Comparison of integral structures on spaces of modular forms of weight two, and computation of spaces of forms mod 2 of weight one

Bas Edixhoven*

April 4, 2002

Contents

1 Introduction

For $N \geq 1$ and k integers, let $S_k(\Gamma_0(N), \mathbb{C})$ denote the $\mathbb{C}$-vector space of holomorphic cusp forms on the congruence subgroup $\Gamma_0(N)$ of $\mathrm{SL}_2(\mathbb{Z})$ (for a definition, see for example the book that contains [18]). To an element f of some $S_k(\Gamma_0(N), \mathbb{C})$ we can associate its q-expansion

*Partially supported by the European Research Training Network Contract HPRN-CT-2000-00120 "arithmetic algebraic geometry". Address: IRMAR, Campus de Beaulieu, 35042 Rennes cedex, France; edix@maths.univ-rennes1.fr

$\sum_{n\geq 1} a_n(f)q^n$ in $\mathbb{C}[[q]]$, by noting that f, as a function on the complex upper half plane, is invariant under translation by all integers, and hence is a power series in $q\colon z \mapsto \exp(2\pi i z)$. So we have q-expansion maps:

$$q\text{-exp}\colon S_k(\Gamma_0(N), \mathbb{C}) \longrightarrow \mathbb{C}[[q]], \qquad f \mapsto \sum_{n\geq 1} a_n(f)q^n,$$

which are injective. For Γ any subgroup of finite index of $\mathrm{SL}_2(\mathbb{Z})$ and k an integer we have an analogous space $S_k(\Gamma, \mathbb{C})$.

The $\mathbb{C}$-vector spaces $S_k(\Gamma_0(N), \mathbb{C})$ have natural $\mathbb{Q}$-structures, i.e., sub $\mathbb{Q}$-vector spaces $S_k(\Gamma_0(N), \mathbb{Q})$ such that the natural maps from $\mathbb{C} \otimes S_k(\Gamma_0(N), \mathbb{Q})$ to $S_k(\Gamma_0(N), \mathbb{C})$ are isomorphisms. One way to define these $\mathbb{Q}$-structures is to take the sub $\mathbb{Q}$-vector space of f in $S_k(\Gamma_0(N), \mathbb{C})$ whose q-expansion is in $\mathbb{Q}[[q]]$. Note that it is not a priori clear that these subspaces indeed are $\mathbb{Q}$-structures. A second way to define the $\mathbb{Q}$-structures is to let $S_k(\Gamma_0(N), \mathbb{Q})$ be the space of global sections of the line sheaf (SLang for invertible sheaf of modules) $\underline{\omega}^{\otimes k}(-\mathrm{cusps})$ on the $\mathbb{Q}$-stack of generalized elliptic curves over $\mathbb{Q}$-schemes with a $\Gamma_0(N)$-level structure. The two definitions agree, but this is not a complete triviality; see below for more details.

Loosely speaking, the two $\mathbb{Q}$-structures come from q-expansions and algebraic geometry over $\mathbb{Q}$. These two methods also give $\mathbb{Z}$-structures. The two of $\mathbb{Z}$-structures do not always coincide.

The first aim of this article is not to study in general the differences between the two kinds of $\mathbb{Z}$-structures, although this is an interesting problem. We restrict ourselves to the relatively simple case of forms of weight two, and we study the differences between the two $\mathbb{Z}$-structures, at primes whose square does not divide the level. The main reason to study just this case is its application in the article [1], where our results are used to obtain information about "generalized Manin constants". Another reason is that more general cases are more difficult to treat, and lead to results that are more complicated.

At the prime 2 the difference between the two $\mathbb{Z}$-structures that we study can be bigger than at other primes. This special behaviour, caused by the Hasse invariant being of weight one, is related to spaces of modular forms modulo 2 of weight one (defined as by Katz, i.e., mod 2 forms that cannot necessarily be lifted to characteristic zero). As a byproduct of our work we find a description of these spaces of weight one forms purely in terms of the integral Hecke algebra associated to weight two cusp forms, together with the Atkin-Lehner involution W_2. These data can be computed from the singular homology group $\mathrm{H}_1(X_0(N)(\mathbb{C}), \mathbb{Z})$, for example using modular symbols algorithms. Section 3 gives this description, as an $\mathbb{F}_2$-vector space equipped with Hecke operators T_n for odd n.

In Section 4, we give another (more general) description of spaces of mod p modular forms of weight one in terms of a Hecke algebra associated to forms of weight p, based on properties of the derivation qd/dq. Theorem 4.11 gives a description of the $\mathbb{F}_p$-vector spaces of cusp forms of weight one on $\Gamma_1(N)$ with a fixed character, equipped with all Hecke operators, in terms of data that can be computed using modular symbols. Section 5 contains a result that says that some mod p Hecke algebras can be computed using modular symbols mod p. Finally, in Section 6, we give a result about eigenspaces.

It should be said that there are published methods about how one can compute spaces of weight one modular forms, and even some tables. For example there are the methods described in [30] (see also [6]). But those methods are aimed at computing spaces $S_1(\Gamma_1(N), \varepsilon, \mathbb{C})$ of characteristic zero forms of weight one. It seems that the methods as in [30] can be adapted to compute spaces of Katz's modular forms mod p, but that, at least for small p, they are less directly related to Hecke algebras that one can easily compute using modular symbols algorithms.

The results in this article (especially the part about computing spaces of mod p weight one forms) are not so original. The methods employed are due for a large part to Katz, and Deligne and Rapoport, and some ideas are already implicitly contained, in special cases, in [6]. But on the other hand there seem to be no tables of mod p modular forms of weight one, and worse, no published algorithm, to computate such tables. We hope that the results of the last three sections will be used for computations. It would be interesting to know if the examples of non-Gorenstein Hecke algebras found by Kilford (see [29] and [35, §3.7.1]) can be "explained" by weight one phenomena. Another example is the question whether the mod 2 Galois representation associated to a mod 2 eigenform of weight one is unramified at 2, even if one is in the exceptional case (see [17, Prop. 2.7], the end of the introduction of [17] and [8, Cor. 0.2]), and the question of companion forms in the exceptional case (see [23] and [32]).

I thank Amod Agashe and William Stein for asking me about differences between $\mathbb{Z}$-structures, and for motivating me enough to write up the results below. I thank Kevin Buzzard and Christophe Breuil for their corrections and comments on a first version of this text.

2 Comparison of two integral structures

2.1 Let $N \geq 1$ be an integer. For A a subring of $\mathbb{C}$, we let $S_2(A) = S_2(\Gamma_0(N), A)$ be the A-module of f in $S_2(\Gamma_0(N), \mathbb{C})$ whose q-expansion is in $A[[q]]$. We want to compare the $\mathbb{Z}$-module $S_2(\mathbb{Z})$ with another one that comes from algebraic geometry over $\mathbb{Z}$. Let $X = X_0(N)$ be the modular curve over $\mathbb{Z}$ that is the compactified coarse moduli scheme for elliptic curves with a given cyclic subgroup scheme of rank N, as constructed and described in the book by Katz and Mazur [28]. Let J be the Néron model over $\mathbb{Z}$ of the jacobian variety of $X_{\mathbb{Q}}$ (see

[3] for generalities about Néron models, and [3, Thm. 9.7] for some special results in the case of modular curves). Then J is a smooth group scheme over $\mathbb{Z}$, of relative dimension the genus of $X_{\mathbb{Q}}$, and its cotangent space at the origin $\mathrm{Cot}_0(J)$ is a $\mathbb{Z}$-structure on $\mathrm{Cot}_0(J_{\mathbb{Q}}) = \mathrm{H}^0(X_{\mathbb{Q}}, \Omega^1)$, with Ω^1 the $\mathcal{O}_{X_{\mathbb{Q}}}$-module of Kähler differentials. The Kodaira-Spencer isomorphism identifies $S_2(\mathbb{C})$ with $\mathrm{H}^0(X_{\mathbb{C}}, \Omega^1) = \mathbb{C} \otimes \mathrm{H}^0(X_{\mathbb{Q}}, \Omega^1)$. We want to compare the sub $\mathbb{Z}$-modules $S_2(\mathbb{Z})$ and $\mathrm{Cot}_0(J)$ of $S_2(\mathbb{C})$. In order to do this we use the following algebraic interpretation of the q-expansion map.

The standard cusp ∞, that corresponds to the generalized elliptic curve $\mathbb{P}^1_{\mathbb{Z}}$ with its points 0 and ∞ identified and equipped with its subgroup scheme μ_N in the terminology of Deligne and Rapoport [7], is a $\mathbb{Z}$-valued point of X, i.e., an element of $X(\mathbb{Z})$. The Tate curve $\mathbb{G}_{\mathrm{m}}/q^{\mathbb{Z}}$ over $\mathbb{Z}((q))$ gives an isomorphism from the formal spectrum of $\mathbb{Z}[[q]]$ to the completion of X along ∞ ([28, Ch. 8] and [16, §1.2]). In particular, the image of ∞ lies in the open subscheme X^{sm} of X on which the morphism to $\mathrm{Spec}(\mathbb{Z})$ is smooth. A differential form ω on some open neighborhood of ∞ in X can be expanded (uniquely) as $\sum_{n\geq 1} a_n(\omega)q^n(dq/q)$, with the a_n in $\mathbb{Z}$. In the same way, we have a q-expansion map from $\mathrm{H}^0(X_{\mathbb{Q}}, \Omega)$ to $\mathbb{Q}[[q]]$.

The following result is well-known, but we give a proof anyway. It will allow us to view $S_2(\mathbb{Z})$ as the subset of elements of $\mathrm{H}^0(X_{\mathbb{Q}}, \Omega^1)$ that satisfy some integrality condition at all prime numbers p.

Proposition 2.2 *The sub $\mathbb{Q}$-vector spaces $S_2(\mathbb{Q})$ and $\mathrm{H}^0(X_{\mathbb{Q}}, \Omega^1)$ of $S_2(\mathbb{C})$ are equal.*

Proof. We follow the arguments used by Katz in [26, 1.6], and by Deligne and Rapoport in [7, VII, 3.9].

The q-expansion map from $\mathrm{H}^0(X_{\mathbb{Q}}, \Omega^1)$ to $\mathbb{C}[[q]]$ has image in $S_2(\mathbb{Q})$. So it remains to prove the other inclusion. Let $\sum a_n q^n$ be in $S_2(\mathbb{Q})$, and let $\omega = \sum a_n q^n\, dq/q$ in $\Omega^1(X_{\mathbb{C}})$ be its associated one-form. The fact that $\mathrm{H}^0(X_{\mathbb{C}}, \Omega^1) = \mathbb{C} \otimes \mathrm{H}^0(X_{\mathbb{Q}}, \Omega^1)$ implies that $\sum a_n q^n$ is actually in the subring $\mathbb{C} \otimes \mathbb{Q}[[q]]$ of $\mathbb{C}[[q]]$. We consider the following commutative diagram:

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \mathrm{H}^0(X_{\mathbb{Q}}, \Omega^1) & \longrightarrow & \mathbb{C} \otimes \mathrm{H}^0(X_{\mathbb{Q}}, \Omega^1) & \longrightarrow & (\mathbb{C}/\mathbb{Q}) \otimes \mathrm{H}^0(X_{\mathbb{Q}}, \Omega^1) & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & \mathbb{Q}[[q]] & \longrightarrow & \mathbb{C} \otimes \mathbb{Q}[[q]] & \longrightarrow & (\mathbb{C}/\mathbb{Q}) \otimes \mathbb{Q}[[q]] & \longrightarrow & 0
\end{array}$$

The two rows are exaxt, and the three vertical arrows are injective (use that $X_{\mathbb{Q}}$ is integral, that $\Omega^1_{X_{\mathbb{Q}}/\mathbb{Q}}$ is a line sheaf, and that the functors $\mathbb{C} \otimes -$ and $(\mathbb{C}/\mathbb{Q}) \otimes -$ are exact). The statement is now obvious. □

