that $\mathbb{Z}_p[g] \cong \mathbb{Z}_p[\gamma]$ for all $||g - \gamma|| < \delta$. In particular, we may then choose $g \in \mathrm{End}(A)$ with $\mathbb{Z}_p[g] \neq \mathbb{Z}_p[\gamma]$, since $\mathrm{End}(A)$ is dense in $\mathrm{End}(\hat{A})$. Then $(F, \rho \circ \alpha)$ has CM because

$$(\rho \circ \alpha)_* \mathrm{End}_R F = \{\rho \circ \alpha \circ \gamma \circ (\rho \circ \alpha)^{-1} \colon \gamma \in \mathrm{End}_R F\} = \rho S \rho^{-1}.$$

Therefore, $g \in (\rho \circ \alpha)_* \mathrm{End}_R(F) \cap \mathrm{End}(A)$. □

COROLLARY 4.2. *Let A be any supersingular elliptic curve over $\mathbb{F}_{p^2}$. Then points corresponding to elliptic curves E with CM by an order of discriminant pM with $(p, M) = 1$ fill out a $\mu_{2(p+1)/i(A)}$ orbit of $G_m \cong \overline{\mathbf{SD}}_A$. Two such curves correspond to points in the same $\mu_{(p+1)/i(A)}$ orbit if and only if $M_1 M_2$ is a square (mod p).*

Proof. First suppose that $A/\mathbb{F}_p$ and $j(A) \neq 0, 1728$. Recall that curves with fake CM by S (as above) correspond to fixed points of the involutions w_ρ for $\rho \in B'$ by [CMc, Prop 4.10]. Remark 4.8 of [CMc] says that such points fill out a $\mu_{2(p+1)}$ orbit of $G_m \cong \overline{\mathbf{SD}}_A$, and that B^* acts like μ_{p+1}. Now we have Theorem 3.3 which says that curves with the same fake endomorphism ring are B^* translates. So this proves the analogous statement for fake CM curves, and by Theorem 4.1 the statement about real CM curves then follows.

Now suppose that $j(A) = 0$ or 1728. Remark 4.8 is based on the explicit formula for the action of B^* on the deformation space, X_K, for the formal group $\hat{A}$. When $j(A) = 0$ or 1728, $W_A(1)$ can be identified with the quotient of X_K by a faithful action of $\mathrm{Aut}(A)/\pm 1$, in a way which is compatible with the natural embedding of $\mathrm{Aut}(A)$ into B^*. So basically, we can use the same argument as above for the circle of X_K which lies over $\mathbf{SD}_A$, and then apply the degree $i(A)$ map. Similarly, if A is not defined over $\mathbb{F}_p$, we can choose some $A_0/\mathbb{F}_p$ and then apply an isomorphism between $W_{A_0}(p)$ and $W_A(p)$ as in [CMc, §4.1]. □

REMARK 4.3. *When $A/\mathbb{F}_p$, a canonical choice of parameter on $\mathbf{SD}_A$ is given by $(j(E) - Teich(j(A)))/\sqrt{p^{i(A)}}$.*

QUESTION: If E and E' both satisfy the above conditions, the residue class of

$$\frac{j(E') - \mathrm{Teich}(j(A))}{j(E) - \mathrm{Teich}(j(A))} \pmod{\sqrt{p}}$$

is the residue class of a $\frac{p+1}{i(A)}$-th root of unity. Which one and when is it 1?

4.1 Heegner Points

By a Heegner point on $X_0(N)$ we mean a pair (E, C) where E is a CM elliptic curve and C is a cyclic subgroup of order N such that $\mathrm{End}(E) \cong \mathrm{End}(E/C)$. Let $\mathcal{X}_0(p^n)$ denote a stable model for $X_0(p^n)$. In this section, we discuss the placement of Heegner points on $\mathcal{X}_0(p^n)$, beginning with those Heegner points which lie in the ordinary region.

Let $R_i(D)$ denote the order of discriminant p^iD in $\mathbb{Q}[\sqrt{p^iD}]$ where $D < 0$, and $(D, p) = 1$. Suppose $\mathrm{End}(E) \cong R_i(D)$. Then E has ordinary reduction if and only if $(\frac{D}{p}) = 1$ and i is even.

In order to study ordinary Heegner points, we interpret the irreducible affinoids, $\mathbf{X}^{\pm}_{a\,b}$, which make up the ordinary locus as in [C1]. Recall that $\mathbf{X}_{a\,b}$ (for $a, b \geq 0$ and $a + b = n$) was defined in Section 2.1 as the affinoid in $X_0(p^n)$ whose points correspond to pairs (E, C) where E is ordinary and $|C \cap K(E)| = p^a$. The first author showed (see [C1, §2] or [CMc, §3.2]) that for $a \geq b$ this is equivalent to the affinoid whose points correspond to pairs, $(E, \mathcal{P})$, where E is ordinary and $\mathcal{P}$ is a certain pairing from $K_a(E) := K(E) \cap E[p^a]$ onto μ_{p^b}. Furthermore, let $C_{a\,b}$ denote the set of isomorphism classes of pairings from $\mathbb{Z}/p^a\mathbb{Z}$ onto μ_{p^b} (which has two elements when $a \geq b \geq 1$). Then for any $\beta \in C_{a\,b}$ the subspace, $\mathbf{X}^{\beta}_{a\,b} \subseteq \mathbf{X}_{a\,b}$, consisting of those pairs for which $\mathcal{P} \in \beta$, is an irreducible affinoid which reduces to $Ig(p^a)$. Now, using the Atkin-Lehner involution, the remaining irreducible affinoids (for $a < b$) in the ordinary locus can be defined by

$$\mathbf{X}^{\beta}_{a\,b} = w_n \mathbf{X}^{(\frac{-1}{p})\beta}_{b\,a}.$$

(Note: This is a slight change from the notation of [C1].) Ordinary points of $X_0(p^n)$ all have smooth reduction on one of these components, and we will show that there are in fact infinitely many Heegner points on each.

Lemma 4.4. *For any $b \geq 0$, there are infinitely many Heegner points on $\mathbf{X}_{b\,b}$.*

Proof. Points of $\mathbf{X}_{b\,b}$ can also be thought of as triples, (E, C_1, C_2), where E is an ordinary elliptic curve and C_i is a cyclic subgroup of order p^b such that $C_1 \cap C_2 = (0)$ and $C_i \cap K(E) = (0)$. If we let ι_C denote the natural map from $E \to E/C$, then the triple, (E, C_1, C_2), just corresponds to the pair, $(E/C_1, C(C_1, C_2))$, where

$$C(C_1, C_2) := \ker(\iota_{C_2} \circ \check{\iota}_{C_1}) \subseteq E/C_1.$$

Now, choose any ordinary elliptic curve, E, with CM by $R_{2i}(D)$, and then choose C_1 and C_2 (as above) so that $\mathrm{End}(E/C_1) \cong \mathrm{End}(E/C_2) \cong R_{2(i+b)}(D)$. If $i > 0$, any choice of C_1 and C_2 (as above) will do. If $i = 0$, one also needs C_i to be disjoint from the kernel of the Verschiebung lifting (which is always possible if $p > 2$). Then $(E/C_1, C(C_1, C_2))$ is a Heegner point on $\mathbf{X}_{b\,b}$. □

There are various maps between ordinary affinoids which can now be used (along with Lemma 4.4) to construct Heegner points on every $\mathbf{X}^{\beta}_{a\,b}$. First of all,

w_n takes Heegner points of $\mathbf{X}_{a\,b}$ to Heegner points of $\mathbf{X}_{b\,a}$ by definition. Secondly, the group $\mathbb{Z}_p^*$ acts through $(\mathbb{Z}/p^b\mathbb{Z})^*$ on $\mathbf{X}_{a\,b}$ via $\tau_r\colon (E,\mathcal{P}) \mapsto (E,\mathcal{P}^r)$. Moreover, τ_r fixes $\mathbf{X}^{\beta}_{a\,b}$ (i.e. preserves the class of the pairing in $C_{a\,b}$) if and only if τ_r is a square. Finally, we have a natural isomorphism, $\alpha_{a\,b}\colon \mathbf{X}_{b\,b} \to \mathbf{X}_{a\,b}$, which takes the pair $(E,\mathcal{P})$ to the pair $(E,\mathcal{P}')$ for

$$\mathcal{P}'(R,S) = \mathcal{P}(p^{a-b}R, p^{a-b}S).$$

We now investigate the effect of these maps on Heegner points.

Lemma 4.5. *Let F be a fixed ordinary elliptic curve. Then $(\mathbb{Z}/p^b\mathbb{Z})^*$ acts transitively on the set of points of the form (F,C) which lie in $\mathbf{X}_{b,b}$.*

Proof. Let $B_b(F)$ denote this set. Then points of $B_b(F)$ correspond to triples (E,C_1,C_2) as above where $E = F/K_b(F)$ and $C_1 = F[p^b]/K_b(E)$. There are $p^{b-1}(p-1)$ such triples. The lemma follows because $(\mathbb{Z}/p^b\mathbb{Z})^*$ acts faithfully on $B_b(F)$. □

Lemma 4.6. *If (F,C) is a Heegner point on $\mathbf{X}_{b\,b}$ and End$(F) = R_{2b}(D)$ then $\alpha_{a\,b}(F,C)$ is a Heegner point.*

Proof. The point (F,C) is $(E/C_1, C(C_1,C_2))$, where $E = F/p^bC$, $C_1 = \iota_{p^bC}(F[p^b])$ and $C_2 = \iota_{p^bC}(C)$. In this case, $(p, \mathrm{disc}(\mathrm{End}(E))) = 1$. Let $\phi^c\colon E \to E^{\sigma^c}$ be the lifting of Frobenius. Then $\alpha_{a\,b}(F,C) =$

$$(F, \ker(\iota_{C_2^{\sigma^{a-b}}} \circ \phi^{a-b} \circ \iota_{p^bC})),$$

which is clearly a Heegner point. □

Theorem 4.7. *There are infinitely many Heegner points lying over each ordinary component of $\mathcal{X}_0(p^n)$ for $n \geq 1$ and $p > 2$ (all with smooth reduction).*

Proof. By Lemma 4.6, it suffices to guarantee at least one Heegner point, (F,C), on each $\mathbf{X}^{\beta}_{b,b}$ with End$(F) \cong R_{2b}(D)$. From the proof of Lemma 4.4, such points correspond to triples (E,C_1,C_2) where End$(E) \cong R_0(D)$. For a fixed F, we must have $E = F/K_b(F)$ and $C_1 = F[p^b]/K_b(E)$. Then we get a point of $\mathbf{X}_{b\,b}$ by choosing any C_2 disjoint from C_1 and $K(E)$, and a Heegner point if C_2 is also disjoint from the kernel of the Verschiebung lifting.

At this point, the argument is reduced to simple counting. We have a total of $p^{b-1}(p-2)$ Heegner points in each $B_b(F)$. The cardinality of $B_b(F)$ is $p^{b-1}(p-1)$, and from Lemma 4.5 half of these points lie in each $X^{\beta}_{b\,b}$. So since $p^{b-1}(p-2) > p^{b-1}(p-1)/2$ if $p > 3$, we are done ($p = 3$ can be handled by Atkin-Lehner). □

Heegner points in the supersingular region of $\mathcal{X}_0(p^n)$ are somewhat easier to describe.

LEMMA 4.8. *Let E be a CM elliptic curve with supersingular reduction, such that p^m exactly divides the discriminant of End(E). Then we have*

$$h(E) = \begin{cases} p^{1-k}/(p+1), & \text{if } m = 2k \\ p^{1-k}/2, & \text{if } m = 2k-1. \end{cases}$$

Furthermore, if End($\hat{E}$) $= \mathbb{Z}_p[\gamma]$ and $\gamma^2 \in \mathbb{Z}_p$, we have Ker($\gamma$) $\cap K(E) = K(E)$ (which has order p^k).

