Minimal resolution and stable reduction of $X_0(N)$.

Bas Edixhoven

November 18, 1998

Bas Edixhoven
Department of Mathematics
University of California at Berkeley
Berkeley, CA 94720
U.S.A.

Contents

Introduction. **3**

Notations. **4**

1. The minimal resolution of $X_0(p^nN)$ at $p \geq 5$. **5**

1.1. Outline of the results and computations in this chapter. 5
1.2. $X_0(p^nN)$ is regular at infinity. 7
1.3. Computations. 9
1.4. Graph and local equations of $\widetilde{X_0}(p^nN) \otimes_{\mathbf{Z}} \overline{\mathbf{F}}_p$. 16
1.5. $\widetilde{X_0}(p^2)$, for example. 18
1.6. Global structure of $\widetilde{X_0}(p^nN) \otimes_{\mathbf{Z}} \mathbf{F}_p$. 20

2. The stable reduction of $X_0(p^2N)$ at $p \geq 5$. **24**

2.1. The result. 24
2.2. Formal computations. 25
2.3. Determination of the vertical components. 29
2.4. The coarse case. 31
2.5. Examples. 31

References. **34**

Introduction.

Let $X_0(N)$ be the compactified coarse moduli scheme over $\mathbf{Z}$ of elliptic curves together with a cyclic subgroup of order N. In chapter 1 the minimal resolution of $X_0(N)$ over $\mathbf{Z}[\frac{1}{6}]$ is determined. In chapter 2 we describe the stable reduction of $X_0(p^2N)$ at p for $p \geq 5$, where p is a prime that does not divide N. It would be very interesting to know the stable reduction of $X_0(p^nN)$ at p, but wild ramification keeps me from finding it.

In a forthcoming chapter the actions of the Hecke algebra and the inertia group on the stable reduction will be studied. I hope that this (faithful) representation of the Hecke algebra will lead to an efficient algorithm for computing all Weil curves with a given conductor. Such an algorithm has already been found in the case of a prime (and maybe also square free) conductor by J.F. Mestre [12]. Until I heard from his results I was developing the same theory. Also the relation to A. Pizers Brandt matrix representation of the Hecke algebra [13] [14] should become clear. Finally I want to thank dr. B. van Geemen for the idea of reducing Hecke operators mod p, and for his proofreading.

After this text was written in November 1986, the actions of the Hecke algebra and the inertia group have been studied in the authors thesis (Stable models of modular curves and applications, Utrecht, June 1989, to be published). This resulted in an analog of the so-called "graph method" of Mestre and Oesterlé [12], and also gave new information concerning strong modular parametrizations of elliptic curves. Another application was given in an article (to appear in Astérisque) to the computation of the action of the Hecke algebra on the groups of connected components of reductions mod p of Néron models over $\mathbf{Z}$ of jacobians of modular curves. Again, I would like to thank my thesis adviser F. Oort and especially B. van Geemen for their advice and support.

Notations.

In this paper, we will freely use notations introduced in the book of Katz and Mazur [9]. For the convenience of the reader, we will list the places where a definition of some of these notations can be found. A few other remarks should be made. Often, "irreducible component" will mean the reduced subscheme corresponding to it. We will also use the expression "local equation" for what should really be called a formal local equation.

(Ell) modular stack of elliptic curves [9] 4.1.

(Ell/R) modular stack of elliptic curves over base schemes over Spec(R) [9] 4.13.

$\mathcal{P}$ moduli problem: a contravariant functor from (Ell) or (Ell/R) to (Sets), see [9] 4.2.

$\mathcal{M}(\mathcal{P})$ (fine) moduli scheme associated to a representable moduli problem, [9] 4.3.

$\mathrm{M}(\mathcal{P})$ coarse moduli scheme associated to a moduli problem $\mathcal{P}$ which is relatively representable and affine, [9] 8.1. If $\mathcal{P}$ is representable, then it is just $\mathcal{M}(\mathcal{P})$.

$\overline{\mathrm{M}}(\mathcal{P})$ compactified coarse moduli scheme, [9] 8.6.

$\overline{\mathcal{M}}(\mathcal{P})$ compactified moduli scheme, [9] 8.6.

$[\Gamma_0(N)]$ the moduli problem that assigns to E/S the set of $\Gamma_0(N)$-structures on E/S, see [9] 3.4 and 5.1.

$[(a,b)\text{-cyclic}]$ the moduli problem on (Ell/$\mathbf{F}_p$), where p is a prime, assigning to E/S the set of (a,b)-cyclic subgroups of E/S, see [9] 13.4.3 and 13.4.5.

$[\mathrm{Ig}(p^n)]$ the moduli problem on (Ell/$\mathbf{F}_p$) that assigns to $E/S/\mathbf{F}_p$ the set of Igusa-structures of level p^n on E/S, see [9] 12.3.

$[\mathrm{ExIg}(p^n, i)]$ the moduli problem on (Ell/$\mathbf{F}_p$) that assigns to $E/S/\mathbf{F}_p$ the set of i-exotic Igusa-structures of level p^n on E/S, see [9] 12.10.5.1.

1. The minimal resolution of $X_0(p^nN)$ at $p \geq 5$.

1.1. Outline of the results and computations in this chapter.

(1.1.1) Let $p > 3$ be a prime, $N > 0$ an integer that is not divisible by p, and $n \geq 1$. Let $[\Gamma_0(p^nN)]$ be the category fibered in groupoids over the category (Sch) of schemes which classifies cyclic p^nN-isogenies between elliptic curves (n.b. *not* between generalized elliptic curves). Then $[\Gamma_0(p^nN)]$ is an algebraic stack because of [3] Ch. III, Thm. 2.5, and [9] Thm. 6.6.1.

Remark 1.1.1.1. The $\mathcal{M}_{\Gamma_0(N)}$ which is described in [4] Ch. III, § 1, is *not* an algebraic stack. For a p-gon with its p-torsion subgroup is an object of $\mathcal{M}_{\Gamma_0(p^2)}$. This object has infinitesimal automorphisms. Note that in the $\mathcal{M}_*$ of [3] Ch. III, Thm. 2.5, n-gons may only occur at points where the characteristic does not divide n.

Let $X_0(p^nN)$ be the compactified coarse moduli scheme $\overline{\mathrm{M}}([\Gamma_0(p^nN)])$ as constructed in [9] Ch. 8, and let $\widetilde{X_0}(p^nN)$ be the minimal resolution of $X_0(p^nN)$. We will give a complete description of $\widetilde{X_0}(p^nN) \otimes_{\mathbf{Z}} \mathbf{F}_p$ in terms of $X_0(N) \otimes_{\mathbf{Z}} \mathbf{F}_p$.

Description 1.1.1.2. *The graph and local equations of $\widetilde{X_0}(p^nN) \otimes_{\mathbf{Z}} \mathbf{F}_p$ can be found in (1.4). The non-reduced irreducible components of $\widetilde{X_0}(p^nN) \otimes_{\mathbf{Z}} \mathbf{F}_p$ are isomorphic to the corresponding infinitesimal neighborhoods of the zero sections of their normal bundles. The conormal bundle of the reduced (a,b)-component (with $a, b > 0$) is:*

$$(\Omega^1_{X_0(N)\otimes_{\mathbf{Z}}\mathbf{F}_p}(\mathrm{cusps}))^{\otimes p^{|a-b|}}(D),$$

where D can be found in Table 1.6.3.2.

(1.1.2) The computation runs as follows. First we show that $X_0(p^nN)$ is regular at the cusps, so there is no problem at infinity. Then we introduce an auxiliary level structure $\mathcal{P}$ to view $\mathrm{M}([\Gamma_0(p^nN)])$ as a quotient of a regular scheme $\mathcal{M}(\mathcal{P}, [\Gamma_0(p^nN)])$ by the action of a finite group.

The only non-trivial stabilizer groups we encounter are cyclic of order 2 or 3. Since $p \geq 5$ the quotients we consider commute with all base changes we will perform, and the quotient of a closed subscheme will be its image in the quotient.

The scheme $\mathcal{M}(\mathcal{P}, [\Gamma_0(p^nN)]) \otimes_{\mathbf{Z}} \mathbf{F}_p$ is completely described in terms of $\mathcal{M}(\mathcal{P}, [\Gamma_0(N)]) \otimes_{\mathbf{Z}} \mathbf{F}_p$ in [9] Thm. 13.4.7. This description yields enough information to get the result.

(1.1.3) We use the notation of [9] Thm. 13.4.7: $\mathcal{M}(\mathcal{P}, [\Gamma_0(p^nN)]) \otimes_{\mathbf{Z}} \mathbf{F}_p$ is the disjoint union, with crossings at the supersingular points, of the $n+1$ schemes $\mathcal{M}(\mathcal{P}, [\Gamma_0(N)], [(a,b)\text{-cyclic}])$ for $a + b = n$. The multiplicity of the (a,b)-component is $\phi(p^{\min(a,b)})$, so only the $(n,0)$ and the $(0,n)$-components are reduced. By taking the quotient we see that $X_0(p^nN) \otimes_{\mathbf{Z}} \mathbf{F}_p$ consists of $n+1$ irreducible components all isomorphic to $X_0(N) \otimes_{\mathbf{Z}} \mathbf{F}_p$ which intersect at every supersingular point and nowhere else. The multiplicity of the (a,b)-component is $\phi(p^{\min(a,b)})$. It follows that $X_0(p^nN) \to \mathrm{Spec}(\mathbf{Z})$ is smooth on the ordinary part of the $(n,0)$ and $(0,n)$-components; since $\mathrm{Spec}(\mathbf{Z})$ is regular, $X_0(p^nN)$ is regular at those points.

Consider the points in the finite part of $X_0(p^nN) \otimes_{\mathbf{Z}} \mathbf{F}_p$ which:

1. have extra automorphisms, and
2. are supersingular or have $a \neq 0 \neq b$.

It is easily checked that these points are isolated in $X_0(p^nN)$ for the property of having extra automorphisms. By purity of branch locus, they must be singular in the surface $X_0(p^nN)$. We will not use this, because it follows directly from the calculations we will do.