Proposition 2.3 *The sub $\mathbb{Z}$-module $\mathrm{Cot}_0(J)$ of $S_2(\mathbb{Q})$ is contained in $S_2(\mathbb{Z})$.*

Proof. We have to show that the q-expansion of an element of $\mathrm{Cot}_0(J)$, viewed as an element of $\mathrm{H}^0(X_{\mathbb{Q}}, \Omega^1)$, lies in $\mathbb{Z}[[q]]$. Evaluation at 0 identifies $\mathrm{H}^0(J_{\mathbb{Q}}, \Omega^1)$ with $\mathrm{Cot}_0(J_{\mathbb{Q}})$, and $\mathrm{H}^0(J, \Omega^1)$ with $\mathrm{Cot}_0(J)$ (use that the elements of $\mathrm{H}^0(J_{\mathbb{Q}}, \Omega^1)$ are translation invariant). The identification of $\mathrm{H}^0(J_{\mathbb{Q}}, \Omega^1)$ with $\mathrm{H}^0(X_{\mathbb{Q}}, \Omega^1)$ is given by pullback via the morphism $X_{\mathbb{Q}} \to J_{\mathbb{Q}}$ that sends an S-valued point P of $X_{\mathbb{Q}}$ to the class of the invertible $\mathcal{O}_{X_S}$-module $\mathcal{O}_{X_S}(P - \infty)$, where S is any $\mathbb{Q}$-scheme. By the Néron property of J, this morphism extends (uniquely) to a morphism $X^{\mathrm{sm}} \to J$. It follows that $\mathrm{H}^0(J, \Omega^1)$ (and hence $\mathrm{Cot}_0(J)$) is mapped into $\mathrm{H}^0(X^{\mathrm{sm}}, \Omega^1)$, and hence, via the q-expansion map, into $\mathbb{Z}[[q]]$. □

2.4 Our aim is to compare $S_2(\mathbb{Z})$ and $\mathrm{Cot}_0(J)$, so we have to describe the quotient $S_2(\mathbb{Z})/\,\mathrm{Cot}_0(J)$. As this quotient is torsion, it is the direct sum over all prime numbers p of its p-primary part. We will give a description of the p-primary part for p such that p^2 does not divide N (recall that $X = X_0(N)$).

By definition, $S_2(\mathbb{Z})$ is the subset of elements of $\mathrm{H}^0(X_{\mathbb{Q}}, \Omega^1)$ that satisfy certain integrality conditions at all prime numbers p. More precisely, for ω in $S_2(\mathbb{Z})$ and p prime, the condition is that the q-expansion of ω at the cusp ∞, which is an element $(\sum_{n\geq 1} a_n q^n)dq/q$ of $\mathbb{Q}[[q]]\cdot dq$, satisfies $v_p(a_n) \geq 0$ for all n. Our first step is to reinterpret these integrality conditions geometrically, as in [7, VII, Thm. 3.10].

Let η denote the generic point of X. We note that $\Omega^1_{X^{\mathrm{sm}}/\mathbb{Z}}$ is an invertible $\mathcal{O}_{X^{\mathrm{sm}}}$-module. Hence, to each element ω of $\Omega^1_{X/\mathbb{Z},\eta}$ we can associate its multiplicity $v_C(\omega)$ along each prime divisor C of X^{sm}. This multiplicity is defined as $v_{\eta_C}(f)$, where η_C is the generic point of C, v_{η_C} the discrete valutation on the discrete valuation ring $\mathcal{O}_{X,\eta_C}$, and $\omega = f\cdot\omega_C$ with $\Omega^1_{X^{\mathrm{sm}}/\mathbb{Z},\eta_C} = \mathcal{O}_{X,\eta_C}\omega_C$. In these terms, we have:

$$\mathrm{H}^0(X^{\mathrm{sm}}, \Omega^1_{X^{\mathrm{sm}}/\mathbb{Z}}) = \{\omega \in \mathrm{H}^0(X_{\mathbb{Q}}, \Omega^1_{X_{\mathbb{Q}}/\mathbb{Q}}) \mid v_C(\omega) \geq 0 \text{ for all } C.\}$$

In order to relate the integrality conditions on q-expansions to the $v_C(\omega)$, we look at what happens under completion at some closed point.

Let x be a closed point of X^{sm}. Then $\mathcal{O}_{X,x}$ is a two-dimensional regular noetherian local ring, and since $X \to \mathrm{Spec}(\mathbb{Z})$ is smooth at x, it has a system of parameters of the form (p, t), with p a prime number. The completion $\mathcal{O}^\wedge_{X,x}$ is then isomorphic to $W(k)[[t]]$, with $W(k)$ the ring of Witt vectors of the residue field k at x. Let C be the irreducible component of $X_{\mathbb{F}_p}$ that x lies on. Then $\mathcal{O}_{C,x} = \mathcal{O}_{X,x}/p\mathcal{O}_{X,x}$ and the morphism from $\mathcal{O}_{C,x}$ to its completion $\mathcal{O}^\wedge_{C,x} = k[[t]]$ is injective. Let now f be in $\mathcal{O}_{X,x}$, and put $m := v_C(f)$. Then, as p is a prime element of $\mathcal{O}_{X,x}$ and a uniformizer of $\mathcal{O}_{X,\eta_C}$, we have $f = p^m f'$, with f' in $\mathcal{O}_{X,x}$ such that the image $\overline{f'}$ of f' in $\mathcal{O}_{C,x}$ is not zero. Let us write the image of f in $W(k)[[t]]$ as $\sum a_n t^n$ (with the a_n in $W(k)$). Then we see that $m = \min_n v_p(a_n)$ (use that the image of $\overline{f'}$ in $k[[t]]$ is non-zero).

If we take for x the cusp ∞ in $X(\mathbb{F}_p)$ for some prime number p, the discussion above gives that the integrality condition at p for ω in $\mathrm{H}^0(X_\mathbb{Q}, \Omega^1_{X_\mathbb{Q}/\mathbb{Q}})$ to be in $S_2(\mathbb{Z})$ is just $v_C(\omega) \geq 0$, with C the irreducible component of $X_{\mathbb{F}_p}$ that contains ∞. This proves the following proposition.

Proposition 2.5 *Let ω be in $\mathrm{H}^0(X_\mathbb{Q}, \Omega^1_{X_\mathbb{Q}/\mathbb{Q}})$. Then ω is in $S_2(\mathbb{Z})$ if and only if for every prime number p it has multiplicity ≥ 0 along the irreducible component of $X_{\mathbb{F}_p}$ that contains ∞. In other words:*

$$S_2(\mathbb{Z}) = \mathrm{H}^0(X_\infty, \Omega^1_{X/\mathbb{Z}}),$$

with X_∞ the complement in X of the union of all the irreducible components of all $X_{\mathbb{F}_p}$ that do not *contain ∞.*

2.6 It may come as a surprise that, with this characterisation, $S_2(\mathbb{Z})$ is a finitely generated $\mathbb{Z}$-module, since X_∞ is not proper if $N \neq 1$. But it is not hard to show that for C and C' irreducible components of the same $X_{\mathbb{F}_p}$, the differences $|v_C(\omega) - v_{C'}(\omega)|$, for $\omega \neq 0$ in $\mathrm{H}^0(X_\mathbb{Q}, \Omega^1_{X_\mathbb{Q}/\mathbb{Q}})$, are bounded uniformly in ω. In fact, after choosing an extension of $\Omega^1_{X_\infty/\mathbb{Z}}$ to an invertible $\mathcal{O}_X$-module $\mathcal{L}$ (after a resolution of singularities, if necessary), one obtains a bound that depends only on the combinatorial data: the dual graph plus intersection numbers, multiplicities, genera and degrees of restrictions of $\mathcal{L}$ associated to $X_{\mathbb{F}_p}$ and $\mathcal{L}$. Such bounds imply that $S_2(\mathbb{Z})$ is a lattice in $\mathrm{H}^0(X_\mathbb{Q}, \Omega^1_{X_\mathbb{Q}/\mathbb{Q}})$. The computations that we will do below are an explicit and exact version of the proof just alluded to, but in a simple case. We note that in [7, VII, §3] similar computations have been done, but for modular forms of arbitrary weight k, seen as sections of $\underline{\omega}^{\otimes k}$.

If p is a prime that does not divide N, then $X_{\mathbb{F}_p}$ is irreducible, and hence the quotient $S_2(\mathbb{Z})/\operatorname{Cot}_0(J)$ is trivial at p. If p is a prime number such that p^2 divides N we do not want to say anything about the p-part of the quotient in this article. A good reason for that is that the results become much more difficult to describe. One finds some computations in [14, §4.6] and [15, §4] for the case where p^2 exactly divides N.

So suppose from now on that p is a prime dividing N exactly, i.e., such that N/p is not divisible by p. Then X is semistable at p; in particular, $X_{\mathbb{Z}_p}$ is normal. Its fibre $X_{\mathbb{F}_p}$ has two irreducible components, C_∞ and C_0, both isomorphic to $X_0(N/p)_{\mathbb{F}_p}$ (and hence smooth), with C_∞ containing the cusp ∞, and hence C_0 the cusp 0. The intersection $C_\infty \cap C_0$ consists of the supersingular points on C_∞ and C_0, and the intersections are transversal. We identify C_∞ with $X_0(N/p)_{\mathbb{F}_p}$ via the following construction:

$$X_0(N/p)_{\mathbb{F}_p} \longrightarrow C_\infty, \quad (E/S/\mathbb{F}_p, G) \mapsto (E/S/\mathbb{F}_p, G, \ker F),$$

where $E/S/\mathbb{F}_p$ is an elliptic curve over an $\mathbb{F}_p$-scheme, where G is a cyclic subgroup scheme of rank N/p of E/S, and where $F\colon E \to E^{(p)}$ is the Frobenius morphism of E over S. Likewise, we identify C_0 with $X_0(N/p)_{\mathbb{F}_p}$ as follows:

$$X_0(N/p)_{\mathbb{F}_p} \longrightarrow C_\infty, \quad (E/S/\mathbb{F}_p, G) \mapsto (E^{(p)}/S/\mathbb{F}_p, G^{(p)}, \ker V),$$

where $V\colon E^{(p)} \to E$ is the Verschiebung (the dual of F).

Let Ω be the dualizing sheaf for $X_{\mathbb{Z}_p}$ over $\mathbb{Z}_p$ (see [31] for a discussion of this sheaf in the context of semi-stable modular curves). Then Ω is the direct image of $\Omega^1_{X^{\mathrm{sm}}_{\mathbb{Z}_p}/\mathbb{Z}_p}$ via the inclusion of $X^{\mathrm{sm}}_{\mathbb{Z}_p}$ into $X_{\mathbb{Z}_p}$, and it is an invertible $\mathcal{O}_{X_{\mathbb{Z}_p}}$-module. We have:

$$\mathrm{Cot}_0(J_{\mathbb{Z}_p}) = \mathrm{H}^1(X_{\mathbb{Z}_p}, \mathcal{O})^\vee = \mathrm{H}^0(X_{\mathbb{Z}_p}, \Omega).$$

Let ω be a non-zero element of $\mathrm{H}^0(X_{\mathbb{Q}_p}, \Omega)$. We want to bound $|v_{C_\infty}(\omega) - v_{C_0}(\omega)|$, since the exponent of p in the exponent of the quotient $S_2(\mathbb{Z})/\operatorname{Cot}_0(J)$ is the maximal value of this expression over all ω. The automorphism W_N of X interchanges ∞ and 0, so we may as well suppose that $v_{C_0}(\omega) = 0$ and that $m := v_{C_\infty}(\omega) \geq 0$. Then the restriction $\omega|_{C_0}$ is a non-zero section of $\Omega|_{C_0}$, and the fact that ω has a zero of order m along C_∞ implies that $\Omega|_{C_0}$ has zeros of at least some order at the supersingular points. As the number of zeros cannot exceed the degree of $\Omega|_{C_0}$, we will get an upper bound for m.

