Stable models of modular curves and applications.

Sebastiaan Johan Edixhoven

05/06/1989

Contents

1 Introduction. **3**

2 The stable reduction at p of $X_0(p^2N)$. **9**

2.1 Construction of the stable model. 9
2.2 The inertia action. 15
2.3 A description of the special fibre. 16

3 The action of the Hecke algebra. **21**

3.1 Reduction to the special fibre. 22
3.2 The inertia decomposition. 24
3.3 Computation of $\mathbb{T}_m$ on the horizontal part. 29
3.4 An algorithm for $\mathbb{T}_2$ on $J_0(p^2)$. 32
3.5 Some examples. 36

4 Weil curves. **41**

4.1 Stable models of elliptic curves. 41
4.2 Reduction of Weil parametrizations. 45
4.3 Horizontal Weil curves. 50
4.4 Examples: conductor p^2. 54
4.5 Vertical Weil curves. 58
4.6 The constant c of a Weil curve. 59

Samenvatting. **71**

Dankwoord. **73**

Curriculum Vitae. **75**

Chapter 1

Introduction.

The aim of this thesis is to get information on the action of the Hecke algebra on modular forms, using the geometry of modular curves over suitable finite fields.

To be more precise, let M and k be positive integers and let $\Gamma_0(M)$ be the congruence subgroup of $SL_2(\mathbf{Z})$ consisting of matrices

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

with $c \equiv 0(M)$. Recall that $SL_2(\mathbf{Z})$ acts on the complex upper half plane $\mathbf{H}$ by fractional linear transformations. We define $S_k(M)$ to be the (finite dimensional) complex vector space of cuspforms of weight k and level M. By definition, elements of $S_k(M)$ are complex analytic functions on $\mathbf{H}$, satisfying certain vanishing conditions at the rational numbers and at "$i\infty$" (the "cusps" of $\Gamma_0(M)$) and transforming in a certain way with respect to the action of $\Gamma_0(M)$. These spaces $S_k(M)$ arise in the theory of automorphic representations of $GL_{2,\mathbf{Q}}$.

The spaces $S_k(M)$ are naturally equipped with a set of operators, called the Hecke operators. For every prime number p there is an operator T_p (if p does not divide M) or U_p (if p divides M). All the T_p and U_p together generate a commutative algebra called the Hecke algebra. The Hecke algebra respects the decomposition of $S_k(M)$ into its old part (coming from lower levels) and its new part (the orthogonal complement of the old part with respect to the Petersson inner product). The new part splits as an orthogonal sum of (one dimensional) eigenspaces. Each eigenspace then gives a system (a_p) of eigenvalues.

These systems (a_p) play an important role in the theory of two dimensional representations (complex, ℓ-adic and modular) of the Galois group of $\overline{\mathbf{Q}}$ over $\mathbf{Q}$. Given an eigenform, one knows (Kuga-Shimura, Deligne, Deligne-Serre) how to construct such a representation with the property that for almost all p, the Frobenius elements at p in the Galois group have trace a_p. In the opposite direction, there are conjectures of Shimura, Taniyama, Weil, Langlands and Serre.

A famous consequence of this construction of Deligne (and of Deligne's proof of the Weil conjectures) is the proof of the Ramanujan conjecture:

$$|\tau(p)| < 2p^{\frac{11}{2}}, \qquad \text{where} \quad q\prod_{n>0}(1-q^n)^{24} = \sum_{n>0}\tau(n)q^n.$$

Another surprising result is Ribet's proof (using ideas of Frey, Serre and Mazur) that the Taniyama-Weil conjecture implies Fermat's Lost Theorem.

One would like to have an algorithm (implemented on a computer) for decomposing the spaces $S_k(M)$ and computing the numbers a_p for small p. Theoretically, this can be done using the Selberg trace formula, but in practice it seems (Mestre) that even in the easiest case ($k = 2$ and M is prime) there is no hope to treat levels larger than 5,000. There are other methods, using Brandt matrices (Eichler, Pizer) or modular symbols (Manin, Tingley), but the computations in them are quite involved.

In 1985, Mestre and Oesterlé developed an extremely efficient algorithm (for $k = 2$ and M prime), known as the "graph method'. As Serre writes, the examples verified by Mestre (using the graph method) convinced him to take his conjecture (concerning mod p Galois representations) serious. The graph method has had also an application to the class number problem for imaginary quadratic fields.

One obtains the graph method by reduction mod p, as we will now explain. The quotient $\mathbf{H}/\Gamma_0(M)$ of the upper half plane by the action of $\Gamma_0(M)$ is a punctured Riemann surface. It can be compactified by adding a finite set of points (the cusps). The resulting compact Riemann surface is denoted by $X_0(M)(\mathbf{C})$, the corresponding complete, smooth, complex algebraic curve is the modular curve $X_0(M)_{\mathbf{C}}$. The genus of this curve is (very) roughly $M/12$. From now on we will only consider weight 2 forms, the reason for this is that $S_2(M)$ can be interpreted as the space of differential forms on $X_0(M)_{\mathbf{C}}$.

The program to be carried out is as follows: show that $X_0(M)_{\mathbf{C}}$ and the Hecke algebra are defined over $\mathbf{Q}$, construct a model over $\mathbf{Z}$ and find a faithful action of the Hecke algebra on some object in characteristic p. At first sight, it seems very improbable that something like this can be done: one should define $X_0(M)_{\mathbf{C}}$ by polynomial equations with coefficients in $\mathbf{Z}$ and then be able to say something about its reduction mod p. Nevertheless, working in this way, Kronecker derived his congruence formula:

$$(x-y^p)(x^p-y)=0,$$

describing the reduction mod p of $X_0(p)_{\mathbf{C}}$. It is clear, however, that this is not the way to proceed. The idea is to interpret the curves $X_0(M)_{\mathbf{C}}$ as moduli spaces for elliptic curves.

One can set up a bijection between $\mathbf{H}/\Gamma_0(M)$ and the set of isomorphism classes of complex elliptic curves with a cyclic subgroup of order M:

$$\mathbf{H}/\Gamma_0(M) \xrightarrow{\sim} \{(E,G)\}/\overset{\sim}{=}$$

$$z \mapsto (\mathbf{C}/(\mathbf{Z}\cdot 1+\mathbf{Z}\cdot z), \langle 1/M\rangle).$$

The right hand side of this bijection makes sense not only over $\mathbf{C}$ but over arbitrary algebraically closed fields, and even over arbitrary schemes. It seems reasonable now that the model over $\mathbf{Z}$ of $X_0(M)_{\mathbf{C}}$ could be provided by a compactified moduli space of elliptic curves with a certain level structure. In the late 50's, Igusa constructed such a moduli space over $\mathbf{Z}[1/M]$. Ten years later, Deligne extended this moduli space to one over $\mathbf{Z}[1/m]$, where m is the largest square dividing M. Another ten years later, using "Drinfeldian" level structures, Katz and Mazur obtained a moduli space $X_0(M)$ over $\mathbf{Z}$. The importance of all this work is that the moduli interpretation of $X_0(M)$ allows one to calculate rather explicitly the reduction mod p of $X_0(M)$. Igusa showed that for p not dividing M, the characteristic p fibre $X_0(M)_p$ is a smooth curve. For p not dividing N, Deligne gave a description of the reducible curve $X_0(pN)_p$. Katz and Mazur described in detail the reducible, non-reduced curves $X_0(p^nN)_p$.

The action of the Hecke operator T_l on $S_2(M)$ is induced by a correspondence:

$$\begin{array}{ccc} & X_0(Ml)_{\mathbf{C}} & \\ \swarrow & & \searrow \\ X_0(M)_{\mathbf{C}} & & X_0(M)_{\mathbf{C}} \end{array}$$

A differential form on $X_0(M)_{\mathbf{C}}$ is pulled back to $X_0(Ml)_{\mathbf{C}}$ along one of the two maps, and pushed down along the other. Doing the same with divisors gives an endomorphism (denoted T_l)of the jacobian variety $J_0(M)_{\mathbf{C}}$ of $X_0(M)_{\mathbf{C}}$. The correspondence inducing T_l extends to the models of Katz and Mazur over $\mathbf{Z}$. Restricting this correspondence to the characteristic p fibres (p a prime) gives an endomorphism T_l of the jacobian variety $J_0(M)_p^0$ of $X_0(M)_p$.

The action of the Hecke algebra on $J_0(M)_p^0$ is faithful if p^2 does not divide M, since then $J_0(M)_p^0$ is a semi-stable (commutative) algebraic group (an extension of an abelian variety by a torus). Eichler and Shimura proved their congruence relation "$T_l = F + V$" (for l not dividing M) by taking $p = l$. Mestre and Oesterlé obtained their graph method by studying the action of the Hecke algebra on the toric part of $J_0(pN)_p^0$ (p not a divisor of N).

In this thesis we study the next case: the action of the Hecke algebra on $J_0(p^2N)$, where p does not divide N. The first problem that arises is the "instability" of $J_0(p^2N)_p^0$: the interesting part of it is the unipotent part. This implies that the action of the Hecke algebra on $J_0(p^2N)_p^0$ is certainly not faithful. The solution to this problem is not to work over $\mathbf{Q}$, but over a suitably ramified (at p) extension over which $X_0(p^2N)$ has stable reduction (above p). In the next chapter we compute the stable reduction at p of $X_0(p^2N)$ together with the action of the inertia subgroup of the Galois group of the extension on it. This computation is quite standard for $p > 3$, because then the extension of $\mathbf{Q}$ that we need is only tamely ramified at p. This explains why we exclude the primes 2 and 3, and also why we cannot deal with levels p^nN with $n > 2$; because of wild ramification we do not know how to compute the stable reduction in these cases. Probably, the results of Chapter 2 will have more applications than those given in this thesis.

In Chapter 3 we study the action of the Hecke algebra on the stable reduction J_t^0 of $J_0(p^2N)$ at p. First we show that the action of the Hecke algebra on J_t^0 is induced by correspondences mod p. Then we start decomposing J_t^0 into parts that are stable under the Hecke action. The first decomposition is into a multiplicative, a horizontal and a vertical part. The horizontal part and the vertical part correspond to the two kinds of irreducible components of the stable reduction at p of $X_0(p^2N)$. In terms of representation theory, this decomposition into three parts is the decomposition of admissible representations of $GL_2(\mathbf{Q}_p)$ into the special, the cuspidal and the principal series representations. Each of these three parts is then decomposed with respect to the inertia action. The rest of Chapter 3 consists of the computation of the Hecke action on the horizontal part. The result is a "graph algorithm" very similar to that of Mestre and Oesterlé. The matrices we get are of the same size, but whereas the coefficients of their matrices are just non-negative integers (sums of 1's) ours are sums of $p+1$-th roots of unity. We end the chapter by giving a very explicit algorithm for computing the action of T_2 on $J_0(p^2)$, plus some examples.

It would be very interesting to obtain some kind of graph algorithm for the vertical part too. Another interesting problem is to do a similar computation for higher weights. It should also be remarked that Birch has recently produced a graph algorithm, using ternary quadratic forms. His algorithm is very fast, but gives only "half" of each $S_2(M)$ (the -1 eigenspace of the Atkin-Lehner involution W_M) and cannot treat square levels. It would be interesting to have a geometric interpretation of his algorithm.

In Chapter 4 we study Weil curves. By definition, these are the elliptic curves occurring in a decomposition (up to isogeny, over $\mathbf{Q}$) of some $J_0(M)_{\mathbf{Q}}$. According to the Taniyama-Weil conjecture, *every* elliptic curve over $\mathbf{Q}$ should be a Weil curve. Let the elliptic curve E be an isogeny factor of $J_0(M)_{\mathbf{Q}}$. Composing the canonical injection of $X_0(M)_{\mathbf{Q}}$ into $J_0(M)_{\mathbf{Q}}$ (use the cusp "∞") with the projection $J_0(M)_{\mathbf{Q}} \to E$ gives a non-constant map $X_0(M)_{\mathbf{Q}} \to E$. Such a non-constant map is called a Weil parametrization. These parametrizations provide a very powerful tool for the study of the arithmetic of Weil curves (for example in the recent work of Kolyvagin). We study Weil parametrizations by looking at their reductions mod p.

Let E be an elliptic curve inside $J_0(M)_{\mathbf{Q}}$ that does not occur in any $J_0(M')_{\mathbf{Q}}$ for proper divisors M' of M. The resulting parametrization ϕ :

$X_0(M)_{\mathbf{Q}} \to E$ is then called a *strong* Weil parametrization and according to work of Carayol, M is the conductor of E. This implies that the primes occurring in M are exactly the primes where E has bad reduction. If E has multiplicative reduction at a prime p, then p divides M exactly once. If E has additive reduction at a prime $p \neq 2, 3$, then p divides M exactly twice. This means that our knowledge of the stable reduction at p of $X_0(p^2N)$ is sufficient to study all Weil parametrizations at primes $p \neq 2, 3$.

First we study stable models for elliptic curves. In the second section we study the reduction mod p ($p > 3$) of a strong Weil parametrization, using stable models. Probably the computation concerning the inseparability degree of this parametrization mod p is the most technical part of this thesis. The rest of the chapter deals with strong Weil curves that have bad, but potentially good reduction at a prime $p > 3$. It turns out that there are two kinds of these, called horizontal or vertical, according to the kind of irreducible components that parametrize them mod p. We study them seperately. In the fourth section we give some examples of horizontal curves of conductor p^2 (these are the Weil curves that can be detected by the graph algorithm of Chapter 3).

Finally, in the last section, we derive some results concerning the constant "c" attached to a strong Weil curve E. Manin conjectured that $c = 1$. It is known that c is a positive integer and Mazur proved that only 2 and primes where E has additive reduction can divide c. Our methods show that primes $p > 7$ where E has additive reduction divide c at most once, and in fact, for most of the possible reduction types (= Kodaira symbols), not (Theorem 4.6.3 and the remarks following this theorem). It might well be that a computation involving the period lattices of normalized newforms can solve the problem in the case of potentially good, ordinary reduction of type II, III or IV. It should also be tried to get bounds on the exponents of 2, 3, 5 and 7 in c.

Chapter 2

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

Let $p > 3$ be a prime, and let N be a positive integer not divisible by p. The first part of this chapter is a review of the construction, given in [Ed 1], of the stable reduction mod p of $X_0(p^2N)$. In order to obtain this stable model we have to perform a ramified base change. After adjoining some roots of unity, this base change is Galois. The inertia subgroup of the Galois group then acts on the special fibre of the stable model. The second part of this chapter deals with the computation of this action.

2.1 Construction of the stable model.

In order to explain the construction of the stable model of $X_0(p^2N)$ at p, it is better to consider the following more general situation. Let S be the spectrum of an excellent discrete valuation ring with perfect residue field. (We demand the ring to be excellent because we want the operations "normalization" and "completion" to commute, cf. [Gro 1] IV 7.8.2 and 7.8.3.1(vii)). Let s be the closed point of S and η be the generic point. Let $\mathcal{C} \longrightarrow S$ be a curve: $\mathcal{C} \longrightarrow S$ is proper, flat, of relative dimension one, $\mathcal{C}_\eta$ is smooth over η and geometrically irreducible. In addition we suppose $\mathcal{C}$ to be regular.

Under the hypotheses above, the irreducible components of $\mathcal{C}_s$ are Cartier divisors on $\mathcal{C}$. By repeated blow ups in closed points of $\mathcal{C}_s$ we can achieve that $\mathcal{C}_s$ is a Cartier divisor on $\mathcal{C}$ with normal crossings. Let n be the least common multiple of the multiplicities of the irreducible components of $\mathcal{C}_s$, and let π_0 be a uniformizer on S. Let T be $S[\pi]$, with $\pi^n = \pi_0$, thus we have $T \longrightarrow S$ totally ramified of degree n. Now we consider $\widetilde{\mathcal{C}_T}$, the normalization of the pullback of $\mathcal{C}$ to T. Let t be the closed point of T.

Proposition 2.1.1 *If n is invertible on S, then the geometric fibre $\widetilde{\mathcal{C}_{T,\bar{t}}}$ of $\widetilde{\mathcal{C}_T}/T$ is a reduced, connected curve whose singularities are ordinary double points.*

Proof. By replacing S by the completion of its strict henselization, we reduce to the case that S is complete and $k(s)$ algebraically closed. We will check that $\widetilde{\mathcal{C}_{T,t}}$ is reduced and has only ordinary double points. In order to do this we compute the complete local rings of $\widetilde{\mathcal{C}_T}$ at closed points. Let $x \in \mathcal{C}(s)$, then the normalization of $\widehat{\mathcal{O}}_{\mathcal{C},x} \otimes_{\mathcal{O}_S} \mathcal{O}_T$ is given by:

$$\widehat{\mathcal{O}}_{\mathcal{C},x} \tilde{\otimes}_{\mathcal{O}_S} \mathcal{O}_T \quad = \quad \bigoplus_{y \mapsto x} \widehat{\mathcal{O}}_{\widetilde{\mathcal{C}_T},y}$$

where the summation is over the $y \in \widetilde{\mathcal{C}_T}(t)$ mapping to x. The next step is to describe $\widehat{\mathcal{O}}_{\mathcal{C},x}$ explicitly by equations. There are two cases to be distinguished. In the first case only one branch of $\mathcal{C}_s$ passes through x. Let a be its multiplicity and let $x, y \in \widehat{\mathcal{O}}_{\mathcal{C},x}$ be a set of parameters such that x is an equation for this branch. Then in $\widehat{\mathcal{O}}_{\mathcal{C},x}$ we have: $\pi_0 = x^a u$, with u a unit. Since a is invertible on S we can change x by an a-th root of u in order to obtain: $\pi_0 = x^a$. It follows that in this case: $\widehat{\mathcal{O}}_{\mathcal{C},x} = \mathcal{O}_S[[x,y]]/(x^a - \pi_0)$. In the second case there are two branches passing (transversally) through x, let the multiplicities be a and b and choose equations x and y. This time we arrive at: $\widehat{\mathcal{O}}_{\mathcal{C},x} = \mathcal{O}_S[[x,y]]/(x^a y^b - \pi_0)$. The tensor product $\widehat{\mathcal{O}}_{\mathcal{C},x} \otimes_{\mathcal{O}_S} \mathcal{O}_T$ is given by:

$$\mathcal{O}_T[[x,y]]/(x^a - \pi^n) \text{ resp. } \mathcal{O}_T[[x,y]]/(x^a y^b - \pi^n).$$

The normalizations of these rings can be easily computed, see for example [Ed 1], 2.2. The result of these computations show that indeed $\widetilde{\mathcal{C}_{T,t}}$ is reduced and has only ordinary double points as singularities.

Remarks.

1. If the genus of $\mathcal{C}_\eta$ is at least 2, one gets the stable model (in the sense of [De-Mu]) of $\mathcal{C}_\eta$ over T by contracting the projective lines in $\widetilde{\mathcal{C}_T}_{,\bar{t}}$ intersecting the rest of $\widetilde{\mathcal{C}_T}_{,\bar{t}}$ in less than 3 points. By contracting and blowing up one also obtains the minimal model of $\mathcal{C}$ over T (n.b. $\widetilde{\mathcal{C}_T}$ itself may not be regular).

2. The computations of the normalizations give the morphism $\widetilde{\mathcal{C}_T} \longrightarrow \mathcal{C}_T$ on the complete local rings. In particular, one knows the ramification structure of $\widetilde{\mathcal{C}_T}_{,t} \longrightarrow \mathcal{C}_{s,\mathrm{red}}$.

3. The choice of the uniformizing element π_0 on S is unimportant, since all totally ramified extensions of degree n of S are isomorphic over the strict henselization of S.

4. On the contrary, if n is not invertible on S, there are lots of non-isomorphic (wildly ramified) extensions of the same degree. If one knows the acion of the inertia subgroup of $\mathrm{Gal}(\bar{\eta}/\eta)$ on $\mathrm{H}^1(\mathcal{C}_{\bar{\eta}}, \mathbf{Q}_\ell)$ one can pick the right extension. In the case of modular curves (of arbitrary level) this action is known. The problem is the description of the rings $\widehat{\mathcal{O}}_{\mathcal{C},x}$.