Proof. This is an exercise in applying [B, Thm 3.3]. The point is that if $E/C \cong E$, we must at least have $h(E/C) = h(E)$. □

THEOREM 4.9. *Let E be a CM elliptic curve with supersingular reduction, such that p^m exactly divides the discriminant of End(E). Then $(E, C) \in X_0(p^n)$ (for $n > 0$) is a Heegner point if and only if $m = n$ and $K(E) \subseteq C$.*

Proof. This follows directly from Lemma 4.8 (and [B, Thm 3.3]). Indeed, if E and m are as above, and $C \subseteq E$ is any cyclic subgroup of order p^n, we have

$$\operatorname{disc}(\operatorname{End}(E/C)) = \frac{\operatorname{disc}(\operatorname{End}(E)) \cdot |C|^2}{|K(E) \cap C|^4} \cdot \begin{cases} p, & \text{if } m \text{ is odd and } K(E) \subseteq C \\ 1, & \text{otherwise.} \end{cases}$$

□

Now, when $n \leq 3$, the above results make it possible to be very explicit about the placement of Heegner points on $\mathcal{X}_0(p^n)$. On $\mathcal{X}_0(p)$, the supersingular Heegner points all lie on $\mathbf{SD}_A$ for some A and have singular reduction (although when $j(A) = 1728$ they have smooth reduction on the Deligne-Rapoport model from [DR, §VI.6.16]). They also correspond to pairs, (E, C), where E has CM by $R_1(D)$ and $C = K(E)$. Heegner points of $X_0(p^2)$ correspond to those pairs, (E, C), where E has CM by $R_2(D)$ (with $(\frac{D}{p}) = -1$) and $K(E) = pC$. They all have smooth reduction on the component of $\mathcal{X}_0(p^2)$ which Edixhoven found (and which we call $\overline{\mathbf{Y}}_A$). Finally, Heegner points on $X_0(p^3)$ correspond to pairs where E has CM by $R_3(D)$ and $K(E) = pC$. This implies that they all lie on the affinoid $\mathbf{Z}_A$. By Theorem 4.1, there are infinitely many which are fixed by some $\widetilde{w}_\rho$. Hence, using the discussion at the beginning of [CMc, §8], they have smooth reduction on each of the new components which lie in the singular residue classes of $\mathbf{Z}_A$. However, there are also infinitely many supersingular Heegner points of $X_0(p^3)$ which are *not* fixed by any $\widetilde{w}_\rho$, from the preceding theorem and Proposition 7.4 of [CMc] (see also [CMc, Rem 7.5]), and it is unclear where the reductions of these points lie on $\overline{\mathbf{Z}}_A$.

5 FIELD OF DEFINITION

Suppose L/K is an unramified extension of local fields. It follows from [DM, Thm 2.4] that an Abelian variety A over K has semi-stable reduction (i.e. has a model with semi-stable reduction over $\mathcal{O}_K$) if and only if A_L has semi-stable reduction. Also, in the special case where A is the Jacobian of a curve, C/K, and L/K is the maximal unramified extension, A has semi-stable reduction if and only if C_L does. It is not true, however, that (in this case) C has semi-stable reduction whenever A does. For example, the Jacobian of $X_0(p)$ has a model with semi-stable reduction over $\mathbb{Z}_p$, while $X_0(p)$ may not (for example, when $p = 37$). This is an important point for us, because Krir determined a field over which the Jacobian of $X_0(p^n)$ attains stable reduction in [K, Théorème 1]. Indeed, let $K = \mathbb{Q}_p(\sqrt{-p}, \sqrt{-Dp})$ for D a quadratic non-residue. Then Krir's result can be stated as follows.

THEOREM 5.1 (Krir). *The Jacobian of $X_0(p^n)$ has stable reduction over the class field M_n over K of the subgroup of K^* given by*

$$\{a \in \mathcal{O}_K^* \colon a^2 \in 1 + \sqrt{p^{n-1}}\mathcal{O}_K\}.$$

By the above reasoning, it follows that $X_0(p^n)$ also has a stable model over this same field, M_n. However, one can not conclude from this result which extensions of $\mathbb{Q}_p$ are sufficient for $X_0(p^n)$ to attain stable reduction (and there may not be a minimal such field). What we do in this section is produce a finite extension, $F_3 \supseteq \mathbb{Q}_p$, over which our stable model for $X_0(p^3)$ can be defined, partially using the result of Krir. Fake and real CM also play a role because of the correspondence between w_ρ and $\widetilde{w}_\rho$ fixed points and fake CM curves. Our final result is the following.

THEOREM 5.2. *If $1 \le n \le 3$, the stable model of $X_0(p^n)$ is defined over the class field F_n over $K := \mathbb{Q}_p(\sqrt{-p}, \sqrt{-Dp})$ of the subgroup of K^* given by*

$$(p^{2a_n})^{\mathbb{Z}}\{a \in \mathcal{O}_K^* \colon a^{b_n} \in 1 + \sqrt{p^{n-1}}\mathcal{O}_K\},$$

where $(a_n, b_n) = (1,1)$ if $n = 1$, $(3,4)$ if $n = 2$, and $(3,2)$ if $n = 3$. In particular,

$$([F_n \colon \mathbb{Q}_p], e(F_n/\mathbb{Q}_p)) = \begin{cases} (2,1), & \text{if } n = 1; \\ (6(p^2-1), (p^2-1)/2), & \text{if } n = 2; \\ (12(p^2-1)p^2, (p^2-1)p^2) & \text{if } n = 3. \end{cases}$$

5.1 TWO INGREDIENTS

One of the main ingredients in our field of definition is the field over which the fixed points of our involutions, $\widetilde{w}_\rho$, are defined. This field is necessary, by our construction, to obtain good reduction for the underlying affinoids in the singular residue classes of $\mathbf{Z}_A$. As real CM curves have been shown to be dense in these points, we are able to apply classical results on CM elliptic curves to determine this field.

Proposition 5.3. *Let A be a supersingular curve over $\mathbb{F}_p$. Let F be the smallest field over which all the fixed points in $W_A(p^3)$ of our involutions $\widetilde{w}_\rho$ are defined. Then,*

$$F = \mathbb{Q}_p(\sqrt{-p}, \sqrt{-Dp}, j(p\sqrt{-p}), j(p\sqrt{-Dp}))$$

where $D \in \mathbb{Z}^+$ is a quadratic non-residue. This is the class field over $K := \mathbb{Q}_p(\sqrt{-p}, \sqrt{-Dp})$ of the subgroup of K^* given by

$$(\sqrt{p})^{\mathbb{Z}} \mu_{p^2-1}(1 + p\mathcal{O}_K).$$

In particular, $[F : K] = p^2$.

Proof. By Theorem 4.1 and Proposition 7.4 of [CMc] we see that F is the field of definition over $\mathbb{Q}_p$ of the set of points (E, C) where E lifts A and has CM by an order whose discriminant is exactly divisible by p (note that here C is not necessarily $H_1(E)$). The proposition now follows from Theorem 5.5 of [S]. □

Remark 5.4. *This field F is the same as that mentioned in Remark 8.1 of [CMc].*

We used a surjection from $W_A(p^n)$ onto $W_{A'}(p^n)$, where A and A' are supersingular elliptic curves over $\mathbb{F}_{p^2}$, to deal with those regions for which $j(A') = 0$ or 1728, or for which A' is not defined over $\mathbb{F}_p$. The surjection can be defined over $W(\mathbb{F}_{p^k})$ as long as A and A' are p-prime isogenous over $\mathbb{F}_{p^k}$. Another ingredient in our determination of a field of definition is the following theorem, that $k = 24$ always suffices.

Theorem 5.5. *Any two supersingular elliptic curves over $\mathbb{F}_{p^2}$ are 2-power isogenous over $\mathbb{F}_{p^{24}}$.*

Proof. Suppose A and B are two supersingular elliptic curves over $\mathbb{F}_{p^2}$. It is well known that there exists a 2^n-isogeny $\alpha\colon A_0 := A \to A_n := B$ over $\bar{\mathbb{F}}_p$ for some n (see [R, Lemma 3.17]). We can factor α as

$$A_0 \xrightarrow{\alpha_1} A_1 \cdots A_{i-1} \xrightarrow{\alpha_i} A_i \cdots A_{n-1} \xrightarrow{\alpha_n} A_n$$

where A_i is an elliptic curve over $\bar{\mathbb{F}}_p$ and α_i is a 2-isogeny. Furthermore, each A_i is supersingular and hence can be defined over $\mathbb{F}_{p^2}$. Thus it suffices to prove the following lemma.

Lemma 5.6. *Any two elliptic curves A and B over $\mathbb{F}_{p^k}$ which are 2-isogenous over $\bar{\mathbb{F}}_p$ are 2-isogenous over $\mathbb{F}_{p^{12k}}$.*

There exists a subgroup C of $A(\bar{\mathbb{F}}_p)$ of order 2 so that B and A/C are isomorphic over $\bar{\mathbb{F}}_p$. Now, $A \to A/C$ is defined over $\mathbb{F}_{p^{6k}}$ because all the points of order 2 on A are defined over the extension of $\mathbb{F}_{p^k}$ of degree either 2 or 3. In particular, $B \cong A/C$ over $\mathbb{F}_{p^{12k}}$ because two elliptic curves with the same j-invariant are isomorphic over the quadratic extension. □

5.2 Proof of Theorem 5.2

The case $n = 1$ follows from [DR, §VI 6.16] and the fact that all supersingular elliptic curves in characteristic p are defined over $\mathbb{F}_{p^2}$. The case $n = 2$ over $\mathbb{Q}_p^{nr}$ was handled by Edixhoven in [E1, Thm 2.1.1].

When $n \in \{2, 3\}$, we defined an admissible rigid open cover $\mathcal{C}_0(p^n)$ of $X_0(p^n)$ in Theorems 5.3 and 9.2 of [CMc] and showed that it was semi-stable over $\mathbb{C}_p$. We must show that the cover is defined and semi-stable (as in [CMc, Prop 2.5]) over F_n. In particular, we must show that (over F_n) each subspace W in the cover is a basic wide open, and that the subspaces intersect each other in the union of annuli.

Recall from [CMc, §3.2] that wide open neighborhoods, $W^{\pm}_{a\,b}$, of the ordinary affinoids, $\mathbf{X}^{\pm}_{a\,b}$, can be constructed by considering pairs (E, C) where E is "nearly ordinary." So we begin by showing that each $W^{\pm}_{a\,b}$ is a basic wide open (using essentially the same argument as was used in the proofs of [CMc, Thm 5.3, 9.2]). The affinoid, $\mathbf{X}^{\pm}_{a\,b}$, is defined and has good reduction over F_n by Lemma 3.6 of [CMc]. Then the intersections, $W^{\pm}_{a\,b} \cap W_A(p^n)$, are shown to be annuli over F_n by choosing an appropriate map to $X_0(p)$ and applying Lemma 2.3 about extensions of annuli. Thus each $W^{\pm}_{a\,b}$ is a basic wide open over F_n. Furthermore, there isn't anything else to show in the $n = 2$ case, since

$$\mathbf{Y}_A = W_A(p^2) - \bigcup W^{\pm}_{a\,b}$$

is defined and has good reduction over F_2 by [CMc, Prop 5.2].

Now suppose that $n = 3$ and fix a supersingular curve, $A/\mathbb{F}_p$, with $j(A) \neq 0$ or 1728. By [CMc, Prop 4.2] and Theorem 5.5, it suffices to verify the above conditions for the subspaces which cover $W_A(p^3)$ for one such A. For convenience, we briefly recall the definitions of these subspaces. Initially, we cover $W_A(p^3)$ with three subspaces: $V_1(A)$, $V_2(A)$, and $U(A)$. Each one is $\pi_{1\,1}^{-1}$ of some sub-annulus of $W_A(p)$, and they are chosen so that $V_i(A)$ is a neighborhood of $\mathbf{E}_{i\,A}$ while $U(A)$ is a neighborhood of $\mathbf{Z}_A$. Now, in order to deal with the singular residue classes of $\mathbf{Z}_A$, we then refine the cover in the following way. Let $\mathcal{S} := \mathcal{S}(A)$ be the set of singular residue classes of $\mathbf{Z}_A$, and let $\mathbf{X}_S$ be the underlying affinoid of any $S \in \mathcal{S}$. Then we basically remove every $\mathbf{X}_S$ from $U(A)$ to get a new neighborhood, $\hat{U}(A)$, of $\mathbf{Z}_A$. Thus the subspaces in $\mathcal{C}_0(p^3)$ which cover $W_A(p^3)$ are given by:

$$\big\{V_1(A), V_2(A), \hat{U}(A)\big\} \cup \mathcal{S}(A).$$

Now, much of the proof of [CMc, Thm 9.2] is still valid, as stated, over F_3. For example, by Proposition 8.7 of [CMc] and Proposition 5.3 the elements in $\mathcal{S}(A)$ are basic wide opens over F_3. Also, $V_i(A)$ and $U(A)$ are at least wide opens over F_3, because they are residue classes of affinoids which are defined over F_3 (exactly as in the proof over $\mathbb{C}_p$). So the only things which we have to justify are that the affinoids, $\mathbf{Z}_A$, $\mathbf{E}_{1\,A}$, and $\mathbf{E}_{2\,A}$ have good reduction over F_3, and that $V_i(A) \cap U(A)$ is an annulus over F_3. This is where we use Krir.