There is now a minor problem: $X_{\mathbb{Z}_p}$ is not necessarily regular, and also, the degree of $\Omega|_{C_0}$ is easier to relate to the number of supersingular points if we were working on a fine moduli space. So we choose to work on some cover X' of $X_{\mathbb{Z}_p}$, say obtained by adding, to the $\Gamma_0(N)$-structure, a $\Gamma(3)$-structure when $p \neq 3$ or a $\Gamma(4)$-structure if $p = 3$. Note that $X' \to X_{\mathbb{Z}_p}$ is finite, and etale outside the locus of j-invariants 0, 1728 and ∞. Let C'_∞ and C'_0 be the inverse images of C_∞ and C_0, respectively, with their reduced scheme structure. Then the pullback of ω to X' has valuation zero along every irreducible component of C'_0, and a zero of order m along every irreducible component of C'_∞. As X' is regular, this implies that $\omega|_{C'_0}$ is a non-zero global section of $\Omega|_{C'_0}$, with zeros of order at least m at all supsersingular points. In other words, ω is a non-zero global section of $\Omega|_{C'_0}(-mS)$, where S is the divisor given by the sum of all supersingular points. Hence $\deg(\Omega|_{C'_0}(-mS)) \geq 0$. Let “cusps” denote the sum of the cups on C'_0. Then we have:

$$\begin{aligned}
\deg(\Omega|_{C'_0}(-mS)) &= \deg(\Omega^1_{C'_0/\mathbb{F}_p}) + \#S - m{\cdot}\#S \\
&= 2{\cdot}\deg(\underline{\omega}) - \#\mathrm{cusps} + (1-m)\#S \\
&= \frac{2}{p-1}\#S - \#\mathrm{cusps} + (1-m)\#S,
\end{aligned}$$

where we have used the equality $\Omega|_{C'_0} = \Omega^1_{C'_0/\mathbb{F}_p}(S)$, the Kodaira-Spencer isomorphism $\Omega^1_{C'_0/\mathbb{F}_p}(\mathrm{cusps}) \to \underline{\omega}^{\otimes 2}$ (for the family of elliptic curves obtained via the isomorphism with C'_∞;

see below for an explanation), and the Hasse invariant in $\mathrm{H}^0(C'_0, \underline{\omega}^{\otimes p-1})$, whose divisor is S. It follows that:

$$m < 1 + \frac{2}{p-1},$$

and we have proved the following result.

Proposition 2.7 *Let $N \geq 1$ be an integer and let p be a prime that exactly divides N. Then the p-part of the quotient $S_2(\mathbb{Z})/\operatorname{Cot}_0(J)$ is annihilated by p, if $p > 2$, and by 4 if $p = 2$.*

2.8 Our next aim is to describe the cokernel more precisely, at least if $p \neq 2$. But let us first compare Proposition 2.7 with [7, VII, Prop. 3.20]. It is clear that that result, stated for modular forms on $\Gamma_0(p)$, remains true if one adds prime to p level structure (the same proof works). It says that for a non-zero weight k form on $\Gamma_0(N)$ with coefficients in $\mathbb{Q}$, corresponding to an element f of $\mathrm{H}^0(X', \underline{\omega}^{\otimes k})$, one has:

$$\left| v_{C'_\infty}(f) - v_{C'_0}(f) + \frac{k}{2} \right| \leq \frac{1}{2} \cdot k \cdot \frac{p+1}{p-1}.$$

This result is not symmetric in C_∞ and C_0 because the sheaf $\underline{\omega}$ is not: the j-invariant is separable on C_∞, and inseparable on C_0. Proposition 2.7 can be deduced from this inequality, if one takes into account in its proof that f is a cuspform, and that the Kodaira-Spencer morphism $\underline{\omega}^{\otimes 2} \to \Omega^1(\mathrm{cusps})$ on X' has a zero of order one along C'_0. This last fact can be seen by looking at the cusps, via the Tate curve:

$$(dt/t)^{\otimes 2} \mapsto dq/q = p \cdot d(q^{1/p})/q^{1/p}.$$

Let us now try to determine the p-part of $S_2(\mathbb{Z})/\operatorname{Cot}_0(J)$ more precisely. Both $S_2(\mathbb{Z})$ and $\operatorname{Cot}_0(J)$ are stable under all endomorphisms T_n, $n \geq 1$, of $S_2(\Gamma_0(N), \mathbb{C})$. For $S_2(\mathbb{Z})$ this follows from the usual formulas in terms of q-expansions ([13, (12.4.1)]):

$$a_m(T_n f) = \sum_{\substack{0<d|(n,m)\\(d,N)=1}} d^{k-1} a_{nm/d^2}(\langle d \rangle f),$$

for f in $S_k(\Gamma_1(N), \mathbb{C})$, n and m positive integers. By construction, $\operatorname{Cot}_0(J)$ is stable under all endormorphisms of $J_{\mathbb{Q}}$, hence in particular under the T_n. The Atkin-Lehner involutions W_d, for d dividing N such that d and N/d are relatively prime, stabilize $\operatorname{Cot}_0(J)$, but do not necessarily stabilize $S_2(\mathbb{Z})$, since they may interchange C_∞ and C_0. In fact, W_d interchanges C_∞ and C_0 if and only if p divides d.

By Proposition 2.7, the cokernel of:

$$\mathrm{H}^0(X_{\mathbb{Z}_p},\Omega) \longrightarrow \{\omega \in \mathrm{H}^0(X_{\mathbb{Q}_p},\Omega) \mid v_{C_0}(\omega) \geq -1\}$$

is the p-part of $S_2(\mathbb{Z})/\operatorname{Cot}_0(J)$ if $p \neq 2$, and the piece killed by p of it if $p = 2$. If ω is in $\mathrm{H}^0(X_{\mathbb{Q}_p},\Omega)$ such that $v_{C_\infty}(\omega) \geq 0$ and $v_{C_0}(\omega) \geq -1$, then $p\omega|_{C_0}$ is an element of $\mathrm{H}^0(C_0,\Omega^1_{C_0/\mathbb{F}_p})$. We have an exact sequence:

$$0 \to \mathrm{H}^0(X_{\mathbb{Z}_p},\Omega) \to \{\omega \in \mathrm{H}^0(X_{\mathbb{Q}_p},\Omega) \mid v_{C_0}(\omega) \geq -1\} \to \mathrm{H}^0(C_0,\Omega^1_{C_0/\mathbb{F}_p}).$$

On the other hand, suppose ω is in $\mathrm{H}^0(C_0,\Omega^1_{C_0/\mathbb{F}_p})$. Then we have an element, call it $(0,\omega)$, of $\mathrm{H}^0(X_{\mathbb{F}_p},\Omega)$ whose restrictions to C_∞ and C_0 are 0 and ω, respectively. The fact that Ω is the dualizing sheaf implies that the formation of its cohomology commutes with the base change $\mathbb{Z}_p \to \mathbb{F}_p$, and hence that $(0,\omega)$ is the reduction mod p of an element, $\widetilde{\omega}$ say, in $\mathrm{H}^0(X_{\mathbb{Z}_p},\Omega)$. Then ω is the image of $p^{-1}\widetilde{\omega}$, in the exact sequence above. We have now proved the first claim of the following proposition.

Proposition 2.9 *Let $N \geq 1$ be an integer and let p be prime that exactly divides N. Then the construction above gives an isomorphism between $\mathrm{H}^0(C_0,\Omega^1_{C_0/\mathbb{F}_p})$ and the p-part of $S_2(\mathbb{Z})/\operatorname{Cot}_0(J)$ if $p > 2$, and its part killed by 2 if $p = 2$. We identify $\mathrm{H}^0(C_0,\Omega^1_{C_0/\mathbb{F}_p})$ and $\mathbb{F}_p \otimes S_2(\Gamma_0(N/p),\mathbb{Z})$, using the chosen isomorphism between $X_0(N/p)_{\mathbb{F}_p}$ and C_0. Then the endomorphism T_n of $S_2(\mathbb{Z})/\operatorname{Cot}_0(J)$ induces T_n on $\mathbb{F}_p \otimes S_2(\Gamma_0(N/p),\mathbb{Z})$ if n is prime to p, and 0 if n is a multiple of p.*

Proof. It remains to prove the second claim. Let l be a prime number, and let ω be in $\mathrm{H}^0(C_0,\Omega^1_{C_0/\mathbb{F}_p})$. Going through the construction of the isomorphism above, one finds that the endomorphism T_l of $S_2(\mathbb{Z})$ sends ω to $(T_l(0,\omega))|_{C_0}$, where $(0,\omega)$ is the element of $\mathrm{H}^0(X_{\mathbb{F}_p,\Omega})$ with restrictions 0 and ω to C_∞ and C_0, respectively. If l is not equal to p, this means that T_l induces the usual T_l on $\mathbb{F}_p \otimes S_2(\Gamma_0(N/p),\mathbb{Z})$. For $l = p$, one notes (see [17, §6.6]) that T_p induces the Frobenius endomorphism of the jacobian of C_0. $\square$

Finally, we investigate what happens at 2. We will prove the following result.

Proposition 2.10 *Let $N \geq 1$ be an integer. Suppose that 2 exactly divides N, and that the automorphism groups of elliptic curves over $\overline{\mathbb{F}_2}$ equipped with a cyclic subgroup of order $N/2$ are all just $\{1,-1\}$. (This last condition exactly means that $N/2$ is divisible by a prime number $q \equiv -1$ modulo 4, and by 9 or by a prime number $q' \equiv -1$ mod 3). Let M denote the 2-part* *of* $S_2(\mathbb{Z})/\operatorname{Cot}_0(J)$*. Then:*

$$\begin{aligned} M[4] &= M, \\ M/M[2] &= \mathrm{H}^0(C_0, \Omega^1_{C_0/\mathbb{F}_2}(-S)) = S_1(\Gamma_0(N/2), \mathbb{F}_2)_{\mathrm{Katz}}, \\ M[2] &= \mathrm{H}^0(C_0, \Omega^1_{C_0/\mathbb{F}_2}), \end{aligned}$$

where $S_1(\Gamma_0(N/2), \mathbb{F}_2)_{\mathrm{Katz}}$ *denotes the* $\mathbb{F}_2$*-vector space of weight one cusp forms on* $\Gamma_0(N/2)$ *over* $\mathbb{F}_2$*, defined as by Deligne and Katz (see [26], [17, §2] or [18, §1] and the references therein for a definition and properties of Katz's modular forms). For* $n \geq 1$*, the endomorphism* T_n *of* $S_2(\mathbb{Z})$ *induces the endomorphism* T_n *of* $S_1(\Gamma_0(N/2), \mathbb{F}_2)_{\mathrm{Katz}}$ *if* n *is odd, and* 0 *if* n *is even.*

Proof. The statements concerning $M[4]$ and $M[2]$ have already been proved in Propositions 2.7 and 2.9, and hence are even valid without the extra condition on $N/2$. It remains to prove the description of $M/M[2]$, and the action of T_n on it.