2.1.2 The curve $X_0(p^2N)$.

We return to the modular curves $X_0(p^2N)$. To be precise, for any positive integer M we define $X_0(M)$ to be the compactified coarse moduli scheme over $\mathbf{Z}$ associated to the moduli problem $[\Gamma_0(M)]$, see [Ka-Ma] 8.6. Let S be the spectrum of the Witt vectors of $\overline{\mathbf{F}}_p$. In order to apply Proposition 2.1.1 we need a regular model over S, but $X_0(p^2N)_S$ is not necessarily regular: it can have some quotient singularities. There are two ways to get around this problem. The first one is to use the minimal resolution of $X_0(p^2N)_S$ (described in [Ed 1]1). The second one is to introduce a suitable extra level structure (e.g. $[\Gamma(3)^{\mathrm{can}}]$), to apply Proposition 2.1.1 to the associated moduli scheme, and to obtain the stable model of $X_0(p^2N)_S$ as a quotient. The second method is the one followed in [Ed 1] 2. The details of the computations can be found in loc. cit. The multiplicities of the components in the special fibre of the normal crossings model are 1, $p-1$ and $p+1$, so $n = \frac{p^2-1}{2}$ and T is obtained by extracting the n-th root of p: $p = \pi^n$.

The next problem is to determine the irreducible components of the stable reduction. This problem is of a more global nature, and considering only complete local rings will not suffice. At this point we must distinguish between the "horizontal" and "vertical" components. The components of the stable reduction originating from components in the normal crossings model having multiplicity $p+1$ are called horizontal, the others vertical. The vertical components originating from multiplicity $p-1$ components are called central, the others outer. The reason for all this terminology is clear from the pictures in [Ed 1] 2.

2.1.3 Horizontal components.

In this section we redo the computation of the horizontal components. The reason for this is that we want to get better coordinates for these components than those given in [Ed 1] 2.2.4. Let x be a supersingular point in $X_0(p^2N)(s)$. We interpret the moduli problem $[\Gamma_0(p^2N)]$ as classifying pairs $(\phi : E_1 \to E_2, G)$, where ϕ is a cyclic isogeny of degree p^2 and G a cyclic subgroup scheme of order N of E_1. Then x corresponds to a pair $([p] : E \to E, G)$, with $E/\overline{\mathbf{F}_p}$ supersingular. We choose a coordinate t of the universal formal deformation space of (E, G) in $[\Gamma_0(N)]$. We consider the map $[\Gamma_0(p^2N)] \to [\Gamma_0(N)] \times [\Gamma_0(N)]$ given by $(\phi : E_1 \to E_2, G) \mapsto ((E_1, G), (E_2, \phi G))$. According to [Ka-Ma] Thm.13.4.7, this map is a formally closed immersion at x, and if we let x and y be t on the first and second factor of $[\Gamma_0(N)] \times [\Gamma_0(N)]$, the image of $[\Gamma_0(p^2N)]$ is given by an equation $f = f_0 + pf_1$ in $W[[x, y]]$, with $f_0 = (x - y^{p^2})(x - y)^{p-1}(x^{p^2} - y)$ and f_1 a unit. Here $W = \mathcal{O}_S(S) =$ the ring of Witt vectors of $\overline{\mathbf{F}_p}$. The universal formal deformation space of x is thus given by $W[[x, y]]/(f)$. Clearly, its special fibre does not have normal crossings, so we blow up in x. An affine open part of the result is $W[v][[x]]/(\tilde{f}_0 + p\tilde{f}_1)$, with $\tilde{f}_0 := f_0(x, vx)$, $\tilde{f}_1 := f_1(x, vx)$. Now we set $W_1 := W[\pi_1]$, with $\pi_1^{p+1} = p$. After extension of scalars to W_1 we have: $W_1[v][[x]]/(\tilde{f}_0 + \pi_1^{p+1}\tilde{f}_1)$. We blow this up along the ideal (x, π_1), i.e. we write $x := u\pi_1$. This gives:

$$\widehat{W_1[v, u]}/(u^{p+1}((u\pi_1)^{p^2-1} - v)(1 - v)^{p-1}(1 - v^{p^2}(u\pi_1)^{p^2-1}) + \tilde{\tilde{f}}_1)$$

where the completion is with respect to the principal ideal $(u\pi_1)$, and $\tilde{\tilde{f}}_1 = \tilde{f}_1(v, u\pi_1) = f_1(u\pi_1, vu\pi_1)$. The curve over $\overline{\mathbf{F}_p}$ we are looking for is now given by $\pi_1 = 0$. Substituting $\pi_1 = 0$ in the equation above yields:

$$u^{p+1}(-v)(1-v)^{p-1} + f_1(0,0) = 0.$$

This is an affine, singular model of the (smooth) horizontal component (at x). The next thing to do is to get better coordinates for this curve.

We set $a := f_1(0,0) \in \overline{\mathbf{F}}_p^*$. We leave it to the reader to check that after the following substitutions: $v := 1 - v_1$, $u := u_1 v_1$, $a := \frac{1}{2} a_1^{-1}$, $v_1 := v_2 - a_1 u_1^{p+1}$, $v_2 := v_3 a_1 u_1^{\frac{p+1}{2}}$ we obtain the equation:

$$v_3^2 = u_1^{p+1} + 4a. \tag{2.1.3.1}$$

This shows that the horizontal component is a double cover of $\mathbf{P}^1$, ramified in $p+1$ points. We will compute the various actions on the horizontal components in these coordinates.

As a first example, let us compute the action of $\mathrm{Aut}(x)$, since the horizontal component in the stable model of $X_0(p^2N)$ is the quotient by this action. First we compute the action of $\mathrm{Aut}(E)$ on its deformation space. Since the automorphism $[-1]$ lifts to every deformation, its action on the deformation space is trivial. There are only two elliptic curves over $\overline{\mathbf{F}}_p$ with automorphisms other than $[\pm 1]$.

1. $j(E) = 0$, E is given by the equation:$y^2 = x^3 - 1$, we have:

$$\mu_6(\overline{\mathbf{F}}_p) \tilde{\to} \mathrm{Aut}(E): \ \zeta \mapsto \begin{cases} x & \mapsto & \zeta^{-2} x \\ y & \mapsto & \zeta^3 y \end{cases} \quad (\text{note: } \zeta^*(\frac{dx}{y}) = \zeta \frac{dx}{y})$$

   The universal formal deformation is given by: $y^2 = x^3 + tx - 1$, and
$$\zeta \in \mu_6(\overline{\mathbf{F}}_p) \text{ acts by: } \begin{cases} y & \mapsto & \zeta^3 y \\ x & \mapsto & \zeta^{-2} x \\ t & \mapsto & \zeta^2 t, \end{cases} \quad \text{since this preserves the equation.}$$

2. $j(E) = 12^3$, $\mathrm{Aut}(E)$ is now isomorphic to $\mu_4(\overline{\mathbf{F}}_p)$, and it acts on the

universal formal deformation $y^2 = x^3 - x + t$ by:

$$\zeta \in \mu_4(\overline{\mathbf{F}}_p) : \begin{cases} y & \mapsto & \zeta y \\ x & \mapsto & \zeta^2 x \\ t & \mapsto & \zeta^2 t. \end{cases}$$

Since $[\Gamma_0(N)]_S$ is etale over $[Ell]$, the coordinate t of the deformation space of E is a coordinate on $[\Gamma_0(N)]_S$ at (E, G). It follows that the action of $\zeta \in \mathrm{Aut}(E)$ on $W[[x,y]]/(f)$ is given by: $x \mapsto \zeta^2 x$, $y \mapsto \zeta^2 y$. Peforming all the following substitutions:

$$\begin{array}{llll} v = y/x, & u = x/\pi_1, & v_1 = 1 - v, & u_1 = uv_1, \\ a_1 = 1/2a, & v_2 = v_1 + a_1 u_1^{p+1}, & v_3 = v_2/a_1 u_1^{\frac{p+1}{2}} & \end{array} \tag{2.1.3.2}$$

one finds that the action of ζ on the horizontal component is given by:

$$\begin{cases} u_1 & \mapsto & \zeta^2 u_1 \\ v_3 & \mapsto & v_3. \end{cases} \tag{2.1.3.3}$$

Of course, this situation only occurs if such a curve E is supersingular ($p \equiv -1(4)$ for $j(E) = 12^3$, and $p \equiv -1(3)$ for $j(E) = 0$), and has a $G \in [\Gamma_0(N)](E)$ fixed by the automorphism group.

2.1.4 The vertical components.

Since these components come from the multiplicity $p-1$ component in $X_0(p^2N)_s$, it is sufficient to consider the normalization of $X_0(p^2N)$ after adjoining the p-th roots of unity: $W[\zeta_p]$ is ramified of degree $p-1$ over W. In [Ed 1] 2.3.2 this normalization is obtained as a quotient of

$$\overline{\mathrm{M}}([\Gamma_0(N)], [\Gamma(p^2)^{\mathrm{can}}]).$$

It would have been easier to use the isomorphism:

$$[\Gamma(p)]/\begin{pmatrix} * & 0 \\ 0 & * \end{pmatrix} \xrightarrow{\sim} [\Gamma_0(p^2)]$$

described in [Ka-Ma] 11.3.5. The advantage is that the group one has to divide out has order prime to p, and that the number of components to deal with is smaller. This method works without any problem for arbitrary levels.

2.2 The inertia action.

Let S still denote the spectrum of the Witt vectors of $\overline{\mathbf{F}}_p$ and let $X \to S$ be the normal crossings model of $X_0(p^2N)_S$ (possibly with some extra level structure). The stable model of X was constructed as the normalization $\widetilde{X_T}$ of X_T, where $T = S[\pi]$, $\pi^n = p$, $n = \frac{p^2-1}{2}$. Since we have the n-th roots of unity on S, the extension $T \to S$ is Galois with group $\mu_n(S) = \mu_n(\mathbf{F}_{p^2})$, where ζ acts by: $\pi \mapsto \zeta\pi$. We let this group act on $X_T = X \times_S T$ via its action on T. It follows that $\mu_n(S) = \mu_n(\mathbf{F}_{p^2})$ also acts on the normalization $\widetilde{X_T}$, and since the morphism $\widetilde{X_T} \to T$ is equivariant, we get a linear action on the special fibre $\widetilde{X_{T,t}}$ (with "linear" we mean that this action is trivial on the base).

On the horizontal components this action is very easy to compute. Let ζ be in $\mu_n(\mathbf{F}_{p^2})$. In 2.1.3 we had $\pi_1^{p+1} = p$, so we let $\pi_1 = \pi^{\frac{p-1}{2}}$. Then ζ acts on π_1 by: $\pi_1 \mapsto \zeta^{\frac{p-1}{2}}\pi_1$. In the notation of 2.1.3, ζ acts trivially on the coordinates x and y. Now all one has to do is to go through all the substitutions 2.1.3.2 and see what comes out. The result is:

$$\zeta : \begin{cases} u_1 & \mapsto & \zeta^{-\frac{p-1}{2}}u_1 \\ v_3 & \mapsto & \zeta^{\frac{n}{2}}v_3 \end{cases} \tag{2.2.0.1}$$

Now we discuss the vertical components. The outer two vertical components have a trivial inertia action, since they were already reduced over S. We want to identify the two central vertical components with

$$\overline{\mathrm{M}}([\Gamma_0(N)], [Ig(p)/\pm 1]).$$

The problem is that there is no privileged identification: it can always be changed by an element of $\mathrm{Aut}([Ig(p)/\pm 1]/[Ell]) = \mu_{p-1}(\mathbf{F}_p)/\pm 1$. We prefer to make the identifications in the following way: for one of the two components we choose an arbitrary one. Now we look for an operator bringing us from this component to the other. If $p \equiv -1(4)$ then the Atkin-Lehner involution W_{p^2} does the job (this can be easily seen from the computations with the complete local rings). If $p \equiv 1(4)$ then we are in trouble, since then W_{p^2} stabilizes the two components. In this case we choose a non-square $d \in \mathbf{F}_p$. Viewed as an element of the inertia group, d interchanges the two components. Using these identifications we get the following inertia action:

$$\begin{array}{lll} p \equiv -1(4): & \zeta \in \mu_{p-1}(\mathbf{F}_p): & (\zeta^{\frac{p+1}{4}}, \zeta^{\frac{p-1}{2}}) \\ & \mathrm{W}_{p^2}: & (1,-1) \\ p \equiv 1(4): & \zeta \in \mu_{p-1}(\mathbf{F}_p): & \begin{cases} (\sqrt{\zeta}, 1) & \text{if } \zeta \text{ is square} \\ (\sqrt{\zeta d^{-1}}, -1) & \text{if } \zeta \text{ is not square} \end{cases} \\ & \mathrm{W}_{p^2}: & (\sqrt{-1}, 1) \end{array} \tag{2.2.0.2}$$

Here we have written the disjoint union of the two components as:

$$\overline{\mathrm{M}}([\Gamma_0(N)], [Ig(p)/\pm 1]) \times \mu_2(\mathbf{F}_p) \tag{2.2.0.3}$$

and the action on the factor $\mu_2(\mathbf{F}_p)$ is multiplication.

Remarks.

1. The ambiguity in the square roots in the formulas above is harmless, since the action of -1 on $[Ig(p)/\pm 1])$ is trivial.

2. From the formulas above we see that in both cases the involution coincides with the element -1 from the inertia group. One can also see this as follows: W_{p^2} commutes with the inertia action and acts trivially on the corresponding quotient (the (1,1)-component in $X_0(p^2N)$). These two facts force W_{p^2} to coincide with some element of the inertia group, but since it is an involution, there is only only one possibility.

2.3 A description of the special fibre.

In this section we suppose that ± 1 are the only automorphisms of points in $X_0(N)(s)$. If we wouldn't do this, the number of formulas to write down would be much larger. Instead, we will compute the actions of the automorphism groups of points in $X_0(M)(s)$, where M is a divisor of N (in that case we view the complete local rings of $X_0(N)$ as deformation spaces of the points in $X_0(M)(s)$). In order to get the formulas in all cases, one then only has to divide out by these actions. The reader is now invited to have a look at the figure on page 18. This figure represents the special fibre of the stable model of $X_0(p^2N)_S$. Here follows a list of its properties that we have been computing until now.

2.3.1 The curve itself.

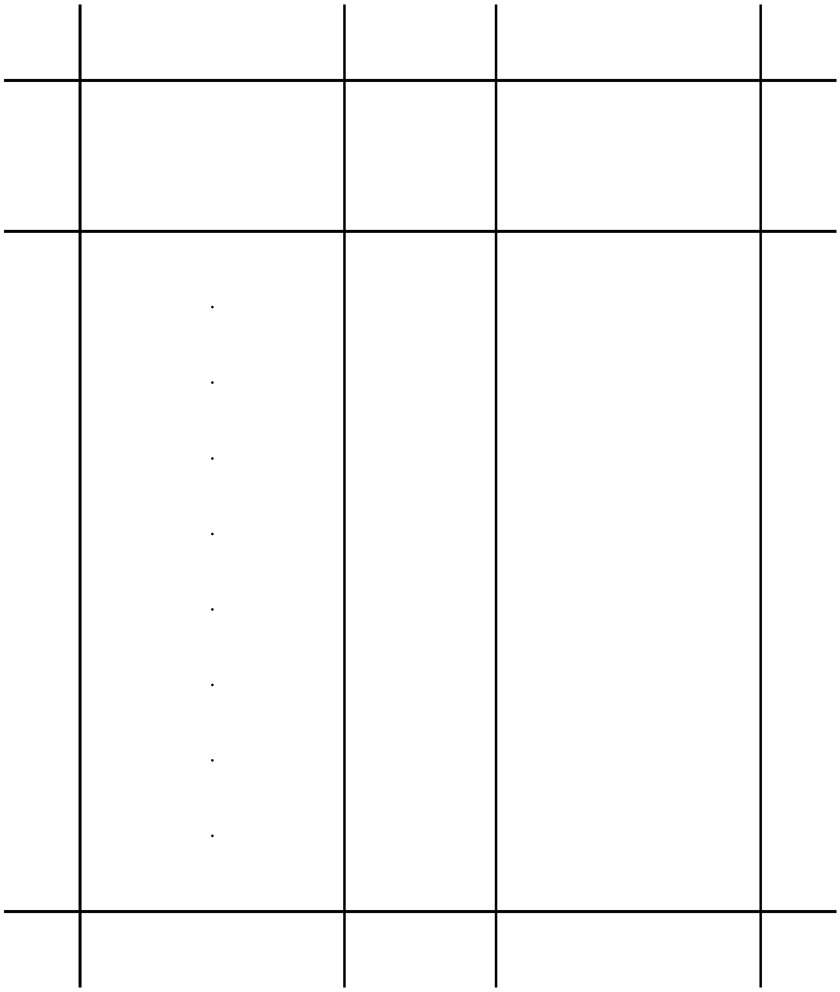
The outer two vertical components are the (2,0) and (0,2) components from $X_0(p^2N)_s$. These curves are both isomorphic to $X_0(N)_s$, however, the usual morphism $X_0(p^2N) \to X_0(N)$ is an isomorphism on one of them and the composition of two Frobenii on the other. The two central vertical components are both isomorphic (over $X_0(N)_s$) to $\overline{\mathrm{M}}([\Gamma_0(N)],[Ig(p)/\pm 1])$. This last curve has degree $(p-1)/2$ over $X_0(N)_s$ and is ramified exactly over the supersingular points. The ramification is total, hence the supersingular points on $\overline{\mathrm{M}}([\Gamma_0(N)],[Ig(p)/\pm 1])$ correspond bijectively to those on $X_0(N)_s$. The horizontal components are all isomorphic to the smooth complete hyperelliptic curve given by the equation:

$$y^2 = x^{p+1} + 1. \tag{2.3.1.1}$$

These coordinates are obtained by scaling the u_1, v_3 of 2.1.3.1. The horizontal components are in bijection with the supersingular points on $X_0(N)_s$. These components are contracted by the usual morphisms $X_0\widetilde{(p^2N)}_T \to X_0(N)_T$.

The glueing relations are as follows. Let $x \in X_0(N)(s)$ be a supersingular point. Then the two points at infinity ($x, y = \infty$) of the corresponding horizontal component must be attached to the points x on the outer components. The two points $x = 0, y = \pm 1$ must be attached to the two points on the central vertical components lying over x. Up to automorphisms of the horizontal component this is well defined. Later, when discussing the Hecke action, we will describe the glueing somewhat more canonically.

Figure 2.1: A picture of the stable reduction of $X_0(p^2N)$ at p.



2.3.2 The complete local rings of the stable model.

These 2-dimensional local rings are all regular, except at the points where the horizontal components intersect the *outer* two vertical components. There the ring has a singularity of type $\mathrm{A}_{\frac{p-1}{2}-1}$, i.e. it is of the type

$$W[\pi][[x,y]]/(xy-\pi^{\frac{p-1}{2}}).$$

2.3.3 The inertia action.

The inertia group is $\mu_n(\mathbf{F}_{p^2})$ (n.b. $n=\frac{p^2-1}{2}$). An element ζ acts on the uniformizer π of the base by: $\pi\mapsto\zeta\pi$. In the sequel we will encounter some other actions, so we need some notation. Let $\chi:\mu_n(\mathbf{F}_{p^2})\to\mu_n(\mathbf{F}_{p^2})$ be the identity. We can now say that $\mu_n(\mathbf{F}_{p^2})$ acts on π by χ.

The action of an element ζ on the horizontal components (eq. 2.3.1.1) is given by:

$$\begin{cases} x & \mapsto & \zeta^{-\frac{p-1}{2}}x \\ y & \mapsto & \zeta^{\frac{n}{2}}y. \end{cases} \tag{2.3.3.1}$$

The action of $\mu_n(\mathbf{F}_{p^2})$ on the (co)tangent space to the horizontal component at the points of intersection with the outer components is given by $\chi^{\frac{p-1}{2}}$. Let x be a point of intersection of a horizontal with a central vertical component. The stabilizer group of such a point is $\mu_{\frac{n}{2}}(\mathbf{F}_{p^2})$. The action of $\mu_{\frac{n}{2}}(\mathbf{F}_{p^2})$ on the tangent space at x to the horizontal component is by $\chi^{-\frac{p-1}{2}}$ (the restriction of χ to $\mu_{\frac{n}{2}}(\mathbf{F}_{p^2})$ is still denoted by χ).

As in formula 2.2.0.3, we write the disjoint union of the two central vertical components as:

$$\overline{\mathrm{M}}([\Gamma_0(N)],[Ig(p)/\pm 1])\times\mu_2(\mathbf{F}_p).$$

The action of $\mu_n(\mathbf{F}_{p^2})$ on this disjoint union is given by:

$$\begin{array}{ll} (\chi^{\frac{(p+1)^2}{8}},\chi^{\frac{n}{2}}) & \text{if } p\equiv -1(4) \\ ((\chi^{\frac{p+1}{2}}d^{\frac{\chi^{\frac{n}{2}}-1}{2}})^{\frac{1}{2}},\chi^{\frac{n}{2}}) & \text{if } p\equiv 1(4), \end{array}$$

where d is some fixed non-square in $\mathbf{F}_p^*$ (compare 2.2.0.2). The stabilizer group of either of the two components is $\mu_{\frac{n}{2}}(\mathbf{F}_{p^2})$. Its action is given by

$\chi^{\frac{p+1}{4}}$. The action of $\mu_{\frac{n}{2}}(\mathbf{F}_{p^2})$ on the tangent space at a supersingular point to these vertical components is by $\chi^{\frac{p+1}{2}}$.