(1.1.4) The first observation we make is that the points on $\mathcal{M}(\mathcal{P}, [\Gamma_0(p^nN)])$ which are candidates to become singular in the quotient, are all singular in $\mathcal{M}(\mathcal{P}, [\Gamma_0(p^nN)]) \otimes_{\mathbf{Z}} \mathbf{F}_p$. Hence at such a point, the cotangent space of the surface equals the cotangent space of the p-fibre. Since we know all about this fibre, we know the actions of the stabilizer groups on the cotangent spaces. We can then apply [15] Thm. 1' of Serre:

Theorem 1.1.4.1. *Let A be a noetherian regular local ring with maximal ideal m and residue field k. Let G be a finite subgroup of* $\mathrm{Aut}(A)$*, and let A^G denote the ring of G-invariants of A. Suppose that:*

1. *the characteristic of k does not divide the order of G,*
2. *G acts trivially on k,*
3. *A is a finitely generated A^G-module.*

Then A^G is regular if and only if the image of G in $\mathrm{Aut}_k(m/m^2)$ *is generated by pseudo-reflections.*

Remark 1.1.4.2. An element σ of $\mathrm{Aut}_k(V)$, where V is a vector space over k, is called a pseudo-reflection if $\mathrm{rank}(1-\sigma) \leq 1$.

(1.1.5) We consider a point x in $\mathcal{M}(\mathcal{P}, [\Gamma_0(p^nN)])$ satisfying the conditions 1 and 2 of 1.1.3. If we find that the image of x in the quotient $X_0(p^nN)$ is a singular point, then we replace $\mathcal{M}(\mathcal{P}, [\Gamma_0(p^nN)])$ by its blow up in x. The second observation we make is that in doing so we do not loose any essential information. The reason for this is the following. The completion of the strict Henselization of $\mathcal{M}(\mathcal{P}, [\Gamma_0(p^nN)])$ at x is of the form $A := W[[x,y]]/(f)$, where x and y are local moduli of source and target (cf. [9] Thm. 13.4.7 with $\mathcal{P} := (\mathcal{P}, [\Gamma_0(N)])$). We can write $f = f_0 + pf_1$ with:

$$f_0 = (x^{p^n} - y)(x - y^{p^n}) \prod_{\substack{a+b=n \\ a,b>0}} (x^{p^{a-1}} - y^{p^{b-1}})^{p-1}, \quad \text{if x is supersingular,}$$

$$f_0 = (x^{p^{a-1}} - y^{p^{b-1}})^{p-1} \quad \text{with } a+b=n \text{ and } a,b>0, \text{ if x is ordinary.}$$

Because A is regular, f_1 has to be a unit in $W[[x,y]]$, and (x,y) is a system of parameters at x. The blow up of A at x can be covered by two open affines. One of these is $\mathrm{Spec}(\tilde{A})$, where $\tilde{A} = W[[x, vx]][v]/(\tilde{f})$, with $\tilde{f}(x,v) = f(x, xv)$, and $\tilde{f} = \tilde{f}_0 + p\tilde{f}_1$. On this part of the blow up, the exceptional divisor (this is the preimage of x) is described by the equation: $x = 0$. It follows that $W[v][[x]]/(\tilde{f})$ is the completion of $\tilde{A}$ along the exceptional divisor.

We see from this that after blowing up we still know the p-fibre + action, and we can repeat the procedure until the quotient will be regular. Then we know the p-fibre of the quotient, and after contracting -1-curves we have the minimal resolution.

(1.1.6) There is still more to know, namely the global structure of the non-reduced irreducible components (the description in [9] Thm. 13.4.7 only gives the fibre of the non-compactified moduli scheme). Following the construction of the minimal resolution we will determine the conormal bundles of the reduced (a,b)-components. We express these bundles in terms of $X_0(N) \otimes_{\mathbf{Z}} \mathbf{F}_p$. The statements of description 1.1.1.2 then follow from the fact that the degrees of these line bundles are sufficiently large.

1.2. $X_0(p^n N)$ is regular at infinity.

(1.2.1) In this section we do not need the restrictions $p > 3$ and $n \geq 1$. Let $\mathcal{P}$ be the moduli problem $([\Gamma(12)], [\Gamma_0(M)])$ on (Ell), where M is an arbitrary non-negative integer, and let $G = GL_2(\mathbf{Z}/12\mathbf{Z})$. Then by [9] Proposition 8.11.7 we have an isomorphism:

$$\mathcal{M}(\mathcal{P})_{\mathbf{Z}((q))} \tilde{\to} \mathcal{P}_{\mathrm{Tate}(q)/\mathbf{Z}((q))}/\{\pm 1\}.$$

Taking the quotient by G and applying [9] Proposition 7.3.1, Theorem 7.4.2 and Corollary 8.11.9 gives:

$$\mathrm{M}([\Gamma_0(M)])_{\mathbf{Z}((q))} \tilde{\to} [\Gamma_0(M)]_{\mathrm{Tate}(q)/\mathbf{Z}((q))}.$$

This implies that the finite $\mathbf{Z}[[q]]$-scheme $\widehat{\mathrm{Cusps}}([\Gamma_0(M)])$ is the normalization of $\mathbf{Z}[[q]]$ in the finite normal $\mathbf{Z}((q))$-scheme $[\Gamma_0(M)]_{\mathrm{Tate}(q)/\mathbf{Z}((q))}$.

Applying factorization into prime powers ([9] Lemma 3.5.1) we get an isomorphism:

$$[\Gamma_0(p^n N)]_{\mathrm{Tate}(q)/\mathbf{Z}((q))} \tilde{\to} [\Gamma_0(p^n)]_{\mathrm{Tate}(q)/\mathbf{Z}((q))} \times_{\mathbf{Z}((q))} [\Gamma_0(N)]_{\mathrm{Tate}(q)/\mathbf{Z}((q))}.$$

We will first compute the two factors of the right hand side.

(1.2.2) By 1.2.1 and [9] Thm. 13.6.6, $\widehat{\mathrm{Cusps}}([\Gamma_0(p^n)])$ is the normalization of $\mathrm{Spec}(\mathbf{Z}[[q]])$ in:

$$\mathrm{Spec}(\mathbf{Z}((q))) \coprod \mathrm{Spec}(\mathbf{Z}((q))[x]/(x^{p^n} - q)) \coprod \\ \coprod_{\substack{a+b=n \\ a,b>0}} \mathrm{Spec}(\mathbf{Z}((q))[z]/(\Phi_p(z^{p^{b-1}}/q^{p^{a-1}}))).$$

Of course the normalization of $\mathbf{Z}[[q]]$ in $\mathbf{Z}((q))$ is $\mathbf{Z}[[q]]$ itself. The normalization of $\mathbf{Z}[[q]]$ in $\mathbf{Z}((q))[x]/(x^{p^n} - q)$ is $\mathbf{Z}[[q]][x]/(x^{p^n} - q)$, because it is finite over $\mathbf{Z}[[q]]$ and regular. If $a \geq b$

then $z^{p^{b-1}}/q^{p^{a-1}} = x^{p^{b-1}}$, with $x = z/q^{p^{a-b}}$, and we must find the normalization of $\mathbf{Z}[[q]]$ in $\mathrm{Spec}(\mathbf{Z}((q))[x]/(\Phi_{p^b}(x)))$, which is $\mathrm{Spec}(\mathbf{Z}[[q]][x]/(\Phi_{p^b}(x)))$, because it is regular and finite over $\mathbf{Z}[[q]]$. Now suppose $b > a \geq 1$, then $z^{p^{b-1}}/q^{p^{a-1}} = x^{p^{a-1}}$, with $x = z^{p^{b-a}}/q$, i.e: $z^{p^{b-a}} = qx$. So we must find the normalization of $\mathbf{Z}[[q]]$ in:

$$(\mathbf{Z}((q))[x]/\Phi_p(x^{p^{a-1}}))[z]/(z^{p^{b-a}} - qx),$$

which is:

$$(\mathbf{Z}[[q]][x]/\Phi_p(x^{p^{a-1}}))[z]/(z^{p^{b-a}} - qx),$$

because it is regular and finite over $\mathbf{Z}[[q]]$. We have proved the following proposition.

Proposition 1.2.2.1. *The $\mathbf{Z}[[q]]$-scheme $\widehat{\mathrm{Cusps}}([\Gamma_0(p^n)])$ is isomorphic to:*

$$\mathrm{Spec}(\mathbf{Z}[[q]]) \coprod \mathrm{Spec}(\mathbf{Z}[[q^{p^{-n}}]]) \coprod \coprod_{\substack{a+b=n \\ a \geq b > 0}} \mathrm{Spec}(\mathbf{Z}[\zeta_{p^b}][[q]]) \coprod$$
$$\coprod_{\substack{a+b=n \\ b > a > 0}} \mathrm{Spec}(\mathbf{Z}[\zeta_{p^a}][[q]][z]/(z^{p^{b-a}} - \zeta_{p^a} q)),$$

and hence is regular.

(1.2.3) We see from the proposition above that locally etale on $\mathrm{Spec}(\mathbf{Z}[1/p])$ the $\mathbf{Z}[[q]]$-scheme $\widehat{\mathrm{Cusps}}([\Gamma_0(p^n)])$ is isomorphic to a disjoint union of schemes of the type $\mathrm{Spec}(\mathbf{Z}[[q^{1/f}]])$, with $f|p^n$. This implies that locally etale on $\mathrm{Spec}(\mathbf{Z}[1/N])$ the $\mathbf{Z}[[q]]$-scheme $\widehat{\mathrm{Cusps}}([\Gamma_0(N)])$ is isomorphic to a disjoint union of schemes of the type $\mathrm{Spec}(\mathbf{Z}[[q^{1/f}]])$, with $f|N$. Now we form the fibre product:

$$X := \widehat{\mathrm{Cusps}}([\Gamma_0(p^n)]) \times_{\mathbf{Z}[[q]]} \widehat{\mathrm{Cusps}}([\Gamma_0(N)]) \times_{\mathbf{Z}} \mathbf{Z}[1/N].$$

The normalization of X is then $\widehat{\mathrm{Cusps}}([\Gamma_0(p^n N)]) \times_{\mathbf{Z}} \mathbf{Z}[1/N]$.