Supppose that ω is an element of $\mathrm{H}^0(X_{\mathbb{Q}_2}, \Omega)$ with $v_{C_\infty}(\omega) \geq 0$. Then $v_{C_0}(\omega) \geq -2$, hence 4ω is an element of $\mathrm{H}^0(X_{\mathbb{Z}_2}, \Omega)$ with at least a double zero along C_∞, and $4\omega|_{C_0}$ is an element of $\mathrm{H}^0(C_0, \Omega^1_{C_0/\mathbb{F}_2}(-S))$. The condition on $N/2$ implies that $X_{\mathbb{Z}_2}$ is regular, and hence C_0 a Cartier divisor on it. We get an exact sequence:

$$0 \to \mathrm{H}^0(X_{\mathbb{Z}_2}, \Omega(C_0)) \to \mathrm{H}^0(X_{\mathbb{Z}_2}, \Omega(2C_0)) \to \mathrm{H}^0(C_0, \Omega^1_{C_0/\mathbb{F}_2}(-S)).$$

We will show that the last map in this sequence is surjective. Let ω be in $\mathrm{H}^0(C_0, \Omega^1_{C_0/\mathbb{F}_2}(-S))$. It suffices to show that there is an element $\widetilde{\omega}$ of $\mathrm{H}^0(X_{\mathbb{Z}_2}, \Omega)$ that has at least a double zero along C_∞, and whose restriction to C_0 is ω. These properties of such an $\widetilde{\omega}$ can already be seen from its restriction to $X_{\mathbb{Z}/4\mathbb{Z}}$. As $\mathrm{H}^1(X_{\mathbb{Z}_2}, \Omega)$ is torsion free, the reduction map from $\mathrm{H}^0(X_{\mathbb{Z}_2}, \Omega)$ to $\mathrm{H}^0(X_{\mathbb{Z}/4\mathbb{Z}}, \Omega)$ is surjective. Let $(0, \omega)$ be the section of Ω on the closed subscheme of $X_{\mathbb{Z}_2}$ defined by $I^2_{C_\infty} I_{C_0}$ that coincides with ω modulo I_{C_0} and is zero modulo $I^2_{C_\infty}$. It is now enough to show that $(0, \omega)$ can be lifted to a section of Ω over $X_{\mathbb{Z}/4\mathbb{Z}}$. The short exact sequence of sheaves corresponding to our lifting problem is:

$$0 \to 2I_{C_0}/4\mathcal{O}_X \to \mathcal{O}_X/4\mathcal{O}_X \to \mathcal{O}_X/2I_{C_0} \to 0,$$

tensored over $\mathcal{O}_{X_{\mathbb{Z}_2}}$ with Ω. So all we have to show is that the map from $\mathrm{H}^1(X, \Omega \otimes 2I_{C_0}/4\mathcal{O}_X)$ to $\mathrm{H}^1(X_{\mathbb{Z}/4\mathbb{Z}}, \Omega)$ is injective. One verifies that $\Omega \otimes 2I_{C_0}/4\mathcal{O}_X = \Omega^1_{C_0/\mathbb{F}_2}$, so that its H^1 is $\mathbb{F}_2$, and that $\mathrm{H}^1(X, \Omega \otimes \mathcal{O}_X/2I_{C_0})$ also has order 2 (use a suitable short exact sequence with terms $\mathcal{O}_X/I_{C_0}$, $\mathcal{O}_X/2I_{C_0}$ and $\mathcal{O}_X/2\mathcal{O}_X$). We have now proved that $M/M[2]$ is the same as $\mathrm{H}^0(C_0, \Omega^1_{C_0/\mathbb{F}_2}(-S))$.

Let us now prove the equality between $\mathrm{H}^0(C_0, \Omega^1_{C_0/\mathbb{F}_2}(-S))$ and $S_1(\Gamma_0(N/2), \mathbb{F}_2)_{\mathrm{Katz}}$. Let $C_0' \to C_0$ be the cover obtained by adding a full level three structure to $\Gamma_0(N/2)$. Then, by our hypotheses on $N/2$, the morphism $C_0' \to C_0$ is unramified outside the cusps, and the ramification at the cusps is tame. Let G denote the group $\mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z})$, which acts on C_0', and on the universal generalized elliptic curve with level structure over it. It follows that:

$$\mathrm{H}^0(C_0, \Omega^1_{C_0/\mathbb{F}_2}(-S)) = \mathrm{H}^0(C_0', \Omega^1_{C_0'/\mathbb{F}_2}(-S'))^G.$$

By definition, we have:

$$S_1(\Gamma_0(N/2), \mathbb{F}_2)_{\mathrm{Katz}} = \mathrm{H}^0(C_0', \underline{\omega}(-\mathrm{cusps}))^G.$$

The Kodaira–Spencer isomorphism and the Hasse invariant, which both exist on C_0' and are G-equivariant, finish the proof of the equality.

The determination of the endomorphism of $\mathrm{H}^0(C_0, \Omega^1_{C_0/\mathbb{F}_2}(-S))$ induced by T_l (with l a prime number) is done in the same way as in the proof of 2.9, and we don't repeat it. To describe it on $S_1(\Gamma_0(N/2), \mathbb{F}_2)_{\mathrm{Katz}}$ one uses the formulas relating Hecke operators and q-expansions, and one uses that T_p acts as zero. □

3 Computation of spaces of forms of weight one: first method.

3.1 Proposition 2.10 leads to an algorithm to compute, for each N satisfying the hypotheses of that proposition, the $\mathbb{F}_2$-vector space $S_1(\Gamma_0(N/2), \mathbb{F}_2)_{\mathrm{Katz}}$ with the action of T_n for all n prime to 2. Let us explain this.

Let N satisfy the hypotheses of Proposition 2.10, and let $\mathbb{T}$ be the the Hecke algebra associated to $S_2(\Gamma_0(N), \mathbb{Z})$, i.e., the sub $\mathbb{Z}$-algebra of $\mathrm{End}(S_2(\Gamma_0(N), \mathbb{Z}))$ (or of $\mathrm{End}_{\mathbb{C}}(S_2(\Gamma_0(N), \mathbb{C}))$, it gives the same algebra) generated by all T_n, $n \geq 1$. Then we have a $\mathbb{Z}$-valued pairing between $S_2(\Gamma_0(N), \mathbb{Z})$ and $\mathbb{T}$, given by $(f, t) \mapsto a_1(tf)$. As $a_1(T_n f) = a_n(f)$ for all n and f, this pairing is perfect. Hence, as a $\mathbb{T}$-module, $S_2(\Gamma_0(N), \mathbb{Z})$ is isomorphic to the $\mathbb{Z}$-dual $\mathbb{T}^\vee$ of $\mathbb{T}$. Let W_2 be the Atkin-Lehner involution that acts on $S_2(\Gamma_0(N), \mathbb{C})$; as it is induced by an automorphism of $X_0(N)_{\mathbb{Z}_2}$ that interchanges the components C_∞ and C_0, we have:

$$W_2(\mathbb{Z}_2 \otimes S_2(\Gamma_0(N), \mathbb{Z})) = \{\omega \in \mathrm{H}^0(X_0(N)_{\mathbb{Q}_2}, \Omega^1) \mid v_{C_0}(\omega) \geq 0\}.$$

Hence:

$$\mathbb{Z}_2 \otimes (S_2(\Gamma_0(N), \mathbb{Z}) \cap W_2 S_2(\Gamma_0(N), \mathbb{Z})) = \mathrm{H}^0(X_0(N)_{\mathbb{Z}_2}, \Omega) = \mathbb{Z}_2 \otimes \mathrm{Cot}_0(J).$$

We define a $\mathbb{T}$-module M by:

(3.1.1) $$M := S_2(\Gamma_0(N), \mathbb{Z})/(S_2(\Gamma_0(N), \mathbb{Z}) \cap W_2 S_2(\Gamma_0(N), \mathbb{Z})) = \mathbb{T}^\vee/(\mathbb{T}^\vee \cap W_2 \mathbb{T}^\vee),$$

where the last intersection can be taken in $\mathbb{Q} \otimes \mathbb{T}^\vee$. Then, by Proposition 2.10 we have an isomorphism of $\mathbb{F}_2$-vector spaces:

$$S_1(\Gamma_0(N/2), \mathbb{F}_2)_{\mathrm{Katz}} = M[4]/M[2], \tag{3.1.2}$$

such that T_n on $M[4]/M[2]$ induces T_n on $S_1(\Gamma_0(N/2), \mathbb{F}_2)_{\mathrm{Katz}}$ if n is odd, and 0 if n is even.

3.2 The theory of modular symbols (see [9], [33] or William Stein's modular forms database web pages) allows one to compute with $\mathrm{H}_1(X_0(N)(\mathbb{C}), \mathbb{Z})$. In particular, one can compute the Hecke algebra $\mathbb{T}$ as well as the involution W_2. Here it is useful to note that the T_n with $n \leq 6^{-1}N\prod_{p|N}(1+p^{-1})$ generate $\mathbb{T}$ as a $\mathbb{Z}$-module: see [2] (which is a simple application of [38]). Hence one can compute M and so one gets $S_1(\Gamma_0(N/2), \mathbb{F}_2)_{\mathrm{Katz}}$ with the Hecke operators T_n with n odd.

The methods of this section can be generalized to mod 2 modular forms on $\Gamma_1(N)$, with N odd, by considering the space $S_2(\Gamma_1(2N), \mathbb{C})$. They can also be generalized to an arbitrary prime number p, by considering the spaces $S_p(\Gamma_0(p) \cap \Gamma_1(N), \mathbb{C})$ with N prime to p. But because of the next section, we think that this is not worth the effort. The results of this section can be used to check some special cases of the results of the next section.

In the next section we will present yet another way to compute more generally the spaces $S_1(\Gamma_1(N), \varepsilon, \mathbb{F}_p)_{\mathrm{Katz}}$, this time with all Hecke operators, and also in a way that should allow for a simple implementation starting from William Stein's Magma package Hecke.

In a sense, our method described in this section uses the Hasse invariant, which is a very natural modular form modulo p. As it is of weight $p-1$, multiplication by it gives a way for passing from weight one forms to weight p forms. In the next section, we also use that if f is a weight one form, then f^p is a weight p form.

4 Spaces of forms of weight one: second method.

4.1 Let p be a prime number, and $N \geq 1$ an integer prime to p. For any integer k and any fintite extension $\mathbb{F}$ of $\mathbb{F}_p$ we have the $\mathbb{F}$-vector space $S_k(\Gamma_1(N), \mathbb{F})_{\mathrm{Katz}}$ of modular forms on $\Gamma_1(N)$ of weight k and with coefficients in $\mathbb{F}$; see [17, §2] or [18, §1] for a definition and a description. We have:

$$S_k(\Gamma_1(N), \mathbb{F})_{\mathrm{Katz}} = \mathrm{H}^0(X_1(N)_{\mathbb{F}}, \underline{\omega}^{\otimes k}(-\mathrm{cusps})), \qquad \text{if } N \geq 5 .$$

As $\mathbb{F}$ is flat over $\mathbb{F}_p$, we have:

$$S_k(\Gamma_1(N), \mathbb{F})_{\mathrm{Katz}} = \mathbb{F} \otimes S_k(\Gamma_1(N), \mathbb{F}_p)_{\mathrm{Katz}}.$$

Let $\varepsilon\colon (\mathbb{Z}/N\mathbb{Z})^* \to \mathbb{F}^*$ be a character with $\mathbb{F}$ a finite field of characteristic p. For any integer k we have the $\mathbb{F}$-vector space $S_k(\Gamma_1(N),\varepsilon,\mathbb{F})_{\mathrm{Katz}}$ of modular forms on $\Gamma_1(N)$ of weight k, character ε, and with coefficients in $\mathbb{F}$; it is the subspace of $S_k(\Gamma_1(N),\mathbb{F})_{\mathrm{Katz}}$ on which $\langle a\rangle$ acts as $\varepsilon(a)$ for all a in $(\mathbb{Z}/N\mathbb{Z})^*$. If $\mathbb{F}$ is sufficiently big (i.e, contains the images of all characters from $(\mathbb{Z}/N\mathbb{Z})^*$ to $\overline{\mathbb{F}}_p^*$) then we have:

$$S_k(\Gamma_1(N),\mathbb{F})_{\mathrm{Katz}} = \bigoplus_{\varepsilon\colon (\mathbb{Z}/N\mathbb{Z})^*\to\mathbb{F}^*} S_k(\Gamma_1(N),\varepsilon,\mathbb{F})_{\mathrm{Katz}}.$$

If $\varepsilon(p) \neq (-1)^k$ then the space $S_k(\Gamma_1(N),\varepsilon,\mathbb{F})_{\mathrm{Katz}}$ is zero.