2.3.4 The action of W_{p^2}.

The operator W_{p^2} preserves the horizontal components, in the coordinates 2.3.1.1 its action is given by:

$$\begin{cases} x & \mapsto & -x \\ y & \mapsto & (-1)^{\frac{p-1}{2}}y. \end{cases} \tag{2.3.4.1}$$

One sees that the action of W_{p^2} on the horizontal components is not by an element of the inertia group (-1 in $\mu_n(\mathbf{F}_{p^2})$ acts by $(-1)^{\frac{p+1}{2}}$ on y). This corresponds to the fact that W_{p^2} doesn't act trivially on the horizontal components in the normal crossings model.

The action of W_{p^2} on the central vertical components is given by:

$$\begin{cases} (1,-1) & \text{if } p \equiv -1(4) \\ (\sqrt{-1},1) & \text{if } p \equiv 1(4). \end{cases} \tag{2.3.4.2}$$

The action of W_{p^2} on these vertical components coincides with the action of -1 in $\mu_n(\mathbf{F}_{p^2})$.

2.3.5 The action of $\mathrm{Aut}(E)$.

Let $x \in X_0(N)(s)$ be a supersingular point, corresponding to a pair (E,G). We will now view the complete local ring of $X_0(N)_S$ at x as the deformation space of E. In this way we get an action of $\mathrm{Aut}(E)$ on the formal completion of the stable model of $X_0(p^2N)$ along the horizontal component corresponding to x. We give this action on the horizontal component itself. Let e be the order of $\mathrm{Aut}(E)$. The action of $\mathrm{Aut}(E)$ on the tangent space of E gives an isomorphism $\mathrm{Aut}(E)\tilde{\to}\mu_e(\mathbf{F}_{p^2})$. The action of $\mathrm{Aut}(E)$ on the horizontal component is via the following morphism to the inertia group:

$$\begin{array}{ccccc} \mathrm{Aut}(E) & \tilde{\to} & \mu_e(\mathbf{F}_{p^2}) & \to & \mu_n(\mathbf{F}_{p^2}) \\ & & \zeta & \mapsto & \zeta^{-2}. \end{array} \tag{2.3.5.1}$$

Chapter 3

The action of the Hecke algebra.

As in Chapter 2, let $p > 3$ be a prime and N a positive integer not divisible by p. Let $X \to T$ be the stable model of $X_0(p^2N)$ over T as described and constructed in Chapter 2. Let $J \to T$ be the Néron model of the jacobian J_η of the generic fibre X_η of X. In this chapter we study the action of the Hecke algebra on the special fibre J_t of J. First we compute J_t and the action of $\mathbb{T}_m$ (m prime to pN) on it in terms of the stable models of $X_0(p^2N)$ and $X_0(p^2Nm)$. In the second section we decompose J_t with respect to the inertia action. This decomposition is stable under the action of the Hecke algebra. In the third section we compute the action of $\mathbb{T}_m$ on the horizontal part of J_t in terms of the correspondence:

$$\begin{array}{ccc} & X_0(Nm)_t & \\ \swarrow & & \searrow \\ X_0(N)_t & & X_0(N)_t \end{array}$$

restricted to the first infinitesimal neighborhood of the supersingular locus. We describe the effect of this correspondence on tangent vectors in terms of m-isogenies between supersingular elliptic curves. Then we give an algorithm for computing $\mathbb{T}_2$ in the case $N = 1$ (i.e. on $J_0(p^2)$).

3.1 Reduction to the special fibre.

Let m be prime to pN. Every cyclic isogeny of degree p^2Nm between elliptic curves (over an arbitrary base scheme): $\phi_{p^2Nm} : E_1 \to E_2$ has unique factorizations (up to isomorphism):

$$E_1 \xrightarrow{\phi_{p^2N,1}} E_3 \xrightarrow{\phi_{m,2}} E_2 \qquad\qquad E_1 \xrightarrow{\phi_{m,1}} E_4 \xrightarrow{\phi_{p^2N,2}} E_2$$

where $\phi_{*,i}$ has degree $*$ (cf. [Ka-Ma] 6.7). On the level of moduli problems this gives two morphisms:

$$\mathrm{S} : [\Gamma_0(p^2Nm)] \to [\Gamma_0(p^2N)] : \quad \mathrm{S}(\phi_{p^2Nm}) = \phi_{p^2N,1}$$

$$\mathrm{T} : [\Gamma_0(p^2Nm)] \to [\Gamma_0(p^2N)] : \quad \mathrm{T}(\phi_{p^2Nm}) = \phi_{p^2N,2},$$

and an involution:

$$\mathrm{W}_m : [\Gamma_0(p^2Nm)] \to [\Gamma_0(p^2Nm)] : \quad \mathrm{W}_m(\phi_{p^2Nm}) = \phi_{p^2N,1}\phi^t_{m,1}.$$

By construction we have: $\mathrm{T} = \mathrm{SW}_m$. We obtain induced morphisms:

$$\mathrm{S}, \mathrm{T} : X_0(p^2Nm) \to X_0(p^2N) \quad \mathrm{W}_m : \ X_0(p^2Nm) \to X_0(p^2Nm)$$

(the morphisms extend over the cusps because of [De-Ra] IV Prop. 3.16, 3.18,Prop. 3.19, ex. 4.4). Over $\mathbf{Q}$, we get the endomorphism $\mathbb{T}_m = \mathrm{T}_*\mathrm{S}^*$ of $J_0(p^2N)_{\mathbf{Q}}$. Note that for non-squarefree m this $\mathbb{T}_m$ is *not* the standard one that has eigenvalue a_m when acting on an eigenform $\sum a_n q^n$.

Let $X \to T$, $Y \to T$ be the stable models over T of $X_0(p^2N)$ and $X_0(p^2Nm)$ respectively. As before, t and η denote the closed and generic point of T. Let J_η be $\mathrm{Pic}^0_{X_\eta/\eta}$, and J its Néron model over T. By pullback to η we get $\mathbb{T}_m \in \mathrm{End}(J_\eta)$, by the Néron property, $\mathbb{T}_m$ extends to $\mathbb{T}_m \in \mathrm{End}_T(J)$. Restricting this $\mathbb{T}_m$ to the connected component of the special fibre, we arrive at $\mathbb{T}_m \in \mathrm{End}_t(J^0_t)$. We want to describe this endomorphism of J^0_t in terms of X_t and Y_t.

Since X_t is reduced and connected, $X \to T$ is cohomologically flat ([Ra 1] 1.4) and satisfies the property $(N)^*$ ([Ra 1] 6.1.4, 6.1.6). By [Ra 1] Thm. 8.2.1 $\mathrm{Pic}^0_{X/T}$ is represented by a smooth group scheme over T. Its special fibre $\mathrm{Pic}^0_{X_t/t}$ is semiabelian (this results from the fact that the only singularities of X_t are ordinary double points, cf. [Sz] I Prop. 5.7). It follows that $\mathrm{Pic}^0_{X/T}$ is the connected component J^0 of J (cf. [Sz] I Prop. 5.4).

Proposition 3.1.1 $J^0 = \mathrm{Pic}^0_{X/T}$, *and* $J^0_t = \mathrm{Pic}^0_{X_t/t}$.

By construction, the morphisms S, W_m and T over $\mathbf{Z}$ induce morphisms S, W_m and T over T. We want to show that the endomorphism T_m of J^0_t is given by the correspondence induced by S and T over t. In order to do this we try to extend T_m to an endomorphism of the functor $\mathrm{Pic}^0_{X/T}$. The pullback construction of line bundles gives $\mathrm{S}^* : \mathrm{Pic}^0_{X/T} \to \mathrm{Pic}^0_{Y/T}$. If $\mathrm{T} : Y \to X$ is finite and flat, then the norm construction ([Gro 1] II 6.5) of line bundles gives $\mathrm{T}_* : \mathrm{Pic}^0_{Y/T} \to \mathrm{Pic}^0_{X/T}$ and T_m would be given by $\mathrm{T}_*\mathrm{S}^*$. Since $\mathrm{T} = \mathrm{SW}_m$ and W_m is an isomorphism, T is finite and flat if and only if S is. The finiteness of S is a consequence of its construction. However, S is only flat at points y in $Y(t)$ with $\mathrm{Aut}(y) = \mathrm{Aut}(\mathrm{S}(y))$ (then the morphism on complete local rings is an isomorphism). We have now proved the following proposition.

Proposition 3.1.2 *If* $\mathrm{Aut}(x) = \{\pm 1\}$ *for all* $x \in X_0(N)(t)$, *then the endomorphism* T_m *of* J^0_t *is given by the correspondence* $\mathrm{S}, \mathrm{T} : Y_t \to X_t$. *The morphisms S and T in this correspondence are finite and flat.*

In the case that there are extra automorphisms we can change X and Y by some blow ups in order to get finite flat morphisms as in [Ed 2] 4.1, but this is a bit messy to write down, and moreover, this would introduce non-reduced special fibres.

Let Z be the stable model over T of $\overline{\mathrm{M}}([\Gamma_0(p^2N)], [\Gamma(m)])$. Then we have a diagram:

$$\begin{array}{ccc} Z & & \\ \downarrow & \searrow & \\ Y & \stackrel{\mathrm{S}}{\to} & X \end{array}$$

where the diagonal arrow is the quotient by the action of $G := GL_2(\mathbf{Z}/m)$ on Z, and the vertical arrow the quotient by the upper triangular subgroup B of G. These quotients commute with arbitrary base changes $U \to T$, since the possible orders of stabilizers of points in $Z(t)$ (these are 2,3 and divisors of m) are prime to p. We will now define $\mathrm{S}_* : \mathrm{Pic}_{Y/T} \to \mathrm{Pic}_{X/T}$. Let therefore $U \to T$ be a morphism of schemes. According to [Gro 1] IV 21.8.2, we have $\mathrm{Pic}(Y_U) = \mathrm{H}^1(X_U, \mathrm{S}_*\mathcal{O}^*_{Y_U})$. We get a "norm" morphism:

$$\mathrm{S}_*\mathcal{O}^*_{Y_U} \to \mathcal{O}^*_{X_U} : \quad f \mapsto \prod_{g \in G/B} g^{\#}(f) \tag{3.1.2.1}$$

where we view f as a function on (some open part of) Z_U. By taking the H^1 we obtain a morphism $\mathrm{Pic}(Y_U) \to \mathrm{Pic}(X_U)$, varying functorially with U.

Proposition 3.1.3 *The endomorphism* T_m *of* J_t^0 *is given by the correspondence* $\mathrm{S}, \mathrm{T} : Y_t \to X_t$, *where* $\mathrm{T}_* : \mathrm{Pic}^0_{Y_t/t} \to \mathrm{Pic}^0_{X_t/t}$ *is defined as* $\mathrm{S}_*\mathrm{W}_{m*}$, S_* *being defined by the norm map* 3.1.2.1.

3.2 The inertia decomposition.

In this section we decompose J_t^0 with respect to the inertia action. By construction, the Hecke algebra commutes with the inertia action, hence this decomposition of J_t^0 is Hecke stable.

First, we consider the usual decomposition of J_t^0 as an extension of an abelian variety by a torus. Since J_t^0 is the jacobian of the stable curve X_t, this decomposition is given as follows. Let $\widetilde{X_t} \to X_t$ be the normalization map: $\widetilde{X_t}$ is the disjoint union of the irreducible components of X_t. It follows that $\mathrm{Pic}^0_{\widetilde{X_t}/t} = \bigoplus \mathrm{Pic}^0_{C/t}$, where C runs through the irreducible components of X_t. In particular, $\mathrm{Pic}^0_{\widetilde{X_t}/t}$ is an abelian variety. The pullback morphism $\mathrm{Pic}^0_{X_t/t} \to \mathrm{Pic}^0_{\widetilde{X_t}/t}$ is surjective and its kernel is a torus whose character group is the H_1 of the dual graph associated to X_t. We conclude that this torus is the toric part of J_t^0 and $\mathrm{Pic}^0_{\widetilde{X_t}/t}$ its abelian variety part. The Hecke algebra acts on these two parts.

The action of the Hecke algebra on the toric part can be seen from the figure on page 18. The "holes" in this picture give a basis for the character group (to be sure: the number of holes is $3(s-1)$, where s is the number of supersingular points in $X_0(N)(t)$). The inertia group interchanges the two central vertical components and stabilizes all the others. It follows that the inertia action is by $\{\pm 1\}$ on the quotient torus given by the central holes. On the remaining part, the inertia action is trivial. In this way we find that the toric part of J_t^0 consists of three copies of the toric part of $J_0(pN)^0_p$, one of which is twisted by -1. As in [Me-Oe] the action of the Hecke algebra on these tori is by Brandt matrices, or equivalently, in terms of isogenies of supersingular elliptic curves over $\overline{\mathbf{F}}_p$. We will not go further into this.

We have already seen that the abelian variety part of J_t^0 is given by $\mathrm{Pic}^0_{\widetilde{X_t}/t} = \bigoplus \mathrm{Pic}^0_{C/t}$, where C ranges through the irreducible components of

X_t. The action of T_m (m prime to pN) on it is given by the correspondence $\mathrm{S}, \mathrm{T} : \widetilde{Y}_t \to \widetilde{X}_t$ (cf. Prop. 3.1.1 and Prop. 3.1.2.1, note that these S and T are finite flat, simply because the source and target are smooth curves). Since these correspondences don't mix horizontal with vertical components, we get a further Hecke stable decomposition:

$$\mathrm{Pic}^0_{\widetilde{X}_t/t} = \bigoplus_{hor} \mathrm{Pic}^0_{C/t} \oplus \bigoplus_{ver} \mathrm{Pic}^0_{C/t}.$$

One can prove (using the description of the vertical part in terms of $X(p)$) that T_m fixes the outer two vertical components, and interchanges the central two components precisely when $(\frac{m}{p}) = -1$. The inertia action on the central parts is through $\mu_{p-1}(\mathbf{F}_p)$. One can show (by the Lefschetz formula) that, apart from some small values of pN, all characters of $\mu_{p-1}(\mathbf{F}_p)$ occur in the Tate module, or equivalently, in the $\mathrm{H}^1(*, \overline{\mathbf{Q}}_\ell)$, of the vertical part. The horizontal components are mixed by the T_m according to the graph of cyclic m-isogenies between supersingular elliptic curves (as in the graph method by [Me-Oe]), but the question is, *how?* Before going into this we split up the horizontal part with respect to the inertia action.

Let C be the horizontal component corresponding to a supersingular point without extra automorphisms. The inertia group $\mu_n(\mathbf{F}_{p^2})$ acts on C through $\mu_{p+1}(\mathbf{F}_{p^2})$. Let $\ell \neq p$ be a prime and $\chi_\ell : \mu_{p+1}(\mathbf{F}_{p^2}) \to \overline{\mathbf{Q}}_\ell^*$ a character of order $p+1$.

Proposition 3.2.1 *As $\mu_{p+1}(\mathbf{F}_{p^2})$ representations we have:*

$$\mathrm{H}^1(C, \overline{\mathbf{Q}}_\ell) = \bigoplus_{\substack{1 \leq a \leq p \\ a \neq \frac{p+1}{2}}} \chi_\ell^a.$$

Proof. Let χ_r be the character of $\mu_{p+1}(\mathbf{F}_{p^2})$ on $\mathrm{H}^r(C, \mathbf{Q}_\ell)$. According to the Lefschetz formula ([Mi] V Thm. 2.5) we have:

$$\forall \zeta \neq 1 \qquad \chi_0(\zeta) - \chi_1(\zeta) + \chi_2(\zeta) = \text{number of fixed points of } \zeta$$

From our description 2.3.1, 2.3.3 we see that this number of fixed points is 4 if ζ is a square (in $\mu_{p+1}(\mathbf{F}_{p^2})$) and 2 if not. We obtain:

$$\chi_1(\zeta) = \begin{cases} -2 & \text{if } 1 \neq \zeta = \text{square} \\ 0 & \text{if } \zeta \neq \text{square.} \end{cases}$$

By the Hurwitz formula the genus of C equals $\frac{p-1}{2}$, this gives $\chi_1(1) = p-1$. Let $a \in \mathbf{Z}/(p+1)$, then the multiplicity of χ_ℓ^a in χ_1 is given by:

$$\langle \chi_1 | \chi_\ell^a \rangle = \frac{1}{p+1} \sum_\zeta \chi_1(\zeta)\chi_\ell(\zeta)^{-a} = \frac{1}{p+1}(p-1-2 \sum_{1 \neq \zeta = \text{square}} \chi_\ell(\zeta)^{-a}) =$$

$$= \frac{1}{p+1}(p+1-2 \sum_{\zeta=\text{square}} \chi_\ell(\zeta)^{-a}) = \begin{cases} 1 & \text{if } 2a \neq 0 \text{ in } \mathbf{Z}/(p+1) \\ 0 & \text{if } a = 0, \frac{p+1}{2}. \end{cases}$$

Let $J(C)$ be the jacobian of C, and let d divide $p+1$. Then we define $J(C)_{(d)}$ to be the largest abelian subvariety of $J(C)$ on which the inertia action is of order d. By this we mean that $J(C)_{(d)}$ has no non-zero abelian subvarieties on which the inertia action has order less than d. We set

$$P_d(x) = \prod_{d \neq d' | p+1} \Phi_{d'}(x) = (x^{p+1}-1)/\Phi_d(x),$$

where $\Phi_m(x)$ is the cyclotomic polynomial of order m. Then $J(C)_{(d)}$ is the image of the endomorphism $P_d(\zeta^*)$ of $J(C)$, if ζ generates $\mu_{p+1}(\mathbf{F}_{p^2})$. By Proposition 3.2.1 we have:

$$\dim J(C)_{(d)} = \begin{cases} 0 & \text{if } d = 1, 2 \\ \frac{1}{2}\phi(d) & \text{otherwise.} \end{cases}$$

Here $\phi(d)$ denotes the Euler ϕ-function.

For future use we state the following proposition.

Proposition 3.2.2 *As $\mu_{p+1}(\mathbf{F}_{p^2})$ representations we have:*

$$\mathrm{H}_0(C, \Omega_C) = \bigoplus_{1 \leq a \leq \frac{p-1}{2}} \chi^a$$

where χ is the identity on $\mu_{p+1}(\mathbf{F}_{p^2})$.

Proof. From equation 2.3.1.1 we see that $\{\omega_m = x^m \frac{dx}{y}\ ;\ 0 \leq m < \frac{p-1}{2}\}$ is a basis of $\mathrm{H}_0(C, \Omega_C)$. The equations for the inertia action 2.3.3.1 then give: $\zeta^* \omega_m = \zeta^{\frac{p-1}{2}} \omega_m$.

3.2.3 The horizontal 3,4 and 6 parts.

Let C be the horizontal component corresponding to a supersingular point without extra automorphisms. We will now give an explicit description of $J(C)_{(d)}$ for $d \in \{3,4,6\}$. Note that for these values of d, $J(C)_{(d)}$ is an elliptic curve if $d|p+1$, and $J(C)_{(d)} = 0$ otherwise.

First we treat the case $d \in \{3,6\}$, supposing $p \equiv -1(3)$. The curve C is given by: $y^2 = x^{p+1} + 1$ and $\zeta \in \mu_{p+1}(\mathbf{F}_{p^2})$ acts by: $x \mapsto \zeta^{-1}x$, $y \mapsto \zeta^{\frac{p+1}{2}}y$. It follows that the quotient of C by the action of $\mu_{\frac{p+1}{6}}(\mathbf{F}_{p^2})$ is given by:

$$C \longrightarrow C' \ : \quad (x,y) \mapsto (x^{\frac{p+1}{6}}, y)$$

where C' is given by the equation: $y^2 = x_1^6 + 1$. The image of the pullback map $J(C') \to J(C)$ is the sum of $J(C)_{(3)}$ and $J(C)_{(6)}$, since the kernel is finite and the dimensions correspond. We claim that in fact this map is a closed immersion: since the degree of $C \to C'$ is $\frac{p+1}{6}$, the kernel is contained in the $\frac{p+1}{6}$-torsion, secondly: since $C \to C'$ is totally ramified over some point in C' there is no such torsion in the kernel. Let $C_{(6)}$ be the curve: $y^2 = x_2^3 + 1$, then we have a morphism:

$$C' \longrightarrow C_{(6)} \ : \quad (x_1, y) \mapsto (x_1^2, y).$$

One can now easily check that $J(C)_{(6)}$ is the image of the closed immersion $J(C_{(6)}) \to J(C)$ corresponding to the composition $C \to C' \to C_{(6)}$. If we let $C_{(3)}$ be the quotient of C by $\mu_{\frac{p+1}{3}}(\mathbf{F}_{p^2})$ we obtain $J(C)_{(3)}$. The case $d = 4$ is similar to the case $d = 3$. We summarize the situation in the following proposition.