We see that in the decompostion of X that comes from the decomposition of $\widehat{\mathrm{Cusps}}([\Gamma_0(p^n)])$ (see Proposition 1.2.2.1), the $(n,0)$, $(0,n)$ and (a,b)-components with $a \geq b$ are regular. For the $(n,0)$ and $(0,n)$-components one uses the fact that $X_0(p^n) \to \mathrm{Spec}(\mathbf{Z})$ is smooth at the cusps of these two components. The (a,b)-components of X with $b > a > 0$ are locally etale isomorphic to:

$$\mathrm{Spec}(\mathbf{Z}[\zeta_{p^a}][[x]][z]/(z^{p^{b-a}} - \zeta_{p^a} x^f)),$$

so they cause a problem. One way to get out of this is to let the involution W_{p^n} act. The action of W_{p^n} on $[\Gamma_0(p^n)]$ is defined by:

$$(\phi : E_1 \to E_2) \mapsto (\phi^t : E_2 \to E_1).$$

This action induces one on $X_0(p^n N)$, and it interchanges the (a,b) and (b,a)-components of the p-fibre, and hence interchanges the (a,b) and (b,a)-components of the scheme of cusps. Then it follows that the components with $b > a > 0$ are regular too. Of course, we could also have directly computed the normalization. Anyhow, we have proved the following theorem.

Theorem 1.2.3.1. *The scheme $X_0(N)$ is regular at infinity for all N.*

1.3. Computations.

(1.3.1) In this section we will do the computations that are outlined in 1.1.5. By the blow up $\widetilde{X}$ of a scheme X in a sheaf of ideals I we will mean the X-scheme $\mathrm{Proj}(\oplus_{n\geq 0} I^n)$, as in [5] II 8.1.3. It is clear from this definition that blowing up commutes with flat base change: if $Y \to X$ is flat, then the fibered product $Y \times_X \widetilde{X}$ is the blow up of Y in the inverse image sheaf of ideals of I. We will use this in the case where X is the spectrum of a noetherian ring A, and Y is the spectrum of some completion $\hat{A}$ of A.

In our application, $X = \mathrm{Spec}(A)$, where A is a regular local ring of dimension 2, and $\widetilde{X}$ is the blow up of X in the sheaf of ideals of the closed point x. Let x, y be a set of parameters of A. According to [5] IV Proposition 19.4.11, $\widetilde{X}$ is the closed subscheme of $\mathbf{P}^1_X = \mathrm{Proj}(A[U,V])$ defined by the equation $xV - yU = 0$, and $\widetilde{X}$ is regular. The scheme $\widetilde{X}$ is covered by the two open affines $D_+(U)$ and $D_+(V)$, where

$$D_+(V) = \mathrm{Spec}(A[u]/(x-yu)), \quad D_+(U) = \mathrm{Spec}(A[v]/(y-xv)).$$

On $D_+(V)$ and $D_+(U)$, the inverse image of x, which we call the exceptional divisor, is described by the equations: $y = 0$ and $x = 0$, respectively.

To be even more specific, we will have $A = W[[x,y]]/(f)$, where $f = f_0 + pf_1$, with f_1 a unit in $W[[x,y]]$ and f_0 as in 1.1.5. In that case,

$$A[v]/(y-xv) = W[[x,y]][v]/(y-xv, f) = W[[x,xv]][v]/(\tilde{f}),$$

where $\tilde{f} = f(x, xv)$. Note that the completion of this ring along the exceptional divisor is given by $W[v][[x]]/(\tilde{f})$. For the other open affine, we have an analogous formula. It follows that we can repeat this blowing up procedure at an arbitrary point of the exceptional divisor.

(1.3.2) *The case $j = 1728$, supersingular (hence $p \equiv -1(4)$).*
Let $k := \overline{\mathbf{F}}_p$. The point x of the moduli stack $[\Gamma_0(p^n)]$ we consider corresponds to: $F^n : E \to E$, where E is the elliptic curve over k given by the Weierstrass equation: $Y^2 = X^3 - X$, which has $\mathrm{Aut}_k(E) \underset{\sim}{=} \mathbf{Z}/(4)$, with generator $[i]^\# : X \to -X, Y \to iY$, with $i \in k^*$ of order 4. The group $\mathrm{Aut}_k(\mathrm{x})$ is then cyclic of order 4 with generator:

$$\begin{array}{ccc} E & \xrightarrow{F^n} & E \\ {\scriptstyle [i]}\downarrow & & \downarrow{\scriptstyle (-1)^n[i]} \\ E & \xrightarrow{F^n} & E \end{array}$$

The elliptic curve over $k[[t]]$ given by $Y^2 = X^3 - X + t$ is a universal formal deformation of E, and $[i]$ acts on it by: $X \mapsto -X$, $Y \mapsto iY$, $t \mapsto -t$ (note that the equation is preserved). It follows that t is a coordinate of the universal formal deformation space of E, such that $[i]$ acts on t by: $t \mapsto -t$.

Let x and y be the local moduli of source and target at x, both corresponding to t. Then $[i]$ acts on x and y by: $x \mapsto -x$, $y \mapsto -y$. The universal formal deformation space of x is isomorphic to the completion of the strict Henselization of $\mathcal{M}(\mathcal{P}, [\Gamma_0(p^n N)])$ at some point over x, where $\mathcal{P}$ is some moduli problem that is etale over (Ell). As in 1.1.5, we have $A = W[[x,y]]/(f)$, with $f = f_0 + pf_1$, f_1 a unit in $W[[x,y]]$, and

$$f_0 = (x^{p^n} - y)(x - y^{p^n}) \prod_{\substack{a+b=n \\ a,b>0}} (x^{p^{a-1}} - y^{p^{b-1}})^{p-1}.$$

Figure 1.3.2.1 gives a picture of the special fibre.

Figure 1.3.2.1.

The action of $[i]$ on the cotangent space at x is not a pseudo-reflection, hence we blow up A in its maximal ideal. As explained above, the result is covered by the two open affines $D_+(V)$ and $D_+(U)$. We visualize the situation in figure 1.3.2.2:

Figure 1.3.2.2.

The action of $[i]$ on u and v is given by: $u \mapsto u$, $v \mapsto v$. The locus of fixed points is now exactly the exceptional divisor. It follows from these formulas that, at every point of the exceptional divisor, the action of $[i]$ on the cotangent space is given by a pseudo-reflection. By Theorem 1.1.4.1, the quotient by $[i]$ is regular. Since $D_+(V)$ and $D_+(U)$ are stable under the action of $[i]$, this quotient is covered by the quotients of $D_+(V)$ and $D_+(U)$ by the action of $[i]$. Coordinates are given by y^2, u and x^2, v, respectively. It is a matter of administration to express $\tilde{f}_0$ in these coordinates. We visualize the quotient in figure 1.3.2.3.

Figure 1.3.2.3.

The multiplicities of the (a, b)-components are unchanged. The selfintersection of the quotient of the exceptional divisor can be obtained from the intersection theory in [2] exp. X.

(1.3.3) *The case* $j = 1728$*, ordinary (hence* $p \equiv 1(4)$*),* (a, b)*-component .*
We suppose that $a \neq 0$, $b \neq 0$. This point x of the moduli stack $[\Gamma_0(p^n)]$, together with a generator $[i]$ of $\mathrm{Aut}_k(\mathrm{x})$ corresponds to:

$$\begin{array}{ccc} E & \xrightarrow{V^b F^a} & E \\ {\scriptstyle [i]}\downarrow & & \downarrow{\scriptstyle [i]} \\ E & \xrightarrow{V^b F^a} & E \end{array}$$

The computation in this case is the same as the one in 1.3.2, the only difference is that the special fibre has only one component at x. There are now three cases corresponding to $a > b$, $a = b$ and $a < b$. We draw three more pictures.

Figure 1.3.3.1. Case $a > b > 0$.

Figure 1.3.3.2. Case $a = b$ (if $n \equiv 0(2)$).

Figure 1.3.3.3. Case $0 < a < b$.

(1.3.4) *The case $j = 0$, supersingular, $n \equiv 0(2)$ (hence $p \equiv -1(3)$).*

This point of the moduli stack $[\Gamma_0(p^n)]$ corresponds to: $F^n : E \to E$, where E is the elliptic curve over k given by the Weierstrass equation: $Y^2 = X^3 - 1$, which has $\mathrm{Aut}_k(E)$ cyclic of order 6, with generator $[\rho] : X \to \zeta^{-1}X$, $Y \to -Y$, with $\zeta \in k^*$ of order 3. The group $\mathrm{Aut}_k(\mathrm{x})$ is cyclic of order 6 with generator ρ:

$$\begin{array}{ccc} E & \xrightarrow{F^n} & E \\ {\scriptstyle [\rho]} \downarrow & & \downarrow {\scriptstyle [\rho]} \\ E & \xrightarrow{F^n} & E \end{array}$$

We can choose again a coordinate t of the universal formal deformation space of E such that $[\rho] : t \mapsto \zeta t$. Namely, in this case a universal formal deformation is given by: $Y^2 = X^3 + tX - 1$, and $[\rho]$ acts on it by: $X \mapsto \zeta^{-1}X$, $Y \mapsto -Y$, $t \mapsto \zeta t$. As in 1.3.2, we take the local moduli x and y of source and target to be equal to t. Then the deformation space of x is $W[[x,y]]/(f_0 + pf_1)$, with:

$$f_0 = (x^{p^n} - y)(x - y^{p^n}) \prod_{\substack{a+b=n \\ a,b>0}} (x^{p^{a-1}} - y^{p^{b-1}})^{p-1},$$

and $[\rho]$ acts on it by: $x \mapsto \zeta x, y \mapsto \zeta y$. Since $[\rho]$ does not act on the cotangent space of x by a pseudo-reflection, we blow up in x. The situation is now the same as in figure 1.3.2.2: the locus of fixed points is the exceptional divisor, and at every fixed point, $[\rho]$ acts on the cotangent space by a pseudo-reflection. Figure 1.3.4.1 gives a picture of the quotient.

Figure 1.3.4.1.

(1.3.5) *The case $j = 0$, supersingular, $n \equiv 1(2)$ (still $p \equiv -1(3)$).*

This point x of $[\Gamma_0(p^n)]$, together with a generator $[\rho]$ of $\mathrm{Aut}_k(\mathrm{x})$ corresponds to:

$$\begin{array}{ccc} E & \xrightarrow{F^n} & E \\ {\scriptstyle [\rho]}\downarrow & & \downarrow{\scriptstyle [\rho^{-1}]} \\ E & \xrightarrow{F^n} & E \end{array}$$

From this we get the action $[\rho] : x \mapsto \zeta x, y \mapsto \zeta y$ on the local moduli of source and target. We blow up because the action on the cotangent space of the deformation space of x is not by a pseudo-reflection. The resulting situation is pictured in figure 1.3.5.1.