We have a $\mathbb{F}_p$-linear maps:

$$S_1(\Gamma_1(N),\mathbb{F}_p)_{\mathrm{Katz}} \longrightarrow S_p(\Gamma_1(N),\mathbb{F}_p)_{\mathrm{Katz}}, \quad A\colon f\mapsto Af, \quad F\colon f\mapsto f^p,$$

where A is the Hasse invariant. In terms of q-expansion at the standard cusp one has $a_n(Af) = a_n(f)$ and $a_n(F(f)) = a_{n/p}(f)$ for all f and n, where $a_{n/p}(f)$ has to be interpreted as zero if n/p is not integer. It follows that both A and F are injective. Combining A and F gives a map:

$$\phi\colon S_1(\Gamma_1(N),\mathbb{F}_p)^2_{\mathrm{Katz}} \longrightarrow S_p(\Gamma_1(N),\mathbb{F}_p)_{\mathrm{Katz}}, \quad (f,g)\mapsto Af + F(g). \tag{4.1.1}$$

A computation using the usual formula $a_n(T_l f) = a_{nl}(f) + l^{k-1}a_{n/l}(\langle l\rangle f)$, valid for f a modular form of weight $k>0$, n integer and l prime (with $\langle l\rangle = 0$ if l divides the level), shows that for a in $(\mathbb{Z}/N\mathbb{Z})^*$, and $l\neq p$ prime:

$$\langle a\rangle\circ\phi = \phi\circ\begin{pmatrix}\langle a\rangle & 0\\ 0 & \langle a\rangle\end{pmatrix}, \quad T_l\circ\phi = \phi\circ\begin{pmatrix}T_l & 0\\ 0 & T_l\end{pmatrix}, \quad T_p\circ\phi = \phi\circ\begin{pmatrix}T_p & 1\\ -\langle p\rangle & 0\end{pmatrix}. \tag{4.1.2}$$

The maps obtained from A, F and ϕ via extension of scalars via $\mathbb{F}_p\to\mathbb{F}$ will be denoted by the same symbols. The compatibility of ϕ with the diamond operators gives an injective $\mathbb{F}$-linear map:

$$F\colon S_1(\Gamma_1(N),\varepsilon,\mathbb{F})_{\mathrm{Katz}} \longrightarrow S_p(\Gamma_1(N),\varepsilon,\mathbb{F})_{\mathrm{Katz}}. \tag{4.1.3}$$

The image of this map F is exactly the subspace of g such that $a_n(g) = 0$ for all n not divisible by p. In order to get an effective description of this image we will use the derivation θ that was constructed by Katz in [27]. In our situation, we have an $\mathbb{F}$-linear map:

$$\theta\colon S_p(\Gamma_1(N),\varepsilon,\mathbb{F})_{\mathrm{Katz}} \longrightarrow S_{p+2}(\Gamma_1(N),\varepsilon,\mathbb{F})_{\mathrm{Katz}},$$

such that for all g in $S_p(\Gamma_1(N),\varepsilon,\mathbb{F})_{\mathrm{Katz}}$ and all $n\geq 1$ we have:

$$a_n(\theta(g)) = na_n(g),$$

i.e., θ acts on q-expansions as qd/dq. For modular forms of arbitrary weight, the usual θ raises the weight by $p+1$, but for g of some weight pk, the resulting form of weight $pk+p+1$ has zeros at the supersingular points, hence can be divided by the Hasse invariant: see the proof of [27, Lemma 3]. The image of F above is the kernel of θ. The fact that the target of θ is $S_{p+2}(\Gamma_1(N),\varepsilon,\mathbb{F})_{\mathrm{Katz}}$ leads to an effective description of its kernel.

Proposition 4.2 *With the notation as above, let g be in $S_p(\Gamma_1(N),\varepsilon,\mathbb{F})_{\mathrm{Katz}}$ and put:*

$$B := \frac{p+2}{12} N \prod_{\substack{l \mid N \\ l \text{ prime}}} (1+l^{-1}).$$

Suppose that $a_n(g) = 0$ for all $n \leq B$ that are not divisible by p. Then there is a unique f in $S_1(\Gamma_1(N),\varepsilon,\mathbb{F})_{\mathrm{Katz}}$ such that $g = F(f)$.

Proof. Let g be as in the statement. Then $\theta(g)$ is a section of $\underline{\omega}^{\otimes p+2}$ on the stack $[\Gamma_1(N)]_{\mathbb{F}}$. The degree of ω on $[\Gamma_1(1)]_{\mathbb{F}}$ is $1/24$ (see [28, Cor. 10.13.12], or [7, VI.4] and use the modular form Δ (of weight 12) plus the fact that the automorphism group of the cusp ∞ of $[\Gamma_1(1)]_{\mathbb{F}}$ has order two). The degree of $[\Gamma_1(N)]_{\mathbb{F}}$ over $[\Gamma_1(1)]_{\mathbb{F}}$ is $N^2\prod_{l|N}(1-l^{-2})$, where the product is taken over the primes l dividing N. It follows that the degree of $\underline{\omega}^{\otimes p+2}$ on the stack $[\Gamma_1(N)]_{\mathbb{F}}$ is $(p+2)N^2\prod_{l|N}(1-l^{-2})/24$. It follows that $\theta(g)$, as a section of $\underline{\omega}^{\otimes p+2}$, cannot have more zeros than this degree. We know that $\theta(g)$ has a zero of order at least $B+1$ at the cusp ∞, and as it is an eigenform for all $\langle a\rangle$ with a in $(\mathbb{Z}/N\mathbb{Z})^*$, the same is true at the cusps in the $\mathbb{Z}/N\mathbb{Z}$-orbit of ∞. One checks that these zeros imply that the divisor of $\theta(g)$ has degree at least $\phi(N)(B+1)/2$. (As we are working on a stack, we have to divide the order of a zero at a point x by the order of $\mathrm{Aut}(x)$ in order to get the contribution of x to the degree of the divisor.) Our choice of B implies that the divisor of $\theta(g)$ (if non-zero) has degree greater than the degree of $\underline{\omega}^{\otimes p+2}$, which means that $\theta(g) = 0$. $\square$

Remark 4.3 In the proof of Proposition 4.2 we have not used that g vanishes at the cusps other than those in the $(\mathbb{Z}/N\mathbb{Z})^*$-orbit of ∞. Hence the result can be improved a little bit, if necessary. If one knows moreover that g is an eigenform for Atkin-Lehner (pseudo) involutions, one can replace B by $B/2^r$, where r is the number of different primes dividing N.

Before we go on, let us record another useful consequence of the existence of θ.

Proposition 4.4 *The map $\phi\colon S_1(\Gamma_1(N),\mathbb{F}_p)^2_{\mathrm{Katz}} \longrightarrow S_p(\Gamma_1(N),\mathbb{F}_p)_{\mathrm{Katz}}$ from equation (4.1.1) is injective.*

Proof. Suppose that $\phi(f,g)=0$. Then we have $0=\theta(Af+F(g))=\theta(Af)$, hence $0=\theta(f)$. But then $f=0$, as the weight of f is not divisible by p. It follows that $F(g)=0$, hence that $g=0$. □

4.5 Now that we know how to characterize the image of $S_1(\Gamma_1(N),\varepsilon,\mathbb{F})_{\mathrm{Katz}}$ under F inside $S_p(\Gamma_1(N),\varepsilon,\mathbb{F})_{\mathrm{Katz}}$, it becomes time to investigate how to compute this ambient vector space. We want to avoid the problems related to the lifting of elements of $S_p(\Gamma_1(N),\varepsilon,\mathbb{F})_{\mathrm{Katz}}$ to characteristic zero with a given character (see [18, §1] and [18, Prop. 1.10], they have to do with what is called Carayol's Lemma). So we describe $S_p(\Gamma_1(N),\varepsilon,\mathbb{F})_{\mathrm{Katz}}$ in terms of the $\mathbb{Z}[1/N]$-module $S_p(\Gamma_1(N),\mathbb{Z}[1/N])_{\mathrm{Katz}}$ of characteristic zero forms of weight p with no prescribed character.

Proposition 4.6 *Let p be a prime number, and $N\geq 1$ an integer not divisible by p. Suppose that $N\neq 1$ or that $p\geq 5$. Then the map:*

$$\mathbb{F}_p\otimes S_p(\Gamma_1(N),\mathbb{Z}[1/N])_{\mathrm{Katz}}\longrightarrow S_p(\Gamma_1(N),\mathbb{F}_p)_{\mathrm{Katz}}$$

is an isomorphism, compatible with all Hecke operators T_n (for $n\geq 1$) and $\langle a\rangle$ (for a in $(\mathbb{Z}/N\mathbb{Z})^*$). Hence for $\mathbb{F}$ a finite extension of $\mathbb{F}_p$ and a character $\varepsilon\colon(\mathbb{Z}/N\mathbb{Z})^*\to\mathbb{F}^*$:

$$S_p(\Gamma_1(N),\varepsilon,\mathbb{F}_p)_{\mathrm{Katz}}=(\mathbb{F}\otimes S_p(\Gamma_1(N),\mathbb{Z}[1/N])_{\mathrm{Katz}})(\varepsilon).$$

Proof. This follows from [18, Lemma 1.9] and its proof. □

4.7 The next goal is to relate $S_p(\Gamma_1(N),\mathbb{Z}[1/N])_{\mathrm{Katz}})$ to the usual description of modular forms as functions on the complex upper half plane. For k an integer, we let $S_k(\Gamma_1(N),\mathbb{C})$ be the $\mathbb{C}$-vector space of holomorphic cusp forms on the congruence subgroup $\Gamma_1(N)=\{\left(\begin{smallmatrix}a & b\\ Nc & d\end{smallmatrix}\right)\}$ of $\mathrm{SL}_2(\mathbb{Z})$, and, for A a subring of $\mathbb{C}$, we let $S_k(\Gamma_1(N),A)$ be its sub A-module of f such that $a_n(f)$ belongs to A for all n.

With these definitions, $S_k(\Gamma_1(N),\mathbb{Z}[1/N])_{\mathrm{Katz}}$ and $S_k(\Gamma_1(N),\mathbb{Z}[1/N])$ are not really the same thing. The problem is that, in terms of moduli problems, the first is defined by considering pairs $(E/S,\alpha)$ with E/S an elliptic curve over a $\mathbb{Z}[1/N]$-scheme and α an embedding of the constant group scheme $(\mathbb{Z}/N\mathbb{Z})_S$ into E, whereas $(\mathbb{Z}/N\mathbb{Z})_S$ is replaced by $\mu_{N,S}$ for the second. Let us write $[\Gamma_1(N)]'_{\mathbb{Z}[1/N]}$ for the stack corresponding to embeddings of μ_N. As $(\mathbb{Z}/N\mathbb{Z})_{\mathbb{Z}}$ and μ_N become canonically isomorphic over $\mathbb{Z}[1/N,\zeta_N]$, the two stacks $[\Gamma_1(N)]_{\mathbb{Z}[1/N]}$ and $[\Gamma_1(N)]'_{\mathbb{Z}[1/N]}$ become canonically isomorphic over $\mathbb{Z}[1/N,\zeta_N]$. It follows that $S_k(\Gamma_1(N),\mathbb{Z}[1/N,\zeta_N])_{\mathrm{Katz}}$ and $S_k(\Gamma_1(N),\mathbb{Z}[1/N,\zeta_N])$ are canonically isomorphic, compatibly with the action of Hecke, diamond and Atkin-Lehner operators. In particular, the Hecke operators T_n $(n\geq 1)$ and diamond operators $\langle a \rangle$ (a in $(\mathbb{Z}/N\mathbb{Z})^*$) generate the same $\mathbb{Z}$-algebra $\mathbb{T}$ in the two endomorphism rings. In particular, $S_k(\Gamma_1(N), \mathbb{Z}[1/N])_{\mathrm{Katz}}$ and $S_k(\Gamma_1(N), \mathbb{Z}[1/N])$ are both modules over $\mathbb{T}$.