By Krir's result we know that the affinoids $\mathbf{Z}_A$, $\mathbf{E}_{1\,A}$ and $\mathbf{E}_{2\,A}$ have good reduction over M_3, and that $V_i(A) \cap U(A)$ is an annulus over M_3. Then it follows from Proposition 3.14 of [CMc] that $V_i(A) \cap U(A)$ is an annulus over F_3. Also, $\mathbf{Z}_A$, $\mathbf{E}_{1\,A}$, and $\mathbf{E}_{2\,A}$ have good reduction over F_3 because any reduced affinoid which acquires good reduction over an unramified extension must have good reduction. Therefore our cover can be defined and is semi-stable over F_3, and hence it corresponds by [CMc, Prop 2.7] to a semi-stable model for the curve over F_3.

6 Action of Inertia

If Y/K is a curve, and $\mathcal{Y}$ its stable model over $\mathbb{C}_p$, there is a homomorphism w_Y from

$$I_K := \mathrm{Aut}_{cont}(\mathbb{C}_p/K^{nr}) \to \mathrm{Aut}(\overline{\mathcal{Y}}).$$

It is characterized by the fact that for each $P \in Y(\mathbb{C}_p)$ and $\sigma \in I_K$,

$$\overline{P^\sigma} = w_Y(\sigma)(\overline{P}). \tag{1}$$

We have something similar if $\mathbf{Y}$ is a reduced affinoid over K. Namely, we have a homomorphism $w_Y \colon I_K \to \mathrm{Aut}(\overline{\mathbf{Y}}_{\mathbb{C}_p})$ characterized by (1). This follows from the fact that I_K preserves $(\mathbf{Y}_{\mathbb{C}_p})^0$ (power bounded elements of $A(\mathbf{Y}_{\mathbb{C}_p})$) and $A(\mathbf{Y}_{\mathbb{C}_p})^v$ (topologically nilpotent elements of $A(\mathbf{Y}_{\mathbb{C}_p})$). Moreover, inertia action behaves well with respect to morphisms in the following sense.

Lemma 6.1. *If $f \colon X \to Y$ is morphism of reduced affinoids over K and $\sigma \in I_K$, then $w_Y(\sigma) \circ \bar{f} = \bar{f} \circ w_X(\sigma)$.*

For convenience, we let $I = I_{\mathbb{Q}_p}$ and let w be the inertia action (over $\mathbb{Q}_p$) on

$$\prod_{n \geq 1} \mathrm{Aut}(\overline{\mathcal{X}_0(p^n)}).$$

Also, let m_n denote the intersection of all extensions of K^{nr} over which $X_0(p^n)$ has semi-stable reduction. It is known that m_n is the minimal such extension. Clearly $m_n \subseteq M_n$ but Krir says the extension M_n "n'est certainement pas minimale." In the case of $X_0(81)$, this is confirmed in [M2, §4], where a stable model for $X_0(81)$ is defined over an extension of $\mathbb{Q}_3^{nr}$ of degree 36 while Krir's field has ramification index $8 \cdot 3^4$. From our calculation of the inertia action, however, it will follow that $m_n = M_n$ for $n \leq 3$.

6.1 Inertial action on the ordinary components

For $a, b \geq 0$, let $X^{\pm}_{a\,b}$ denote the reduction of the ordinary affinoid, $(\mathbf{X}^{\pm}_{a\,b})_{\mathbb{C}_p}$, in the sense of Remark 2.3. Then since $\mathbf{X}_{a\,b}$ is defined over $\mathbb{Q}_p$, $w(\sigma)$ must preserve $X_{a\,0}$, $X_{0\,b}$ and $X_{a\,b} = X^{+}_{a\,b} \coprod X^{-}_{a\,b}$ (for $ab \neq 0$). Also, as explained in [C1, §1] (or the previous section on Heegner points), if $a \geq b$, $\mathbf{X}_{a\,b}$ is naturally isomorphic to $\mathbf{X}_{b\,a}$ and to $\mathbf{X}_{b\,b}$. Therefore, by Lemma 6.1, it suffices to compute the inertial action on $X_{b\,b}$.

So recall first that there is an isomorphism between $X^{\beta}_{b\,b}$ and $Ig(p^b)$ which can be constructed as follows. First we choose a primitive p^b-th root of unity, ζ, which represents β in the sense that whenever $(E,\mathcal{P}) \in \mathbf{X}^{\beta}_{b\,b}$ and P generates $K_b(E)$ we have $\mathcal{P}(P,P) = \zeta^{k^2}$ for some $k \in (\mathbb{Z}/p^b\mathbb{Z})^*$ (this is explained on page 5 of [C1]). Then we can define an embedding, $\alpha_\zeta : \mathbf{X}^{\beta}_{b\,b} \to X_1(p^b)$, given by $\alpha_\zeta(E,\mathcal{P}) = (E, p^bQ)$, where $Q \in E[p^{2b}]$ such that there exists $P \in K_b(E)$ with

$$e_{p^{2b}}(P,Q) = \mathcal{P}(P,P) = \zeta.$$

This passes to an isomorphism, $X^{\beta}_{b\,b} \to Ig(p^b)$.

Now, let d be a quadratic non-residue. Identify $\mathbf{X}^{+}_{b\,b}$ with $\mathbf{X}^{-}_{b,b}$ by $(E,\mathcal{P}) \to (E,\mathcal{P}^d)$, and correspondingly $X_{b\,b}$ with $Ig(p^b) \times \{\pm 1\}$. Suppose that $\sigma \in I$ and $\sigma(\zeta) = \zeta^{d^i t^2}$, where $i \in \{0,1\}$ and $t \in (\mathbb{Z}/p^b\mathbb{Z})^*$. Then we have $\sigma(E,\mathcal{P}) = (E^\sigma, \mathcal{P}^\sigma)$, where

$$\mathcal{P}^\sigma(\sigma(A),\sigma(B)) = \sigma(\mathcal{P}(A,B)).$$

So if $\mathcal{P}(P,P) = \zeta$, it follows that

$$e_{p^{2b}}(\sigma(P)/t, \sigma(Q)/T) = \mathcal{P}^\sigma(\sigma(P)/t, \sigma(P)/t) = \zeta^{d^i},$$

where $T \in \mathbb{Z}/p^{2b}\mathbb{Z}$ and $T \equiv t \pmod{p^b}$. Identify (the obvious subgroup of) $\mathrm{Aut}(Ig(p^n))$ with $(\mathbb{Z}/p^n\mathbb{Z})^*$. Then we see that $w(\sigma)$ acts on $X_{b\,b}$ as follows.

PROPOSITION 6.2. *The inertial action on the ordinary components of $X_0(p^n)$ is given by*

$$w(\sigma)|_{X_{b\,b}} = (t^{-1}, (-1)^i).$$

COROLLARY 6.3. *The field $\mathbb{Q}_p^{nr}(\mu_{p^{[n/2]}})$ is contained in m_n.*

6.2 ACTION OF INERTIA ON $\overline{\mathcal{X}_0(p^2)}$

Suppose A is a supersingular elliptic curve over $\mathbb{F}_{p^2}$. Inside the corresponding residue class, $W_A(p^2) \subseteq X_0(p^2)$, we have an affinoid $\mathbf{Y}_A$ defined over $W(\mathbb{F}_{p^2}) \otimes \mathbb{Q}_p$ such that $Y_A := \overline{\mathbf{Y}_A \otimes \mathbb{C}_p}$ is the set of non-singular points in a component of the stable reduction of $\mathcal{X}_0(p^2)$. Now we determine the action of I on Y_A.

First assume that A is defined over $\mathbb{F}_p$ and that $j(A) \neq 0$ or 1728 (general case will follow from Lemma 6.1). Let κ be as in Theorem 2.2. We know there are series $F(T), G(T) \in T\mathbb{Z}_p[[T]]$ such that $\mathbf{Y}_A$ is the affinoid

$$\mathrm{MAX}\ (\mathbb{Q}_p\langle a, a^{-1}, b, b^{-1}, x, y\rangle / M)$$

where M is the ideal generated by $\kappa^p a = x^{p+1}$, $\kappa^p b = y^{p+1}$ and

$$(F(x) + G(\kappa/x) - F(y) - G(\kappa/y)).$$

Suppose $\alpha^{p+1} = \kappa$. Then if $K = \mathbb{Q}_p(\alpha)$, $(\mathbf{Y}_A)_K$ is

$$\text{Max}\ \big(K\langle u, v, u^{-1}, v^{-1}\rangle/(F(\alpha^p/u) + G(\kappa u/\alpha^p) - F(\alpha^p/v) - G(\kappa v/\alpha^p))\big),$$

where $u = \alpha^p/x$ and $v = \alpha^p/y$. It follows that Y_A has the equation,

$$uv(v-u)^{p-1} = 1,$$

or $s^{p+1} = (r^2-1)/4$, if we let $s = 1/(v-u)$ and $r = (u+v)/(v-u)$. Now, on one hand we have $\overline{\sigma(u(P))} = \overline{u(P)}$. On the other, if $\sigma(\alpha) = \zeta\alpha$ for a $p+1$-st root of unity, ζ, we have $\sigma(u(P)) = \zeta^p u(\sigma(P))$. Thus, on Y_A, $w(\sigma)$ is the automorphism $(u,v) \to (\zeta u, \zeta v)$, or equivalently $(r,s) \to (r, \zeta^{-1}s)$.

Since we have a finite morphism from $\mathbf{Y}_A$ to $\mathbf{Y}_{A'}$ over $W(\bar{\mathbb{F}}_p) \otimes \mathbb{Q}$ for arbitrary supersingular A' (an isomorphism when $j(A') \neq 0$ or 1728) we know by Lemma 6.1 the action of I on $Y_{A'}$ for all A' as long as $p \geq 13$. In general, Y_A has the equation

$$s^{(p+1)/i(A)} = (r^2-1)/4$$

and $w(\sigma)$ is the automorphism $(r,s) \to (r, \zeta^{-i(A)}s)$. This also determines the action on $E_{i\,A}$, $i \in \{1,2\}$, since as explained in Remark 9.3 of [CMc] we have finite degree p morphisms $\mathbf{E}_{1\,A} \to \mathbf{Y}_A$ and $\mathbf{E}_{2\,A} \to \mathbf{Y}_{A^{Frob}}$ with purely inseparable reduction.

Remark 6.4. *It follows from the above and Corollary 6.3 that $K^{nr}(\mu_p,\alpha) \subseteq m_2$. Therefore, since*

$$Gal(K^{nr}(\mu_p,\alpha)/K^{nr}) \cong \mathcal{O}_K^*/\{a \in \mathcal{O}_K^* \colon a^2 \in 1 + \sqrt{p}\mathcal{O}_K\},$$

we see that $M_2 = m_2$.

6.3 Action of Inertia on $\overline{\mathcal{X}_0(p^3)}$

Suppose A is a supersingular elliptic curve over $\mathbb{F}_p$ with $B = \text{End}(\hat{A})$. Suppose $\rho \in B'$ and x is a fixed point of $\overline{w}_\rho$. Then we know w_ρ has a unique fixed point $\tilde{x} := (F, \iota, C)$ in $\mathbf{SD}(\mathbb{C}_p)$ above x. Let C_x be the smooth locus of the corresponding component of the stable reduction of $X_0(p^3)$ (which is affine and hyper-elliptic, with equation $y^2 = x^p - x$). By Proposition 7.4 of [CMc] the fixed points $\mathcal{F}_x$ of the hyper-elliptic involution τ_x of C_x are naturally in 1-1 correspondence with the p non-canonical subgroups of $F[p]$. So $\text{Aut}(F)$ acts on $\mathcal{F}_x$.

If L is a finite extension of $\mathbb{Q}_p$, let Art_L denote the Artin map from L^* to $\text{Gal}(L^{ab}/L)$. Let $D \in \mathbb{Z}^+$ be a quadratic non-residue mod p and $K = \mathbb{Q}_p(\sqrt{-p}, \sqrt{-Dp})$.