Figure 1.3.5.1.

We are left with two fixed points. There the action is *not* given by a pseudo-reflection. We blow up in these points. Figure 1.3.5.2 gives the new situation.

Figure 1.3.5.2.

Now the action at the fixed points is given by pseudo-reflections, so we take the quotient. The situation then looks like the one in figure 1.3.5.2, but the selfintersections -1 have turned into -3, and the -3 has turned into -1 (because the quotient map has degree 3 on this $\mathbf{P}^1_k$). We contract this last one, see for example [10] Thm. 27.1. The selfintersections of the remaining two $\mathbf{P}^1_k$'s are -2. The final state is pictured in figure 1.3.5.3.

Figure 1.3.5.3.

(1.3.6) *The case $j = 0$, ordinary (hence $p \equiv 1(3)$), on the (a, b)-component.*
We suppose that $a \neq 0$,$b \neq 0$. The point x together with the automorphism $[\rho]$ corresponds to:

$$\begin{array}{ccc} E & \stackrel{V^bF^a}{\longrightarrow} & E \\ {\scriptstyle [\rho]}\downarrow & & \downarrow{\scriptstyle [\rho]} \\ E & \stackrel{V^bF^a}{\longrightarrow} & E \end{array}$$

Hence the action to consider is $[\rho]^{\#} : x \mapsto \zeta x, y \mapsto \zeta y$. The computation is the same as in 1.3.4, but now the divisor has only one component, and we have the three cases $a > b$, $a = b$ and $a < b$. We draw three pictures.

Figure 1.3.6.1. Case $a > b > 0$.

Figure 1.3.6.2. Case $a = b$ (if $n \equiv 0(2)$).

Figure 1.3.6.3. Case $0 < a < b$.

1.4. Graph and local equations of $\widetilde{X_0}(p^n N) \otimes_{\mathbf{Z}} \overline{\mathbf{F}}_p$.

(1.4.1) By "graph of $\widetilde{X_0}(p^n N) \otimes_{\mathbf{Z}} \overline{\mathbf{F}}_p$" we mean the data:

1. the irreducible components,
2. their multiplicities,
3. where they intersect.

The local equations then give the intersection numbers. We describe step by step how to get all this. Let $k = \overline{\mathbf{F}}_p$.

(1.4.2) *Step 1.* Take the disjoint union of $n+1$ copies of $X_0(N) \otimes_{\mathbf{Z}} k$, and let Φ be the morphism:

$$\Phi : \coprod_{a+b=n} X_0(N) \otimes_{\mathbf{Z}} k \longrightarrow X_0(N) \otimes_{\mathbf{Z}} k$$

given by:

the identity morphism if $a \geq b$,

(absolute Frobenius)$^{b-a} \otimes \mathrm{id}_k$ if $a \leq b$.

Give the (a,b)-component multiplicity $\phi(p^{\min(a,b)})$.

(1.4.3) *Step 2.* At every supersingular point x of $X_0(N) \otimes_{\mathbf{Z}} k$ contract Φ^{-1}x to one point. The local equation at such a point is:

$$(x^{p^n} - y)(x - y^{p^n}) \prod_{\substack{a+b=n \\ a,b>0}} (x^{p^{a-1}} - y^{p^{b-1}})^{p-1} = 0.$$

(1.4.4) *Step 3.* Let x $\in X_0(N)(k)$ be a point with $\mathrm{Aut}_k(\mathrm{x}) \cong \mathbf{Z}/4\mathbf{Z}$ (these are the points in $X_0(N)(k)$ corresponding to an elliptic curve with j-invariant 12^3, together with a cyclic subgroup of order N which is invariant under the automorphism of order 4). If x is supersingular (this corresponds to $p \equiv -1(4)$) then replace the unique point lying over x by figure 1.3.2.3. If x is ordinary ($p \equiv 1(4)$) then let $\{\mathrm{x}_{a,b} | a+b=n\}$ be the set of points lying over x, and replace $\mathrm{x}_{a,b}$ by figure

1.3.3.1, if $a > b > 0$,

1.3.3.2, if $a = b$,

1.3.3.3, if $0 < a < b$.

The multiplicities are left unchanged.

(1.4.5) *Step 4.* Let x $\in X_0(N)(k)$ be a point with $\mathrm{Aut}_k(x) \cong \mathbf{Z}/6\mathbf{Z}$ (in this case $j(E) = 0$, and the cyclic N-group has to be invariant under the automorphism of order 6). If x is supersingular ($p \equiv -1(3)$) then replace the unique point lying over x by figure

1.3.4.1, if $n \equiv 0(2)$,

1.3.5.3, if $n \equiv 1(2)$.

If x is ordinary ($p \equiv 1(3)$) then let $\{\mathrm{x}_{a,b} | a+b=n\}$ be the set of points lying over x, and replace $\mathrm{x}_{a,b}$ by figure

1.3.6.1, if $a > b > 0$,

1.3.6.2, if $a = b$,

1.3.6.3, if $0 < a < b$.

1.5. $\widetilde{X_0}(p^2)$, for example.

(1.5.1) The case $X_0(pN)$ is done in [3] VI §6, see also the appendix of [11]. We will apply section 1.4 in the case $X_0(p^2)$, that is, we give the results.

(1.5.2) *The case* $p \equiv 1(12)$. Write $p = 12k+1$. The number of supersingular j-invariants is k, and $j = 0, 12^3$ are both ordinary. Figure 1.5.2.1 gives a picture of $\widetilde{X_0}(p^2) \otimes_{\mathbf{Z}} \overline{\mathbf{F}}_p$.

Figure 1.5.2.1.

In this picture the numbers in circles denote selfintersections, the other numbers denote multiplicities. The irreducible components are just projective lines over $\overline{\mathbf{F}}_p$. From this picture one can compute the genus of $\widetilde{X_0}(p^2) \otimes_{\mathbf{Z}} \overline{\mathbf{F}}_p$, and hence the genus of $X_0(p^2) \otimes_{\mathbf{Z}} \mathbf{C}$ (cf. [2] X, compare [8] V, exc. 1.3). It is a nice verification to show that it is indeed $12k^2 - 3k - 1$.

(1.5.3) *The case* $p \equiv 5(12)$. Write $p = 12k+5$. See figure 1.5.3.1.

Figure 1.5.3.1.

(1.5.4) *The case* $p \equiv 7(12)$. Write $p = 12k + 7$. See figure 1.5.4.1.

Figure 1.5.4.1.

(1.5.5) *The case* $p \equiv 11(12)$. Write $p = 12k + 11$. See figure 1.5.5.1.

Figure 1.5.5.1.

1.6. Global structure of $\widetilde{X_0}(p^nN) \otimes_{\mathbf{Z}} \mathbf{F}_p$.

(1.6.1) In this section we determine the global structure of the non-reduced irreducible components in $\widetilde{X_0}(p^nN) \otimes_{\mathbf{Z}} \mathbf{F}_p$ and $\overline{\mathcal{M}}(\mathcal{P}, [\Gamma_0(p^n)]) \otimes_{\mathbf{Z}} \mathbf{F}_p$ in terms of $\widetilde{X_0}(N) \otimes_{\mathbf{Z}} \mathbf{F}_p$ and $\overline{\mathcal{M}}(\mathcal{P}) \otimes_{\mathbf{Z}} \mathbf{F}_p$. We will apply the following theorem.

Theorem 1.6.1.1. *Let $X \to S$ be an integral regular two dimensional scheme flat and proper over the spectrum of a discrete valuation ring. Let s be the closed point of S, and let X_s be the special fibre. Let Y be an irreducible component of X_s and suppose that Y is smooth over $k := k(s)$, let N be the multiplicity of Y in X_s, and let $\mathcal{I}$ be the sheaf of ideals of Y in X. Let Y_n be the n-th infinitesimal neighborhood of $Y = Y_0$ in X. Finally suppose that there is given a projection:*

$$Y_{N-1} \rightleftarrows Y_0 \qquad \mathrm{id}_{Y_0},$$

and that $-Y.Y > 2.genus(Y) - 2$. Then there exists an isomorphism:

$$\begin{array}{ccc} Y_1 & \xrightarrow{\sim} & \mathrm{Spec}_{Y_0}(\mathcal{O}_{Y_0} \oplus \mathcal{I}/\mathcal{I}^2 \oplus \ldots \oplus \mathcal{I}^{N-1}/\mathcal{I}^N) \\ & \searrow \quad \swarrow & \\ & Y_0 & \end{array}$$

(this means that Y_{N-1} + projection is isomorphic to the $N-1$-th infinitesimal neighborhood of the zero section in the normal bundle on Y_0).