Proposition 4.8 *In the notation of above, $S_k(\Gamma_1(N), \mathbb{Z}[1/N])_{\mathrm{Katz}}$ and $S_k(\Gamma_1(N), \mathbb{Z}[1/N])$ are isomorphic as $\mathbb{T}$-modules, for all positive integers N and k.*

Proof. Let $N \geq 1$. The description of $[\Gamma_1(N)]'_{\mathbb{Z}[1/N]}$ as a twist of $[\Gamma_1(N)]_{\mathbb{Z}[1/N]}$ over $\mathbb{Z}[1/N, \zeta_N]$ shows that one of the two $\mathbb{T}[1/N]$-modules in question is obtained by twisting the other over $\mathbb{Z}[1/N, \zeta_N]$ via the morphism of groups $(\mathbb{Z}/N\mathbb{Z})^* \to \mathbb{T}^*$ that sends a to the diamond operator $\langle a \rangle$. In fact, this twisting can be done on any $\mathbb{T}[1/N]$-module, and gives an auto equivalence of the category of $\mathbb{T}[1/N]$-modules. Hence it is not surprising that this twisting functor is isomorphic to the functor $M \otimes_{\mathbb{T}[1/N]} -$, where M is the twist of $\mathbb{T}[1/N]$ itself. Just this fact is already sufficient to conclude that a module and its twist are locally isomorphic, since M is an invertible $\mathbb{T}[1/N]$-module. In the following we will only use that for prime numbers p not dividing N, $\mathbb{Z}_p \otimes S_k(\Gamma_1(N), \mathbb{Z}[1/N])_{\mathrm{Katz}}$ and $\mathbb{Z}_p \otimes S_k(\Gamma_1(N), \mathbb{Z}[1/N])$ are isomorphic as $\mathbb{Z}_p \otimes \mathbb{T}$-modules.

The proof that M is actually free of rank one depends on computations that we do not want to reproduce here in detail. First one replaces $\mathbb{T}[1/N]$ by the group ring $\mathbb{Z}[1/N][(\mathbb{Z}/N\mathbb{Z})^*]$. One has to find a unit $t = \sum_a t_a \langle a \rangle$ in $\mathbb{Z}[1/N, \zeta_N][(\mathbb{Z}/N\mathbb{Z})^*]$ such that:

$$\sigma_b(t) = \langle b \rangle t, \qquad \text{for all } b \text{ in } (\mathbb{Z}/N\mathbb{Z})^*,$$

where σ_b is induced by the automorphism of $\mathbb{Z}[\zeta_N]$ that sends ζ_N to ζ_N^b.

Let us just treat the case where $N = p > 2$ is prime. Then one can take:

$$t := \sum_a (1 - \zeta_p^{-a}) \langle a^{-1} \rangle, \qquad t' := \sum_a \zeta_p^a \langle a \rangle,$$

and verify that $tt' = -p$.

In the case of a prime power one uses the intermediate fields and the extraction of pth roots. The general case is treated by reduction to the prime power case. $\square$

Remark 4.9 In order to avoid the problem of comparing the two Hecke modules we could have worked from the start with the moduli problem $[\Gamma_1(N)]'_{\mathbb{Z}[1/N]}$, but on the other hand it seems useful to have a comparison as Proposition 4.8 available.

It should be noted that our notation $S_k(\Gamma_1(N), \mathbb{Z}[1/N])_{\mathrm{Katz}}$ and $S_k(\Gamma_1(N), \mathbb{Z}[1/N])$ for the two types of modular forms is not good, since Katz's definition of modular forms as sections of an invertible module on a stack has nothing to do with a choice between the group schemes $\mathbb{Z}/N\mathbb{Z}$ and μ_N.

To complicate things even further, let us mention that the two stacks $[\Gamma_1(N)]_{\mathbb{Z}[1/N]}$ and $[\Gamma_1(N)]'_{\mathbb{Z}[1/N]}$ are isomorphic, via the following construction. To E/S with a closed immersion $\alpha\colon (\mathbb{Z}/N\mathbb{Z})_S \to E$ one associates E'/S and $\alpha'\colon \mu_{N,S} \to E'$, where $\pi\colon E \to E'$ is the quotient of E by the image of α, and α' the natural isomorphism from $\mu_{N,S}$ (the Cartier dual of $(\mathbb{Z}/N\mathbb{Z})_S$) to the kernel of the dual of π (see [28, §2.8]). In the terminology of [28], this isomorphism is called exotic, and seems to be of no help for comparing $S_k(\Gamma_1(N), \mathbb{Z}[1/N])_{\mathrm{Katz}}$ and $S_k(\Gamma_1(N), \mathbb{Z}[1/N])$ as Hecke modules.

The following proposition is well known. It is the final ingredient that we use to describe the $S_1(\Gamma_1(N), \varepsilon, \mathbb{F})$ in terms of a Hecke algebra that can be computed using modular symbols.

Proposition 4.10 *Let $N \geq 1$ and k be integers. Let $\mathbb{T}$ be the subring of $\mathrm{End}_{\mathbb{C}}(S_k(\Gamma_1(N), \mathbb{C}))$ generated by the T_n, $n \geq 1$. Then $\mathbb{T}$ contains the $\langle a \rangle$ for all a in $(\mathbb{Z}/N\mathbb{Z})^*$, and is generated as $\mathbb{Z}$-module by the T_n. The pairing:*

$$(t, f) \mapsto a_1(tf)$$

from $\mathbb{T} \times S_k(\Gamma_1(N), \mathbb{Z})$ to $\mathbb{Z}$ is perfect, and gives an isomorphism of $\mathbb{T}$-modules:

$$S_k(\Gamma_1(N), \mathbb{Z}) = \mathbb{T}^\vee.$$

Proof. For $k \leq 0$ the space of cusp forms is zero, and the result is trivially true. So we suppose that $k \geq 1$. The fact that $\mathbb{T}$ contains all $\langle a \rangle$ is well known: one uses that for all prime numbers l one has $l^{k-1}\langle l \rangle = T_l^2 - T_{l^2}$, and one takes two distinct primes l_1 and l_2 that both have image a in $\mathbb{Z}/N\mathbb{Z}$. The fact that the T_n generate $\mathbb{T}$ as a $\mathbb{Z}$-module follows from the formula that expresses a product $T_n T_m$ as the sum $\sum_d d^{k-1}\langle d \rangle T_{nm/d^2}$ over the positive common divisors of n and m that are prime to N. To prove the second statement, one uses the formula $a_n(f) = a_1(T_n f)$ and that $S_k(\Gamma_1(N), \mathbb{Z})$ is by definition the sub $\mathbb{Z}$-module of f in $S_k(\Gamma_1(N), \mathbb{C})$ such that $a_n(f)$ is in $\mathbb{Z}$ for all n. $\square$

Theorem 4.11 *Let $N \geq 5$ be an integer, p a prime number not dividing N, $\mathbb{F}$ a finite extension of $\mathbb{F}_p$ and $\varepsilon\colon (\mathbb{Z}/N\mathbb{Z})^* \to \mathbb{F}^*$ a character. Let $\mathbb{T}$ be the subring of $\mathrm{End}_{\mathbb{C}}(S_p(\Gamma_1(N), \mathbb{C}))$ generated by the T_n, $n \geq 1$. Put $B := \frac{p+2}{12} N \prod_l (1 + l^{-1})$, with the product taken over the prime divisors of N. Let L_ε be the sub $\mathbb{F}$-vector space of f in $\mathbb{F} \otimes \mathbb{T}^\vee = \mathrm{Hom}(\mathbb{T}, \mathbb{F})$ that satisfy:*

(4.11.1) $\quad \langle a \rangle f = \varepsilon(a) f \quad$ *for all a in $(\mathbb{Z}/N\mathbb{Z})^*$;*

(4.11.2) $\quad f(T_n) = 0 \quad$ *for all $n \leq B$ not divisible by p.*

For f in L_ε one has $f(T_n) = 0$ for all n not divisible by p. For such an f, we have $(T_p f)(T_n) = f(T_{pn})$ for all $n \geq 1$, and T_p induces an isomorphism from L_ε to its image L'_ε.

The subspace L'_ε is stable under all T_l with $l \neq p$ prime, and by $T'_p := T_p + \varepsilon(p)F$, with $F\colon L'_\varepsilon \to \mathbb{F}\otimes\mathbb{T}^\vee$ defined by: $(Ff)(T_n) = f(T_{n/p})$ (with $T_{n/p} = 0$ if n/p is not integer). Then there is an isomorphism of Hecke modules between $S_1(\Gamma_1(N), \varepsilon, \mathbb{F})_{\mathrm{Katz}}$ and L'_ε, with T_l for $l \neq p$ prime corresponding on both sides, and T_p corresponding to T'_p on L'_ε.

In terms of q-expansions: there is an isomorphism (unique) of $\mathbb{F}$-vector spaces between $S_1(\Gamma_1(N)', \varepsilon, \mathbb{F})_{\mathrm{Katz}}$ (defined with μ_N-structures) and L'_ε such that for f in L'_ε its image in $S_1(\Gamma_1(N)', \varepsilon, \mathbb{F})_{\mathrm{Katz}}$ has q-expansion $\sum_n f(T_n)q^n$.

Proof. Everything follows directly from the previous propositions in this section, so we just say how those are combined. The image of $S_1(\Gamma_1(N), \varepsilon, \mathbb{F})_{\mathrm{Katz}}$ in $S_1(\Gamma_1(N), \varepsilon, \mathbb{F})_{\mathrm{Katz}}$ under F is characterized by Proposition 4.2. The space $S_1(\Gamma_1(N), \varepsilon, \mathbb{F})_{\mathrm{Katz}}$ is described in terms of $S_p(\Gamma_1(N), \mathbb{Z}[1/N])_{\mathrm{Katz}}$ by Proposition 4.6. Proposition 4.8 says that $S_p(\Gamma_1(N), \mathbb{Z}[1/N])_{\mathrm{Katz}}$ and $S_p(\Gamma_1(N), \mathbb{Z}[1/N])$ are isomorphic. Proposition 4.10 says that $S_p(\Gamma_1(N), \mathbb{Z})$ and $\mathbb{T}^\vee$ are isomorphic. $\square$

For convenience of the reader we also state a version of Theorem 4.11 where the character is not fixed.

Theorem 4.12 *Let $N \geq 5$ be an integer, and p a prime number not dividing N. Let $\mathbb{T}$ be the subring of $\mathrm{End}_{\mathbb{C}}(S_p(\Gamma_1(N), \mathbb{C}))$ generated by the T_n, $n \geq 1$. Put $B' := \frac{p+2}{24}N^2\prod_l(1-l^{-2})$, with the product taken over the prime divisors of N. Let L be the sub $\mathbb{F}$-vector space of f in $\mathbb{F}\otimes\mathbb{T}^\vee = \mathrm{Hom}(\mathbb{T}, \mathbb{F})$ that satisfy:*

$$f(T_n) = 0 \quad \text{for all } n \leq B' \text{ not divisible by } p. \tag{4.12.1}$$

For f in L one has $f(T_n) = 0$ for all n not divisible by p. For such an f, we have $(T_pf)(T_n) = f(T_{pn})$ for all $n \geq 1$, and T_p induces an isomorphism from L to its image L'. The subspace L' is stable under all T_l with $l \neq p$ prime, and by $T'_p := T_p + \langle p\rangle F$, with $F\colon L' \to \mathbb{F}\otimes\mathbb{T}^\vee$ defined by: $(Ff)(T_n) = f(T_{n/p})$ (with $T_{n/p} = 0$ if n/p is not integer). Then there is an isomorphism of Hecke modules between $S_1(\Gamma_1(N), \mathbb{F}_p)_{\mathrm{Katz}}$ and L', with T_l for $l \neq p$ prime corresponding on both sides, and T_p corresponding to T'_p on L'.

In terms of q-expansions: there is an isomorphism (unique) of $\mathbb{F}_p$-vector spaces between $S_1(\Gamma_1(N)', \mathbb{F}_p)_{\mathrm{Katz}}$ (defined with μ_N-structures) and L' such that for f in L' its image in $S_1(\Gamma_1(N)', \mathbb{F}_p)_{\mathrm{Katz}}$ has q-expansion $\sum_n f'(T_n)q^n$.