Theorem 6.5. *Let N_F denote the norm from K^* to $\mathbb{Q}_p \otimes End F$. If $b \in \mathcal{O}_K^*$ and $Q \in \mathcal{F}_x$, then*

$$w(Art_K(b))Q = N_F(b^{-1})Q.$$

This makes sense because End F maps naturally into K. Also, if M_3 is the class field over K of the subgroup of K^* given by $(\sqrt{p})^{\mathbb{Z}}\mu_{p^2-1}(1+p\mathcal{O}_K)$, then the non-canonical subgroups of $F[p]$ are defined over M_3 by Proposition 5.3.

PROPOSITION 6.6. *Suppose K is an imaginary quadratic field and $\mathfrak{p}$ is a prime ideal of $\mathcal{O}_K$. If E is an elliptic curve with good reduction over the ring of integers R of a finite unramified extension L of $K_{\mathfrak{p}}$ with CM in K then the formal group of E over R is a relative Lubin-Tate group as defined by de Shalit in [dS2].*

LEMMA 6.7. *Suppose E and L are as above and σ is the Frobenius automorphism of $L/K_{\mathfrak{p}}$. Then there is an isomorphism of $E' := E/\ker(\mathfrak{p} \cap EndE)$ with E^σ so that the reduction of the natural map $\alpha\colon E \to E'$ is Frobenius.*

Proof. This follows from [S, Thm 5.4]. Indeed, identify $\mathbb{C}$ with $\mathbb{C}_{\mathfrak{p}}$, and take σ to be an automorphism of $\mathbb{C}$ which restricts to $[s,K]$ on K^{ab} where $s_{\mathfrak{l}} = 1$ for $\mathfrak{l} \neq \mathfrak{p}$ and $(s_{\mathfrak{p}}) = \mathfrak{p}(\mathcal{O}_K)_{\mathfrak{p}}$. Then Shimura's theorem implies that there exists an isomorphism, $\xi\colon E' \xrightarrow{\sim} E^\sigma$, such that if P is a torsion point on E of order prime to $\mathfrak{p}$, $\xi(\alpha(P)) = P^\sigma$. Because σ is a lifting of Frobenius and the points of order prime to $\mathfrak{p}$ reduce to infinitely many distinct points of $E \mod \mathfrak{p}$, the lemma follows. $\square$

Proof. (of proposition) Let $\beta\colon E \to E^\sigma$ be the isogeny of the above lemma. If T is a parameter at the origin on E, let $f(T) = \beta^* T^\sigma$ and $f(T) = \pi' T + \cdots$. Then $f \in \mathcal{F}_{N_{L/K}(\pi')}$ (notation as in [dS2]), and if p_1 and p_2 are the natural projections of $E \times E$ onto E, with $X = p_1^* T$ and $Y = p_2^* T$, then $\hat{E}(X,Y) = F_f(X,Y)$. $\square$

PROPOSITION 6.8. *If E/R has fake CM, then $\hat{E}$ is a relative Lubin-Tate group.*

Proof. Suppose $S \in \mathcal{R}$, $E = (F,\alpha)$ and $\mathrm{End}_R F \cong S$. Then, by Theorem 4.1, we know $\exists \rho \in B^*$, such that $(F, \rho\alpha)$ has CM. $\square$

The theorem now follows from (6.4) of [Iw].

COROLLARY 6.9. *$M_3 = m_3$.*

Proof. It follows from Corollary 6.3 and the remarks at the end of §6.2 that $M_2 = K^{nr}(\mu_p, p^{1/(p+1)}) \subseteq m_3$. (In general, it follows from Lemma 2 and Theorem 6 of [BLR, §6] that $m_n \subseteq m_{n+1}$.) The theorem implies that $(1 + \sqrt{p}\mathcal{O}_K)/(1+p\mathcal{O}_K)$ injects into $\mathrm{Gal}(m_3/K)$ via the Artin map. Indeed, if $K_1 = \mathbb{Q}_p(\sqrt{p})$ and $K_2 = \mathbb{Q}_p(\sqrt{pD})$, the map $(N^K_{K_1}, N^K_{K_2})$ from $(1+\sqrt{p}\mathcal{O}_K)/(1+p\mathcal{O}_K)$ to

$$(1 + \sqrt{p}\mathcal{O}_{K_1})/(1 + p\mathcal{O}_{K_1}) \times (1 + \sqrt{pD}\mathcal{O}_{K_2})/(1 + p\mathcal{O}_{K_2})$$

is an isomorphism. $\square$

REMARK 6.10. *This implies the existence of a weight 2 newform on $X_0(p^3)$ whose corresponding representation is wildly ramified at p, which has been independently verified by Jared Weinstein.*

Let $\mathcal{D}_x$ be the wide open residue class above x in $\mathbf{SD}_A$ (recall that x is a fixed point of $\overline{w}_\rho$) and $\tilde{\mathcal{D}}_x$ the residue class above $\mathcal{D}_x$ in $\mathbf{Z}_A$. Let $s\colon \mathcal{D}_x \to X_1(p)$ be a section of $X_1(p) \to X_0(p)$ on the image of $\mathcal{D}_x$ as in Lemma 8.6 of [CMc]. For $\zeta \in \mu_p$ we defined an automorphism $\tilde{S}_{s,\zeta}$ of $\tilde{\mathcal{D}}_x$. For $b \in \mathcal{O}_K^*$, let $\nu(b) = 0$ if b is a square and 1 otherwise.

Corollary 6.11. *Suppose $\tilde{x} = (E, C)$. Then there exists an $n_x \in \{0, 1\}$ such that for $b \in \mathcal{O}_K^*$*

$$w(Art_K(b))\big|_{C_x} = \overline{\tilde{S}_{s,e_1(P,Q)}}\tau_x^{\nu(b)n_x},$$

where $s(E, C) = (E, P)$, $Q \in E[p]\backslash C$, $e_1(\ ,\ )$ is the Weil pairing on $E[p]$ and $(P + Q) = N_F(b^{-1})(Q)$.

This follows from the theorem and the following lemma whose proof we leave as an exercise for the reader.

Lemma 6.12. *The automorphism group of the affine curve $y^2 = x^p - x$ has order $2(p-1)p$ and is generated by $\alpha : (x, y) \mapsto (x + 1, y)$ and $\beta_b : (x, y) \mapsto (ax, by)$, where $a \in \mathbb{F}_p^*$ and $b^2 = a$. These satisfy $\alpha^p = \beta_b^{2(p-1)} = 1$ and $\beta_b\alpha\beta_b^{-1} = \alpha^a$. In particular, there is only one p-Sylow subgroup, and its centralizer is Abelian and generated by α and β_{-1}.*

We will show that $n_x = 1$. Suppose $\sigma \in I$ and $\sigma(\sqrt{p}) = -\sqrt{p}$. Then $w(\sigma)$ on the bridging component above A, which has the equation

$$X^{(p+1)/i(A)} + X^{-(p+1)/i(A)} = Z^p,$$

is $X \to (-1)^{i(A)}X$. When $j(A) \neq 0$ or 1728, this follows from Equation (4) of [CMc, §8]. The general case then follows from Lemma 6.1. As in the proof of Proposition 8.3 of [CMc], the involutions $\overline{\tilde{w}}_\rho$ are

$$(X, Z) \to (\zeta/X, Z),$$

where ζ runs over the $(p + 1)/i(A)$-th roots of unity (X^{-p} may be identified with a parameter U on $\mathbf{SD}_A$ so that the involutions $\overline{w}_\rho$ are $U \to \zeta/U$). The fixed points of $\overline{w}_\rho$ on $\overline{\mathbf{SD}}_A$ are the solutions x of $U(x)^2 \equiv \zeta$. We now label the fixed points of the involutions $\overline{w}_\rho$ by the $2(p+1)/i(A)$-th roots of unity. So for each such root of unity ξ, there is a component C_ξ of $\overline{\mathcal{X}_0(p^3)}$. It follows from the above that $w(\sigma)$ restricts to an isomorphism from C_ξ to $C_{(-1)^{i(A)}\xi}$.

The group B^* acts on the part of stable model over A. If $\alpha \in B^*$, let $h(\alpha)$ be the corresponding automorphism of that part of the reduction. If $\sigma \in I$, because the action of B^* is defined over $\mathbb{Q}_p^{nr}$ (and by Lemma 6.1), we have

$$w(\sigma) \circ h(\alpha) = h(\alpha) \circ w(\sigma). \tag{2}$$

Using Lemma 3.6, we see that if $\alpha \in B'$ and $\alpha^2 \in \mathbb{Z}_p^*$, then

$$0 = \alpha^2 - (\alpha')^2 = (\alpha - \alpha')(\alpha + \alpha'),$$

and thus $\alpha = \pm\alpha'$. In particular, we have $\alpha\tilde{x} = \alpha'\tilde{x}$. So

$$w_\rho(\alpha\tilde{x}) = \rho w(\alpha'\tilde{x}) = \rho\alpha w(\tilde{x}),$$

which equals $\alpha\tilde{x}$ if $\alpha\rho = \rho\alpha$ and doesn't equal $\tilde{x}$ if $\alpha \notin \mathrm{Aut}(A)\mathbb{Z}_p^*(1 + jB)$. (So for example, if $\rho \in \mathbb{Z}_p[i]$ and $\alpha = i$ and $j(A) \neq 1728$.) Suppose this to be the case (i.e. α satisfies these conditions). Then if $\tilde{x} \sim (F, \iota, C)$, the other fixed point of w_ρ is $\alpha\tilde{x} \sim (F, \alpha\iota, C)$. (This implies Corollary 3.10 in this case.) Let $x' = \overline{\alpha x}$. Then $h(\alpha)$ takes C_x to $C_{x'}$ and vice-versa.

Let $X_\xi = C_\xi \coprod C_{-\xi}$. For $\tau \in I$, identifying C_ξ with $C_{-\xi}$ via $h(\alpha)$ and using (2), we can write

$$w(\tau)|_{X_\xi} = (a(\tau), s(\tau)) \in \mathrm{Aut}(C_\xi) \times \{\pm 1\}$$

where $s(\tau) = \tau(\sqrt{p})/\sqrt{p}$. If $\tau = \mathrm{Art}_K(v)$, it follows that $s(\tau) = 1$. Suppose $s(\sigma) = -1$. Then on X_ξ, on one hand we have

$$w(\sigma)w(\tau)w(\sigma^{-1}) = w(\sigma\tau\sigma^{-1}) = (a(\tau^{-1}), 1),$$

and on the other we have

$$w(\sigma)w(\tau)w(\sigma^{-1}) = (a(\sigma)a(\tau)a(\sigma^{-1}), 1).$$

It follows that $a(\sigma)$ is not in the commutative subgroup (α, β_{-1}) of $\mathrm{Aut}(y^2 = x^p - x)$. This implies $a(\sigma)^2 \notin (\alpha)$ so $n_x = 1$. Thus, in particular, there exists σ such that $s(\sigma) = -1$, $a(\sigma) = \beta_\epsilon$, where $\epsilon^2 = -1$.

Suppose now that $j(A) = 1728$. Let ξ be a $(p+1)/2$-th root of unity and $X = C_\xi$. It follows that if $\sigma \in I$, $w(\sigma)(X) = X$. Let $L = \mathrm{End}\, F \otimes \mathbb{Q}_p$. We know X is a double cover of $\mathbf{P}^1$ and its branch points correspond to non-canonical subgroups of $F[p]$. Moreover, if Q is such a subgroup and $b \in \mathcal{O}_L^*$, we have

$$w(\mathrm{Art}_L(b))Q = b^{-1}Q.$$

In particular, $w(\mathrm{Art}_L(\mathbb{Z}_p^*(1+p\mathcal{O}_L)))$ is the identity. Now suppose that $\sigma|_L \neq id$. Then

$$\sigma \mathrm{Art}_L(b) = \mathrm{Art}_L(\bar{b})\sigma.$$

So if $\tau = \mathrm{Art}_L(b)$, then

$$w(\sigma)w(\tau)w(\sigma)^{-1} = w(\tau)^{-1}.$$

It follows from the theorem and Lemma 6.12 that if the order of $w(\sigma)$ is prime to p, $w(\sigma^2) = w(\sigma)^2 = \tau_x$ and thus $n_x = 1$.