Proposition 3.2.4 *Let $d \in \{3,4,6\}$ and let $p \equiv -1(d)$. Then $C \to C'$ induces a closed immersion $J(C_{(d)}) \to J(C)$ with image $J(C)_{(d)}$. The various actions on $C_{(d)}$ are:*

$$\text{1.} \quad \begin{cases} d = 4, p \equiv -1(4) & C_{(4)}: & y^2 = x_1^4 + 1 \\ & C \to C_{(4)}: & x_1 = x^{\frac{p+1}{4}} \\ \zeta \in \mu_n(\mathbf{F}_{p^2}): & x_1 \mapsto \zeta^{\frac{n}{4}} x_1 & y \mapsto \zeta^{\frac{n}{2}} y \\ \mathrm{W}_{p^2}: & x_1 \mapsto (-1)^{\frac{p+1}{4}} x_1 & y \mapsto -y \end{cases}$$

$$
2.\quad \begin{cases}
d=3, p\equiv -1(3) & C_{(3)}: \qquad\qquad y_1^2 = x_2^4 + x_2 \\
 & C \to C_{(4)}: \quad y_1 = x^{\frac{p+1}{6}} y, x_2 = x^{\frac{p+1}{3}} \\
\zeta \in \mu_n(\mathbf{F}_{p^2}): & x_2 \mapsto \zeta^{-\frac{n}{6}} x_2 \quad y_1 \mapsto \zeta^{\frac{n}{3}} y_1 \\
\mathrm{W}_{p^2}: & x_2 \mapsto x_2 \qquad\quad y_1 \mapsto -y_1
\end{cases}
$$

$$
3.\quad \begin{cases}
d=6, p\equiv -1(3) & C_{(6)}: \qquad\qquad y^2 = x_2^3 + 1 \\
 & C \to C_{(6)}: \quad x_2 = x^{\frac{p+1}{3}} \\
\zeta \in \mu_n(\mathbf{F}_{p^2}): & x_2 \mapsto \zeta^{-\frac{n}{6}} x_2 \quad y \mapsto \zeta^{\frac{n}{2}} y \\
\mathrm{W}_{p^2}: & x_2 \mapsto x_2 \qquad\quad y_1 \mapsto (-1)^{\frac{p-1}{2}} y_1
\end{cases}
$$

Let x be a supersingular point in $X_0(N)(s)$ having extra automorphisms. Then the horizontal component C_x at x is the quotient of C by the action of $\mathrm{Aut}(x)$, and $J(C_x)_{(d)}$ is the jacobian of $C_{x(d)} := C_{(d)}/\mathrm{Aut}(x)$. The action of $\mathrm{Aut}(x)$ on $C_{(d)}$ can be easily computed from the formulas above and 2.3.5.1. If this action is not trivial then $C_{(d)}/\mathrm{Aut}(x)$ is a $\mathbf{P}^1$ and its jacobian is 0. One finds the following table.

Table 3.2.5 *The dimension of* $J(C_x)_{(d)}$.

$\#\mathrm{Aut}(x)$	d	p	$\dim J(C_x)_{(d)}$
4	4	$p \equiv -1(8)$	1
		$p \equiv 3(8)$	0
	$3,6$	$p \equiv -1(4)$	1
6	4	$p \equiv -1(3)$	1
	$3,6$	$p \equiv -1(9)$	1
		$p \equiv 2,5(9)$	0

In the proposition above we have described the action of W_{p^2} on $C_{(d)}$. The action on $J(C)_{(d)}$ is given in the following table.

Table 3.2.6 *The action of* W_{p^2} *on* $C_{(d)}$.

d	p	W_{p^2} on $J(C)_{(d)}$
4	$p \equiv -1(8)$	-1
	$p \equiv 3(8)$	1
3	$p \equiv -1(3)$	-1
6	$p \equiv -1(12)$	-1
	$p \equiv 5(12)$	1

3.3 Computation of $\mathbb{T}_m$ on the horizontal part.

The horizontal part of J_t^0 was defined as $\bigoplus_x J(C_x)$, where the sum is over $s.s.X_0(N)(s)$, (the supersingular points in $X_0(N)(s)$), and C_x is the horizontal component of X_t at x. From Propositions 3.1.2 and 3.1.3 it follows that the action of $\mathbb{T}_m$ (m prime to pN) is given by the correspondence:

$$\begin{tikzcd} & \coprod_y C_y \arrow[dl, "\mathrm{S}"'] \arrow[dr, "\mathrm{T}"] & \\ \coprod_x C_x & & \coprod_x C_x \end{tikzcd}$$

where the disjoint unions are labeled by the $x \in s.s.X_0(N)(s)$ and the $y \in s.s.X_0(Nm)(s)$. We will now compute the contribution to $\mathbb{T}_m$ of one component C_y. Let $x = \mathrm{S}y$ and $x' = \mathrm{T}y$. We suppose that $\mathrm{Aut}(x) = \mathrm{Aut}(x') = \mathrm{Aut}(y) = \pm 1$. Let $x \sim (E, G)$, $y \sim (\phi : E \to E', G)$ and $x' \sim (E', \phi G)$, where $\phi : E \to E'$ is a cyclic m-isogeny between supersingular elliptic curves, and G a cyclic subgroup of order N of E. We choose coordinates t and t' of the deformation spaces of E and E' : these spaces are $\mathrm{W}[[t]]$ and $\mathrm{W}[[t']]$ respectively. Since $[\Gamma_0(N)]_S$ is etale over $[Ell]_S$, t and t' are coordinates at x and x'. The morphisms S, T: $[\Gamma_0(Nm)] \to [\Gamma_0(N)]$ give isomorphisms between the deformation spaces at x, y and x':

$$\mathrm{TS}^{-1} : [\Gamma_0(N)]_x \tilde{\to} [\Gamma_0(Nm)]_y \tilde{\to} [\Gamma_0(N)]_{x'}.$$

We write $(\mathrm{TS}^{-1})^{\#}t' = a_0 t + pa_p(t) + t^2 a_1(t)$, with $a_0 \in \mathrm{W}^*$, $a_p(t)$ and $a_1(t)$ in $\mathrm{W}[[t]]$. Since x is supersingular there is a unique point (also denoted by x) in $[\Gamma_0(p^2N)]$ over x: $x \sim ([p] : E \to E, G)$. The same holds for y and x': $y \sim (p\phi : E \to E', G)$. The two morphisms S,T: $[\Gamma_0(p^2Nm)] \to [\Gamma_0(p^2N)]$ give an isomorphism: $\mathrm{TS}^{-1} : [\Gamma_0(p^2N)]_x \to [\Gamma_0(p^2N)]_{x'}$. The commutativity of:

$$\begin{array}{ccc} E & \xrightarrow{p} & E \\ \phi\downarrow & & \phi\downarrow \\ E' & \xrightarrow{p} & E' \end{array}$$

implies the commutativity of:

$$\begin{array}{ccccc} [\Gamma_0(p^2N)]_x & \to & [\Gamma_0(N)]_x & \times & [\Gamma_0(N)]_x \\ \mathrm{TS}^{-1}\downarrow & & \mathrm{TS}^{-1}\downarrow & & \mathrm{TS}^{-1}\downarrow \\ [\Gamma_0(p^2N)]_{x'} & \to & [\Gamma_0(N)]_{x'} & \times & [\Gamma_0(N)]_{x'} \end{array}$$

where the horizontal arrows are the closed immersions composed of the source and target morphisms relative to the degree p^2 isogeny. Written out in coordinates as in Section 2.1.3 this means:

$$\mathrm{TS}^{-1\#} : \begin{cases} x' \mapsto a_0 x + pa_p(x) + x^2 a_1(x) \\ y' \mapsto a_0 y + pa_p(y) + y^2 a_1(y). \end{cases}$$

Going through the substitutions 2.1.3.2 and reducing mod π_1 gives the map on horizontal components:

$$v_3' \mapsto a_0^{\frac{p+1}{2}} v_3 \qquad u_1' \mapsto a_0 u_1 \tag{3.3.0.1}$$

where C_x and $C_{x'}$ are given by the equations:

$$v_3^2 = u_1^{p+1} + 4a \qquad (v_3')^2 = (u_1')^{p+1} + 4a'.$$

We also get he information: $a' = a_0^{p+1} a$. Specializing to the case that ϕ is an endomorphism $\phi : E \to E$ with $\phi G = G$, we get the following proposition.

Proposition 3.3.1 *Let $x \in X_0(N)(s)$ be a supersingular point with* $\mathrm{Aut}(x) = \pm 1$ *and let $\phi \in \mathrm{End}(x)$ be an endomorphism of degree m prime to pN. Let $a_0 \in \overline{\mathbb{F}}_p$ be the automorphism induced by ϕ (as above) on the tangent space to $X_0(N)_s$ at x. Then $a_0^{p+1} = 1$ and the contribution of ϕ to T_m is the automorphism:*

$$\begin{cases} x \mapsto a_0 x \\ y \mapsto a_0^{\frac{p+1}{2}} y \end{cases}$$

of C_x.

Remark. Note that the automorphism induced by ϕ on C_x is in the inertia group (compare 2.3.3.1).

We will now compute the "a_0" in the proposition above in terms of ϕ itself. We do this computation in the context of abelian varieties because that's just as easy.

Let A be an abelian variety over a field k, then the deformations of A over $k[\varepsilon]$ ($\varepsilon^2 = 0$) correspond to $\mathrm{H}^1(A, T_A)$, where T_A is the tangent sheaf $Der_k(\mathcal{O}_A)$ on A. This works as follows ([Gro 2] exp. III, or [Oo 2] Proposition 2.2.5). Given $t \in \mathrm{H}^1(A, T_A)$, represent it by a 1-cocycle $D_{ij} \in T_A U_{ij}$, where U_i is an affine open cover of A. Let $\tilde{U}_i := U_i \times_k k[\varepsilon]$, the constant deformation of U_i. Define "glueing" isomorphisms:

$$\psi_{ij} : \tilde{U}_i \supset \tilde{U}_{ij} \tilde{\to} \tilde{U}_{ij} \subset \tilde{U}_j \tag{3.3.1.1}$$

by:

$$\psi_{ij}^{\#}(f_0 + \varepsilon f_1) = f_0 + \varepsilon(f_1 + D_{ij} f_0).$$

Glueing the $\tilde{U}_i$ by the ψ_{ij} then gives the deformation $\widetilde{A}$ corresponding to t. Since A is a group, we have $T_A = T_{A,0} \otimes_k \mathcal{O}_A$, whence:

$$\mathrm{H}^1(A, T_A) = T_{A,0} \otimes_k \mathrm{H}^1(A, \mathcal{O}_A) = T_{A,0} \otimes_k T_{A^t,0},$$

where A^t is the dual abelian variety $\mathrm{Pic}^0_{A/k}$ of A.

Let $\pi : A_1 \to A_2$ be an isogeny of abelian varieties over k, such that $\deg \pi$ is invertible in k. Deformations of A_1 correspond bijectively to deformations of A_2 by demanding that π can be extended (note that $\ker \pi$ and $\ker \pi^t$ are etale over k).

Proposition 3.3.2 *The isomorphism:* $T_{A_1,0} \otimes T_{A_1^t,0} \tilde{\to} T_{A_2,0} \otimes T_{A_2^t,0}$ *induced by* π *as above is given by* $T_{\pi,0} \otimes T_{\pi^t,0}^{-1}$.

Proof. We start with a deformation over $k[\varepsilon]$ of A_2: let $A_2 = \cup U_i^2$ and let $D_{ij}^2 \in Der_k(\mathcal{O}_{A_2} U_{ij}^2)$ be a 1-cocycle. We put $U_i^1 := \pi^{-1} U_i^2$, then we have $A_1 = \cup U_i^1$. We get $\pi^\# D_{ij}^2$ in $Der_k(\mathcal{O}_{A_2} U_{ij}^2, \mathcal{O}_{A_1} U_{ij}^1)$. Since π is etale, this can be extended in exactly one way to a derivation D_{ij}^1 in $Der_k(\mathcal{O}_{A_1} U_{ij}^1)$. These D_{ij}^1 give a deformation of A_1. We claim that π extends to an isogeny $\tilde{\pi}$, and that $\tilde{\pi}_i := \tilde{\pi}|_{\tilde{U}_i^1}$ is constant:

$$\tilde{\pi}_i^\#(f_0 + \varepsilon f_1) = \pi^\# f_0 + \varepsilon \pi^\# f_1.$$

The only thing to be checked is that these $\tilde{\pi}_i$ are compatible with the glueing isomorphisms:

$$\psi_{ij}^2 \tilde{\pi}_i = \tilde{\pi}_j \psi_{ij}^1,$$

where the $\psi_{ij}^\bullet$ are defined as in 3.3.1.1. This is a trivial verification.

The map $D_{ij}^2 \mapsto D_{ij}^1$ is given by a morphism of sheaves:

$$\pi_* Der_k(\mathcal{O}_{A_1}) \tilde{\to} Der_k(\mathcal{O}_{A_2}, \pi_* \mathcal{O}_{A_1}) \leftarrow Der_k(\mathcal{O}_{A_2}).$$

Taking $\mathrm{H}^1(A_2, -)$ and making the right identifications then proves the proposition.

Corollary 3.3.3 *The number* a_0 *of Proposition 3.3.2 is given by:*

$$a_0 = T_{\phi,0} \otimes T_{\phi^t,0}^{-1} = T_{\phi,0}^2 / \deg(\phi).$$

3.4 An algorithm for T_2 on $J_0(p^2)$.

We will now present an algorithm for the computation of T_2 on the horizontal 3,4 and 6-parts of $J_0(p^2)$. This algorithm is very similar to the graph algorithm of [Me-Oe]. It uses explicit equations for the correspondence on the j-line given by $X_0(2)$. In order to describe and compute the isomorphisms between the horizontal components (the numbers "a_0" from proposition 3.3.2) we must equip the supersingular j-values with tangent vectors. This means that we will work with $\mathbf{F}_{p^2}[\varepsilon]$ valued points of $\mathrm{Spec}(\mathbf{F}_p[j])$, where

$\varepsilon^2 = 0$, (usually). The j-invariants 0 and 12^3 cause some problems, because the correspondence given by $X_0(2)$ is ramified over these points. We start with some formulas.

The correspondence on $X_0(1)$ induced by $X_0(2)$ is given by:

$$\begin{cases} xy = 2^{12} \\ j = \frac{(x+16)^3}{x} \\ \mathrm{W}_2 : x \longleftrightarrow y \end{cases} \tag{3.4.0.1}$$

These formulas are copied from [Me]. Next we give the number of automorphisms of points j on the j-line and points x on the x-line $X_0(2)$.

$$e(j) := \frac{1}{2}\#\mathrm{Aut}(j) = \begin{cases} 3 & \text{if } j = 0 \\ 2 & \text{if } j = 12^3 \\ 1 & \text{otherwise} \end{cases} \tag{3.4.0.2}$$

$$e(x) := \frac{1}{2}\#\mathrm{Aut}(x) = \begin{cases} 2 & \text{if } x = -64 \\ 1 & \text{otherwise} \end{cases}$$

Let $d \in \{3,4,6\}$. The horizontal d-part is 0 if $p \not\equiv -1(d)$, so we suppose $p \equiv -1(d)$.

Step 1. Find a supersingular j-value j_0 in $\mathbf{F}_{p^2}$. This is very easy: since $p \equiv -1(d)$ we can take $j_0 = 0$ if $d \in \{3,6\}$ and $j_0 = 12^3$ if $d = 4$. ■

Step 2. Build the graph of supersingular 2-isogenies. The vertices of this directed graph are the supersingular j-values (these lie in $\mathbf{F}_{p^2}$), the edges are the supersingular x-values (these lie in $\mathbf{F}_{p^2}$ too). The edge x has source $j = (x+16)^3/x$ and target $j' = (y+16)^3/y$, where $xy = 2^{12}$ (note that an edge can be a loop). The connectedness of this graph ([Me-Oe]) ensures that it can be built starting with j_0. In order to find the edges with source j one has to solve the equation: $(x+16)^3 - jx = 0$. Since one of the three roots is already known (after the first step) one only has to solve a quadratic equation, which is very easy. ■

In the next step we will compute a suitable system of "tangent vectors" at the supersingular points on the j-line. Such a tangent vector at the point j will be an $\mathbb{F}_{p^2}[\varepsilon]$ valued point of the j-line of the form: $j + \varepsilon^{e(j)} v^{e(j)}$, where $\varepsilon^{e(j)+1} = 0$ and $v^{e(j)} \in \mathbb{F}_{p^2}$ (for $e(j)$, see 3.4.0.2). In practice this means that we put a number $v^{e(j)} \in \mathbb{F}_{p^2}$ at every vertex j of the graph. We do not want nor need to compute the numbers v themselves, writing $v^{e(j)}$ is just a matter of notation.

Step 3. Choose a vertex j such that $j \in \mathbb{F}_p$, $j \neq 0, 12^3$ (if $p > 11$ there is always such a j: a neighbor of j_0). Let the number $v = v^{e(j)}$ at this vertex be 1 (this is an arbitrary choice). Now compute one tangent vector at every vertex by transporting them along the edges as follows. Suppose we have $j + \varepsilon^{e(j)} v^{e(j)}$ at $j = (x+16)^3/x$. Solve $w^{e(x)}$ in the equation:

$$j + \varepsilon^{e(j)} v^{e(j)} = \frac{(x + \varepsilon^{e(x)} w^{e(x)} + 16)^3}{x + \varepsilon^{e(x)} w^{e(x)}} \qquad (\pmod{\varepsilon^{e(j)+1}}).$$

The right hand side of this equation is $j + \varepsilon^{e(j)} w^{e(j)} a$ for a certain non-zero $a \in \mathbb{F}_{p^2}$, hence we must have: $w^{e(x)} = v^{e(x)} a^{\frac{e(x)}{e(j)}}$. Since $j = 0, 12^3$ are always endpoints of the graph, we may suppose that $e(j) = e(x) = 1$. We have now a tangent vector $x + \varepsilon^{e(x)} w^{e(x)}$ at x. Solve $xy = 2^{12}$. Solve:

$$(x + \varepsilon^{e(x)} w^{e(x)})(y + \varepsilon^{e(y)} t^{e(y)}) = 2^{12}.$$

Noting that $e(y) = e(x)$ one finds: $t^{e(y)} = -\frac{y}{x} w^{e(x)}$. Compute j' and $u^{e(j')}$ in:

$$((y + \varepsilon^{e(y)} t^{e(y)} + 16)^3 / (y + \varepsilon^{e(y)} t^{e(y)}) = j' + \varepsilon^{e(j')} u^{e(j')}.$$

Note that now $e(j')$ can be 1,2 or 3. Let $j' + \varepsilon^{e(j')} v'^{e(j')}$ denote the tangent vector at j' that we want in our "suitable system". If $j' \notin \mathbb{F}_p$ then we take $(v')^{e(j')} := u^{e(j')}$ at j', and $\overline{u^{e(j')}}$ at $\overline{j'}$, where the bar denotes Galois conjugation over $\mathbb{F}_p$. Suppose $j' \in \mathbb{F}_p$. If $u^{e(j')} \in \mathbb{F}_p$ then we take $(v')^{e(j')} := u^{e(j')}$. If $u^{e(j')} \notin \mathbb{F}_p$, we take $(v')^{e(j')} := (u^{e(j')})^{\frac{p+1}{2}}$. ∎

We will now explain the use of this system of tangent vectors. Remember that in the computation of the horizontal components (2.1.3) we had to choose a coordinate t. Taking only t that coincide up to first order with our tangent vectors then gives the *same* equation $v_3^2 = u_1^{p+1} + 4a$ for every horizontal component. Note that $a \in \mathbf{F}_p^*$, and that $\mathbf{F}_p^*$ acts on our system of tangent vectors. It follows that a can be changed by a square. It is thus interesting to know whether a is a square or not. One can show that a is a square.