Proof. One just adapts the proof of Theorem 4.11. The value of B' is gotten by inspection of the proof of Proposition 4.2. $\square$

5 Some remarks on modular symbols modulo p.

5.1 This seems an appropriate point to make a few remarks on what is actually computed by the modular symbols algorithms. Suppose that $N \geq 5$. (Most of what follows still works for arbitrary $N \geq 1$ if one replaces $Y_1(N)$ by the stack $[\Gamma_1(N)]_{\mathbb{C}}$; we intend to give precise statements in a future article.) Let $\pi\colon \mathbb{E} \to Y_1(N)_{\mathbb{Q}}$ be the universal elliptic curve. Consider the locally constant sheaf $\mathrm{R}^1\pi_*\mathbb{Z}_{\mathbb{E}}$ of free $\mathbb{Z}$-modules of rank two on $Y_1(N)(\mathbb{C})$. For $k \geq 2$ let $\mathcal{F}_k := \mathrm{Sym}^{k-2}(\mathrm{R}^1\pi_*\mathbb{Z}_{\mathbb{E}})$. Then one defines:

$$\mathrm{H}^1_{\mathrm{par}}(Y_1(N)(\mathbb{C}), \mathcal{F}_k) := \mathrm{Image}(\mathrm{H}^1_{\mathrm{c}}(Y_1(N)(\mathbb{C}), \mathcal{F}_k) \to \mathrm{H}^1(Y_1(N)(\mathbb{C}), \mathcal{F}_k)), \tag{5.1.1}$$

with the subscript "c" standing for compactly supported cohomology. Let j denote the inclusion of $Y_1(N)_{\mathbb{Q}}$ into $X_1(N)_{\mathbb{Q}}$. Then one has:

$$\begin{aligned} \mathrm{H}^1_{\mathrm{c}}(Y_1(N)(\mathbb{C}), \mathcal{F}_k) &= \mathrm{H}^1(X_1(N)(\mathbb{C}), j_!\mathcal{F}_k), \\ \mathrm{H}^1_{\mathrm{par}}(Y_1(N)(\mathbb{C}), \mathcal{F}_k) &= \mathrm{H}^1(X_1(N)(\mathbb{C}), j_*\mathcal{F}_k), \\ \mathrm{H}^1_{\mathrm{par}}(Y_1(N)(\mathbb{C}), \mathcal{F}_2) &= \mathrm{H}^1(X_1(N)(\mathbb{C}), \mathbb{Z}). \end{aligned} \tag{5.1.2}$$

The Shimura isomorphism is the Hodge decomposition (see [13, §12]):

$$\mathbb{C} \otimes \mathrm{H}^1_{\mathrm{par}}(Y_1(N)(\mathbb{C}), \mathcal{F}_k) = S_k(\Gamma_1(N), \mathbb{C}) \oplus \overline{S_k(\Gamma_1(N), \mathbb{C})}. \tag{5.1.3}$$

It follows that the Hecke correspondences and diamond operators generate the same sub $\mathbb{Z}$-algebra $\mathbb{T}(N,k)$ of $\mathrm{End}(\mathbb{Q} \otimes \mathrm{H}^1_{\mathrm{par}}(Y_1(N)(\mathbb{C}), \mathcal{F}_k))$ and of $\mathrm{End}(S_k(\Gamma_1(N), \mathbb{C}))$. The modular symbols algorithm compute (among other things) the Hecke modules $\mathrm{H}^1_{\mathrm{par}}(Y_1(N)(\mathbb{C}), \mathcal{F}_k)$, interpreted in group cohomological terms. To be precise, we mention that:

$$\mathrm{H}^1(Y_1(N)(\mathbb{C}), \mathcal{F}_k) = \mathrm{H}^1(\Gamma_1(N), \mathrm{Sym}^{k-2}(\mathbb{Z}^2)),$$

and that the submodule $\mathrm{H}^1_{\mathrm{par}}(Y_1(N)(\mathbb{C}), \mathcal{F}_k)$ is obtained as the subgroup of elements of $\mathrm{H}^1(\Gamma_1(N), \mathrm{Sym}^{k-2}(\mathbb{Z}^2))$ whose restriction to all unipotent subgroups of $\Gamma_1(N)$ is zero (see for example [13, §12.2]). For more details on this, especially in relation to Serre's conjectures in [37], one may consult [24].

For p and k with p a prime not dividing N and $2 \leq k \leq p+1$, the $\mathbb{Z}_p$-module $\mathrm{H}^1_{\mathrm{par}}(Y_1(N)(\mathbb{C}), \mathbb{Z}_p \otimes \mathcal{F}_k)$ is free, and the morphism:

$$\mathbb{F}_p \otimes \mathrm{H}^1_{\mathrm{par}}(Y_1(N)(\mathbb{C}), \mathcal{F}_k) \longrightarrow \mathrm{H}^1_{\mathrm{par}}(Y_1(N)(\mathbb{C}), \mathbb{F}_p \otimes \mathcal{F}_k) \tag{5.1.4}$$

is an isomorphism. (To prove this, one uses among other things that the monodromy of $\mathrm{R}^1\pi_*\mathbb{Z}_{\mathbb{E}}$ at a cusp is given, up to conjugation, by some $\left(\begin{smallmatrix} 1 & d \\ 0 & 1 \end{smallmatrix}\right)$, with d dividing N, hence prime to p.)

The descriptions of spaces of mod p modular forms of weight one given in Theorems 4.11 and 4.12 are in terms of the $\mathbb{F}_p$-algebra $\mathbb{F}_p \otimes \mathbb{T}(N,p)$. In view of the isomorphism (5.1.4) one would hope that $\mathbb{F}_p \otimes \mathbb{T}(N,p)$ is the sub $\mathbb{F}_p$-algebra of $\mathrm{End}_{\mathbb{F}_p}(\mathrm{H}^1_{\mathrm{par}}(Y_1(N)(\mathbb{C}), \mathbb{F}_p \otimes \mathcal{F}_p))$ generated by the T_n and $\langle a \rangle$. But some thinking shows that it is not clear at all whether $\mathrm{H}^1_{\mathrm{par}}(Y_1(N)(\mathbb{C}), \mathbb{F}_p \otimes \mathcal{F}_p)$ is a faithful $\mathbb{F}_p \otimes \mathbb{T}(N,p)$-module. As we do know that $S_k(N, \mathbb{F}_p)$ is isomorphic to $\mathbb{F}_p \otimes \mathbb{T}(N,k)^\vee$, when $k \geq 2$, some integral p-adic Hodge theory should be applied at this point. The usual theory for étale cohomology and analytic theory give isomorphisms of $\mathbb{T}(N,k)$-modules:

$$\mathrm{H}^1_{\mathrm{par}}(Y_1(N)(\mathbb{C}), \mathbb{F}_p \otimes \mathcal{F}_k) = \mathrm{H}^1_{\mathrm{par}}(Y_1(N)_{\overline{\mathbb{Q}}_p,\mathrm{et}}, \mathcal{F}_{k,p}), \tag{5.1.5}$$

where $\mathcal{F}_{k,p}$ is the mod p étale counterpart of $\mathcal{F}_k$.

Theorem 5.2 *Let $N \geq 5$ and $k \geq 2$ be integers, and p a prime number not dividing N. If $k < p$ or $k = p = 2$, then $\mathrm{H}^1_{\mathrm{par}}(Y_1(N)(\mathbb{C}), \mathbb{F}_p \otimes \mathcal{F}_k)$ is a faithful $\mathbb{F}_p \otimes \mathbb{T}(N,k)$-module. In particular, $\mathrm{H}^1(X_1(N)(\mathbb{C}), \mathbb{F}_2)$ is a faithful $\mathbb{F}_2 \otimes \mathbb{T}(N,2)$-module if 2 does not divide N. It follows that, for $k < p$ or $k = p = 2$, the $\mathbb{F}_p$-algebra $\mathbb{F}_p \otimes \mathbb{T}(N,k)$ is the sub $\mathbb{F}_p$-algebra of endomorphisms of $\mathrm{H}^1_{\mathrm{par}}(Y_1(N)(\mathbb{C}), \mathbb{F}_p \otimes \mathcal{F}_k)$ generated by the $\langle a \rangle$ (a in $(\mathbb{Z}/N\mathbb{Z})^*$) and T_n ($n \geq 1$), and, in fact, that $\mathbb{F}_p \otimes \mathbb{T}(N,k)$ is generated as an $\mathbb{F}_p$-vector space by the $\langle a \rangle$ (a in $(\mathbb{Z}/N\mathbb{Z})^*$) plus the T_n, $1 \leq n \leq 12^{-1}kN\prod_{l|N}(1+l^{-1})$.*

Proof. Let us first deal with the case $2 \leq k < p$. We follow Fontaine and Laffaille as in [21], adapting it to the special case that we need, and using some notation as in [19]. We let $\mathrm{MF}_{[0,p-2]}$ be the category of filtered ϕ-modules (D, Fil, ϕ) where D is a finite dimensional $\mathbb{F}_p$-vector space, Fil a decreasing filtration on D such that $D = \mathrm{Fil}^0(D)$ and $\mathrm{Fil}^{p-1}(D) = 0$, and $\phi\colon\ \mathrm{Gr}(D) \to D$ an isomorphism of $\mathbb{F}_p$-vector spaces to D from the graded object $\oplus_{i=0}^{p-2} \mathrm{Fil}^i(D)/\mathrm{Fil}^{i+1}(D)$ associated to (D, Fil). Fontaine and Laffaille construct a fully faithful contravariant functor $\mathbb{V}$ from $\mathrm{MF}_{[0,p-2]}$ to the category $\mathrm{Rep}_{\mathbb{F}_p}(G_{\mathbb{Q}_p})$ of continuous representations of $G_{\mathbb{Q}_p} := \mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$ on finite dimensional $\mathbb{F}_p$-vector spaces, see [21, Thm. 6.1]. The objets in the essential image of $\mathbb{V}$ are called crystalline representations.

In order to relate this functor $\mathbb{V}$ to our problem, we can refer to work of Faltings and Jordan ([19] and [20]), or of Fontaine and Messing and Kato (see [22], [25], or better, the introduction of [4]). In the latter case one has to use the description of $\mathrm{H}^1_{\mathrm{par}}(Y_1(N)(\mathbb{C}), \mathbb{F}_p \otimes \mathcal{F}_{k,p})$ as a suitable piece of $\mathrm{H}^{k-1}(E^{k-2}(\mathbb{C}), \mathbb{F}_p)$, where E^{k-2} is the proper smooth $\mathbb{Z}[1/N]$-model of the $k-2$-fold power of the universal elliptic curve over $Y_1(N)$, as described in Deligne [10] and Scholl [36]. In both cases, one gets the result that $\mathrm{H}^1_{\mathrm{par}}(Y_1(N)_{\overline{\mathbb{Q}}_p,\mathrm{et}}, \mathcal{F}_{k,p})^\vee$ is crystalline. In the first case, the corresponding object (D, Fil, ϕ) of $\mathrm{MF}_{[0,p-2]}$ is written $\mathrm{H}^1_{\mathrm{par}}(Y_{\overline{\mathbb{F}}_p}, \mathrm{Sym}^{k-2}(\mathcal{E}))$ (see

[20, Thm 1.1]). In the second case, it is a suitable piece of $\mathrm{H}^{k-1}_{\mathrm{dR}}(E^{k-2}_{\mathbb{F}_p})$. In both cases, (D, Fil, ϕ) satisfies (see [20, Thm 1.1]):

$$
\begin{aligned}
&\mathrm{Fil}^k(D) = 0\\
&\mathrm{Fil}^{k-1}(D) = \mathrm{Fil}^1(D) = S_k(\Gamma_1(N), \mathbb{F}_p)_{\mathrm{Katz}},\\
&\mathrm{Fil}^0(D)/\mathrm{Fil}^1(D) = S_k(\Gamma_1(N), \mathbb{F}_p)^{\vee}_{\mathrm{Katz}}
\end{aligned}
\tag{5.2.1}
$$

By [20, Thm. 1.2], the functor $\mathbb{V}$ transforms the Hecke operators T_n and the $\langle a\rangle$ on D into the duals of the same operators on $\mathrm{H}^1_{\mathrm{par}}(Y_1(N)_{\overline{\mathbb{Q}}_p,\mathrm{et}}, \mathcal{F}_{k,p})$. As $S_k(\Gamma_1(N), \mathbb{F}_p)_{\mathrm{Katz}}$ is a faithful $\mathbb{F}_p \otimes \mathbb{T}(N, k)$-module, the same holds for D, hence for $\mathrm{H}^1_{\mathrm{par}}(Y_1(N)_{\overline{\mathbb{Q}}_p,\mathrm{et}}, \mathcal{F}_{k,p})$.