7 Stable Model of $X_0(p^3)$ when $p < 13$

Recall from Section 2 that the argument which we used in [CMc] to compute the stable model of $X_0(p^3)$ does not only apply when $p < 13$. The reason for this is that in these cases there is no supersingular region where one can apply analysis of de Shalit, as restated in Theorem 2.2, which approximates the forgetful map from $X_0(p)$ to $X(1)$. In this section, we recall in greater detail how the theorem is used to construct components in the supersingular regions of $X_0(p^2)$ and $X_0(p^3)$ when $p \geq 13$. We then use explicit equations for $X_0(p)$ when $p = 5$, 7, and 11, to derive formulas analogous to Theorem 2.2, and subsequently construct the analogous stable reduction components. This should serve not only to extend the result of [CMc] to $p > 3$, but also to make the construction more understandable and concrete.

7.1 Explicit Analysis of a "Good" Supersingular Region

Suppose that $p > 13$, and hence by the result of Howe that there is a supersingular $A/\mathbb{F}_p$ with $j(A) \neq 0, 1728$. All of the information from Theorem 2.2 which we need to do the explicit analysis of [CMc] can be summarized as follows. First of all, we have parameters, t and s, on $W_A(p)$ and $W_A(1)$ (respectively), which identify these regions with the annulus, $0 < v(t) < 1$, and the disk, $v(s) > 0$. Moreover, in terms of these parameters, the maps π_f and w_1 satisfy

$$w_1(t) = \frac{\kappa}{t} \qquad \text{and} \qquad s = \pi_f(t) \equiv t + \left(\frac{\kappa}{t}\right)^p \pmod{p},$$

for some $\kappa \in W(\mathbb{F}_{p^2})$ with $v(\kappa) = 1$. Finally, the three special circles inside $W_A(p)$, namely $\mathbf{TS}_A$, $\mathbf{SD}_A$, and $\mathbf{C}_A$, are described by $v(t) = \frac{p}{p+1}$, $v(t) = \frac{1}{2}$, and $v(t) = 1 - \frac{1}{2p}$ (respectively).

Using the above information, we now recall briefly how to explicitly calculate the reduction of the affinoid, $\mathbf{Y}_A := \pi_\nu^{-1}(\mathbf{TS}_A) \subseteq W_A(p^2)$. First of all, we show in [CMc, Lemma 5.1] that $\mathbf{Y}_A$ is isomorphic to the rigid space:

$$T_A := \{\ (x, y) \in \mathbf{TS}_A \times \mathbf{TS}_A \mid x \neq y,\ \pi_f(x) = \pi_f(y)\ \}.$$

Then we take $u, v = \alpha^p/t$ as parameters on two copies of $\mathbf{TS}_A$, for any α with $v(\alpha) = \frac{1}{p+1}$. With these parameters, the condition that $\pi_f(x) = \pi_f(y)$ leads to the following congruence.

$$u^{-1} - v^{-1} \equiv (v^p - u^p)(\kappa/\alpha^{p+1})^p \pmod{\alpha}.$$

By making the change of variables $s = 1/(v-u)$ and $r = (v+u)/(v-u)$, we disregard the $u = v$ component and arrive at an isomorphism between $\overline{\mathbf{Y}}_A$ and an affine curve of the form $s^{p+1} = c(r^2 - 1)$. Note that this equation also ends up describing the reductions of the affinoids, $\mathbf{E}_{1\,A}, \mathbf{E}_{2\,A} \subseteq W_A(p^3)$, which lie over $\mathbf{Y}_A$ via π_f and π_ν (see [CMc, Remark 9.3]).

Similarly, we compute the reduction of $\mathbf{Z}_A := \pi_{1\,1}^{-1}(\mathbf{SD}_A) \subseteq W_A(p^3)$ by first identifying it with the rigid space:

$$S_A := \{\ (x, y) \in \mathbf{C}_A \times \mathbf{C}_A \mid \tau_f(x) = w_1 \circ \tau_f(y)\ \}$$

(this is done in [CMc, Prop 7.1]). Recall that $\tau_f : \mathbf{C}_A \to \mathbf{SD}_A$ is the map which takes (E, C) to $(E, H_1(E))$, and hence that $\pi_f \circ \tau_f = \pi_f$. Therefore, in terms of the parameter t from above, it is easy to show that

$$\tau_f(t) \equiv t + (\kappa/t)^p \pmod{p}.$$

Now we may proceed as before, taking $U = t/\sqrt{\kappa}$ as a parameter on $\mathbf{SD}_A$ (note that $w_1(U) = 1/U$), and taking $X, Y = t/\alpha$ as parameters on two copies of $\mathbf{C}_A$, for any α with $v(\alpha) = 1 - \frac{1}{2p}$. With a careful choice of α (see [CMc, Prop 8.2]), the definition of S_A translates into the following congruence.

$$(X^{-p} + \alpha X/\sqrt{\kappa})(Y^{-p} + \alpha Y/\sqrt{\kappa}) \equiv 1 \pmod{\sqrt{p}}$$

Finally, after a second change of variables of the form, $Z = c(XY - 1)$, we obtain the following equation for $\overline{\mathbf{Z}}_A$.

$$X^{p+1} + X^{-(p+1)} = Z^p$$

Once again, when $p < 13$, the preceding calculations do not apply because there is no such A. So for the specific primes, $p = 5$, 7, and 11, we will now derive a formula which is analogous to Theorem 2.2 for each supersingular region, and then use it to compute the reductions of $\mathbf{Y}_A$ and $\mathbf{Z}_A$ (as above). In each case, we do arrive at equations which are consistent with Theorem 2.5. Our claim is that the rest of the argument of [CMc] (as summarized in Section 2) is completely analogous for these primes, and need not be repeated. As a final note, we do not address $X_0(8)$ and $X_0(27)$ primarily because both have good reduction. Additionally, complications arise from the fact that $j = 0$ and $j = 1728$ lie in the same residue disk of $X(1)$ in both cases.

7.2 $X_0(5^3)$

Borrowing directly from [M1, §4], we can choose a parameter on the genus 0 curve, $X_0(5)$, by taking $t = \eta_1^6/\eta_5^6$. The only supersingular j-invariant is $j = 0$, and the corresponding annulus is described by $0 < v(t) < 3$. Furthermore, from [M1, Table 3], the formulas for the forgetful map and Atkin-Lehner involution are then given by

$$\pi_f^* j = \frac{(t^2 + 2 \cdot 5^3 t + 5^5)^3}{t^5} \qquad \text{and} \qquad w_1^* t = 125/t.$$

The circles $\mathbf{SD}$ and $\mathbf{C}$ are described by $v(t) = 1.5$ and $v(t) = 2.7$ (respectively), and the too-supersingular circle, $\mathbf{TS}$, is where $v(t) = 2.5$.

First we compute the reduction of the affinoid, $\mathbf{Y} := \pi_\nu^{-1}(\mathbf{TS}) \subseteq X_0(25)$, by embedding it into $\mathbf{TS} \times \mathbf{TS}$ as above. For parameters on two copies of $\mathbf{TS}$, we may choose $X, Y = t/(25\sqrt{5})$. Then plugging these parameters into the equation, $\pi_f(x) = \pi_f(y)$, we quickly arrive at the congruence:

$$(X^2 + 1)^3/X^5 \equiv (Y^2 + 1)^3/Y^5 \pmod{\sqrt{5}}.$$

From the definition of T_A, we are interested only in the component where $X \neq Y$, and by letting $X = s/(r-1)^3$ and $Y = s/(r+1)^3$ we see that this is isomorphic to the affine curve:

$$s^2 = r^2 - 1. \tag{3}$$

Now we compute the reduction of $\mathbf{Z} := \pi_{1\,1}^{-1}(\mathbf{SD}) \subseteq X_0(125)$ by means of the embedding into $\mathbf{C} \times \mathbf{C}$. We need an approximation for $\tau_f : \mathbf{C} \to \mathbf{SD}$, and from the above formula for π_f, it is easy to show that

$$\tau_f(t) \equiv \frac{5^{15}}{t^5} + \frac{3 \cdot 5^{10}}{t^3} \pmod{5^2}.$$

As in [CMc, §8.1], we need to work over a larger extension of $\mathbb{Z}_5$ to define and compute the reduction of $\mathbf{Z}$. In particular, it suffices to work over $R := \mathbb{Z}_5[\beta, \sqrt{5}]$, where $\beta \in \mathbb{C}_5$ is chosen so that $\beta^{25} \equiv 5 \pmod{5\sqrt{5}}$. For parameters on $\mathbf{SD}$ and (both copies of) $\mathbf{C}$, we then choose the functions $U = t/(5\sqrt{5})$ and $X, Y = t/(25\beta^5\sqrt{5})$. Using these parameters and our formula for τ_f, the equation $\tau_f(x) = w_1 \circ \tau_f(y)$ then leads to the following congruence.

$$\left(\frac{1}{X^5} + \frac{3\beta^{10}}{X^3}\right)\left(\frac{1}{Y^5} + \frac{3\beta^{10}}{Y^3}\right) \equiv 1 \pmod{\sqrt{5}}$$

After making the substitution, $Z = (XY - 1)/(3\beta^2)$, we arrive at our final equation for $\overline{\mathbf{Z}}$.

$$X^2 + X^{-2} = Z^5 \tag{4}$$

Remark 7.1. *Note that Equations* (3) *and* (4)*, describing* $\overline{\mathbf{Y}}$ *and* $\overline{\mathbf{Z}}$*, are consistent with Theorem 2.5, since* $p = 5$ *and* $i(A) = 3$ *in this case.*

7.3 $X_0(7^3)$

This is very similar to the previous example, as $X_0(7)$ also has genus 0 and only one supersingular annulus corresponding to $j = 1728$. If we take $t = \eta_1^4/\eta_7^4$ as a parameter (see [M1, §2]), the supersingular annulus is the region described by $0 < v(t) < 2$, and the formulas for the forgetful map and Atkin-Lehner involution are as follows.

$$\pi_f^*(j - 1728) = \frac{(t^4 - 10 \cdot 7^2 t^3 - 9 \cdot 7^4 t^2 - 2 \cdot 7^6 t - 7^7)^2}{t^7} \qquad w_1^* t = \frac{49}{t}$$

The circles, $\mathbf{SD}$ and $\mathbf{C}$, are now given by $v(t) = 1$ and $v(t) = 13/7$ (respectively), and $\mathbf{TS}$ is the circle where $v(t) = 7/4$.

We begin by embedding $\mathbf{Y} := \pi_\nu^{-1}(\mathbf{TS}) \subseteq X_0(49)$ into $\mathbf{TS} \times \mathbf{TS}$, taking $X, Y = \alpha t/49$ as parameters on both copies of $\mathbf{TS}$, where $\alpha^4 = -7$. With these parameters, the equation $\pi_f(x) = \pi_f(y)$ yields the congruence:

$$(X^4 + 1)^2/X^7 \equiv (Y^4 + 1)^2/Y^7 \pmod{\alpha}.$$

Then the substitution, $X = s/(r-1)^2$ and $Y = s/(r+1)^2$, defines an isomorphism between the component with $X \neq Y$ and the genus 1 affine curve:

$$s^4 = r^2 - 1. \tag{5}$$

Likewise we compute the reduction of $\mathbf{Z}$ by embedding it into $\mathbf{C} \times \mathbf{C}$. This time the approximation formula for $\tau_f : \mathbf{C} \to \mathbf{SD}$, which we derive from the formula for π_f, is as follows.

$$\tau_f(t) \equiv \frac{7^{14}}{t^7} - \frac{2 \cdot 7^7}{t^3} \pmod{7\sqrt{7}}$$

Working over the extension given by $R = \mathbb{Z}_7[\beta]$ with $\beta^{49} \equiv 7 \pmod{7\sqrt{7}}$, we take $X, Y = \beta^7 t/49$ as parameters on two copies of $\mathbf{C}$. We also take $U = t/7$ as our parameter on $\mathbf{SD}$. Then the equation $\tau_f(x) = w_1 \circ \tau_f(y)$ gives us the congruence:

$$\left(\frac{1}{X^7} - \frac{2\beta^{21}}{X^3}\right)\left(\frac{1}{Y^7} - \frac{2\beta^{21}}{Y^3}\right) \equiv 1 \pmod{\sqrt{7}}.$$

To complete the calculation, we make the substitution, $Z = (1 - XY)/(2\beta^3)$, which results in our final equation for $\overline{\mathbf{Z}}$.

$$X^4 + X^{-4} = Z^7 \tag{6}$$

REMARK 7.2. *Once again, note that Equations* (5) *and* (6) *are consistent with Theorem 2.5, as* $p = 7$ *and* $i(A)$ *is now* 2.