Anyhow, we are now able to compare every horizontal component to a fixed one. Let $\phi : E \to E'$ be an isogeny sending v at $j(E)$ to $a_0 v'$ at $j(E')$. Then formula 3.3.0.1 tells us that ϕ acts on our fixed curve as the element a_0^{-1} in the inertia group $\mu_{p+1}(\mathbf{F}_{p^2})$. For the moment, we did forget the points with extra automorphisms. These will cause some trouble in the next steps.

Step 4. If $d \in \{3, 6\}$ and $p \not\equiv -1(9)$ then delete the vertex 0 and the edges having this vertex as an endpoint. If $d = 4$ and $p \not\equiv -1(8)$ then delete the vertex 12^3 and the edges having 12^3 as an endpoint. This step is the deletion of the horizontal components having no d-part (cf. table 3.2.5). ■

The d-part of $J_0(p^2)$ is now given by: $\oplus_{vertices} E$, where E is an elliptic curve over $\mathbf{F}_p$ having $\mu_d \subset \mathrm{Aut}_{E/\mathbf{F}_p}$ (one can compute which one of the two $\mathbf{F}_p$-forms it is). Note that E is supersingular. We will write E_j for the summand E at the vertex j. Then we have:

$$\mathrm{End}_{\mathbf{F}_{p^2}}(\oplus E_j) = \bigoplus_{j,j'} \hom(E_{j'}, E_j).$$

This means that we write endomorhisms as matrices, where the rows are labeled by j and the columns by j'. The next step computes the matrix of T_2. The coefficients are sums of d-th roots of unity in $\mathrm{End}_{\mathbf{F}_{p^2}}(E)$. We view these roots of unity as elements of $\mu_d(\mathbf{F}_{p^2})$, the identification is the action of $\mathrm{End}_{\mathbf{F}_{p^2}}(E)$ on the tangent space at 0 of E.

Step 5. Let j be a vertex. Let x_1, x_2, x_3 be the roots of $(x + 16)^3/x = j$. The row of T_2 labeled by j is the sum of the contributions from the x_i. Let x be one of the x_i. Consider the equation:

$$j + \varepsilon^{e(j)} v^{e(j)} = \frac{(x + \varepsilon^{e(x)} w^{e(x)} + 16)^3}{x + \varepsilon^{e(x)} w^{e(x)}} \qquad (\pmod{\varepsilon^{e(j)+1}}).$$

As in step 3, the RHS can be written as $j + \varepsilon^{e(j)} w^{e(j)} a$ for some $a \in \mathbf{F}_{p^2}^*$, giving: $w^{e(j)} = v^{e(j)}a^{-1}$. We do not need to know $w^{e(x)}$ since in the final formula for the coefficient of the matrix only powers of $w^{e(j)}$ will occur. However, this would force us to do the rest of the computation formally, treating $w^{e(x)}$ as a symbol. Let us therefore take $w^{e(x)}$ to be one of the $(e(x)/e(j))$-th roots of $w^{e(j)}$. Let $y := 2^{12}x^{-1}$. Let $t^{e(y)} := -\frac{y}{x}w^{e(x)}$. Compute j' and $u^{e(j')}$ in:

$$((y+\varepsilon^{e(y)}t^{e(y)}+16)^3/(y+\varepsilon^{e(y)}t^{e(y)}) = j' + \varepsilon^{e(j')}u^{e(j')}.$$

Remember that we have a "standard" tangent vector $j' + \varepsilon^{e(j')}(v')^{e(j')}$. The contribution of x to $a_{jj'}$ is:

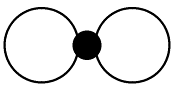
$$(\frac{v'}{u})^{\frac{p+1}{d}} = (\frac{(v')^{e(j')}}{u^{e(j')}})^{\frac{p+1}{de(j')}} \quad \blacksquare \tag{3.4.0.3}$$

Remark. One can compute the matrices of T_l for $l = 3, 5, 7$ and 13 by repeating step 5, with the formulas for $X_0(2)$ replaced by those for $X_0(l)$ (see [Me]).

3.5 Some examples.

3.5.1 $p = 7$.

$X_0(7^2)$ is the elliptic curve 49A of [Bi-Ku] table 1. According to table 3 of [Bi-Ku] the operator T_2 has eigenvalue 1 on $J_0(7^2)$. We will now check this, using the algorithm of the preceding section. The graph of 2-isogenies has only one vertex: $j = -1$, with $e(-1) = 2$. There are two edges: $x = -1, 1$, with $e(-1) = 2$ and $e(1) = 1$. In a picture, this graph looks as follows:



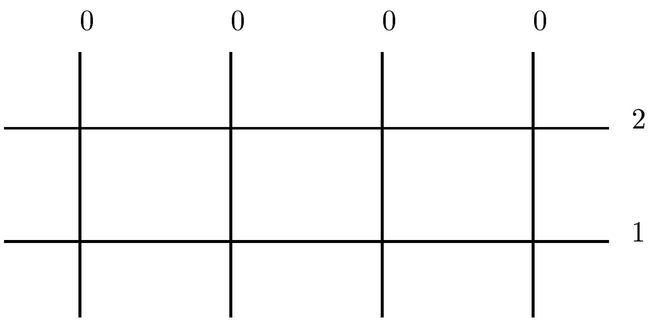
Note that this is a picture of an undirected graph. When drawing pictures like this, we will always identify the edges x and y with $xy = 2^{12}$. In other words, an edge corresponds to an isogeny together with its transpose. At

$j = -1$ we choose the tangent vector $-1 + \varepsilon^2$. Now we consider the 4-part of $J_0(p^2)$, this is $J_0(p^2)$ itself. The equation $-1 = j = (x+16)^3/x$ has the three solutions $x = -1, 1, 1$. At $x = -1$ we find the tangent vector $-1 - 2\varepsilon^2$. Solving $xy = 2^{12}$ gives the tangent vector $-1 + 2\varepsilon^2$ at -1. At $j' = -1$ we find $-1 - \varepsilon^2$. This implies that the contribution of the loop $x = -1$ equals $(-1)^{\frac{7+1}{4\cdot 2}} = -1$. At $x = 1$ we get $1 + 2\varepsilon$ (in the computation one has to solve $w^2 = 4$, so we could also take $1 - 2\varepsilon$). At $y = 1$ we find $1 - 2\varepsilon$. We arrive at $j' = -1$ with $-1 + \varepsilon^2$. The contribution of $x = 1$ is thus 1. The total contribution is $-1 + 1 + 1 = 1$, giving the right eigenvalue for $\mathbb{T}_2$.

Now we do the same computation directly in terms of the moduli interpretation. The vertex corresponds to the elliptic curve E with automorphism group $\mu_4(\mathbf{F}_{p^2})$. Let i be a generator of this group. The vertex $x = -1$ corresponds to the endomorphism $1 + i$. By corollary 3.3.3, $1 + i$ acts by $\frac{1+i}{1-i} = i$ on the deformation space of E. It follows that the action on the 4-part is by $i^{\frac{7+1}{4}} = -1$. The edge $x = 1$ corresponds to the endomorphism $\frac{1+\mathrm{F}}{2}$ (F is Frobenius). Since F acts by 0 on the tangent space of E, we get a trivial action of $\frac{1+\mathrm{F}}{2}$ on the deformation space of E. On the 4-part we find 1.

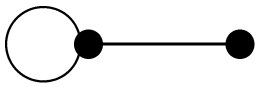
3.5.2 $p = 11$.

The special fibre of the stable model of $X_0(11^2)$ looks as follows:



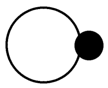
The numbers denote the genera of the components. The genus 1 component corresponds to the supersingular point $j = 0$. The other supersingular j-

value is $12^3 = 1$. The graph of 2-isogenies looks as follows:



The graph of the 4-part is:

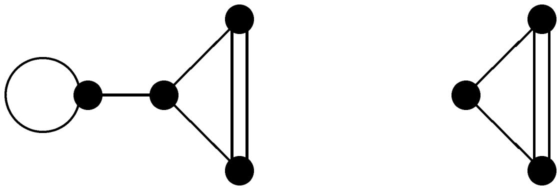
Since there are no edges, we get T_2=0. From the tables of [Bi-Ku] we see that the 4-part is the elliptic curve 121D. The graph of the 3 and 6-parts is:



The loop again represents the endomorphism $1 + i$. For the action on the 3 and 6-parts one finds: $i^{\frac{11+1}{3}} = 1$ and $i^{\frac{11+1}{6}} = -1$. The 3 and 6-parts must be the curves 121F and 121H.

3.5.3 $p = 43$.

We get the graph of 2-isogenies:



The second graph is the graph for the 4-part. The matrix for T_2 on the 4-part is:

$$\begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 2i \\ 1 & -2i & 0 \end{pmatrix}.$$

The characteristic polynomial of this matrix is: $\lambda(\lambda^2 - 6)$. The eigenvalue $\lambda = 0$ corresponds to the complex multiplication curve of conductor 43^2 (cf. [Gr]).

Chapter 4

Weil curves.

Let E be an elliptic curve over $\mathbf{Q}$ and let M be its conductor. Conjecturally (Taniyama-Weil), E is an isogeny factor of the new part of the jacobian variety $J_0(M)_{\mathbf{Q}}$ of $X_0(M)_{\mathbf{Q}}$. Elliptic curves satisfying this conjecture are called Weil curves. First we will study the stable models of elliptic curves (outside characteristics 2 and 3). In the rest of this chapter we use our knowledge of stable models to study Weil curves. We give some examples of Weil curves of conductor p^2. In the last section we derive some results concerning the Manin constant c attached to a Weil curve.

4.1 Stable models of elliptic curves.

In this section we apply the method for constructing stable models, as described in Section 2.1, to elliptic curves. We compute the inertia action on the stable models and on their differential forms.

Let S be the spectrum of a complete discrete valuation ring with algebraically closed residue field. In order to satisfy the condition "n is invertible on S" of Proposition 2.1.1 we suppose that 6 is invertible on S. Let s be the closed point of S and η the generic point. Let E be an elliptic curve over η, and $\mathcal{E}$ its minimal model over S (as a surface, not as an abelian variety). The special fibre of $\mathcal{E}$ is of one of the following types: I_0, I_ν, II, III, IV, I_0^*, I_ν^*, IV^*, III^*, II^*. These types are described in [Ta]. Let $\mathcal{E}_S$ denote the model of E obtained by blowing up $\mathcal{E}$ until its special fibre has normal crossings. In all cases except II, III and IV, we do not need any blow ups and $\mathcal{E}_S$ is just $\mathcal{E}$ itself. In the remaining cases, we need 3, 2 and 1 blow up(s) respectively. A picture of this blowing up process can be found in Figure 4.1.

Let π_0 be a uniformizer on S. We will now describe which base change $T \to S$ of the form: $T = S[\pi]$, $\pi^n = \pi_0$ we need in order to get a stable model of E (over T). If E is of type I_0 or I_ν ($\nu > 0$) then E is already stable over S.

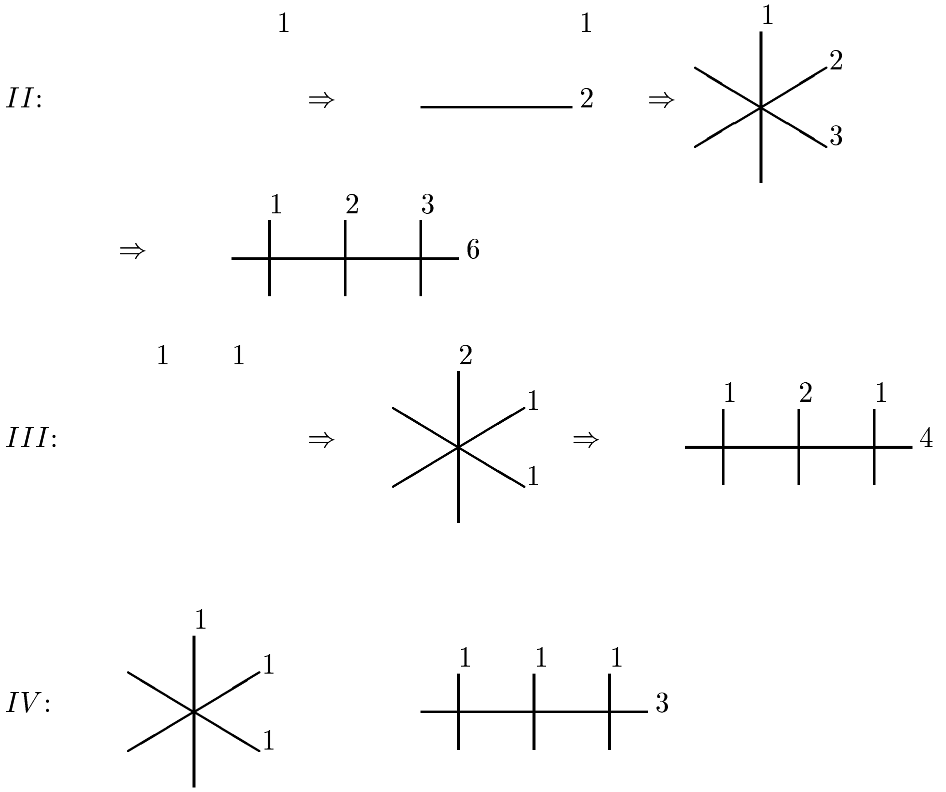
Suppose that E is of type I_ν^* ($\nu > 0$). Then the l.c.m. of the multiplicities of the components of $\mathcal{E}_s$ is 2, so we must take $n = 2$. From the picture in [Ta] we see that E has reduction type $I_{2\nu}$ over T.

In the remaining cases E has bad but potentially good reduction. There is a unique component in $\mathcal{E}_s$ (:= the special fibre of $\mathcal{E}_S$) that intersects more than two other components. This is the component that gives rise to the elliptic curve in the stable model. Let n be its multiplicity. Then E acquires good reduction over T.

Next we compute the inertia action on the stable reduction. The base change $T \to S$ is Galois, with group $\mu_n(S)$: $\zeta \in \mu_n(S)$ acts by $\zeta^\#(\pi) = \zeta\pi$. Let $\widetilde{\mathcal{E}_T}$ be the Néron model of E over T. Then $\mu_n(S)$ acts on $\widetilde{\mathcal{E}_T}/T$. Let t be the closed point of T. We get a linear action of $\mu_n(S)$ on $\widetilde{\mathcal{E}_{T,t}}^0/t$. Since n is chosen minimal, this action is faithful. The group $\mathrm{Aut}_t(\widetilde{\mathcal{E}_{T,t}}^0)$ acts faithfully on the tangent space at 0 of $\widetilde{\mathcal{E}_{T,t}}^0$, or equivalently, on the translation invariant differential forms. The inertia action of $\mu_n(S)$ on $\widetilde{\mathcal{E}_{T,t}}^0$ is thus described by the character $\chi_\omega : \mu_n(S) \to \mu_n(S)$, giving the action of $\mu_n(S)$ on the translation invariant differential forms on $\widetilde{\mathcal{E}_{T,t}}^0$. The computation of these characters is very easy and is therefore omitted (in fact, they can be read off from the pictures of the normal crossings model directly). The characters χ_ω can be found in the next proposition.

Proposition 4.1.1 *Let S be the spectrum of a complete discrete valuation ring, with algebraically closed residue field not of characteristic* 2 *or* 3*. Let E be an elliptic curve over the generic point of S. We attach a number n and a character $\chi_\omega : \mu_n(S) \to \mu_n(S)$ to E according to its reduction type as*

Figure 4.1: Construction of the normal crossings model.



follows ($\chi : \mu_n(S) \to \mu_n(S)$ *denotes the identity*):

type	I_0	I_ν	II	III	IV	I_0^*	I_ν^*	IV^*	III^*	II^*
n	1	1	6	4	3	2	2	3	4	6
χ_ω	χ	χ	χ	χ	χ	χ	χ	χ^{-1}	χ^{-1}	χ^{-1}

Let π_0 *be a uniformizer on* S. *Then* E *acquires stable reduction over* $T := S[\pi]$, *where* $\pi^n = \pi_0$. *The Galois group of* T *over* S *is identified with* $\mu_n(S)$ *by:* $\zeta^\# \pi = \zeta\pi$ *for all* $\zeta \in \mu_n(S)$. *Let* t *be the closed point of* T *and* $\widetilde{\mathcal{E}_T}$ *the Néron model of* E_T. *The the action of* $\mu_n(S)$ *on the tangent space at* 0 *of* $\widetilde{\mathcal{E}_{T,t}}$ *is given by* χ_ω.

Let S and E be as before. Let $\mathcal{E}$ denote the Néron model of E over S. Let $T \to S$ be the base change as given in Proposition 4.1.1, and let $\widetilde{\mathcal{E}_T}$ be the Néron model of E_T. Since $\widetilde{\mathcal{E}_T}$ has the Néron property, we get a (unique) morphism $f : \mathcal{E}_T \to \widetilde{\mathcal{E}_T}$ extending the identity on the generic fibres. Note that the kernel of f contains $\mathcal{E}_s^0$, if E has additive reduction. On the cotangent spaces along the zero sections f induces an injection

$$f^* : \ \omega_{\widetilde{\mathcal{E}_T}/T} \longrightarrow \omega_{\mathcal{E}_T/T} = \omega_{\mathcal{E}_S/S} \otimes_{\mathcal{O}_S} \mathcal{O}_T.$$

Let ω_S be a generator of $\omega_{\mathcal{E}_S/S}$: $\omega_{\mathcal{E}_S/S} = \mathcal{O}_S \cdot \omega_S$.

Proposition 4.1.2 *Let* $\omega_{\mathcal{E}_S/S} = \mathcal{O}_S \cdot \omega_S$ *and let* a *be as follows:*

type	I_0	I_ν	II	III	IV	I_0^*	I_ν^*	IV^*	III^*	II^*
a	0	0	1	1	1	1	1	2	3	5

Let $\omega_T := \pi^a \omega_S$. *Then* $\omega_{\widetilde{\mathcal{E}_T}/T} = \mathcal{O}_T \cdot \omega_T$.

Proof. This is done by explicit computation using minimal Weierstrass equations (see [Ta]). We only give the computation for reduction type II^*, the computations for the other cases are almost the same.

The minimal Weierstrass equation for $\mathcal{E}$ (over S) is:

$$y^2 = x^3 + ax + b$$

where $a = \frac{-c_4}{48}$ and $b = \frac{-c_6}{864}$, hence $v_{\pi_0}(a) = 4$ and $v_{\pi_0}(b) = 5$. We take $\omega_S := \frac{dx}{2y}$. We have $\pi_0 = \pi^6$. We rewrite the Weierstrass equation:

$$y^2 = x^3 + ax + b = x^3 + \pi_0^4 a_4 x + \pi_0^5 b_5 = x^3 + \pi^{24} a_4 x + \pi^{30} b_5.$$

We set $x := \pi^{10} u$, $y := \pi^{15} v$ and find the new equation:

$$v^2 = u^3 + \pi^4 a_4 u + b_5.$$

The generating differential form for this model is $\frac{du}{2v} = \pi^5 \frac{dx}{2y}$.

4.2 Reduction of Weil parametrizations.

Let $p > 3$ be a prime and N an integer not divisible by p. Let E be an elliptic curve over $\mathbf{Q}$ with a strong Weil parametrization $\phi : X_0(p^2N)_{\mathbf{Q}} \to E$ ([Ma 1], [Ma 2], [Ma-SD], [Bi-SD], [Ca]). In this section we study the reduction of ϕ mod p using stable models. We will be mainly interested in curves E having potentially good reduction at p. This means that most of the time we will exclude the case where E has reduction type I_ν^* ($\nu > 0$) at p (from [Ca] we know that the conductor of E is p^2N, hence the types I_0 and I_ν are already excluded)[1].

Let $S := \mathrm{Spec}(W(\overline{\mathbf{F}}_p))$, where $W(\overline{\mathbf{F}}_p)$ is the ring of Witt vectors of $\overline{\mathbf{F}}_p$. Let $n := \frac{p^2-1}{2}$ and $U := S[\pi]$ with $\pi^n = p$. Both E and $X_0(p^2N)$ acquire stable reduction over U (cf. Proposition 4.1.1 and Section 2.1.2). Let $\widetilde{\mathcal{E}_U}$ be the Néron model of E over U and let $\widetilde{X_U}$ be the stable model of $X := X_0(p^2N)_S$. The Weil parametrization $\phi : X_0(p^2N)_{\mathbf{Q}} \to E$, when pulled back to U, gives a morphism (still denoted ϕ) between the generic fibres of $\widetilde{X_U}$ and $\widetilde{\mathcal{E}_U}$. Let u be the closed point of U.