Proof. Let $Z \to Y_0$ be the normal bundle of Y_0 in X:

$$Z = \mathrm{Spec}_{Y_0}(\mathrm{Symm}(\mathcal{I}/\mathcal{I}^2)) = \mathrm{Spec}_{Y_0}(\mathcal{O}_{Y_0} \oplus \mathcal{I}/\mathcal{I}^2 \oplus \mathcal{I}^2/\mathcal{I}^3 \oplus \ldots).$$

For $N=1$ the proof is trivial, hence we assume that $N>1$. The projection $\underset{\sim}{Y}_{N-1}\to Y_0$ gives us a projection $Y_1\to Y_0$. This results in an isomorphism of sheaves of rings $\mathcal{O}_{Y_1}=\mathcal{O}_{Y_0}\oplus\mathcal{I}/\mathcal{I}^2$. This means that we have a closed immersion:

$$
\begin{tikzcd}
g_1 : Y_1 \arrow[rr] \arrow[dr] & & Z \arrow[dl] \\
& Y_0 &
\end{tikzcd}
$$

We have to show that this closed immersion can be lifted to Y_{N-1}. In order to do this, we use obstruction theory as in [7] §4, i.e. we apply [6] exp. III Cor. 5.2 + the first alinea following this. Suppose that we have a Y_0-morphism $g_n : Y_n\to Z$ lifting g_1, with $1\le n<N-1$. Note that such a g_n is automatically a closed immersion. We will now show that g_n can be lifted to a Y_0-morphism $g_{n+1}:Y_{n+1}\to Z$. Let $P(g_n)$ be the sheaf of sets on Y_0 with

$$P(g_n)(U)=\{\text{liftings } g_{n+1} \text{ of } g_n \text{ over } U\}$$

for every open subset U of Y_0. According to [6] exp. III Cor. 5.2, $P(g_n)$ is a G-torsor, where

$$G=g_n^*(\Omega^1_{Z/Y_0})^\vee\otimes_{\mathcal{O}_{Y_n}}\mathcal{I}^{n+1}/\mathcal{I}^{n+2}.$$

We have now to show that $P(g_n)$ has a global section, i.e., that $P(g_n)$ is trivial as a G-torsor. The totality of G-torsors (up to isomorphism) is parametrized by $\mathrm{H}^1(Y_0,G)$, hence a sufficient condition for the existence of a lifting g_{n+1} is that $\mathrm{H}^1(Y_0,G)=0$. Therefore we compute G. Note that since $\mathcal{I}^{n+1}/\mathcal{I}^{n+2}$ is a $\mathcal{O}_Y$-module, G is a $\mathcal{O}_Y$-module too. Let $g_0:Y_0\to Z$ be the zero section. Then we have:

$$G=g_0^*(\Omega^1_{Z/Y_0})^\vee\otimes_{\mathcal{O}_Y}\mathcal{I}^{n+1}/\mathcal{I}^{n+2}=(\mathcal{I}/\mathcal{I}^2)^\vee\otimes_{\mathcal{O}_Y}(\mathcal{I}/\mathcal{I}^2)^{\otimes n+1}=(\mathcal{I}/\mathcal{I}^2)^{\otimes n}$$

Note that G is an invertible $\mathcal{O}_Y$-module. The calculation of G gives: $\deg(G)=n\deg(\mathcal{I}/\mathcal{I}^2)=n(-Y.Y)$. We can write $X_s=NY+R$ as divisors on X, with R effective and not containing Y. Then it follows that $0=Y.X_s=N(Y.Y)+Y.R$. Since $Y.R$ is non-negative, $-Y.Y$ is non-negative too. We find that $\deg(G)\ge -Y.Y>2.\mathrm{genus}(Y)-2$. By Serre duality on Y this implies that $\mathrm{H}^1(Y_0,G)=0$.

(1.6.2) It remains to determine the conormal bundles of the irreducible components of the curves $\widetilde{X_0}(p^nN)\otimes_{\mathbf{Z}}\mathbf{F}_p$ and $\overline{\mathcal{M}}(\mathcal{P},[\Gamma_0(p^n)])\otimes_{\mathbf{Z}}\mathbf{F}_p$, and to show that the conditions of Thm. 1.6.1.1 are satisfied. Let $\mathcal{L}$ denote the conormal bundle of a component Y of type (a,b) with $a,b>0$. The intersection of Y with the other components gives us $\phi(p^{\min(a,b)})\deg(\mathcal{L})$, and hence the degree of $\mathcal{L}$ itself.

In the rigidified case [9] Thm. 13.4.7 tells us that $\mathcal{M}(\mathcal{P},(a,b)\text{-cyclic})$ is isomorphic to the $\phi(p^{\min(a,b)})$-th infinitesimal neighborhood of the graph of $\mathrm{F}^{|a-b|}$ (Frobenius iterated $|a-b|$ times) in $\mathcal{M}(\mathcal{P})\times_{\mathbf{Z}}\mathcal{M}(\mathcal{P})\times_{\mathbf{Z}}\mathbf{F}_p$. This gives us an isomorphism:

$$\mathcal{L}|_{\mathcal{M}(\mathcal{P})\otimes\mathbf{F}_p}\tilde{\to}(\Omega^1_{\mathcal{M}(\mathcal{P})\otimes\mathbf{F}_p})^{\otimes p^{|a-b|}}$$

and hence:

$$\mathcal{L}\tilde{\to}(\Omega^1_{\overline{\mathcal{M}}(\mathcal{P})\otimes\mathbf{F}_p})^{\otimes p^{|a-b|}}(D),$$

with D a cuspidal divisor. Since we know the degree of $\mathcal{L}$, we know the degree of D. A modular interpretation of the cusps would be helpful at this point, but since we do not have one, we proceed in a not so elegant way.

For $\mathcal{P}$ representable finite etale Galois over $(\mathrm{Ell}/\mathbf{Z}_p)$ the divisor D has to be equally distributed over the cusps. Let us compute the degree of $\mathcal{L}$ on the (a,b)-component Y in this case. Since this degree for (a,b) is the same as for (b,a), we may suppose that $b\geq a>0$. Let m be the multiplicity of Y, then we have:

$$\deg(\mathcal{L}) = -Y.Y = m^{-1}(Y.-mY) = m^{-1}(Y.X_s - mY) = m^{-1}(Y.\sum_{C\neq Y} m_C C),$$

where the sum is over the components C of X_s other than Y, and where the m_C denote their multiplicities. Hence:

$$m\deg(\mathcal{L}) = \sum_{C\neq Y} m_C(Y.C) = \sum_{\substack{0\leq a'\leq n\\ a'\neq a}} m_{a'}sl_{a,a'},$$

where $m_{a'}$ denotes the multiplicity of the $(a', n-a')$-component, where s is the number of supersingular points on Y, and where $l_{a,a'}$ is the local intersection number of the (a,b) and $(a',n-a')$-components at a supersingular point. According to [9] Thm. 13.4.7, $m_{a'}$ is the minimum of $\phi(p^{a'})$ and $\phi(p^{n-a'})$. From the local equation for $\widetilde{X_0}(p^nN)\otimes_{\mathbf{Z}}\mathbf{F}_p$ at such a point (see [9] Thm. 13.4.7) it follows that

$$l_{a,a'} = \begin{cases} p^{n-2a} & \text{if} \quad 0\leq a'<a<\frac{n}{2}\\ p^{n-2a'} & \text{if} \quad a<a'<\frac{n}{2}\\ 1 & \text{if} \quad \frac{n}{2}\leq a'.\end{cases}$$

Evaluating the sum gives:

$$\deg(\mathcal{L}) = 2m^{-1}sp^{n-a-1} = \frac{2s}{p-1}p^{b-a}.$$

We can compute s using the Kodaira-Spencer isomorphism of [9] Thm. 10.13.11 and the Hasse invariant [9] Thm. 12.4.3:

$$\Omega^1_{\overline{\mathcal{M}}(\mathcal{P})\otimes\mathbf{F}_p}(\text{cusps})\tilde{\to}\underline{\omega}^{\otimes 2}, \qquad \mathcal{O}_{\overline{\mathcal{M}}(\mathcal{P})\otimes\mathbf{F}_p}(\text{s.s.})\tilde{\to}\underline{\omega}^{\otimes(\mathrm{p}-1)}.$$

From these two formulas we see that:

$$\frac{2s}{p-1} = \deg(\Omega^1_{\overline{\mathcal{M}}(\mathcal{P})\otimes\mathbf{F}_p}(\text{cusps})).$$

It follows that for $\mathcal{P}$ representable finite etale Galois over $(\mathrm{Ell}/\mathbf{Z}_p)$ we have that:

(1.6.2.1) $$\mathcal{L}\tilde{\to}(\Omega^1_{\overline{\mathcal{M}}(\mathcal{P})\otimes\mathbf{F}_p}(\text{cusps}))^{\otimes p^{|a-b|}}.$$

Let us now consider the moduli problem $(\mathcal{P},[\Gamma_0(N)])$. The morphism from this moduli problem to $\mathcal{P}$ is finite and etale. It follows that the morphism from $\overline{\mathcal{M}}(\mathcal{P},[\Gamma_0(N)])$ to $\overline{\mathcal{M}}(\mathcal{P})$ can only be ramified along the cusps. From [9] Thm. 8.6.8 it follows that locally etale the morphism from $\widehat{\mathrm{Cusps}}(\mathcal{P},[\Gamma_0(N)])$ to $\widehat{\mathrm{Cusps}}(\mathcal{P})$ is of the form:

$$\mathrm{Spec}(\mathbf{Z}_p[[q^{1/e}]]) \to \mathrm{Spec}(\mathbf{Z}_p[[q^{1/d}]]),$$

with d and e both prime to p. This implies that the pullback of the conormal bundle of the (a,b)-component of $\overline{\mathcal{M}}(\mathcal{P},[\Gamma_0(p^n)])$ is the conormal bundle of the (a,b)-component of $\overline{\mathcal{M}}(\mathcal{P},[\Gamma_0(p^nN)])$, and that the pullback of $\Omega^1_{\overline{\mathcal{M}}(\mathcal{P})\otimes\mathbf{F}_p}(\mathrm{cusps})$ is $\Omega^1_{\overline{\mathcal{M}}(\mathcal{P},[\Gamma_0(N)])\otimes\mathbf{F}_p}(\mathrm{cusps})$. It follows that we have the isomorphism 1.6.2.1 for $\mathcal{P}$ replaced by $(\mathcal{P},[\Gamma_0(N)]$.

It is now obvious that the only non-obvious condition of Thm. 1.6.1.1 ($-Y.Y > 2g(Y)-2$) is satisfied in the rigidified case.

(1.6.3) Following the construction of $\widetilde{X_0}(p^nN)$ as the quotient of a blow up of $\overline{\mathcal{M}}(\mathcal{P},[\Gamma_0(p^nN)])$ we get on the (a,b)-component of $\widetilde{X_0}(p^nN)\otimes_{\mathbf{Z}}\mathbf{F}_p$:

(1.6.3.1) $$\mathcal{L}\tilde{\to}(\Omega^1_{X_0(N)\otimes\mathbf{F}_p}(\mathrm{cusps}))^{\otimes p^{|a-b|}}(D),$$

with D a divisor supported on the points in the finite part which have extra automorphisms. In order to compute D, we have to see what happens to $\mathcal{L}$ and Ω^1 when we blow up or take a quotient. Let P be a point on the (a,b)-component such that its image in $\widetilde{X_0}(p^nN)$ has extra automorphisms. After d blow ups in P, the conormal bundle of the (a,b)-component is isomorphic (Zariski locally at P) to $(\Omega^1_{\overline{\mathcal{M}}(\mathcal{P},[\Gamma_0(N)])\otimes\mathbf{F}_p})^{\otimes p^{|a-b|}}(dP)$, and the stabilizer G_P of P acts on the cotangent space at P by pseudo-reflections. Let z be a local coordinate on the (a,b)-component at P, and let e be the order of G_P. Then $u:=z^e$ is a local coordinate on the quotient of the (a,b)-component, and $(du)^{p^{|a-b|}}$, as a section of $(\Omega^1_{\overline{\mathcal{M}}(\mathcal{P},[\Gamma_0(N)])\otimes\mathbf{F}_p})^{\otimes p^{|a-b|}}(dP)$, has a zero at p of order $d+(e-1)p^{|a-b|}$. It follows that on the quotient it has a zero of order $\frac{d+(e-1)p^{|a-b|}}{e}$. The results in the various cases are summarized in the following table, which gives the multiplicity of P in D.