7.4 $X_0(11^3)$

When $p = 11$, $X_0(p)$ has genus 1 and two supersingular annuli corresponding to $j = 0$ and $j = 1728$. In order to work out formulas for the forgetful map on these supersingular regions, we must choose an appropriate model for the overall curve. One convenient model relates the following two functions.

$$t = \left(\frac{\eta_1}{\eta_{11}}\right)^{12} \qquad\qquad x = \frac{dt/t}{(\eta_1\eta_{11})^2}$$

The first function has divisor $5(0) - 5(\infty)$, and the second is a degree 2 function with a simple pole at each cusp. Since w_1 interchanges the two cusps, it follows that x is actually a parameter on the genus 0 quotient, $X_0(11)^+ := X_0(11)/w_1$. Therefore, t must be quadratic over x, and indeed by comparing q-expansions we have the equation:

$$t^2 + \frac{1}{5^5}(x^5 + 170x^4 + 9345x^3 + 167320x^2 - 7903458)t + 11^6 = 0.$$

This model is singular, but we can normalize by adjoining a square root of the discriminant. In particular, the following gives a nonsingular model for $X_0(11)$.

$$y = \frac{2\cdot 5^5 t + (x^5 + 170x^4 + 9345x^3 + 167320x^2 - 7903458)}{(x+47)(x^2+89x+1424)}$$

$$y^2 = f(x) = (x-8)(x^3+76x^2-8x+188)$$

Remark 7.3. *Since x is invariant under w_1, the formulas for the Atkin-Lehner involution are given by $w_1^* t = 11^6/t$ and $w_1^* y = -y$.*

Note that there are two pairs of branch points in the degree two extension from $X_0(11)^+$ up to $X_0(11)$, and they lie in the two residue disks where $v(x-2) > 0$ and $v(x+3) > 0$. It follows that the regions lying over these residue disks are annuli. In fact, from [DR, §VI 6.16] (or the explicit calculations which follow) these are precisely the two supersingular annuli.

7.4.1 $j = 0$

Let r_1, r_2 be the two roots of $f(x)$ close to $x = -3$, and let s_1, s_2 be those close to $x = 2$. Then the following map defines an isomorphism (over $\mathbb{Q}_{11}$) between the annulus, $0 < v(z) < 3$, and the subspace of $X_0(11)$ which lies over the residue disk, $v(x-2) > 0$.

$$\begin{aligned}
x &= z + \frac{(s_1+s_2)}{2} + \frac{(s_1-s_2)^2}{16z} \equiv z + 310 - 212\left(\frac{11^3}{z}\right) \pmod{11^3}\\
y &= \left(-z + \frac{(s_1-s_2)^2}{16z}\right)\sqrt{(x(z)-r_1)(x(z)-r_2)}\\
&\approx \left(-z - 212\left(\frac{11^3}{z}\right)\right)\left(\cdots + 484\left(\frac{11^3}{z}\right)^3 + 363\left(\frac{11^3}{z}\right)^2 + \right.\\
&\qquad\qquad \left. 393\left(\frac{11^3}{z}\right) + 775 + 243z + 484z^2 + 968z^3 + \cdots\right)
\end{aligned}$$

To obtain an approximation formula for π_f over the annulus, we begin with the following explicit formula (easily verified by q-expansions).

$$\pi_f^* j = \frac{(60y + 61x^2 + 864x - 2016)^3}{5^6 t}$$

Over the whole annulus, $60y + 61x^2 + 864x - 2016$ is well approximated by $5z - 11^{11}/z^3$, in the sense that the error is always strictly smaller than the larger of these two terms. Similarly, t is always close to $-4z^2$. From this we may conclude that $v(j) > 0$ over the whole annulus (as claimed).

Now we are able to embed $\mathbf{Z} \subseteq X_0(11^3)$ into $\mathbf{C}\times\mathbf{C}$ and explicitly compute its reduction. We know that the circles, $\mathbf{SD}$ and $\mathbf{C}$, are described by $v(z) = 3/2$ and $v(z) = 63/22$ (respectively). So our formula for π_f leads to the following approximation for $\tau_f : \mathbf{C} \to \mathbf{SD}$ in terms of z.

$$\tau_f(z) \equiv \frac{-3\cdot 11^{33}}{z^{11}} + \frac{11^{22}}{z^7} \pmod{11^2}.$$

Also, from the fact that $x(z)$ must be fixed by w_1, we see that

$$w_1(z) = \frac{(s_1 - s_2)^2}{16z} \equiv \frac{-3 \cdot 11^3}{z}.$$

At this point our analysis closely parallels that of the two previous examples. In particular, let $R = \mathbb{Z}_{11}[\sqrt{-11}, \beta]$ where $\beta \in \mathbb{C}_{11}$ satisfies $\beta^{121} \equiv -11 \pmod{11\sqrt{-11}}$, and choose the following functions as parameters on **SD** and (two copies of) **C**.

$$U = \frac{2z}{11\sqrt{-11}} \qquad X, Y = \frac{-2z}{121\beta^{44}\sqrt{-11}}$$

In terms of these new parameters, the relation $\tau_f(x) = w_1 \circ \tau_f(y)$ leads to the following congruence.

$$\left(\frac{1}{X^{11}} + \frac{3\beta^{55}}{X^7}\right)\left(\frac{1}{Y^{11}} + \frac{3\beta^{55}}{Y^7}\right) \equiv 1 \pmod{\sqrt{-11}}$$

Finally, with the substitution, $Z = (XY - 1)/(3\beta^5)$, we obtain the desired equation for the reduction of **Z** over R.

$$X^4 + X^{-4} = Z^{11}$$

Similarly, the equation for the $(j = 0)$ supersingular component of $X_0(11^2)$ follows directly from the embedding of **Y** into **TS** $\times$ **TS** (where **TS** is now the circle, $v(z) = 11/4$). The approximating formula for π_f on that circle is

$$j = \pi_f(z) \equiv \frac{(5z - 11^{11}/z^3)^3}{5^6(-4z^2)} \pmod{11^3}.$$

So now let $\alpha^2 = \sqrt{-11}$ and take as parameters on both copies of **TS** the functions $X, Y = \alpha z/(5 \cdot 11^3)$. Then the relation $\pi_f(x) = \pi_f(y)$ reduces to

$$(X^4 + 1)^3/X^{11} \equiv (Y^4 + 1)^3/Y^{11} \pmod{\alpha}.$$

The irreducible component of this curve where $X \neq Y$ is then isomorphic to the genus 1 curve, $s^4 = r^2 - 1$, by the following map.

$$X = s/(r-1)^3 \qquad Y = s/(r+1)^3$$

REMARK 7.4. *These equations match those of Theorem 2.5 when* $p = 11$ *and* $i(A) = 3$.

7.4.2 $j = 1728$

The supersingular annulus of $X_0(11)$ corresponding to $j = 1728$ is the region which lies over the residue disk, $v(x + 3) > 0$. To see this, we first parameterize the region using the annulus, $0 < v(z) < 2$, and the following map.

$$
\begin{aligned}
x &= z + \frac{(r_1+r_2)}{2} + \frac{(r_1-r_2)^2}{16z} \equiv z + 2318 + 12356\left(\frac{11^2}{z}\right) \pmod{11^4}\\
y &= \left(-z + \tfrac{(r_1-r_2)^2}{16z}\right)\sqrt{(x(z)-s_1)(x(z)-s_2)}\\
&\approx \left(-z + 12356\left(\frac{11^2}{z}\right)\right)\left(\cdots + 5324\left(\frac{11^2}{z}\right)^3 + 3993\left(\frac{11^2}{z}\right)^2 + \right.\\
&\qquad\left. 4370\left(\frac{11^2}{z}\right) + 6001 + 11980z + 5324z^2 + 3993z^3 + \cdots\right)
\end{aligned}
$$

Then we choose an explicit formula for the forgetful map which is convenient for analysis near $j = 1728$, in particular

$$\pi_f^*(j-1728) = \frac{(665x^3 + 666xy + 22680x^2 + 2592y - 120960x + 22680)^2}{5^6 t}.$$

Over the entire annulus, the cubic function in the numerator is well approximated (in the above sense) by $5z^2 - 3\cdot 11^{11}/z^4$, and t is well approximated by $-3z^3$. Therefore by counting valuations it follows that $v(j-1728) > 0$ over the entire annulus, as claimed.

As in the previous examples we now compute the equations for the bridging component of $X_0(11^3)$ and supersingular component of $X_0(11^2)$ corresponding to $j = 1728$. By approximating π_f on **C** (where $v(z) = 21/11$) and **SD** (where $v(z) = 1$), we find the following formula for τ_f in terms of z.

$$\tau_f(z) \equiv 3\left(\frac{11^2}{z}\right)^{11} + 11\left(\frac{11^2}{z}\right)^5 \pmod{11\sqrt{11}}$$

After an appropriate choice of parameters on **C** and **SD**, this leads to the equation,

$$X^6 + X^{-6} = Z^{11},$$

which describes the bridging component. Then on the too-supersingular circle, where $v(z) = 11/6$, we approximate π_f by

$$j - 1728 = \pi_f(z) \equiv \frac{(5z^2 - 3\cdot 11^{11}/z^4)^2}{5^6(-3z^3)} \pmod{11^2}.$$

After making an appropriate change of variables, this leads to the equation which one should expect for $\overline{\mathbf{Y}}$:

$$s^6 = r^2 - 1.$$

8 Stable Model of $X_0(Np^3)$

Intuitively, one might expect the stable model of $X_0(Np^3)$ (when $(N,p) = 1$) to follow fairly directly from the stable model of $X_0(p^3)$. Indeed, $X_0(Np^3)$ is birational to $X_0(p^3) \times_{X(1)} X_0(N)$, and $X_0(N)$ has good reduction. Using semi-stable maps (as in [C2]) to make this line of reasoning precise, we are able to show the following (compare with Theorem 2.5).

Theorem 8.1. *The stable reduction of $X_0(Np^3)$ has six ordinary components: two isomorphic to $X_0(N)$ and four isomorphic to (the normalization of) $Ig(p) \times X_0(N)$. Also, for each supersingular point P of $X_0(N)$, there is a "necklace" of components whose graph is given below in Figure 2. Set $i(P) = 2$ or 3 if P is elliptic and $j(P) = 1728$ or 0 (respectively). Set $i(P) = 1$ otherwise. Then $E_{2,P}$ and $E_{1,P}$ are isomorphic to $y^2 = x^{(p+1)/i(P)} + 1$, while Z_P is crossed by $2(p+1)/i(P)$ components isomorphic to $y^2 = x^p - x$.*

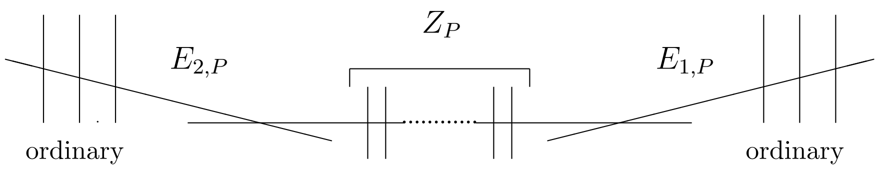

Figure 2: Partial Graph of the Stable Reduction of $X_0(Np^3)$

Corollary 8.2. *The stable reduction of the p-new part of the Jacobian of $X_0(Np^3)$ has $c_N(p^2-1)/6$ copies of the Jacobian of $y^2 = x^p - x$, where $c_N = [\Gamma : \Gamma_0(N)]$.*

8.1 Semi-stable Maps

We begin by giving the definition of semi-stable map, and by proving the lemma which will form the blueprint for our overall construction.