Proposition 4.2.1 *Suppose that E has potentially good reduction at p. Then the morphism ϕ extends to a morphism $\phi : \widetilde{X_U} \to \widetilde{\mathcal{E}_U}$.*

Proof. Let $\widetilde{X_U}^0$ be the open subscheme of $\widetilde{X_U}$ where the morphism $\widetilde{X_U} \to U$ is smooth (its complement is the set of double points in $\widetilde{X_{U,u}}$). By the Néron property of $\widetilde{\mathcal{E}_U}$ we get $\phi : \widetilde{X_U}^0 \to \widetilde{\mathcal{E}_U}$. It remains to extend this ϕ over

[1] It is not difficult to prove that I_0 and I_ν are excluded using the description by [Ka-Ma] of $X_0(p^2N)$

the double points. It follows from [Li] Thm.26.1 or Thm.4.1. that there is a composition $f : X' \to \widetilde{X_U}$ of blow ups in closed points of $\widetilde{X_U}$ such that ϕ can be extended to a morphism $\phi' : X' \to \widetilde{\mathcal{E}_U}$ (the normalizations in [Li] Thm. 26.1 do nothing in this case). Since $\widetilde{\mathcal{E}_{U,u}}$ is an elliptic curve, ϕ' contracts the exceptional divisor of X'. It follows that ϕ' factorizes through f, hence that ϕ extends over the double points.

We still suppose that E has potentially good reduction. Then we have two $\mu_n(S)$-equivariant diagrams:

$$\begin{array}{ccccccccc} \widetilde{X_U} & \xrightarrow{\phi} & \widetilde{\mathcal{E}_U} & \qquad & \widetilde{X_{U,u}} & \xrightarrow{\phi} & \widetilde{\mathcal{E}_{U,u}} \\ \searrow & & \swarrow & & \searrow & & \swarrow \\ & U & & & & u & \end{array}$$

It may be useful to note that by dividing out by part of the action of $\mu_n(S)$, one gets other versions of Proposition 4.2.1. Comparing the inertia actions on $\widetilde{X_{U,u}}$ (Section 2.3.3, Proposition 3.2.1, Proposition 3.2.2 and Proposition 3.2.4) and on $\widetilde{\mathcal{E}_{U,u}}$ (Proposition 4.1.1) gives lots of information. For the moment we only ask ourselves on which components ϕ has to be constant.

Proposition 4.2.2 *Suppose that E has potentially good reduction at p. Let $\phi : \widetilde{X_{U,u}} \to \widetilde{\mathcal{E}_{U,u}}$ be the Weil parametrization mod p (Proposition 4.2.1). Then ϕ is constant on the outer two vertical components. On the other components we have:*

type	p	hor. components	central vert. comps.
I_0^*		contracted	
II, IV, IV^*, II^*	$p \equiv 1(3)$	contracted	
	$p \equiv -1(3)$		contracted
III, III^*	$p \equiv 1(4)$	contracted	
	$p \equiv -1(4)$		contracted

The next thing we discuss is the degree of the Weil parametrization. We still suppose that E has potentially good reduction. Over the complement of a finite set of points of $\widetilde{\mathcal{E}_U}(u)$, the morphism $\phi : \widetilde{X_U} \to \widetilde{\mathcal{E}_U}$ is finite and flat. This gives the following proposition.

Proposition 4.2.3 *Suppose that E has potentially good reduction at p. Then the degree of $\phi : X_0(p^2N)_{\mathbf{Q}} \to E$ is the sum over the irreducible components C of $\widetilde{X_{U,u}}$ of the degrees of the $\phi|_C : C \to \widetilde{\mathcal{E}_{U,u}}$ (the degree of a constant map is zero).*

In the next section we will need some kind of "upper bound" on ϕ. This upper bound is a consequence of the injectivity of

$$\phi^* : E \longrightarrow J_0(p^2N)_{\mathbf{Q}}.$$

Proposition 4.2.4 *Let G be the kernel of $\phi^* : \widetilde{\mathcal{E}_{U,u}} \longrightarrow \widetilde{J_{U,u}}$. Then G is a finite group scheme, annihilated by some power of p. Suppose that $p > 7$, then we have:*

1. *if $\widetilde{\mathcal{E}_{U,u}}^0 \stackrel{\sim}{=} \mathbf{G}_{\mathrm{m},u}$ then $G \cap \widetilde{\mathcal{E}_{U,u}}^0 = 0$.*
2. *if $\widetilde{\mathcal{E}_{U,u}}$ is supersingular then either $G = 0$ or $G = \ker \mathrm{F} : \widetilde{\mathcal{E}_{U,u}} \to \widetilde{\mathcal{E}_{U,u}}$ (where F is the Frobenius morphism of degree p).*
3. *if $\widetilde{\mathcal{E}_{U,u}}$ is ordinary then either $G = 0$ or $G = \ker \mathrm{V} : \widetilde{\mathcal{E}_{U,u}} \to \widetilde{\mathcal{E}_{U,u}}$ (where V is the Verschiebung of degree p).*

Proof. The morphism $\phi^* : \widetilde{\mathcal{E}_U} \longrightarrow \widetilde{J_U}$ is injective on the generic fibre. This implies that ϕ^* is injective on the prime to p torsion in $\widetilde{\mathcal{E}_{U,u}}$. It follows that G is a finite group scheme consisting of p-power torsion.

Let $T \to S$ be the minimal base change such that E acquires stable reduction over T (this base change is given in Proposition 4.1.1). Then $T \to S$ is totally ramified of degree 2,3,4 or 6. Let $\widetilde{X_T}/T$ be the quotient of $\widetilde{X_U}/U$ by the action of $\mathrm{Gal}(U/T) \subset \mu_n(S)$. Then $\widetilde{X_T}/T$ satisfies property N^* of [Ra 1](6.1.4) and (6.1.6) since $\widetilde{X_T}$ is normal (being the quotient of $\widetilde{X_U}$ with $\widetilde{X_U}$ normal) and $\mathrm{H}^0(\widetilde{X_T}, \mathcal{O}_{\widetilde{X_T}}) = \mathcal{O}_T$ ($\mathcal{O}_T = \mathrm{Gal}(U/T)$-invariants in $\mathcal{O}_U = \mathrm{H}^0(\widetilde{X_U}, \mathcal{O}_{\widetilde{X_U}})$). By [Ra 1] Theorem 8.2.1, Proposition 8.0.1 and Proposition 8.1.2(ii) $\mathrm{Pic}^0_{\widetilde{X_T}/T}$ is representable by a smooth group scheme

$\widetilde{J_T}^0$ (we do not know whether $\widetilde{J_T}^0$ is the connected component of the Néron model of $J_0(p^2N)_{\mathbf{Q}}$ over T: $\widetilde{X_T}$ can have some singularities). If E has potentially multiplicative reduction at p, then $T \to S$ has degree 2, $\widetilde{X_T}$ is regular and $\widetilde{J_T}^0$ is the connected component of its Néron model. If E has potentially good reduction, then (by taking the quotient by $\mathrm{Gal}(U/T)$) we have $\phi : \widetilde{X_T} \to \widetilde{\mathcal{E}_T}$. In both cases we get a morphism $\phi^* : \widetilde{\mathcal{E}_T}^0 \to \widetilde{J_T}^0$. Since the absolute ramification index of T is less than $p-1$ we can apply [Ra 2] Corollaire 3.3.6.1 (see also [Ma 1] Proposition 1.1). It follows that $\phi^* : \widetilde{\mathcal{E}_T}^0 \to \widetilde{J_T}^0$ is injective. We have $\widetilde{\mathcal{E}_U}^0 = \widetilde{\mathcal{E}_{T,U}}^0$ because $\widetilde{\mathcal{E}_T}$ is stable. The morphism $\phi^* : \widetilde{\mathcal{E}_U}^0 \to \widetilde{J_U}^0$ is the composition:

$$\widetilde{\mathcal{E}_{T,U}}^0 \longrightarrow \widetilde{J_{T,U}}^0 \longrightarrow \widetilde{J_U}^0$$

and we know that the first one of these two is an injection. We conclude that:

$$\ker(\phi^* : \widetilde{\mathcal{E}_{U,u}}^0 \to \widetilde{J_{U,u}}^0) = \widetilde{\mathcal{E}_{T,t}}^0 \cap \ker(\widetilde{J_{T,t}}^0 \to \widetilde{J_{U,u}}^0).$$

Claim. The kernel of $\widetilde{J_{T,t}}^0 \to \widetilde{J_{U,u}}^0$ is purely additive: it is isomorphic to a direct sum of $\mathrm{G}_{a,t}$'s.

Proof (of the claim). For the moment, let X denote $\widetilde{X_{U,u}}$ and let Y denote $\widetilde{X_{T,t}}$. Then $\widetilde{J_{T,t}}^0 = \mathrm{Pic}^0_{Y/t}$ and $\widetilde{J_{U,u}}^0 = \mathrm{Pic}^0_{X/u}$, the morphism between them is the pullback along $X \to Y$. Since X is reduced, this morphism has the facorization $X \to Y_{\mathrm{red}} \to Y$. On Y we have the exact sequence of sheaves:

$$0 \to \mathcal{I} \to \mathcal{O}_Y \to \mathcal{O}_{Y_{\mathrm{red}}} \to 0.$$

The multiplicities of the components of Y are at most $\frac{p+1}{2}$, hence less than p. This means that we get an exact sequence:

$$0 \to \mathcal{I} \overset{\exp}{\to} \mathcal{O}_Y^* \to \mathcal{O}_{Y_{\mathrm{red}}}^* \to 1$$

where exp is given by the usual power series (note that for f a local section of $\mathcal{I}$ we have $f^p = 0$). Taking $\mathrm{H}^1(Y, -)$ gives an exact sequence:

$$0 \to \mathrm{H}^1(Y, \mathcal{I}) \to \mathrm{Pic}(Y) \to \mathrm{Pic}(Y_{\mathrm{red}}) \to 0.$$

We conclude that $\ker(\mathrm{Pic}^0_{Y/t} \to \mathrm{Pic}^0_{Y_{\mathrm{red}}/t})$ is purely additive. Let $\widetilde{X}$ and $\widetilde{Y_{\mathrm{red}}}$ denote the normalizations of X and Y_{red}. Then we have a diagram with exact rows:

$$\begin{array}{ccccccccc}
0 & \to & T_Y & \to & \mathrm{Pic}^0_{Y_{\mathrm{red}}/t} & \to & \mathrm{Pic}^0_{\widetilde{Y_{\mathrm{red}}}/t} & \to & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \to & T_X & \to & \mathrm{Pic}^0_{X/u} & \to & \mathrm{Pic}^0_{\widetilde{X}/u} & \to & 0
\end{array}$$

It is not difficult to check that the morphisms $T_Y \to T_X$ and $\mathrm{Pic}^0_{\widetilde{Y_{\mathrm{red}}}/t} \to \mathrm{Pic}^0_{\widetilde{X}/u}$ are injective (for the latter case one can use the fact that on every component of $\widetilde{Y_{\mathrm{red}}}$ there are points over which the ramification is total). This completes the proof of the claim.

It remains to find out what the intersection of $\widetilde{\mathcal{E}}^{\,0}_{T,t}$ with a direct sum of additive groups can be. If $\widetilde{\mathcal{E}}^{\,0}_{T,t} \overset{\sim}{=} \mathrm{G}_{m,t}$ then this intersection is 0, because $\mu_{p,t}$ cannot be embedded in a direct sum of copies of $\mathrm{G}_{a,t}$. If $\widetilde{\mathcal{E}}^{\,0}_{T,t}$ is an ordinary elliptic curve over t, then its p^m-torsion is isomorphic to $\mu_{p^m,t} \times \mathbf{Z}/p^m$ and it follows that the intersection is at most $\mathbf{Z}/p$, the kernel of V. If $\widetilde{\mathcal{E}}^{\,0}_{T,t}$ is a supersingular elliptic curve, then its p-torsion subgroup is a group scheme called M_2 (see [Oo 1](15.5)). This M_2 cannot be embedded in a direct sum of additive groups, hence the intersection is at most the Frobenius kernel (which is isomorphic to $\alpha_{p,t}$). This completes the proof of the proposition.

Remark. The condition "$p > 7$" is a bit stronger than we need: the proof also works without change if :

1. E is of type I_ν^* or I_0^* and $p > 3$,

2. E is of type III or III^* and $p > 5$,

3. E is of type IV or IV^* and $p > 3$.

If E has type I_ν^* the proposition is even true for all p. One can show for $p = 5$, 7 that G is contained in $\ker \mathrm{F} * 2$ or in $\ker \mathrm{V} * 2$.

4.3 Horizontal Weil curves.

Let p and N be as in the preceding section. In this section we investigate the strong Weil curves of conductor p^2N that are parametrized by the horizontal components. Proposition 4.2.2 tells us that these are the strong Weil curves with reduction type (at p): II, IV, IV^* or II^* if $p \equiv -1(3)$ and III or III^* if $p \equiv -1(4)$. Equivalently, they are the strong Weil curves with potentially good, supersingular reduction at p, that are not of type I_0^*. Let $\phi : X \to E$ be the strong Weil parametrization over $\overline{\mathbf{F}}_p$ between the stable reductions of $X_0(p^2N)$ and the Weil curve (Proposition 4.2.1). Let d be the order of the inertia action on E (this is the number "n" in Proposition 4.1.1), hence $d \in \{3, 4, 6\}$ and $p \equiv -1(d)$. Let C_x be the horizontal component in X corresponding to a supersingular point $x \in X_0(N)(\overline{\mathbf{F}}_p)$. Then $\phi|_{C_x} : C_x \to E$ factorizes as:

$$C_x \longrightarrow C_{x(d)} \xrightarrow{\phi_x} E$$

(for $C_x \to C_{x(d)}$, see Proposition 3.2.4 and Table 3.2.5). If $C_{x(d)}$ happens to have genus 0, then $\phi_x = 0$ (of course). In the other cases, $C_{x(d)}$ is isomorphic to E. For every such x, we choose an isomorphism : $E \tilde{\to} C_{x(d)}$. The ϕ_x are now elements of $\mathrm{End}_{\overline{\mathbf{F}}_p}(E)$. Since E is supersingular, its ring of endomorphisms is a maximal order in a quaternion algebra. Let $\zeta_d \in \mathbf{F}_{p^2}$ be a primitive d-th root of 1 and let $\mathrm{F} : E \to E$ be the $\overline{\mathbf{F}}_p$-linear Frobenius of degree p (note that indeed $E^{(p)} = E$). Then in $\mathrm{End}_{\overline{\mathbf{F}}_p}(E)$ we have the commutation rule: $\mathrm{F}\zeta_d = \zeta_d^{-1}\mathrm{F}$.

Proposition 4.3.1 *1. If the strong Weil curve has reduction type II, III or IV, then $\phi_x \in \mathbf{Z}[\zeta_d]$, let $\psi_x := \phi_x$.*

2. *In the other cases (reduction types IV^*, III^* and II^*) we have $\phi_x \in \mathrm{F}\mathbf{Z}[\zeta_d]$, we write $\phi_x = \mathrm{F}\psi_x$, with $\psi_x \in \mathbf{Z}[\zeta_d]$.*

3. *for all x, x':*

$$\psi_x \equiv \psi_{x'} \mod \begin{cases} 1 - \zeta_3 & if \quad d = 3 \\ 2 & if \quad d = 4 \\ 1 + \zeta_6 & if \quad d = 6. \end{cases}$$

4.

$$g.c.d.((\psi_x)_x) \in \begin{cases} \{1, 1-\zeta_3\} & if \quad d=3 \\ \{1, 1+i, 2\} & if \quad d=4 \\ \{1, 1+\zeta_6\} & if \quad d=6. \end{cases}$$

Proof. Comparing the inertia actions on X (Section 2.3.3, Propositions 3.2.1, 3.2.2 and 3.2.4) and on E (Proposition 4.1.1) gives (1) and (2). We give the proof for parts (3) and (4) for $d=4$ only. The other 2 cases can be done in the same way. The 4 intersection points of the horizontal component C_x with the vertical components map to 4 points on the elliptic curve $C_{x(4)}$. The cusp "∞" lies on one of the outer two vertical components, choose the corresponding point on $C_{x(4)}$ as origin. Then the other 3 points are the 2-torsion points (one of them is fixed by i, the other two by i^2). Part (3) of the proposition now follows from the fact that ϕ contracts the vertical components.

Let $X \to X_{(4)}$ be the quotient by the action of $\mu_{\frac{n}{4}}(\mathbf{F}_{p^2})$ on X. Then $\phi : X \to E$ factorizes as:

$$X \longrightarrow X_{(4)} \xrightarrow{\phi_{(4)}} E.$$

From Proposition 4.2.4 we get: $\ker(\phi^*_{(4)} : E \to \mathrm{Pic}^0_{X_{(4)}/t})$ is either 0 or $\ker \mathrm{F}$. We will now construct a commutative diagram:

$$\begin{array}{ccc} X_{(4)} & \longrightarrow & Y \\ \downarrow \phi_{(4)} & & \downarrow \\ E & \xrightarrow{2} & E \end{array}$$

The components of Y are: one copy of $X_0(N)_t$ and the horizontal components $C_{x(4)}$ of $X_{(4)}$. The origin of each $C_{x(4)}$ is glued to $x \in X_0(N)(\overline{\mathbf{F}}_p)$. The vertical components of $X_{(4)}$ are canonically isomorphic to $X_0(N)_t$. The morphism $X_{(4)} \to Y$ is multiplication by two on the horizontal components and the canonical isomorphism on the vertical components. The morphism

$Y \to E$ contracts the vertical component and is ϕ_x on the component $C_{x(4)}$. Taking Pic^0 we obtain a commutative diagram:

$$\begin{array}{ccc} \mathrm{Pic}^0_{X_{(4)}/t} & \longleftarrow & \oplus_x C_{x(4)} \\ \uparrow \phi^*_{(4)} & & \uparrow \oplus\phi^*_x \\ E & \xleftarrow{2} & E \end{array}$$

Part (4) of the proposition is now a consequence of the fact that $\ker(2\phi^*_{(4)})$ is either $E[2]$ or $E[2\mathrm{F}]$.

Remarks.

1. It follows from (3) and (4) that usually we will have to expect that the g.c.d. of the ψ_x is maximal.
2. If one of the $C_{x(d)}$ has genus 0 then the g.c.d. of the ψ_x is maximal.

It is known that twists of Weil curves are again Weil curves. The quadratic twist of the horizontal curves we consider over the unique quadratic extension of $\mathbf{Q}$ ramified only at p is again a Weil curve of conductor p^2N. This twist acts on the reduction types as follows:

original type	II	III	IV	IV^*	III^*	II^*
type of twist	IV^*	III^*	III^*	II	III	IV

(4.3.1.1)

We see that the twist is again a horizontal Weil curve. We will now discuss the relation between the two strong Weil parametrizations.

Theorem 4.3.2 *Let E be a strong, horizontal Weil curve. Let ϕ denote its (strong) Weil parametrization. Let $\widetilde{E}$ denote the strong Weil curve that is isogenous to the twist of E over the quadratic extension of $\mathbf{Q}$ that is ramified only at p. Let $\tilde{\phi}$ denote its strong Weil parametrization. Then we have $\deg(\tilde{\phi}) = \frac{a}{b}p^{\varepsilon}\deg(\phi)$, with $a, b \in \{1,2,4\}$ if $d = 4$, $a, b \in \{1,3\}$ if $d = 3,6$ and $\varepsilon \in \{-1,0,1\}$. If E has reduction type II, III or IV (at p) then $\varepsilon \in \{0,1\}$. If E has reduction type IV^*, III^* or II^* (at p) then $\varepsilon \in \{0,-1\}$.*

Proof. The proof gives much more information than the theorem itself: we will describe $\tilde{\phi}$ in terms of ϕ (up to a small factor). Let $\psi := (\psi_x)_x$ be the vector with coefficients in $\mathbf{Z}[\zeta_d]$ associated to ϕ and let $\tilde{\psi}$ be the same for $\tilde{\phi}$. We will show that $\deg(\psi)$ and $\deg(\tilde{\psi})$ difer only by one of the factors listed in Proposition 4.3.1(4). The factor p is then explained by the Frobenius occurring in Proposition 4.3.1(1) and (2).

In the proof we will use some properties of the Hecke operators T_m on the horizontal part. We describe these properties in terms of the matrix of T_m, but then we have to be a bit careful with the choice of isomorphisms between the horizontal components. Let x and x' be supersingular points in $X_0(N)(\overline{\mathbf{F}}_p)$. Let A and A' be the supersingular elliptic curves associated to x and x'. Then an isogeny $A \to A'$ of degree prime to p induces an isomorphism $C_x \tilde{\to} C_{x'}$ (see Section 3.4, between step 3 and step 4). We demand that for all x and x' the identification $C_x \tilde{\to} C_{x'}$ is induced by an isogeny $A \to A'$ whose degree is a square in $\mathbf{F}_p^*$. Now let $\varphi : x \to x'$ be an isogeny of degree m. Then it is not hard to see that the contribution of φ to T_m(this is an element of $\mu_{p+1}(\mathbf{F}_{p^2})$, see Sections 3.3 and 3.4) is in $\mu_{\frac{p+1}{2}}$ if and only if $(\frac{m}{p}) = 1$, where $(\frac{m}{p})$ denotes the Legendre symbol.