Table 1.6.3.2.

$j=1728$			$(p^{\lvert a-b\rvert}+1)/2$
$j=0$	ordinary $(p\equiv 1(3))$		$(2p^{\lvert a-b\rvert}+1)/3$
	supersingular $(p\equiv -1(3))$	$n\equiv 0(2)$	$(2p^{\lvert a-b\rvert}+1)/3$
		$n\equiv 1(2)$	$2(p^{\lvert a-b\rvert}+1)/3$

It is now obvious from the isomorphism 1.6.3.1, plus the fact that D in Table 1.6.3.2 is an effective divisor, that the condition "$-Y.Y > 2g(Y)-2$" of Thm. 1.6.1.1 is satisfied.

2. The stable reduction of $X_0(p^2N)$ at $p \geq 5$.

2.1. The result.

Theorem 2.1.1. *Let $\mathcal{P}$ be a representable finite etale moduli problem over (Ell/W), where W is the ring of Witt vectors over $k := \overline{\mathbf{F}}_p$. We suppose that $p \geq 5$. Then the curve $\overline{\mathcal{M}}(\mathcal{P}, [\Gamma_0(p^2)])$ over W acquires stable reduction over $W[z]/(z^{(p^2-1)/2} - p)$. The special fibre of the stable model is as follows:*

The horizontal curves are all isomorphic to the smooth model C of the singular curve given by the equation: $y^{p+1} = x(x-1)^{p-1}$. The points on C over $x = 0$, $x = \infty$ are glued to the outer components. The two points over $x = 1$ are glued to the two middle components.

Theorem 2.1.2. *Let $k := \overline{\mathbf{F}}_p$ with $p \geq 5$, $W := W(k)$. Let $\mathcal{P}$ be relatively representable finite etale over (Ell/W), e.g. $\mathcal{P} = [\Gamma_0(N)]$ with $(p, N) = 1$. Then the curve $\overline{\mathrm{M}}(\mathcal{P}, [\Gamma_0(p^2)])$ over W acquires stable reduction over $W[z]/(z^{(p^2-1)/2} - p)$. The special fibre of the stable model is as follows:*

The horizontal component over a supersingular point x *on* $\overline{\mathrm{M}}(\mathcal{P}) \otimes k$ *is isomorphic to the smooth model of the singular curve given by:*

$$\begin{aligned} y^{p+1} &= x(x-1)^{p-1} && \text{if } \operatorname{Aut}_k(\mathrm{x}) \overset{\sim}{=} \mathbf{Z}/(2) \\ y^{(p+1)/2} &= x(x-1)^{p-1} && \text{if } \operatorname{Aut}_k(\mathrm{x}) \overset{\sim}{=} \mathbf{Z}/(4) \\ y^{(p+1)/3} &= x(x-1)^{p-1} && \text{if } \operatorname{Aut}_k(\mathrm{x}) \overset{\sim}{=} \mathbf{Z}/(6). \end{aligned}$$

The points over $x = 0$, $x = \infty$ are glued to the outer components. The two points over $x = 1$ are glued to the two middle components.

(2.1.3) The proof of these theorems is given in sections 2.2, 2.3 and 2.4.

2.2. Formal computations.

(2.2.1) For simplicity we work over $W := W(k)$, where $k := \overline{\mathbf{F}}_p$. Let $\mathcal{P}$ denote a representable moduli problem on (Ell/W), which is finite etale over (Ell/W). Let X_0 denote $\overline{\mathcal{M}}(\mathcal{P}, [\Gamma_0(p^2)])$. This is a regular W-scheme. The finite part of its special fibre is described in [9] Thm. 13.4.7. This fibre is a Cartier divisor on X_0. To get normal crossings it suffices to blow up once in each supersingular point. Let X_1 denote this blow up. The special fibre of X_1 is a Cartier divisor with normal crossings. Its picture is in figure 2.2.1.1.

Figure 2.2.1.1. Picture of $X_1 \otimes_W k$. The numbers denote the multiplicities.

(2.2.2) The least common multiple of the multiplicities of the components of $X_1 \otimes_W k$ is $(p^2-1)/2$. Let $W_1 := W[t]/(t^{(p^2-1)/2} - p)$, and let $t \in W_1$ denote the image of t. Define $X_2 := X_1 \otimes_W W_1$, and let $\widetilde{X_2} \to X_2$ be its normalization. This $\widetilde{X_2}$ will be our stable model, and therefore we want to compute its special fibre. First we do this formally, i.e. we compute the complete local rings of $\widetilde{X_2}$.

Let x be a closed point of $X_1 \otimes_W k = X_2 \otimes_{W_1} k$. Then $\widehat{\mathcal{O}}_{X_1,\mathrm{x}}$ is of the form $\underset{\sim}{W}[[x,y]]/(x^a y^b - p)$, with $a, b \in \{0, 1, p-1, p+1\}$, $a \neq 0$ and $\{a, b\} \neq \{1, p-1\}$. This gives $\widehat{\mathcal{O}}_{X_2,\mathrm{x}} = W[[x,y]]/(x^a y^b - t^{(p^2-1)/2})$. We must find its normalization, since (by [5] IV, 7.8.2 and 7.8.3(vii))

$$\widetilde{X_2} \times_{X_2} \mathrm{Spec}(\widehat{\mathcal{O}}_{X_2,\mathrm{x}}) = \mathrm{Spec}(\text{this normalization}).$$

We treat the different cases separately.

(2.2.2.1) *The case $b = 0, a = 1$.*
The ring in question is regular, hence normal.

(2.2.2.2) *The case $b = 0, a = p-1$.*
We can write:

$$x^{p-1} - t^{(p^2-1)/2} = \prod_{\zeta \in \mu_{p-1}(W_1)} (x - \zeta t^{(p+1)/2}).$$

From this it follows:

$$\widetilde{X_2} \times_{X_2} \mathrm{Spec}(\widehat{\mathcal{O}}_{X_2,\mathrm{x}}) = \coprod_{\zeta \in \mu_{p-1}(W_1)} \mathrm{Spec}(W_1[[x,y]]/(x - \zeta t^{(p+1)/2})).$$

In this case the normalization is regular too.

(2.2.2.3) *The case $b = 0, a = p+1$.*
Just as in (2.2.2.2) we get:

$$\widetilde{X_2} \times_{X_2} \mathrm{Spec}(\widehat{\mathcal{O}}_{X_2,\mathrm{x}}) = \coprod_{\zeta \in \mu_{p+1}(W_1)} \mathrm{Spec}(W_1[[x,y]]/(x - \zeta t^{(p-1)/2})).$$

(2.2.2.4) *The case $b = 1, a = p+1$.*
We can split the base change $\mathrm{Spec}(W_1) \to \mathrm{Spec}(W)$ up in two. Let $W_2 := W[z]/(z^{p+1} - p)$, and let z denote the image of z in W_2. First we compute the normalization of $W_2[[x,y]]/(x^{p+1}y - z^{p+1})$. To do this, we blow it up along the ideal (x,z), i.e. we set $z := ux$. This gives us $W_2[[x,y,u]]/(z - ux, y - u^{p+1})$, or, equivalently: $W_2[[x,y]]/(z - ux)$. After the base change $\mathrm{Spec}(W_1) \to \mathrm{Spec}(W_2)$ we get $W_1[[x,u]]/(ux - t^{(p-1)/2})$. Its singular locus is given by $u = x = t = 0$, so it is the closed point. The exceptional divisor of the minimal resolution is a chain of projective lines. This implies that $W_1[[x,u]]/(ux - t^{(p-1)/2})$ is normal. We have:

$$\widetilde{X_2} \times_{X_2} \mathrm{Spec}(\widehat{\mathcal{O}}_{X_2,\mathrm{x}}) = \mathrm{Spec}(W_1[[x,u]]/(ux - t^{(p-1)/2})),$$

with $y = u^{p+1}$. In this case the normalization is *not* regular.

(2.2.2.5) *The case $a = p-1, b = p+1$.*
We split the base change $\mathrm{Spec}(W_1) \to \mathrm{Spec}(W)$ up in three. Let $W_2 := W[z]/(z^2 - p)$, and let z denote the image of z in W_2. We write $x^{p-1}y^{p+1} - z^2 = (x^{(p-1)/2}y^{(p+1)/2} - z)(x^{(p-1)/2}y^{(p+1)/2} + z)$. The normalization of $\mathrm{Spec}(W_2[[x,y]]/(x^{p-1}y^{p+1} - z^2))$ is isomorphic to the disjoint union of two copies of $\mathrm{Spec}(W_2[[x,y]]/(x^{(p-1)/2}y^{(p+1)/2} - z))$ (here one uses that either $\frac{p-1}{2}$ or $\frac{p+1}{2}$ is odd). Let $W_3 := W_2[s]/(s^{(p+1)/2} - z)$, and let s denote the image of s in W_3. We blow up $W_3[[x,y]]/(x^{(p-1)/2}y^{(p+1)/2} - s^{(p+1)/2})$ along (y,s), i.e. we set $s = uy$. This gives $W_3[[x,y,u]]/(s - uy, x^{(p-1)/2} - y^{(p+1)/2})$. We blow it up along (x,u), i.e. we set $x = vu$. This gives $W_3[[y,u,v]]/(s - uy, v^{(p-1)/2} - u) = W_3[[y,v]]/(s - v^{(p-1)/2}y)$. We blow up $W_1[[y,v]]/(t^{(p-1)/2} - v^{(p-1)/2}y)$ along (t,v), i.e. we set $t = uv$. This gives $W_1[[y,v,u]]/(t - uv, u^{(p-1)/2} - y) = W_1[[u,v]]/(t - uv)$, which is regular. Hence we have:

$$\widetilde{X_2} \times_{X_2} \mathrm{Spec}(\widehat{\mathcal{O}}_{X_2,\mathrm{x}}) = \mathrm{Spec}(W_1[[v,u]]/(t - uv)) \coprod \mathrm{Spec}(W_1[[v,u]]/(t - uv)).$$

(2.2.3) Now look at figure 2.2.1.1, and consider $\widetilde{X_2} \otimes_{W_1} k \to X_1 \otimes_W k$. From the computations in (2.2.2) it follows that:

1. over each of the outer two vertical components lies one component, and the map is an isomorphism,
2. over each of the horizontal components lies one component, the map has degree $p+1$ and ramifies in the following way:

3. over the $(1,1)$-component there are one or two components, and the ramification is as follows:

It follows that there are two possible pictures:

Our task is:

- to determine the horizontal components,
- to decide between the two pictures, and to determine the vertical component(s).