Definition 8.3. *Let $K \subseteq \mathbb{C}_p$ be a complete subfield with ring of integers R. Then $f : X \to Y$ is a semi-stable map over R, if X/R and Y/R are semi-stable (as in [CMc, Definition 2.6]) and f is finite. In this case we say that f extends the restriction map, $f_K : X_K \to Y_K$, on generic fibers.*

Lemma 8.4. *Let $f : X \to Z$ and $g : Y \to Z$ be semi-stable maps over R. Suppose that the following conditions hold.*
(i) $\bar{X}$ and $\bar{Y}$ have (only) smooth components.
(ii) f and g take singular points to singular points (and vice-versa).
(iii) For each pair, (x_i, y_i), of singular points in $\bar{X}$ and $\bar{Y}$ with $f(x_i) = g(y_i)$, $A_{x_i} \times A_{y_i}$ is the disjoint union of annuli (over K), where $A_P = red^{-1}(P)$.

(iv) For each pair, (X_i, Y_i), of components of $\bar{X}$ and $\bar{Y}$ with $f(X_i) = g(Y_i)$, $X_i \times Y_i$ is irreducible, and smooth away from all the points from (iii).
Then $f \times g : X \times Y \to Z$ is a semi-stable map (over R), and in particular $X \times Y$ is semi-stable.

Proof. Choose any pair (X_i, Y_i) of irreducible components of $\bar{X}$ and $\bar{Y}$ with $f(X_i) = g(Y_i)$. Let $W_i = \mathrm{red}^{-1}(X_i) \times \mathrm{red}^{-1}(Y_i)$ and $A_i = \mathrm{red}^{-1}(X_i^{\mathrm{ns}}) \times \mathrm{red}^{-1}(Y_i^{\mathrm{ns}})$. Then (i)-(iv) guarantee that each W_i is a basic wide open (as in [CMc, §2]. Furthermore, the W_i's forms a semi-stable covering of $X_K \times Y_K$, and then it follows from [CMc, Prop 2.7] that $X \times Y$ is semi-stable. Finiteness of $f \times g$ is immediate. □

REMARK 8.5. *We will apply Lemma 8.4 to semi-stable extensions of the forgetful maps from $X_0(p^3)$ and $X_0(N)$ to $X(1)$, but with one caveat. Technically, condition (iv) will fail at all points of the form $(P, Q) \in X_0(p^3) \times X_0(N)$ where P and Q lie over $j = 0$ (or $j = 1728$) and both ramify. This issue can basically be ignored, however, as these singularities are resolved in $X_0(Np^3)$.*

8.2 Semi-stable Extensions of the Forgetful Map

We begin by constructing a semi-stable map which extends $\pi_f : X_0(p^3) \to X(1)$ (as in the main theorem of [C2]). This can be done by starting with the stable models for $X_0(p^3)$ and $X(1)$ (say, $\mathrm{Spec}(\mathbb{Z}_p[j])$) and performing a series of blow-ups. At each step, we choose a component of $X_0(p^3)$ which has finite image in $X(1)$. There is a unique minimal way to blow-up our models for $X(1)$ and $X_0(p^3)$ so that this component no longer has finite image and so that π_f still extends. After finitely many steps, the process terminates and we have our semi-stable map. A partial picture of this map (showing one supersingular region only) is given below in Figure 3, and the components in the final models for $X_0(p^3)$ and $X(1)$ can be described in words as follows.

First of all, the ordinary regions of $X_0(p^3)$ and $X(1)$ are unchanged. In other words, the final model for $X_0(p^3)$ still has six ordinary components corresponding to the six ordinary affinoids, $\mathbf{X}^{\pm}_{a\,b}$ (defined in §2), and these all map onto the same component of $X(1)$. For each supersingular elliptic curve, A, the special fiber of $X(1)$ also contains a "necklace" of trivial components. More specifically, each necklace contains a chain of four components which correspond to the circles (and disk) where $h(E) = \frac{1}{p(p+1)}$, $h(E) = \frac{1}{2p}$, $h(E) = \frac{1}{p+1}$, and $h(E) \geq \frac{p}{p+1}$ (as in §2.1). Intersecting the second of these we also have $2(p+1)/i(A)$ components which correspond to residue classes within that circle. The components in our final model for $X_0(p^3)$ can be given similar descriptions, i.e. we can describe the components within a fixed supersingular region by describing points of the corresponding affinoids in moduli-theoretic terms. Remember that these affinoids should map onto the ones which were just described for $X(1)$ via the forgetful map.

$$\begin{aligned}
\mathbf{E}_{2,A} &= \{\ (E,C) \mid h(E) = \tfrac{1}{p(p+1)},\ pC = K_2(E)\ \} \\
\mathbf{Z}_A &= \{\ (E,C) \mid h(E) = \tfrac{1}{2p},\ pC = K_2(E)\ \} \\
&\qquad \text{(with its } 2(p+1)/i(A) \text{ nontrivial residue classes)} \\
\mathbf{E}_{1,A} &= \{\ (E,C) \mid h(E) = \tfrac{1}{p+1},\ p^2C = K_1(E)\ \} \\
W^{\pm}_{1,2} &\supseteq \{\ (E,C) \mid h(E) = \tfrac{1}{2p},\ |C \cap K_2(E)| = p\ \} \\
&\qquad \text{(also blow-up } 2(p+1)/i(A) \text{ residue classes)} \\
&\supseteq \{\ (E,C) \mid h(E) = \tfrac{1}{p(p+1)},\ |C \cap K_2(E)| = p\ \} \\
W_{0,3} &\supseteq \{\ (E,C) \mid h(E) = \tfrac{p}{p+1}\ \} \text{ (so } E \text{ is too-ss)} \\
&\supseteq \{\ (E,C) \mid h(E) = \tfrac{1}{p+1},\ |C \cap K_1(E)| = 1\ \} \\
&\supseteq \{\ (E,C) \mid h(E) = \tfrac{1}{2p},\ |C \cap K_2(E)| = 1\ \} \\
&\qquad \text{(also blow-up } 2(p+1)/i(A) \text{ residue classes)} \\
&\supseteq \{\ (E,C) \mid h(E) = \tfrac{1}{p(p+1)},\ |C \cap K_2(E)| = 1\ \}
\end{aligned}$$

REMARK 8.6. *Recall that $W^{\pm}_{a\,b}$ is a wide open neighborhood of the ordinary affinoid, $\mathbf{X}^{\pm}_{a\,b}$, which extends into the supersingular locus (see [CMc, §3.2]).*

In order to apply Lemma 8.4, we also need to construct a semi-stable map extending $\pi_f : X_0(N) \to X(1)$ (involving the same model for $X(1)$). Basically, we start with the good reduction model for $\pi_f : X_0(N) \to X(1)$. Then every time we blow-up $X(1)$ (as above), this forces a blow-up of $X_0(N)$ so that π_f still extends. Again the ordinary locus of $X_0(N)$ is unchanged. To understand the supersingular regions, consider $\pi_f : X_0(N) \to X(1)$ first as a map of smooth curves over $\overline{\mathbb{F}}_p$, and let P be a point of $X_0(N)$ such that $\pi_f(P)$ is supersingular. If P does not ramify, π_f must restrict to an isomorphism on the corresponding residue class of $X_0(N)$. The only other option is that either $e(P) = 3$ and $j(\pi_f(P)) = 0$, or $e(P) = 2$ and $j(\pi_f(P)) = 1728$. There are two key points to make in either case. First of all, the corresponding residue class of $X_0(N)$ (over $\mathbb{C}_p$) is an extension of a disk which is ramified (totally) at exactly one point (degree 2 if $j = 1728$, degree 3 if $j = 0$). Hence, the extension can be generated analytically by adjoining either $\sqrt{j-1728}$ or $\sqrt[3]{j}$. Secondly, when $j = 0$ or 1728 is supersingular, it is necessarily too-supersingular. Hence it reduces to a smooth point on the innermost component of its residue class in our final model for $X(1)$. Therefore, like its image in $X(1)$, the residue class of $X_0(N)$ corresponding to such a P contains a chain of 4 components on which π_f is given locally by $t \to t^2$ or $t \to t^3$. The "bridging component" then intersects $2(p+1)$ copies of $\mathbf{P}^1$, which map $2:1$ or $3:1$ onto analogous components of $X(1)$.

To summarize the semi-stable extensions of both forgetful maps to $X(1)$, a picture of the special fibers is now given below in Figure 3. Once again, the graph shows the entire ordinary locus, but only one supersingular region for each curve.

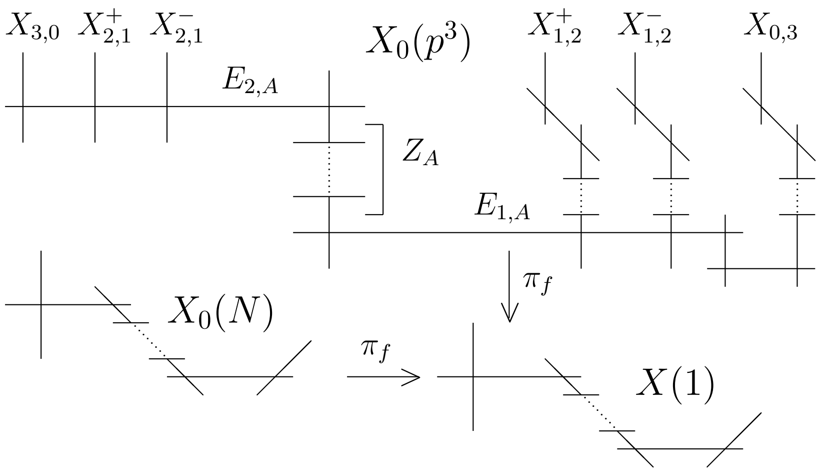

Figure 3: Partial Graph of Semi-Stable Maps from $X_0(p^3)$ and $X_0(N)$ to $X(1)$

8.3 Crossing the Semi-Stable Maps

At this point the proof comes down to verifying the hypotheses of Lemma 8.4 and computing the products of irreducible components with common image. The first two hypotheses follow immediately from the construction. To verify condition (iii), we first observe that $\pi_f : X_0(N) \to X(1)$ can only ramify over $j = 0$, 1728, or ∞, all of which have smooth reduction on our model for $X(1)$. Furthermore, each supersingular residue class of $X_0(N)$ maps with total degree at most 3. Therefore, for any pair of double points, (x, y) (as in the lemma), the corresponding product of annuli, $A_x \times A_y$, is an unramified extension of some annulus of $X_0(p^3)$ with degree less than p. Hence it can only be the disjoint union of annuli by [CMc, Lemma 3.3].

Now we compute the products of the irreducible components, starting with the ordinary locus. When we cross $X_0(N)$ with the reduction of $X_{3,0}$, we are essentially crossing with $\mathbf{P}^1$ trivially (as π_f has degree 1 on $X_{3,0}$). So we simply get a copy of $X_0(N)$. When we cross $X_0(N)$ with the reduction of $X^{\pm}_{2,1}$, we get the curve $Ig(p) \times X_0(N)$ which is at least irreducible from [E1, Thm 2.1.2]. Recall that $Ig(p)/X(1)$ is a degree $(p-1)/2$ extension which is totally ramified over supersingular points, ramified with index 3 or 2 when $j = 0$ or 1728 is ordinary, and unramified elsewhere. Hence the only singular points of $Ig(p) \times X_0(N)$ can be ignored as a result of Remark 8.5. The remaining ordinary components can be dealt with by applying an appropriate Atkin-Lehner involution.

Next we consider a fixed supersingular region corresponding to a point P of $X_0(N)$ (as above). If $j(P) \neq 0, 1728$, or if P is an elliptic point, there's nothing to do, since $\pi_f : X_0(N) \to X(1)$ must be an isomorphism on the residue class corresponding to P. But now suppose that $j(P) = 0$ or 1728, and P is not elliptic. By [E2, 2.3.1] we can choose parameters on $E_{2,A}$ so that it has the equation,

$$y^2 = x^{\frac{p+1}{i(A)}} + 1.$$

Furthermore, the two infinite points are where $E_{2,A}$ meets $X_{3,0}$ and Z_A, and $(0, \pm 1)$ are the points where $E_{2,A}$ meets $X_{2,1}^{\pm}$. The forgetful map induces a degree p map on $E_{2,A}$ which has ramification indices of 1, $(p-1)/2$, and p at the intersections with $X_{3,0}$, $X_{2,1}^{\pm}$, and Z_A. Therefore, if t is a parameter on the image of $E_{2,A}$ in $X(1)$, with $t = 0$ and ∞ at the double points, it follows that

$$\pi_f^* t = \frac{c x^{\frac{p-1}{2}}}{(y - x^{\frac{p+1}{2i(A)}})^{i(A)}}.$$

Now, we have already seen that the extension from $X(1)$ up to $X_0(N)$ is equivalent to adjoining an $i(A)$-th root of t in this case. Hence one can show that the extension of $E_{2,A}$ can be obtained by adjoining an $i(A)$-th root of x. Subsequently, by a change of coordinates, the component lying over $E_{2,A}$ in $X_0(Np^3)$ will have the equation, $y^2 = x^{p+1} + 1$. The argument for the remaining components is very similar. For example, on the bridging component, Z_A, we may choose a parameter x such that it meets $E_{1,A}$ and $E_{2,A}$ at 0 and ∞, and such that π_f is given by $t = x^p$. Adjoining an $i(A)$-th root of t then generates the same extension as adjoining an $i(A)$-th root of x. Thus we obtain a bridging component, Z_P, as in the statement of the theorem, which is crossed by $2(p+1)$ components that lie $i(A) : 1$ over their counterparts on Z_A. At this point the remaining components can be computed in a similar manner, or dealt with by applying an appropriate Atkin-Lehner involution. Thus all the supersingular components of $X_0(Np^3)$ are as claimed, and the theorem is proved. One final remark is that when P ramifies over $j = 0$ or $j = 1728$ and is supersingular, we do technically get singularities in $X_0(N) \times X_0(p^3)$ which lie over the (smooth) reduction of $j = 0$ or 1728. These singularities can be ignored, however, by Remark 8.5.