All the horizontal components are given by the equation $y^2 = x^{p+1} + 1$. On the disjoint union of the horizontal components we define an involution α by:

$$\alpha^{\#} : \begin{cases} x & \mapsto & x^{-1} \\ y & \mapsto & yx^{-\frac{p+1}{2}} \end{cases}$$

For $\zeta \in \mu_{p+1}(\mathbf{F}_{p^2})$ we find (see Formula 2.3.3.1):

$$(\alpha\zeta\alpha)^{\#} : \begin{cases} x & \mapsto & \zeta x \\ y & \mapsto & y \end{cases}$$

It follows that on the jacobian of each horizontal curve we have:

$$(\alpha\zeta\alpha)^* = [\zeta^{\frac{p+1}{2}}]\zeta^{-1*} \tag{4.3.2.1}$$

where $[\zeta^{\frac{p+1}{2}}]$ is multiplication by ± 1. This formula implies that α^* exchanges the 3- and 6-parts, and maps the 4-part to itself. We have just seen that all contributions to T_m are either squares or non-squares (in $\mu_{p+1}(\mathbf{F}_{p^2})$). It follows that:

$$\alpha^* T_m \alpha^* = (\frac{m}{p}) \overline{T_m} \qquad (4.3.2.2)$$

where the bar denotes complex conjugation. We conclude that:

$$T_m \alpha^* \bar{\psi}^* = \alpha^* \alpha^* T_m \alpha^* \bar{\psi}^* = (\frac{m}{p}) \alpha^* \overline{T_m} \bar{\psi}^* = (\frac{m}{p}) a_m \alpha^* \bar{\psi}^*$$

if $T_m \psi^* = a_m \psi^*$. It follows that up to one of the factors of Proposition 4.3.1(4) we have $\tilde{\psi}^* = \alpha^* \bar{\psi}^*$. The proof is finished.

Remarks.

1. It follows from the proof that if the conditions (3) and (4) of Proposition 4.3.1 force the g.c.d. of the ψ_x to be maximal, then they also force the g.c.d. of the $\tilde{\psi}_x$ to be maximal. The factor $\frac{a}{b}$ in the theorem is then 1.

2. Combining the theorem with a computation similar to one of Zagier ([Za], page 382) one gets the result that the factor $\frac{a}{b}$ is always 1.

4.4 Examples: conductor p^2.

In this section we discuss some examples of horizontal Weil curves of conductor p^2. These examples were obtained by a computer calculation using the algorithm described in Section 3.4.

For primes p up to $3,500$ the matrices of T_2 on the horizontal 3,4 and 6-parts of $J_0(p^2)$ were computed. Then the program computed the dimensions of the eigenspaces with eigenvalues $-2, -1, 0, 1, 2$. For one dimensional eigenspaces the program computed an eigenvector.

The program was written in Pascal and executed on a (1-megabyte) Atari ST home computer. The reason to stop at $3,500$ was the limitation on the memory: the matrix of T_2 was implemented as a two dimensional array. If the program would take into account the sparsity of the matrix of T_2 one could go much further (not quite as far as Mestre and Oesterlé, since their matrices are twice as small).

Another program, written (in C) by drs. A. de Groot, looked for solutions of the equation: $c_4^3 - c_6^2 = 12^3\Delta$, where Δ was supposed to $\pm p^2$, $\pm p^3$ or $\pm p^4$. For each solution, this program computed the minimal Weierstrass equation (using Tate's algorithm [Ta]) of the corresponding elliptic curve over $\mathbf{Q}$ and checked whether its conductor was p^2. The list of elliptic curves of conductor p^2 found by this program is contained in [E-G-T].

For every Weil curve detected by the first program, the second program found an elliptic curve over $\mathbf{Q}$ with the right reduction type. In order to actually *prove* that these curves are the same (or at least isogenous) one should bound the c_4 and c_6 of the Weil curve (as in [Me-Oe]) in terms of p and the degree of the Weil parametrization (which can be computed from the eigenvector) and check that below this bound there is no other elliptic curve with the right discriminant and a_2. This has not (yet) been done.

For every elliptic curve found by the search program that should be a horizontal Weil curve (potentially supersingular reduction at p), the eigenspace of $\mathbb{T}_2$ for the corresponding eigenvalue had the right dimension (the twist over $\mathbf{Q}(\sqrt{\pm p})$ can be in the same eigenspace!).

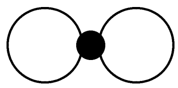
4.4.1 Complex multiplication curves.

For $p = 7, 11, 19, 43, 67$ and 163 the 0-eigenspace for $\mathbb{T}_2$ acting on the 4-part is one dimensional. These eigenspaces correspond to the complex multiplication curves over $\mathbf{Q}$ of conductor p^2. Equations for them can be found in [Gr] (24).

1. $p = 7$. $X_0(7^2)$ is an elliptic curve, the degree d of the strong Weil parametrization is 1.

2. $p = 11$. From the description of the stable model of $X_0(11^2)$ in Section 3.5.2 it follows that $d = \frac{11+1}{3} = 4$ (according to the tables in [Bi-Ku] the strong Weil curve is of type III).

3. $p = 19$. The graph for T_2 on the 4-part is:



   For the degree d of the strong Weil parametrization we find $\frac{19+1}{4} \cdot 4 = 20$ (according to Cremona [Cr] the strong Weil curve has reduction type III).

4. $p = 43$. The matrix of T_2 acting on the 4-part is:

$$\begin{pmatrix} 0 & -i & i \\ i & 0 & -2i \\ -i & 2i & 0 \end{pmatrix} = i \cdot \begin{pmatrix} 0 & -1 & 1 \\ 1 & 0 & -2 \\ -1 & 2 & 0 \end{pmatrix}.$$

   This matrix differs from the one in Section 3.5.3 because the identifications between the horizontal components are different. The primitive eigenvector with eigenvalue 0 is now $(2,1,1)$. It follows that the vector $(\psi_x)_x$ is $(0,4,2,2)$. The degree d of the Weil parametrization is

$$\frac{43+1}{4} \cdot 4 \cdot (0^2 + 2^2 + 1^2 + 1^2) \cdot 43^{\varepsilon} = 2^3 \cdot 3 \cdot 11 \cdot 43^{\varepsilon}$$

   where $\varepsilon = 0$ (or 1) if the reduction type of the strong Weil curve is III (or III^*).

5. For $p = 67$ we find: $d = 2^2 \cdot 17 \cdot 19 \cdot 67^{0,1}$.

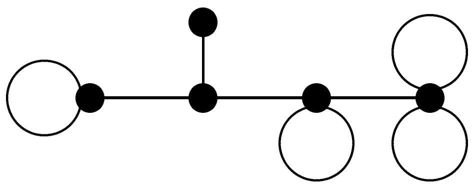
6. For $p = 163$ we find: $d = 2^3 \cdot 41 \cdot 181 \cdot 163^{0,1}$.

Remark. It follows from work of Stevens ([St] Thm. 6.4) that in these examples of complex multiplication curves the strong curve has reduction type III at p. This implies that the à priori possible factor p in the degree of the parametrizations does not occur.

For all primes $p \equiv 3(8)$ up to $3,500$ (except $p = 3$) the dimension of the 0-eigenspace of T_2 acting on the 4-part turned out to be exactly the class number of $\mathbf{Q}(\sqrt{-p})$. The corresponding abelian variety should be the Weil restriction of scalars of an elliptic curve with complex multiplication (cf. [Gr] (20), or [Sh]). This has not been checked.

4.4.2 Another example: $p = 47$.

Let $p = 47$. The graph of T_2 is:



The matrix of T_2 acting on the 3-part is:

$$\begin{pmatrix} 1 & 2 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & -1 \end{pmatrix}$$

with characteristic polynomial $(x+1)(x^3 - 2x^2 - 3x + 5)$. The vector $(1, -1, 0, 1)$ is an eigenvector with eigenvector -1. However, this is *not* the vector $(\psi_x)_x$ describing the Weil parametrization. The vector $(\psi_x)_x$ is an eigenvector of the transposed martix. One gets:

$$(\psi_x)_x = (1 - \zeta_3) \cdot (0, 1, -2, 0, 2)$$

and the degree of the strong Weil parametrization is:

$$\frac{47+1}{3} \cdot 3 \cdot (1^2 + 2^2 + 2^2) \cdot 47^{\varepsilon} = 2^4 \cdot 3^3 \cdot 47^{\varepsilon}$$

where $\varepsilon = 0$ (or 1) if the reduction type of the corresponding strong Weil curve is IV (or IV^*). Until now we do not know how to see whether $\varepsilon = 0$ or 1.

4.5 Vertical Weil curves.

Let p and N be as before: $p > 7$ and p doesn't divide N. In this section we consider strong Weil curves of conductor p^2N that are parametrized (mod p) by the vertical components. We exclude the reduction types I_0^* and I_ν^*. According to Proposition 4.2.2 we are left with the strong Weil curves with potentially good, ordinary reduction at p, that are not of type I_0^*. Let $\phi : X \to E$ be the strong Weil parametrization over $\overline{\mathbf{F}}_p$ between the stable reductions of $X_0(p^2N)$ and the Weil curve (cf. Proposition 4.2.1). Let d be the order of the inertia action on E (this is the number "n" in Proposition 4.1.1), hence $d \in \{3, 4, 6\}$ and $p \equiv 1(d)$. Let C_1 and C_2 be the central vertical components of X and let $\phi_i : C_i \to E$ be the restriction of ϕ to C_i. Let ζ_{p-1} be a generator of $\mu_{p-1}(\mathbf{F}_p)$. The inertia action of $\mu_{p-1}(\mathbf{F}_p)$ is given in the formulas 2.2.0.2 and 2.2.0.3. We choose an isomorphism:

$$\overline{\mathrm{M}}([\Gamma_0(N)], [Ig(p)/\pm 1]) \tilde{\longrightarrow} C_1.$$

We identify C_2 with the Igusa curve by using this isomorphism composed with $\zeta_{p-1} : C_1 \tilde{\to} C_2$. Let ζ_d be the primitive d-th root of unity (in $\mathbf{F}_p$) by which ζ_{p-1} acts on E (see Proposition 4.1.1). Since ϕ commutes with the inertia action, we have $\phi\zeta_{p-1} = \zeta_d\phi$, giving:

$$\phi_2 = \zeta_d\phi_1 \qquad (4.5.0.1)$$

Because E is ordinary, we have $\mathrm{End}_{\overline{\mathbf{F}}_p}(E) = \mathbf{Z}[\zeta_d]$. Let $J := \mathrm{Pic}^0_{X/\overline{\mathbf{F}}_p}$, and let:

$$0 \to T \to J \to A \to 0$$

be its decomposition in a toric and abelian variety part.

Proposition 4.5.1 $\ker(\phi_1^*)$ *is a subgroup scheme of* $\ker((\zeta_d^2 - 1)\mathrm{V})$.

Proof. Recall (Proposition 4.2.4) that

$$G := \ker(\phi^* : E \to J) \subset \ker(\mathrm{V}).$$

It follows that $\ker(\phi_1^*)/G = (\phi^*E) \cap T$. The inertia action on the torus T has order 2, implying that $\mathrm{V}\ker(\phi_1^*)$ is contained in $\ker(\zeta_d^2 - 1)$.

Proposition 4.5.2 *Let $\tilde{\phi} : X \to \widetilde{E}$ denote the strong Weil parametrization (reduced mod p) corresponding to the twist of E over the quadratic extension of $\mathbf{Q}$ that is ramified only at p. Then:*

$$\deg(\tilde{\phi}) = \frac{a}{b} p^{\varepsilon} \deg(\phi)$$

with $\varepsilon \in \{-1, 0, 1\}$, $a, b \in \{1, 2, 4\}$ if $d = 4$ and $a, b \in \{1, 3\}$ if $d = 3$ or $d = 6$. Moreover, if $\varepsilon = 1$ the ϕ is separable and $\tilde{\phi}$ is inseparable. If $\varepsilon = -1$ then $\tilde{\phi}$ is separable and ϕ is inseparable.

Proof. Let ψ denote the separable part of ϕ. It follows from Proposition 4.2.4 that $\phi = \mathrm{F}^{0,1}\psi$. Let ψ_i be the restriction of ψ to C_i. Put $\tilde{\psi}_1 := \psi_1$ and $\tilde{\psi}_2 := -\psi_2$. Let m be prime to p, then we have $\mathrm{T}_m \phi^* = a_m \phi^*$ with $a_m \in \mathbf{Z}$. If $(\frac{m}{p}) = 1$, then T_m preserves the components C_1 and C_2. It follows immediately that in this case $\mathrm{T}_m \tilde{\psi}^* = a_m \tilde{\psi}^*$. If $(\frac{m}{p}) = -1$ then T_m interchanges C_1 and C_2. We find $\zeta_{p-1}^* \mathrm{T}_m \tilde{\psi}_1^* = -a_m \tilde{\psi}_2^*$, implying that $\mathrm{T}_m \tilde{\psi}^* = -a_m \tilde{\psi}^*$. Thus $\tilde{\psi} : X \to E$ is an eigenvector for the Hecke operators T_m (m prime to pN) and its eigenvalues are those of ϕ, but twisted by $(\frac{m}{p})$. This implies that $\tilde{\psi}^*$ and $\tilde{\phi}^*$ have the same image in J. The proposition now follows from Proposition 4.5.1.

Remark. As in the remarks following Theorem 4.3.2 one can show that the factor $\frac{a}{b}$ is 1. One can also show that $\varepsilon \neq 0$. It would be very useful (especially in the next section) to know how the seperability of ϕ is related to the reduction type of E.

4.6 The constant c of a Weil curve.

Let $\phi : X_0(M)_{\mathbf{Q}} \to E$ be a strong Weil parametrization. The relative cotangent space at the zero section of the Néron model of E over $\mathbf{Z}$ is a rank 1 (locally) free $\mathbf{Z}$ module, let $\omega_{\mathbf{Z}}$ be one of the two generators. Then $\omega_{\mathbf{Z}}$ is called a Néron differential on E. The differential form $\phi^*\omega_{\mathbf{Z}}$ is an eigenvector for the Hecke algebra, with the same eigenvalues as the normalized newform $\sum_{n \geq 1} a_n q^n \frac{dq}{q}$ corresponding to E (normalized means: $a_1 = 1$). It follows that we have:

$$\phi^*\omega_{\mathbf{Z}} = c\sum_{n\geq 1} a_n q^n \frac{dq}{q}$$

with $c \in \mathbf{Q}^*$. Changing $\omega_{\mathbf{Z}}$ by a factor ± 1 we can achieve that $c > 0$. Manin has conjectured that $c = 1$ (c is sometimes called the Manin constant of E).

Proposition 4.6.1 *The number c is an integer.*

Proof. Let $X_0(M)$ be the compactified coarse moduli scheme $\overline{\mathrm{M}}([\Gamma_0(M)])$ (cf. [Ka-Ma] (8.6)). Let $X_0(M)^0$ be the open part of $X_0(M)$ where the projection to $\mathrm{Spec}(\mathbf{Z})$ is smooth. Let $\mathcal{E}$ be the Néron model of E over $\mathbf{Z}$. By the Néron property ϕ extends to $\phi : X_0(M)^0 \longrightarrow \mathcal{E}$. It follows immediately from [Ka-Ma] Thm.8.11.10 that the formal completion of $X_0(M)$ along the (unramified) cusp ∞ is $\mathrm{Spf}(\mathbf{Z}[[q]])$. We see that $\infty \in X_0(M)^0(\mathbf{Z})$ and that $\phi^*\omega_{\mathbf{Z}}$ is a differential form (without poles!) in a neighborhood of ∞. If c would not be integral, then $\phi^*\omega_{\mathbf{Z}}$ would have poles along the fibers of $X_0(M)^0$ in characteristics dividing the denominator of c.

Remark. This proposition is sometimes attributed to Gabber (not published). The analogous result for parametrizations involving the modular curve $X_1(M)$ is proved by Stevens in [St].

Next we cite a result of Mazur ([Ma 1] Corollary 4.1).

Theorem 4.6.2 (Mazur) *Let m be the largest square dividing M, then c is a unit in $\mathbf{Z}[\frac{1}{2m}]$.*

In other words, if p is a prime different from 2 such that E has stable reduction at p, then p does not divide c. Our aim is to prove the following theorem.

Theorem 4.6.3 *Let E be a strong Weil curve. Let $p > 7$ be a prime such that:*

1. *E has additive reduction at p, not of type I_0^* or I_ν^*,*
2. *E does not admit an isogeny (over $\mathbf{Q}$) of degree p.*

If E has potentially supersingular reduction at p then p does not divide the (Manin) constant c attached to E. Let $\widetilde{E}$ be the strong Weil curve in the isogeny class of the twist of E over the quadratic extension of $\mathbf{Q}$ that is ramified only at p. Let $\tilde{c}$ be its Manin constant. If E has potentially ordinary reduction then p divides $c\tilde{c}$ at most once.

Remarks. 1. By the deep theorem [Ma 1] Thm. 7.1 of Mazur on rational isogenies, condition (2) is satisfied for $p \notin \{2, 3, 5, 7, 11, 13, 17, 19, 37, 43, 67, 163\}$. Moreover, the list of elliptic curves over $\mathbf{Q}$ admitting an isogeny of degree $p > 13$ (p a prime) is finite (up to twist).
2. In the beautiful paper [St] Stevens studies parametrizations of Weil curves by the modular curves $X_1(M)$. He conjectures ([St] Conj. I) that *every* Weil curve E (not just the strong ones) admits a parametrization by $X_1(M)$ (where M is the conductor of E) with Manin constant equal to 1. He shows this conjecture to be compatible with quadratic twists over fields that are unramified at the primes where E has additive reduction. He also shows, using results of Rubin on special values of L-functions, that a weak form of his conjecture holds for certain elliptic curves with complex multiplication.

It is easy to show that up to primes that can occur as degrees of isogenies over $\mathbf{Q}$ (see the list above) his version of Manin's conjecture is equivalent to Manin's conjecture. It follows that the Manin constant c of a strong Weil curve E is not divisible by primes $p > 163$ where E has reduction type I_0^* or I_ν^*. Combining the results of Stevens on complex multiplication curves with the results in this thesis one can show that elliptic curves over $\mathbf{Q}$ with complex multiplication by $\mathbf{Q}(\sqrt{-p})$, $p > 3$, have Manin constants (in the original sense as well as in the sense of Stevens) equal to 1 or 2.

We will first prove the following lemma.

Lemma 4.6.4 *Let E be a strong Weil curve with potentially good reduction at a prime $p > 7$. Suppose that the stable reduction mod p of its Weil parametrization (Proposition 4.2.1) is not inseparable on all the irreducible components. Then p does not divide the constant c of E.*

Proof. We use the notation of Section 4.2: let $\phi : \widetilde{X_U} \to \widetilde{\mathcal{E}_U}$ be the Weil parametrization extended to the stable models over U ($S = \mathrm{Spec}(W(\overline{\mathbf{F}}_p))$,

$U = S[\pi]$, $\pi^n = p$, $n = \frac{p^2-1}{2}$). Let ω_S be a generator of $\omega_{\mathcal{E}_S/S}$. Let $\omega_U := \pi^a \omega_S$ where a is as follows:

type	II	III	IV	I_0^*	IV^*	III^*	II^*
a	$\frac{1}{6}\cdot\frac{p^2-1}{2}$	$\frac{1}{4}\cdot\frac{p^2-1}{2}$	$\frac{1}{3}\cdot\frac{p^2-1}{2}$	$\frac{1}{2}\cdot\frac{p^2-1}{2}$	$\frac{2}{3}\cdot\frac{p^2-1}{2}$	$\frac{3}{4}\cdot\frac{p^2-1}{2}$	$\frac{5}{6}\cdot\frac{p^2-1}{2}$

(4.6.4.1)

Then according to Proposition 4.1.2 ω_U is a generator of $\omega_{\widetilde{\mathcal{E}_U}/U}$. Its pullback $\phi^*\omega_U$ is a differential form on $\widetilde{X_U}$. The $\mathcal{O}_{\widetilde{X_U}}$ module $\Omega_{\widetilde{X_U}}$ of (Kähler) differentials is invertible outside the double points of $\widetilde{X_{U,u}}$. We will investigate the multiplicities of the irreducible components of $\widetilde{X_{U,u}}$ in the divisor (of zeros) of $\phi^*\omega_U$. We replace the strong Weil parametrization $\phi : X_0(p^2N)_{\mathbf{Q}} \to E$ by a composition:

$$X_0(p^2Nm)_{\mathbf{Q}} \longrightarrow X_0(p^2N)_{\mathbf{Q}} \longrightarrow E$$

where m is prime to p, $X_0(p^2Nm) \to X_0(p^2N)$ is the usual morphism and points in $X_0(p^2Nm)(s)$ have no extra automorphisms. This does not change the multiplicities that we want to know. In order to deal with the double points we use the embedding

$$0 \longrightarrow \Omega_{\widetilde{X_U}} \longrightarrow \omega_{\widetilde{X_U}}$$

of $\Omega_{\widetilde{X_U}}$ in the invertible sheaf of the socalled "regular" differentials ($\omega_{\widetilde{X_U}}$ is the dualizing sheaf, cf. [De-Ra] I.2).