(2.2.4) We will now compute the horizontal components. Let x be a supersingular point of $X_0 \otimes_W k$. We write $\widehat{\mathcal{O}}_{X_0,\mathrm{x}} = W[[x,y]]/(f_0 + pf_1)$, with $f_0 = (x^{p^2} - y)(x-y)^{p-1}(x - y^{p^2})$, and f_1 a unit of $W[[x,y]]$. We blow up $\widehat{\mathcal{O}}_{X_0,\mathrm{x}}$ in its maximal ideal. As explained in 1.3.1, an affine open part of the result is $W[[v,xv]][v]/(\tilde{f})$, with $\tilde{f}(x,v) = f(x,vx)$ and $\tilde{f} = \tilde{f}_0 + p\tilde{f}_1$. Taking the completion of this ring along the exceptional divisor gives $W[v][[x]]/(\tilde{f})$. Let $W_1 := W[z]/(z^{p+1} - p)$, and let z denote the image of z in W_1. After extension of scalars to W_1 we have: $W_1[v][[x]]/(\tilde{f}_0 + p\tilde{f}_1)$. We blow this up along the ideal (x,z), i.e. we write $x := uz$. We get:

$$\widehat{W_1[v,u]}/(u^{p+1}((uz)^{p^2-1} - v)(1-v)^{p-1}(1 - v^{p^2}(uz)^{p^2-1}) + \tilde{\tilde{f}}_1),$$

where the completion is with respect to the principle ideal (uz), and $\tilde{\tilde{f}}_1 = \tilde{f}_1(v,uz) = f_1(uz,vuz)$. The curve we are looking for is described by the equation $z = 0$. Substituting $z = 0$ in the equation above yields $u^{p+1}(-v)(1-v)^{p-1} + f_1(0,0) = 0$. It follows that (in new coordinates) a (singular) model of our smooth curve is given by the equation:

$$y^{p+1} = x(x-1)^{p-1}.$$

2.3. Determination of the vertical components.

(2.3.1) In this section we determina the "vertical component(s)" that arise in the computations of 2.2.2. These vertical components are evolution products of the $(1,1)$-component of $\overline{\mathcal{M}}(\mathcal{P},[\Gamma_0(p^2)])\otimes_W k$. They already live in the normalization of $\overline{\mathcal{M}}(\mathcal{P},[\Gamma_0(p^2)])\otimes_W W_1$, where W_1 is ramified over W of degree $p-1$. Since they are stable, they will not evolve any further, whatever base changes and normalizations we let them undergo. We will determine them in two different ways.

(2.3.2) *The first method.* Let $W_1 := W[\zeta_{p^2}]$, W_1 is ramified over W of degree $p(p-1)$. As remarked in 2.3.1, we must determine the irreducible components of the special fibre of the normalization of $\overline{\mathcal{M}}(\mathcal{P},[\Gamma_0(p^2)])\otimes_W W_1$. This normalization is:

$$\overline{\mathcal{M}}(\mathcal{P},[\Gamma(p^2)^{\mathrm{can}}])/G, \qquad \text{with} \quad G=\left\{\begin{pmatrix} * & * \\ 0 & * \end{pmatrix}\right\}\subset SL_2(\mathbf{Z}/p^2\mathbf{Z}).$$

We see this as follows: the normalization of $\overline{\mathcal{M}}(\mathcal{P},[\Gamma(p^2)])\otimes_W W_1$ is $\coprod_{\zeta\in\mu^\times_{p^2}(W_1)}\overline{\mathcal{M}}(\mathcal{P},[\Gamma(p^2)^{\mathrm{can}}])$, now take quotients.

Note that the order of G is divisible by p. Therefore the special fibre of the quotient may not be the same as the quotient of the special fibre. However the morphism:

$$(\overline{\mathcal{M}}(\mathcal{P},[\Gamma(p^2)^{\mathrm{can}}])\otimes_{W_1} k)/G \to (\overline{\mathcal{M}}(\mathcal{P},[\Gamma(p^2)^{\mathrm{can}}])/G)\otimes_{W_1} k \tag{2.3.2.1}$$

is surjective and radicial ([9] A7.2.1). The $\overline{\mathcal{M}}(\mathcal{P})\otimes_W k$-scheme $\overline{\mathcal{M}}(\mathcal{P},[\Gamma(p^2)^{\mathrm{can}}])\otimes_{W_1} k$ is described in [9] Thm. 13.7.6. It is the disjoint union, with crossings at the supersingular points, of the $\overline{\mathcal{M}}(\mathcal{P})\otimes_W k$-schemes $\overline{\mathcal{M}}(\mathcal{P},[\mathrm{ExIg}(p^2,2)])$, indexed by $\mathbf{P}^1(\mathbf{Z}/(p^2))$. The group G acts on $\mathbf{P}^1(\mathbf{Z}/(p^2))$ by:

$$(x:y)\begin{pmatrix} t & s \\ 0 & t^{-1}\end{pmatrix}=(tx:sx+t^{-1}y).$$

This action has 4 orbits. They are generated by $(0:1)$, $(1:0)$, $(p:1)$ and $(dp:1)$, with d a non-square in $\mathbf{F}_p$. The first two orbits correspond to the $(2,0)$ and $(0,2)$-components of $[\Gamma_0(p^2)]\otimes k$. The other two give the curve(s) we are looking for. At this moment we see that the $(1,1)$-component gets replaced by two components. Hence the first of the two pictures in 2.2.3 is the correct one.

The stabilizer group of $(p:1)$ and $(dp:1)$ is $\left\{\begin{pmatrix} t & s \\ 0 & t^{-1}\end{pmatrix}\in G; t^2=1\right\}$. This group acts on $\overline{\mathcal{M}}(\mathcal{P},[\mathrm{ExIg}(p^2,2)])$. The subgroup $\left\{\begin{pmatrix} 1 & * \\ 0 & 1\end{pmatrix}\right\}$ acts trivially. We are left with the group $(\pm1+p\mathbf{Z})/(1+p^2\mathbf{Z})\subset(\mathbf{Z}/p^2\mathbf{Z})^*$. There is an exact sequence:

$$\{1\}\to(1+p\mathbf{Z})/(1+p^2\mathbf{Z})\to(\pm1+p\mathbf{Z})/(1+p^2\mathbf{Z})\to\{\pm1\}\to\{1\}.$$

We want to determine the quotient of the $\overline{\mathcal{M}}(\mathcal{P})\otimes_W k$-scheme $\overline{\mathcal{M}}(\mathcal{P},[\mathrm{ExIg}(p^2,2)])$ by the kernel.

Consider the following diagram from [9] Thm. 12.10.6.:

$$\begin{array}{ccc}
\mathcal{M}((\mathcal{P}\otimes_W k)^{(\sigma^{-2})},[\mathrm{Ig}(p^2)]) & \xrightarrow{\sim} & \mathcal{M}(\mathcal{P},[\mathrm{ExIg}(p^2,2)]) \\
\downarrow \mathrm{pr} & \searrow^{\mathrm{pr}_2} & \downarrow \mathrm{pr} \\
\mathcal{M}((\mathcal{P}\otimes_W k)^{(\sigma^{-2})}) & \xrightarrow{F^2} & \mathcal{M}(\mathcal{P}\otimes_W k)
\end{array}$$

By [9] Thm. 12.6.1(3) we get an isomorphism:

$$\begin{array}{ccc}
\overline{\mathcal{M}}((\mathcal{P}\otimes_W k)^{(\sigma^{-2})},[\mathrm{Ig}(p)]) & \xrightarrow{\sim} & \overline{\mathcal{M}}(\mathcal{P},[\mathrm{ExIg}(p^2,2)])/((1+p\mathbf{Z})/(1+p^2\mathbf{Z})) \\
\searrow^{\mathrm{pr}_2} & & \swarrow_{\mathrm{pr}} \\
& \overline{\mathcal{M}}(\mathcal{P}\otimes_W k) &
\end{array}$$

Taking the quotient by $\{\pm 1\}$ gives:

$$\begin{array}{ccc}
\overline{\mathcal{M}}((\mathcal{P}\otimes_W k)^{(\sigma^{-2})},[\mathrm{Ig}(p)]/\{\pm 1\}) & \xrightarrow{\sim} & \overline{\mathcal{M}}(\mathcal{P},[\mathrm{ExIg}(p^2,2)])/((\pm 1+p\mathbf{Z})/(1+p^2\mathbf{Z})) \\
\searrow^{\mathrm{pr}_2} & & \swarrow_{\mathrm{pr}} \\
& \overline{\mathcal{M}}(\mathcal{P}\otimes_W k) &
\end{array}$$

This is a component of the source of the morphism 2.3.2.1. Both source and target of this $\overline{\mathcal{M}}(\mathcal{P})\otimes_W k$-morphism are reduced. A degree consideration over $\overline{\mathcal{M}}(\mathcal{P})\otimes_W k$ then implies that the component in the target is $\overline{\mathcal{M}}(\mathcal{P},[\mathrm{Ig}(p)]/\{\pm 1\})$. We have proved:

Theorem 2.3.2.2. *In the stable reduction of $\overline{\mathcal{M}}(\mathcal{P},[\Gamma_0(p^2)])$ the $(1,1)$-component gives two components, each $\overline{\mathcal{M}}(\mathcal{P})\otimes_W k$-isomorphic to $\overline{\mathcal{M}}(\mathcal{P},[\mathrm{Ig}(p)]/\{\pm 1\})$.*

(2.3.3) *The second method.* This method is a global version of the formal computations of (2.2). Consider $\overline{\mathcal{M}}(\mathcal{P},[\Gamma_0(p^2)])$. We blow it up in the supersingular points. Let X be the formal completion of this blow up along the $(1,1)$-component. We claim the existence of a global function f on X such that $f^2 = p\cdot\mathrm{unit}$. The divisor of such a f must be (cf. 2.2.1.1):

This can be checked in the special fibre itself. Let $\mathcal{I}$ be the ideal of the reduced $(1,1)$-component of X, and let X_n be the subscheme of X defined by $\mathcal{I}^{n+1}$. Then Theorem 1.6.1.1 gives:

$$X_{p-2}\tilde{\to}\mathrm{Spec}_{X_0}(\mathcal{O}_{X_0}\oplus\mathcal{L}\oplus ..\oplus\mathcal{L}^{p-2}),$$

with $\mathcal{L} := \mathcal{I}/\mathcal{I}^2$ the conormal bundle of X_0 in X. The isomorphism 1.6.2.1 plus the Kodaira-Spencer isomorphism and the Hasse invariant give: $\mathcal{L}\tilde{\rightarrow}\underline{\omega}^{\otimes p+1}$. Let $A \in \underline{\omega}^{\otimes p-1}(X_0)$ be the Hasse invariant. Its divisor is exactly the supersingular locus. Let

$$A_{(p+1)/2} := A^{\otimes(p+1)/2} \in \underline{\omega}^{\otimes(p+1)(p-1)/2}(X_0) \overset{\sim}{=} \mathcal{L}^{\otimes(p-1)/2}(X_0).$$

Then $A_{(p+1)/2}$ is a global function on X_{p-2} which has the right divisor. We will now try to lift this function to one on X which still has the right divisor.

Let $\mathcal{J}$ be the ideal of the reduced horizontal components. Let $n \geq p-1$. We suppose that we have a lifting f_{n-1} to X_{n-1}. We want to lift it to a f_n on X_n, with f_n a global section of $(\mathcal{I}^{n+1} + \mathcal{J}^{(p+1)/2})/\mathcal{I}^{n+1}$. Consider the diagram:

$$\begin{array}{ccccc}
 & & (\mathcal{I}^{n+1} + \mathcal{J}^{\frac{p+1}{2}})/\mathcal{I}^{n+1} & \longrightarrow & (\mathcal{I}^{n} + \mathcal{J}^{\frac{p+1}{2}})/\mathcal{I}^{n} \\
 & & \| & & \| \\
\mathcal{J}^{\frac{p+1}{2}} \cdot \mathcal{I}^n/\mathcal{J}^{\frac{p+1}{2}} \cdot \mathcal{I}^{n+1} & \longrightarrow & \mathcal{J}^{\frac{p+1}{2}}/\mathcal{J}^{\frac{p+1}{2}} \cdot \mathcal{I}^{n+1} & \longrightarrow & \mathcal{J}^{\frac{p+1}{2}}/\mathcal{J}^{\frac{p+1}{2}} \cdot \mathcal{I}^{n} \\
\| & & & & \\
(\mathcal{J}^{\frac{p+1}{2}} \cdot \mathcal{I}^n)|_{X_0} & & & &
\end{array}$$

Since $\mathrm{H}^1(X_0, \mathcal{J}^{(p+1)/2}\mathcal{I}^n|_{X_0}) = \{0\}$ for $n > (p-1)/2$, the required f_n exists. This gives us a f on X with $f^2 = p \cdot \text{unit}$, and $f|_{X_{p-2}} = A_{(p+1)/2}$. The two vertical components of the stable reduction are obtained by extracting the $((p-1)/2)$-th root of f. This amounts to extracting the $((p-1)/2)$-th root of the Hasse invariant. By [9] Thm. 12.8.2 we see that the vertical components are $\overline{\mathcal{M}}(\mathcal{P}, [\mathrm{Ig}(p)]/\{\pm 1\})$.

2.4. The coarse case.

Let $\mathcal{P}$ be relatively representable finite etale over (Ell/W). Let $\mathcal{D}$ be representable finite etale Galois (with group G) over (Ell/W). Then by construction:

$$\overline{\mathrm{M}}(\mathcal{P}, [\Gamma_0(p^2)]) = \overline{\mathcal{M}}(\mathcal{D}, \mathcal{P}, [\Gamma_0(p^2)])/G.$$

Let X_2/W_1 be the stable model of $\overline{\mathcal{M}}(\mathcal{D}, \mathcal{P}, [\Gamma_0(p^2)])$ as constructed in 2.2.2. From the construction it follows that G operates on X_2/W_1. Therefore X_2/G is a model of $\overline{\mathrm{M}}(\mathcal{P}, [\Gamma_0(p^2)]) \otimes_W W_1$. The only singularities of its special fibre are ordinary double points. We will call this model the stable model of $\overline{\mathrm{M}}(\mathcal{P}, [\Gamma_0(p^2)])$ over W_1. Strictly spoken this is not always true, for the genus can be less than two, and also the condition on the rational components need not be satisfied. Following the computations of 2.2.4 and 2.3, the statements in Thm. 2.1.2 about the components of $(X_2/G) \otimes_{W_1} k$ are easily checked.

2.5. Examples.

(2.5.1) We apply Thm. 2.1.2 to $X_0(p^2)$. We draw pictures in the various cases for p mod 12. The numbers denote the genera of the components.

Figure 2.5.1.1. $p = 12k + 1$.

Figure 2.5.1.2. $p = 12k + 5$.

Figure 2.5.1.3. $p = 12k + 7$.

Figure 2.5.1.5. $p = 12k + 11$.

(2.5.2) *The case* $X_0(7^2)$. We have the picture:

The elliptic curve over k is the smooth model of: $y^2 = x(x-1)^2$. The automorphism of order 4: $(x, y) \mapsto (x, iy)$ fixes the regular point $(0, 0)$, hence the elliptic curve has $j \equiv 2^6 3^3 \equiv -1(7)$. From Table 1 of [1] we extract: $X_0(7^2)$ over $\mathbf{Q}$ is the elliptic curve given by the equation: $y^2 + xy = x^3 - x^2 - 2x - 1$. Its j-invariant is $-3^3 5^3$, and indeed $-3^3 5^3 \equiv -1(7)$.

(2.5.3) *The case* $X_0(35^2)$. Let $p = 5$. We have the picture:

The genus 2 curve is the smooth model C of: $y^6 = x(x-1)^4$. Another model of C is: $y^2 = x^6 - 1$. In these coordinates a basis for the global differential forms is: $\omega_1 := (dx)/y$, $\omega_2 := x(dx)/y$. The involution $W : (x, y) \mapsto (-x, y)$ acts by: $W^*\omega_1 = -\omega_1$, $W^*\omega_2 = \omega_2$. The quotient C/W is the elliptic curve: $v^2 = u^3 - 1$, it has $j = 0$. It follows that up to isogeny the jacobian of C is the product of two elliptic curves, one of which is isogenous to the curve with $j = 0$. Since $j = 0$ is the only supersingular j-invariant mod 5, it has $j = 0$. The automorphism $(x, y) \mapsto (x^{-1}, iyx^{-3})$ of C interchanges the two eigenspaces of W acting on the differentials. It follows that both elliptic curves have $j = 0$. Table 1 of [1] gives us two strong Weil curves with conductor 3.5^2 having potentially good reduction at 5:

$$
\begin{aligned}
75A: &\quad y^2 + y = x^3 - x^2 - 8x - 7 \quad j = -2^{12}.3^{-1}.5^2 \equiv 0(5) \\
75B: &\quad y^2 + y = x^3 + x^2 + 2x + 4 \quad j = 2^{12}.3^{-5}.5 \equiv 0(5)
\end{aligned}
$$

References

[1] B.J. Birch and W. Kuyk. *Modular functions of one variable IV.* Springer Lecture Notes in Mathematics 476 (1975).

[2] P. Deligne and N. Katz. *Séminaire de géométrie algébrique 7 II.* Springer Lecture Notes in Mathematics 340 (1973).

[3] P. Deligne and M. Rapoport. *Les schémas de modules des courbes elliptiques.* In Modular Functions of One Variable II. Springer Lecture Notes in Mathematics 349 (1973).

[4] B.H. Gross and D.B. Zagier. *Heegner points and derivatives of L-series.* Invent. Math. 84, 225–320 (1986).

[5] A. Grothendieck. *Éléments de géométrie algébrique, Ch. I, II, III, IV.* Publications Mathématiques de l'I.H.E.S. 4, 8, 11, 17, 20, 24, 28, 32 (1960–1967).

[6] A. Grothendieck. *Séminaire de géométrie algébrique I: Revêtements étales et groupe fondamental.* Springer Lecture Notes in Mathematics 224 (1971).

[7] R. Hartshorne. *Curves with high selfintersection on algebraic surfaces.* Publications Mathématiques de l'I.H.E.S. 36 (1969).

[8] R. Hartshorne. *Algebraic geometry.* Springer Graduate Texts in Mathematics 52 (1977).

[9] N.M. Katz and B. Mazur. *Arithmetic moduli of elliptic curves.* Annals of Mathematics Studies 108, Princeton University Press (1985).

[10] J. Lipman. *Rational singularities, with applications to algebraic surfaces and unique factorization.* Publications Mathématiques de l'I.H.E.S. 36 (1969).

[11] B. Mazur *Modular curves and the Eisenstein ideal.* Publications Mathématiques de l'-I.H.E.S. 47, 33–186 (1977).

[12] J.F. Mestre. *Courbes de Weil et courbes supersingulières.* Séminaire de théorie des nombres 1984–1985, université de Bordeaux 1.

[13] A. Pizer. *An algorithm for computing modular forms on* $\Gamma_0(N)$. Journal of algebra 64, 340–390 (1980).

[14] A. Pizer. *Theta series and modular forms of level* p^2M. Compositio Math. 40, 177–241 (1980).

[15] J.-P. Serre. Colloque d'algèbre, 6–7 mai 1967, ENSJF.