8.4 Examples

It is now fairly straightforward to generate complete graphs with genera for the stable reduction of $X_0(Np^3)$. First we determine the supersingular values mod p, and the ramification of $\pi_f : X_0(N) \to X(1)$ over $j = 0$ and $j = 1728$. The latter can be derived from [S, Prop 1.43], which gives both the degree and number of elliptic points of each type. The components in the supersingular region then follow directly from Theorem 8.1. The only things which remain to be computed are the genera of $X_0(N)$ and $Ig(p) \times X_0(N)$.

The genus of $X_0(N)$ can be computed with [S, Prop 1.40]. Then Riemann-Hurwitz can be applied to the forgetful map from $X_0(N) \times Ig(p)$ to $X_0(N)$. By way of illustration, we now describe the stable reductions of $X_0(Np^3)$ in two examples: $X_0(3 \cdot 11^3)$ and $X_0(7 \cdot 13^3)$.

Example 1: $X_0(3 \cdot 11^3)$

Only $j = 0$ and $j = 1728$ are supersingular mod 11. In the degree 4 extension from $X_0(3) \to X(1)$, $j = 0$ splits into two points with $e = 1$ and $e = 3$, while $j = 1728$ splits into two points with $e = 2$. So we have a total of four supersingular necklaces. For the one corresponding to the unique elliptic point, there are 8 genus 5 components along the bridging component, and two outer components which meet the ordinary locus and have genus 1. The other three supersingular regions have 24 genus 5 components along the bridging component, and two outer components which also have genus 5. Now we compute the genera of the ordinary components. $X_0(3)$ has genus 0, and by Riemann-Hurwitz the genus of $Ig(11) \times X_0(3)$ is then 4. Indeed, it lies over $X_0(3)$ with degree 5, and is totally ramified over 4 points and unramified elsewhere. This implies a total genus of:

$$2(0) + 4(4) + 1[2(1) + 8(5)] + 3[2(5) + 24(5)] + (4 - 1)(6 - 1) = 463,$$

which can easily be verified with [S, Prop 1.40].

Example 2: $X_0(7 \cdot 13^3)$

The unique supersingular j-invariant for $p = 13$ is $j = 5$. Since this is neither 0 nor 1728, we simply get 8 supersingular regions which are all isomorphic to the supersingular region of $X_0(13^3)$. In particular, each necklace has 28 genus 6 components along the bridging component and then 2 more genus 6 components which meet the ordinary locus. Now we compute the genera of $X_0(7)$ and $X_0(7) \times Ig(13)$. The first has genus 0, and for the second we again apply Riemann-Hurwitz. The degree is 6, and we have total ramification over the 8 supersingular points. There are also two elliptic points of $X_0(7)$ lying over $j = 0$, each of which must split into two points with $e = 3$ in $X_0(7) \times Ig(13)$. So the genus of $Ig(13) \times X_0(7)$ is 19. That means if we add up the total genus of $X_0(7 \cdot 13^3)$ we get

$$2(0) + 4(19) + 8[2(6) + 28(6)] + (8 - 1)(6 - 1) = 1551,$$

which again can be easily verified with [S, Prop 1.40].

9 Index of Important Notation

$K(E)$, canonical subgroup of E	§2.1
$H_n(E)$, canonical subgroup of E of order p^n	
$\mathbf{X}^{\pm}_{a\,b}$, ordinary affinoids	
$Ig(p^n)$, level p^n Igusa curve	
$h(E)$, valuation of Hasse invariant of E	
$W_A(p^n)$, wide open subspace of $X_0(p^n)$ where $\bar{E} \cong A$	
$i(A) := \lvert \mathrm{Aut}(A) \rvert / 2$	
$\mathbf{TS}_A$, $\mathbf{SD}_A$, too-supersingular and self-dual circles inside $W_A(p)$	
w_n, Atkin-Lehner involution on $X_0(p^n)$	
(F, A, α), Woods Hole representation of an elliptic curve	
π_f, forgetful map	
$W(\mathbb{F}_{p^n})$, Witt vectors of $\mathbb{F}_{p^n}$	
B, quaternionic order over $\mathbb{Z}_p$ isomorphic to $\mathrm{End}(\hat{A})$	
B', special subset of B^*	
Φ, Gross-Hopkins period map	
w_ρ, generalized Atkin-Lehner involution of $\mathbf{SD}_A$ for $\rho \in B'$	
$\mathbf{Y}_A$, nontrivial affinoid in $W_A(p^2)$	§2.2
π_ν, moduli-theoretic map taking (E, C) to $(E/C[p], C/C[p])$	
$\mathbf{E}_{1,A}$, $\mathbf{E}_{2,A}$, two pullbacks of $\mathbf{Y}_A$ to $X_0(p^3)$	
$\pi_{1\,1} := \pi_f \circ \pi_\nu$	
$\mathbf{Z}_A$, affinoid in $W_A(p^3)$ corresponding to "bridging component"	
$\mathbf{C}_A$, τ_f, special circle of $W_A(p)$ and map to $\mathbf{SD}_A$	
$\tilde{w}_\rho$, generalized Atkin-Lehner involution of $\mathbf{Z}_A$ for $\rho \in B'$	
$\mathcal{R}$, maximal orders in the quadratic extensions of $\mathbb{Q}_p$	§3
α_*, embedding of $\mathrm{End}(F)$ into B when (F, α) has fake CM	§3.2
$\mathcal{X}_0(p^n)$, stable model of $X_0(p^n)$	§4.1
$\mathcal{P}$, pairing on $K_a(E)$ onto μ_{p^b} which distinguishes $\mathbf{X}^{\pm}_{a\,b}$	
M_n, field found by Krir over which $J_0(p^n)$ has stable reduction	§5
F_n, field over which our stable model for $X_0(p^n)$ is defined ($n \leq 3$)	
$W^{\pm}_{a\,b}$, wide open neighborhood of $\mathbf{X}^{\pm}_{a\,b}$	§5.2
$V_i(A)$, $U(A)$, wide open neighborhoods of $\mathbf{E}_{i,A}$ and $\mathbf{Z}(A)$	
$\mathcal{S}(A)$, singular residue classes of $\mathbf{Z}_A$	
$\hat{U}(A)$, basic wide open refinement of $U(A)$	
$I = I_{\mathbb{Q}_p}$, $w = w_X$, inertia group and inertia action on $X = \mathcal{X}_0(p^n)$	§6
m_n, minimal extension of $\mathbb{Q}_p^{nr}$ over which $X_0(p^n)$ has stable reduction	
C_x, component of $\mathcal{X}_0(p^3)$ corresponding to a w_ρ fixed point	§6.3
τ_x, $\underset{\sim}{\mathcal{F}_x}$, hyper-elliptic involution on C_x, and its p fixed points	
$\mathcal{D}_x$, $\widetilde{\mathcal{D}}_x$, residue classes of $\mathbf{SD}_A$ and $\mathbf{Z}_A$	
$\tilde{S}_{s,\zeta}$, order p automorphism of $\widetilde{\mathcal{D}}_x$	

References

[B] K. Buzzard, *Analytic continuation of overconvergent eigenforms*, J. Amer. Math. Soc. 16 (2003), no. 1, 29–55.

[BLR] S. Bosch, W. Lütkebohmert, M. Raynaud, *Néron models*, Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)], 21. Springer-Verlag, Berlin, 1990.

[C1] R. Coleman, *On the Components of* $X_0(p^n)$, J. Number Theory 110 (2005), no. 1, 3–21.

[C2] R. Coleman, *Stable Maps of Curves*, Kazuya Kato's fiftieth birthday, Doc. Math. (extra volume), 217–225.

[CMc] R. Coleman, K. McMurdy, *Stable Reduction of* $X_0(p^3)$, preprint available at http://math.berkeley.edu/∼coleman/X_0(pˆ3)/Stable_Xp3.pdf

[dS1] E. de Shalit, *Kronecker's polynomial, supersingular elliptic curves, and p-adic periods of modular curves*, p-adic monodromy and the Birch and Swinnerton-Dyer conjecture, (Boston, 1991), 135–148, Contemp. Math. 165 (1994)

[dS2] E. de Shalit, *Relative Lubin-Tate Groups*, Proceedings of the AMS 95 (1985), no. 1,1–4.

[DR] P. Deligne, M. Rapoport, *Schemas de modules de courbes elliptiques*, Lecture Notes in Math. 349 (1973), 143–316.

[DM] ———, D. Mumford, *The irreducibility of the space of curves of given genus*, Inst. Hautes Études Sci. Publ. Math. 36 (1969), 75–109.

[E1] B. Edixhoven, *Minimal resolution and stable reduction of* $X_0(N)$, Ann. Inst. Fourier (Grenoble) 40 (1990), no. 1, 31–67.

[E2] ———, *Stable models of modular curves and applicatons*, Thèse de doctorat à l'université d'Utrecht, juin 1989. Available at http://www.math.leidenuniv.nl/∼edix/public_html_rennes/publications/prschr.html

[G] B. Gross, *On canonical and quasi-canonical liftings*, Invent. Math. 84 (1986), no. 2, 321–326.

[GH] ———, M. Hopkins, *Equivariant vector bundles on the Lubin-Tate moduli space*, Topology and representation theory (Evanston, IL, 1992), 23–88, Contemp. Math., 158 (1994).

[Ig] J-i Igusa, *On the algebraic theory of elliptic modular functions*, J. Math. Soc. Japan 20 (1968), 96–106.

[Iw] K. Iwasawa, *Local class field theory*, Oxford Science Publications. Oxford Mathematical Monographs. The Clarendon Press, Oxford University Press, New York, 1986. viii+155 pp

[K] M. Krir, *Degré d'une extension de* Q_p^{nr} *sur laquelle* $J_0(N)$ *est semi-stable*, Ann. Inst. Fourier (Grenoble) 46 (1996), no. 2, 279–291.

[M1] K. McMurdy, *Explicit parameterizations of ordinary and supersingular regions of* $X_0(p^n)$, Modular curves and abelian varieties (Barcelona, 2002), 165–179, Prog. Math. 224 (2004).

[M2] ___________, *Stable Reduction of* $X_0(81)$, preprint available.

[R] K. Ribet, *On modular representations of* $\mathrm{Gal}(\overline{Q}/Q)$ *arising from modular forms*, Invent. Math. 100 (1990), no. 2, 431–476.

[S] G. Shimura, *Introduction to the arithmetic theory of automorphic functions*, Princeton Univ. Press, Princteon, N.J., 1971.

[T] J. Tate, *Endomorphisms of abelian varieties over finite fields*, Invent. Math. 2 (1966), 134–144.

[WH] J. Lubin, J.-P. Serre, J. Tate, *Elliptic curves and formal groups*, Lecture notes from the Summer Institute on Algebraic Geometry (Woods Hole, MA, 1964), available at
http://www.ma.utexas.edu/users/voloch/lst.html

Ken McMurdy
Department of Mathematics
Rose-Hulman Institute of Technology
USA
mcmurdy@rose-hulman.edu

Robert Coleman
Department of Mathematics
U. C. Berkeley
USA
coleman@math.berkeley.edu