Suppose now that E is a horizontal Weil curve. Then E has reduction type II, III or IV (see Proposition 4.3.1). Since ϕ is not inseparable mod p, there must be a horizontal component C_x such that $\phi^*\omega_U$ is not zero on C_x. The action of $\mu_n(\mathbf{F}_{p^2})$ on this differential form is by χ^a (χ is the identity: $\mu_n(\mathbf{F}_{p^2}) \to \mu_n(\mathbf{F}_{p^2})$). The action of $\mu_n(\mathbf{F}_{p^2})$ on the cotangent space to C_x at the intersection point x of C_x with an outer vertical component is by $\chi^{\frac{p-1}{2}}$ (see Section 2.3.3). Let z be a local coordinate on C_x at x. It follows that $\phi^*\omega_U|_{C_x}$ is of the form:

$$(z^b + \text{higher terms})\frac{dz}{z}$$

with $b \equiv \frac{2a}{p-1} \mathrm{mod}(p+1)$. The genus of C_x is $\frac{p-1}{2}$, hence $\phi^*\omega_U$ has exactly $p-3$ zeros. It follows that $b = \frac{2a}{p-1}$. This number b is the order of vanishing of $\phi^*\omega_U$ at x as a section of the sheaf $\omega_{\widetilde{X_U}}$ restricted to C_x. Obviously this puts a bound on the multiplicity of the outer vertical component in the divisor of $\phi^*\omega_U$, but we have to be a bit careful because $\widetilde{X_U}$ has a singularity at x (Section 2.3.2). An easy computation (see Lemma 4.6.5) shows that $\phi^*\omega_U$ has a zero of order at most $\frac{p-1}{2}\frac{2a}{p-1} = a$ along the vertical component on which the cusp ∞ lies. But this means that $\phi^*\omega_S = \pi^{-a}\phi^*\omega_U$ does *not* vanish on this vertical component. We conclude that in this case p does not divide c.

Now suppose that E is a vertical Weil curve. Then $\phi^*\omega_U$ vanishes on the horizontal and outer vertical components, but doesn't vanish on the two central vertical components. We pick one of these two components, call it C. The action of $\mu_{\frac{n}{2}}(\mathbf{F}_{p^2})$ on $\phi^*\omega_U|_C$ is by χ^a. The action of $\mu_{\frac{n}{2}}(\mathbf{F}_{p^2})$ on the cotangent space at a supersingular point x of C is by $\chi^{\frac{p+1}{2}}$ (see Section 2.3.3). Let z be a local coordinate at x. Then $\phi^*\omega_U$ is of the form:

$$(z^b + \text{higher terms})\frac{dz}{z}$$

with $b \equiv \frac{2a}{p+1}\mathrm{mod}(\frac{p-1}{2})$. We will now compute the degree of the canonical divisor of C. On $X_0(Nm)_s$ we have the Kodaira-Spencer isomorphism:

$$\underline{\omega}^{\otimes 2} \xrightarrow{\sim} \Omega(\text{cusps})$$

(cf. [Ka-Ma] Thm.10.13.11, note that ± 1 are the only automorphisms of points in $X_0(Nm)(s)$). There is also the Hasse invariant ([Ka-Ma] Th.12.4.3):

$$\mathcal{O}(s.s.) \xrightarrow{\sim} \underline{\omega}^{\otimes p-1}$$

Combining these two gives: $\mathcal{O}(s.s.) \tilde{\to} \Omega(\text{cusps})^{\otimes \frac{p-1}{2}}$. Taking the degree yields:

$$s = \frac{p-1}{2}(2g(X_0(Nm) - 2 + c)$$

where s and c are the number of supersingular points and the number of cusps in $X_0(Nm)(\overline{\mathbf{F}}_p)$. The morphism $C \to X_0(Nm)_s$ is ramified exactly over the supersingular points (and there the ramification is total) of degree $\frac{p-1}{2}$. The Hurwitz formula gives:

$$2g(C) - 2 = \frac{p-1}{2}(s - c) \tag{4.6.4.2}$$

We are very lucky, since this last formula implies that there exist supersingular points x on C where $\phi^*\omega_U$ has a zero of order less than $\frac{p-1}{2}$. It follows that at such a point, $\phi^*\omega_U$, considered as a regular differential on $\widetilde{X_{U,u}}$, has a zero of order r, where r is given in the following table:

type	II	III	IV	I_0^*	IV^*	III^*	II^*
r	$\frac{p-1}{6}$	$\frac{p-1}{4}$	$\frac{p-1}{3}$	$\frac{p-1}{2}$	$\frac{p-1}{6}$	$\frac{p-1}{4}$	$\frac{p-1}{3}$

Let now b denote the multiplicity of the horizontal component C_x in the divisor of $\phi^*\omega_U$. Then we have $0 < b \leq r$. But since $\frac{\phi^*\omega_U}{\pi^b}$ is a non-zero differential form on C_x we must have: $(\chi^{a-b})^{p+1} = 1$, or equivalently, $a-b$ must be divisible by $\frac{p-1}{2}$. Since $a \equiv r(\frac{p-1}{2})$ we have $b = r$. Write $a-b = \frac{p-1}{2}c$, then $\mu_n(\mathbf{F}_{p^2})$ acts on $\frac{\phi^*\omega_U}{\pi^b}$ by $(\chi^{\frac{p-1}{2}})^c$. We list the various c:

type	II	III	IV	I_0^*	IV^*	III^*	II^*
c	$\frac{p-1}{6}$	$\frac{p-1}{4}$	$\frac{p-1}{3}$	$\frac{p-1}{2}$	$\frac{2p+1}{3}$	$\frac{3p+1}{4}$	$\frac{5p+1}{6}$

As before, we get a congruence mod $p+1$ on the orders of the zeros of the differential form $\frac{\phi^*\omega_U}{\pi^b}|_{C_x}$ at the intersection points of C_x with the outer two vertical components. We know that the polar part of the divisor has degree $2(b+1)$. One easily checks that at the intersection points of C_x with the outer vertical components $\frac{\phi^*\omega_U}{\pi^b}$, considered as a regular differential, has zeros of order c. We conclude (by Lemma 4.6.5) that $\phi^*\omega_U$ has a zero of multiplicity at most $b + \frac{p-1}{2}c$ along the outer vertical components. Equivalently, $\phi^*\omega_S = \pi^{-a}\phi^*\omega_U$ has valuation at most $b + \frac{p-1}{2}c - a$ along the outer vertical components. A trivial case by case computation shows that $\phi^*\omega_S$ does *not* vanish on the outer vertical components. We conclude that in this case p does not divide the Manin constant either.

Lemma 4.6.5 *Let W be a complete discrete valuation ring with uniformizer π. Let $X := \mathrm{Spec}W[[x,y]]/(xy - \pi^n)$, with $n \in \mathbf{Z}_{>0}$. Suppose that $f \in \mathcal{O}_X(X)$, considered as a function on the subscheme defined by $y = 0$, has a zero of order k at the point $x = 0$. Then the multiplicity of the (Weil) divisor $x = 0$ on X in the divisor of f is at most kn.*

Proof. Let $\tilde{f} = \sum_{i,j\geq 0} a_{ij}x^i y^j \in W[[x,y]]$ be a lift of f. Using the relation $xy = \pi^n$ we can rewrite $\tilde{f}$:

$$\tilde{f} = a_0 + \sum_{i>0} a_i x^i + \sum_{j>0} b_j y^j.$$

Modulo y and π we have: $\tilde{f} = \overline{a_0} + \sum_{i>0} \overline{a_i} x^i$, hence $\overline{a_0} = \ldots = \overline{a_{k-1}} = 0$ and $\overline{a_k} \neq 0$. Now we localize with respect to y: $x = \pi^n y^{-1}$, and we get

$$\tilde{f} = a_0 + \sum_{i>0} a_i \pi^{ni} y^{-i} + \sum_{j>0} b_j y^j$$

(in $W[[y, \pi^n y^{-1}]]$). The coefficient of y^{-k} is $a_k \pi^{nk}$, with valuation nk. The proof of Lemma 4.6.4 is now complete.

Theorem 4.6.3 has now been proved for potentially supersingular E with reduction type II, III or IV since we know (Theorem 4.3.2) that their Weil parametrizations are separable. We attack the other cases by considering E and $\widetilde{E}$ at the same time, but first we prove another preliminary lemma.

Lemma 4.6.6 *Let $\phi : X_0(M)_{\mathbf{Q}} \to E$ be a not necessarily strong Weil parametrization. Let ω be a Néron differential on E. Write $\phi^*\omega = cf\frac{dq}{q}$, where f is the normalized newform corresponding to E. Then we have:*

$$\frac{\deg(\phi)}{c^2} = \frac{\|f\|^2}{\mathrm{vol}(E,\omega)}$$

where

$$\|f\|^2 = \int_{X_0(M)(\mathbf{C})} \frac{i}{2}|f|^2 \frac{dq \wedge dq}{q\bar{q}} \quad \textit{and} \quad \mathrm{vol}(E,\omega) = \int_{E(\mathbf{C})} \frac{i}{2}\omega \wedge \overline{\omega}.$$

Proof. Use:

$$\int_{X_0(M)(\mathbf{C})} \frac{i}{2}\phi^*\omega \wedge \overline{\phi^*\omega} = \deg(\phi) \int_{E(\mathbf{C})} \frac{i}{2}\omega \wedge \overline{\omega}.$$

Proof. (of Theorem 4.6.3). We start with a strong Weil parametrization $\phi : X_0(p^2N)_{\mathbf{Q}} \to E$ satisfying hypotheses (1) and (2) of the theorem. Let E' be the twist of E over $\mathbf{Q}(\sqrt{\pm p})$, where the sign is such, that there is only ramification at p. According to the hypotheses of the theorem, we have a commutative diagram:

$$\begin{tikzcd} X_0(p^2N)_{\mathbf{Q}} \arrow[rr, "\tilde{\phi}"] \arrow[dr, "\phi'"'] & & \widetilde{E} \arrow[dl, "\alpha"] \\ & E' & \end{tikzcd}$$

with $\tilde{\phi}$ strong, α cyclic and $\deg(\alpha)$ not divisible by p. It is easy to see (from the inertia action, Prop. 4.1.1) that $\widetilde{E}$ and E' have the same reduction type at p. The relation between the reduction types of E and E' is given in (4.3.1.1). By replacing E if necessary by $\widetilde{E}$ we may suppose that E is of type II, III or IV. Using Proposition 4.1.2 it is easy to compute that: $\mathrm{vol}(E', \omega') = p \cdot \mathrm{vol}(E, \omega)$, where ω' is a Néron differential on E'. Let $f = \sum a_n q^n$ and $\tilde{f} = \sum \tilde{a}_n q^n$ be the normalized newforms corresponding to E and $\widetilde{E}$. Since we have $|a_n|^2 = |\tilde{a}_n|^2$ for all n, the formula:

$$\|f^2\| = C \cdot [\mathrm{PSL}_2(\mathbf{Z}) : \Gamma_0(p^2N)] \cdot \mathrm{Res}_{s=2} \sum_{n=1}^{\infty} \frac{|a_n|^2}{n^s}$$

(where C is some fixed constant) from [Za] shows that $\|f\|^2 = \|\tilde{f}\|^2$. From Lemma 4.6.6 we get the equalities:

$$\frac{\deg(\phi')}{(c')^2} = p\frac{\deg(\phi)}{c^2} \qquad\qquad \deg(\tilde{\phi}) = p\deg(\phi)\frac{(c')^2}{c^2}\frac{1}{\deg(\alpha)}.$$

Since p does not divide $\deg(\alpha)$, we have $v_p(\tilde{c}) = v_p(c')$, where v_p denotes the valuation on $\mathbf{Q}$ corresponding to p. We arrive at:

$$v_p(\deg\tilde{\phi}) = v_p(\deg\phi) + 1 + 2v_p(\frac{\tilde{c}}{c}).$$

If E is horizontal (= potentially supersingular) then Theorem 4.3.2 tells us that $v_p(\tilde{c})$ equals $v_p(c)$, and we already know that $v_p(c) = 0$. If E is vertical, then Proposition 4.5.2 shows that either $v_p(\tilde{c}) = v_p(c)$ and ϕ is not inseparable (hence $v_p(c) = 0$) or $v_p(\frac{\tilde{c}}{c}) = -1$, and $\tilde{\phi}$ is separable and ϕ is inseparable, hence $v_p(\tilde{c}) = 0$ and $v_p(c) = 1$.

Remark. Of course, if the last case occurs, Manin's conjecture would not be true.

Bibliography

[Bi-Ku] B.J. Birch and W. Kuyk. *Modular Functions of One Variable IV.* Springer Lecture Notes in Mathematics 476 (1975).

[Bi-SD] B.J. Birch and H.P.F. Swinnerton-Dyer. *Elliptic curves and modular functions.* In Modular Functions of One Variable IV (2-32), Springer Lecture Notes in Mathematics 476 (1975).

[Ca] H. Carayol. *Sur les représentations ℓ-adiques associées aux formes modulaires de Hilbert.* Ann. scient. Éc. Norm. Sup., série 4, t.19, 409-468 (1986).

[Cr] J. Cremona. *Computation of modular elliptic curves and the Birch-Swinnerton Dyer Conjecture.* To be published.

[De-Ra] 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).

[De-Mu] P. Deligne and D. Mumford. *The irreducibility of the space of curves of given genus.* Publications Mathématiques de l'I.H.E.S. 36, 75-125, (1969).

[Ed 1] S.J. Edixhoven. *Minimal resolution and stable reduction of $X_0(N)$.* Preprint November 1986 (submitted for publication in the Annales de l'Institut Fourier in June 1988).

[Ed 2] S.J. Edixhoven. *L'action de l'algèbre de Hecke sur les groupes de composantes des jacobiennes des courbes modulaires est "Eisenstein".* Preprint May 1988 (accepted for publication in an Astérisque volume).

[E-G-T] S.J. Edixhoven, A. de Groot and J.Top. *Elliptic curves over the rationals with bad reduction at only one prime.* Submitted for publication in Mathematics of Computation (1988).

[Gr] B.H. Gross. *Arithmetic on Elliptic Curves with Complex Multiplication.* Springer Lecture Notes in Mathematics 776 (1980).

[Gro 1] 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.

[Gro 2] A. Grothendieck. *Séminaire de Géométrie Algébrique I: Revêtements Etales et Groupe Fondamental.* Springer Lecture Notes in Mathematics 224 (1971).

[Ka-Ma] N.M. Katz and B. Mazur. *Arithmetic Moduli of Elliptic Curves.* Annals of Mathematics Studies 108, Princeton University Press (1985).

[Li] J. Lipman. *Rational singularities, with applications to algebraic surfaces and unique factorization.* Publications Mathématiques de l'I.H.E.S. 36, 195-297 (1969).

[Ma 1] B. Mazur. *Rational Isogenies of Prime Degree.* Invent. Math. 44, 129-162 (1978).

[Ma 2] B. Mazur. *Courbes Elliptiques et Symboles Modulaires.* Séminaire Bourbaki juin 1972. Springer Lecture Notes in Mathematics 317.

[Ma-SD] B. Mazur and H.P.F. Swinnerton-Dyer. *Arithmetic of Weil curves.* Invent. Math. 25, 1-16 (1974).

[Me] J.-F. Mestre. *La méthode des graphes, exemples et applications.* Proceedings of the international conference on class numbers and fundamental units of algebraic number fields, June 1986, Katata, Japan.

[Me-Oe] J.-F. Mestre and J. Oesterlé. Article on the graph method. To appear.

[Mi] J.S. Milne. *Étale Cohomology.* Princeton Mathematical Series 33 (1980).

[Oo 1] F. Oort. *Commutative Group Schemes.* Springer Lecture Notes in Mathematics 15 (1966).

[Oo 2] F. Oort. *Finite group schemes, local moduli for abelian varieties, and lifting problems.* Proceedings of the 5-th Nordic Summer-School in Mathematics, 223-254, Oslo (1970).

[Ra 1] M. Raynaud. *Spécialisation du foncteur de Picard.* Publications Mathématiques de l'I.H.E.S. 38 (1970).

[Ra 2] M. Raynaud. *Schémas en groupes de type* $(p, ..., p)$. Bull. Soc. Math. France 102, 241-280 (1974).

[Sh] G. Shimura. *On the factors of the Jacobian variety of a modular function field.* Jour. Math. Soc. Japan 25, 504-533 (1973).

[St] G. Stevens. *Stickelberger Elements and Modular Parametrizations of Elliptic Curves.* To be published.

[Sz] L. Szpiro. Séminaire sur les pinceaux de courbes de genre au moins deux. Astérisque 86 (1981).

[Ta] J. Tate. *Algorithm for determining the type of a singular fibre in an elliptic pencil.* In Modular Functions of One Variable IV, 33-52. Springer Lecture Notes in Mathematics 476 (1975).

[Za] D. Zagier. *Modular parametrizations of elliptic curves.* Canad. Math. Bull. 28(3), 372-384 (1985).

Samenvatting.

Het doel van dit proefschrift is het bestuderen van de actie van de Hecke algebra op modulaire vormen met behulp van stabiele modellen van modulaire krommen.

Eerst worden deze modellen geconstrueerd en wordt de actie van de inertie groep op de speciale vezels uitgerekend. Vervolgens wordt de actie van de Hecke algebra op deze vezels bestudeerd. Het resultaat hiervan is een generalisatie van het grafen algoritme van Mestre en Oesterlé.

Het laatste hoofdstuk is gewijd aan Weil krommen. Er wordt een vrij sterk resultaat bewezen betreffende Manin constanten van sterke Weil krommen.

Dankwoord.

Allereerst wil ik mijn promotor Frans Oort bedanken voor de algebraische meetkunde die ik van hem heb geleerd in mijn studietijd en voor zijn begeleiding gedurende het promotie onderzoek. Zijn inzicht dat met de mij bekende methoden informatie gekregen kan worden omtrent Manin constanten is juist gebleken.

Veel dank ben ik verschuldigd aan Bert van Geemen. Zijn invloed op mijn onderzoek is van groot belang geweest. Veel van wat ik weet van modulaire krommen heb ik van hem geleerd. Van hem is ook het idee afkomstig om Hecke operatoren mod p te reduceren (onafhankelijk van Mestre en Oesterlé).

Gerard van der Geer wil ik bedanken voor zijn colleges, voor de discussies die wij hadden en voor zijn opmerkingen over een voorlopige versie van dit proefschrift.

Gedurende de laatste vier jaar was mijn gezellige kamergenoot Jaap Top mijn steun en toeverlaat bij vragen over getaltheorie en elliptische krommen.

Verder wil ik Jean-François Mestre, Joseph Oesterlé, Ken Ribet en René Schoof bedanken voor hun belangstelling in mijn werk en voor de gesprekken met hen daarover.

Tenslotte dank aan Shell Nederland B.V. voor het betalen van een reis naar de U.S.A.

Curriculum Vitae.

Op 12 maart 1962 ben ik geboren te Leiden. In 1980 behaalde ik het diploma Voorbereidend Wetenschappelijk Onderwijs aan het Erasmus-College te Zoetermeer. Daarna begon ik de studie natuurkunde aan de Rijksuniversiteit te Utrecht. In december 1982 en maart 1983 behaalde ik de kandidaatsexamens natuurkunde met bijvak wiskunde en wiskunde met bijvak natuurkunde (beide cum laude). In augustus 1985 ben ik (cum laude) afgestudeerd in de zuivere wiskunde. Sinds september 1985 werk ik als promovendus bij de vakgroep wiskunde van de Rijksuniversiteit te Utrecht.