Now suppose that $k = p = 2$. Let J denote the jacobian of the curve $X_1(N)$ over $\mathbb{Z}_2$. Then $\mathrm{H}^1(X_1(N)(\mathbb{C}), \mathbb{F}_2)$ is the same as $\mathrm{H}^1(X_1(N)(\overline{\mathbb{Q}}), \mathbb{F}_2)$, and as $\mathrm{H}^1(X_1(N)(\overline{\mathbb{Q}}_2), \mathbb{F}_2)$, after a choice of embeddings of $\overline{\mathbb{Q}}$ into $\mathbb{C}$ and $\overline{\mathbb{Q}}_2$. Hence, as $\mathbb{T}(N, 2)$-modules, $\mathrm{H}^1(X_1(N)(\mathbb{C}), \mathbb{F}_2)$ is the same as $J[2](\overline{\mathbb{Q}}_2)$, the group of $\overline{\mathbb{Q}}_2$-points of the 2-torsion subgroup scheme of J. Suppose now that an element t of $\mathbb{T}(N, 2)$ acts as zero on $\mathrm{H}^1(X_1(N)(\mathbb{C}), \mathbb{F}_2)$. Then it acts as zero on $J[2](\overline{\mathbb{Q}}_2)$, hence on the group scheme $J[2]$, since $J[2]_{\mathbb{Q}_2}$ is reduced and $J[2]$ is flat over $\mathbb{Z}_2$. Hence t acts as zero on the special fibre $J[2]_{\mathbb{F}_2}$ of $J[2]$. But then t acts trivially on $\mathrm{H}^1_{\mathrm{dR}}(J_{\mathbb{F}_2})$ since this cohomology group is the Dieudonné module of $J[2]_{\mathbb{F}_2}$ by [34, Cor. 5.11] of Oda. It follows that t acts as zero on $\mathrm{Fil}^1(\mathrm{H}^1_{\mathrm{dR}}(J_{\mathbb{F}_2}))$, which is the same as $S_2(\Gamma_1(N), \mathbb{F}_2)_{\mathrm{Katz}}$. Hence the image of t in $\mathbb{F}_2 \otimes \mathbb{T}(N, 2)$ is zero. The first claim of Theorem 5.2 has now been proved.

The claim that $\mathbb{F}_p \otimes \mathbb{T}(N, k)$ is the subalgebra of endomorphisms generated by Hecke correspondences is an immediate consequence. The last statement then follows from the fact that $\mathbb{T}(N, k)$ is generated as $\mathbb{Z}$-module by the $\langle a\rangle$ (a in $(\mathbb{Z}/N\mathbb{Z})^*$) and the T_n with $1 \leq n \leq 12^{-1}kN\prod_{l|N}(1 + l^{-1})$, which is proved by an argument similar to [2], see also the proof of Proposition 4.2. □

Remark 5.3 We do not know if $\mathrm{H}^1_{\mathrm{par}}(Y_1(N)(\mathbb{C}), \mathbb{F}_p \otimes \mathcal{F}_p)$ is a faithful $\mathbb{F}_p \otimes \mathbb{T}(N, p)$-module, for $N \geq 5$ and p a prime not dividing N. We strongly suspect that this is true and that it can be proved by the usual reduction to weight two, by working with $X_1(Np)$, as for example in [23] and [17]. Of course, it would be nicer to have a more direct proof in terms of p-adic Hodge theory. In this case there still is an exact faithful functor $\mathbb{V}$ from $\mathrm{MF}_{[0,p-1]}$ to $\mathrm{Rep}_{\mathbb{F}_p}(G_{\mathbb{Q}_p})$ (see [21, Thm. 3.3]), and $\mathrm{H}^{p-1}_{\mathrm{dR}}(E^{p-2}_{\mathbb{F}_p})$ is naturally an object of $\mathrm{MF}_{[0,p-1]}$ (see[5, Thm. 3.2.1]). If $\mathbb{V}$ sends $\mathrm{H}^{p-1}_{\mathrm{dR}}(E^{p-2}_{\mathbb{F}_p})$ to $\mathrm{H}^{p-1}(E^{p-2}_{\overline{\mathbb{Q}}_p,\mathrm{et}}, \mathbb{F}_p)$ then it follows that $\mathrm{H}^1_{\mathrm{par}}(Y_1(N)(\mathbb{C}), \mathbb{F}_p \otimes \mathcal{F}_p)$ is a faithful $\mathbb{F}_p \otimes \mathbb{T}(N, p)$-module. However it seems not be be known if $\mathbb{V}$ satisfies this property (see the first sentence after Theorem 3.2.3 in [5]).

We note that for $2 \leq k < p$, much more is known about $\mathrm{H}^1_{\mathrm{par}}(Y_1(N)(\mathbb{C}), \mathbb{F}_p \otimes \mathcal{F}_k)$ as $\mathbb{F}_p \otimes \mathbb{T}(N, k)$-module, and about the ring $\mathbb{T}(N, k)$ itself, see for example [20, Thm. 2.1]. Especially, after localisation at a maximal ideal m of $\mathbb{F}_p \otimes \mathbb{T}(N, k)$ such that the corresponding Galois representation to $\mathrm{GL}_2((\mathbb{F}_p \otimes \mathbb{T}(N,k))/m)$ is irreducible, one knows that $(\mathbb{F}_p \otimes \mathbb{T}(N,k))_m$ is Gorenstein, and with $\mathrm{H}^1_{\mathrm{par}}(Y_1(N)(\mathbb{C}), \mathbb{F}_p \otimes \mathcal{F}_k)_m$ free of rank two over it. In a lot of cases one even knows that $(\mathbb{F}_p \otimes \mathbb{T}(N,k))_m$ is a complete intersection, see [12], and also [11].

6 Eigenspaces in weight p and eigenforms of weight one.

6.1 The results of the previous section make it possible to compute the spaces $S_1(\Gamma_1(N), \mathbb{F}_p)$, with $N \geq 1$ and p a prime not dividing N, as Hecke modules. This is useful if one is interested in ring theoretic properties of the associated Hecke algebras. For example, one would like to know if Kilford's examples of non-Gorenstein Hecke algebras (see [29]) can be explained by weight one phenomena. Sometimes one is just interested in the systems of eigenvalues. The aim of this section is to give a result about eigenspaces.

Proposition 6.2 *Let $N \geq 1$ be an integer, p a prime number that does not divide N, and $\varepsilon\colon (\mathbb{Z}/N\mathbb{Z})^* \to \overline{\mathbb{F}}_p$ a character. Let V be a common non-zero eigenspace in $S_p(\Gamma_1(N), \varepsilon, \overline{\mathbb{F}}_p)_{\mathrm{Katz}}$ for all T_l, $l \neq p$ prime. Let a denote the system of eigenvalues attached to V: T_l acts as a_l on V. Then V is of dimension at most two. If $\dim(V) = 1$, then a does not occur in $S_1(\Gamma_1(N), \varepsilon, \overline{\mathbb{F}}_p)_{\mathrm{Katz}}$. If $\dim(V) = 2$, then the eigenspace V_1 in $S_1(\Gamma_1(N), \varepsilon, \overline{\mathbb{F}}_p)_{\mathrm{Katz}}$ attached to a is of dimension one. In this case, the T_p eigenvalue of V_1 is the trace of T_p on V.*

Proof. We consider q-expansions at the standard cusp, and use the formulas for the action of the T_n and $\langle a \rangle$. Let V be as in the proposition. Let d be the dimension of V. As T_p commutes with all T_l, T_p acts on V, hence V contains a non-zero eigenvector f for all T_n ($n \geq 1$). In particular, $a_1(f) \neq 0$. It follows that the subspace V' of V consisting of the g in V with $a_1(g) = 0$ is of dimension $d-1$. For every element g of V', we have $0 = a_n(g) = a_1(T_n(g))$ for all n not divisible by p. It follows that $V' = FV_1$, with F as in (4.1.3), and V_1 the eigenspace of $S_1(\Gamma_1(N), \varepsilon, \overline{\mathbb{F}}_p)_{\mathrm{Katz}}$ associated to a.

Suppose that g is in V_1 and that $a_1(g) = 0$. Then $a_n(g) = 0$ for all n prime to p. But then $\theta(g) = 0$, implying that $g = 0$, as p does not divide the weight of g (see [27]). We have proved that $d \leq 2$.

If $V_1 \neq \{0\}$, then $d \geq 2$ by Proposition 4.4 and the identities (4.1.2). Hence if $d = 1$, $V_1 = \{0\}$, and a does not occur in $S_1(\Gamma_1(N), \varepsilon, \overline{\mathbb{F}}_p)_{\mathrm{Katz}}$. If $d = 2$, then $\dim(V_1) = 1$, and the trace of T_p on V is the T_p-eigenvalue a_p of V_1 by the identities (4.1.2). □

Remark 6.3 For computational purposes, let us add the following. In Proposition 6.2 one only needs to take into account the T_l with $l \leq B$, where B is as in Proposition 4.2. The proof that these T_l define the same eigenspaces as all the T_l with $l \neq p$ is given by Proposition 4.2.

References

[1] A. Agashe and W.A. Stein. *The generalized Manin constant, congruence primes, and the modular degree.* In preparation.

[2] A. Agashe and W.A. Stein. Appendix to "*Some computations with Hecke rings and deformation rings*" by J-C. Lario and R. Schoof. To appear in Experimental Mathematics.

[3] S. Bosch, W. Lütkebohmert and M. Raynaud. *Néron models.* Springer Verlag, Ergebnisse 3, 21 (1990).

[4] C. Breuil. *Cohomologie étale de p-torsion et cohomologie cristalline en réduction semi-stable.* Duke Mathematical Journal 95, No. 3, (1998).

[5] C. Breuil and W. Messing. *Torsion étale and crystalline cohomologies.* To appear in the "proceedings of the p-adic semester at the IHP, Paris", Astérisque, 2002.

[6] K. Buzzard and W.A. Stein. *A mod five approach to modularity of icoshedral Galois representations.* To appear in Pac. J. Math.

[7] 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).

[8] R.F. Coleman and J.F. Voloch. *Companion forms and Kodaira-Spencer theory.* Invent. math. **110** (1992), 263–281.

[9] J.E. Cremona. *Algorithms for modular elliptic curves.* Second edition, Cambridge University Press, Cambridge, 1997.

[10] P. Deligne. *Formes modulaires et représentations l-adiques.* Séminaire Bourbaki exp. 355. Lecture Notes in Mathematics **179**, Springer, Heidelberg, 1969.

[11] M. DICKINSON – *On the modularity of certain 2-adic Galois representations.* Duke Mathematical Journal, Vol 109, No. 2, 2001, 319–383.

[12] F. Diamond – *The Taylor–Wiles construction and multiplicity one.* Invent. math. **128** (1997), 379–391.

[13] F. Diamond and J. Im. *Modular forms and modular curves.* CMS Conf. Proc. Vol. 17, AMS Publ., Providence, "Seminar on Fermat's Last Theorem", edited by V.K. Murty.

[14] S.J. Edixhoven. *Stable models of modular curves and applications.* Thesis, University of Utrecht (1989). Available on the author's home page.

[15] S.J. Edixhoven. *On the Manin constants of modular elliptic curves.* Arithmetic algebraic geometry (Texel, 1989), Birkhäuser Boston 1991, 25–39. Available on the author's home page.

[16] S.J. Edixhoven. *Minimal resolution and stable reduction of* $X_0(N)$. Annales de l'Institut Fourier, Grenoble, **40**, 1, 31–67 (1990).

[17] S.J. Edixhoven. *The weight in Serre's conjectures on modular forms.* Invent. Math. **109** (1992), 563–594.

[18] S.J. Edixhoven. *Serre's conjecture.* In: Modular Forms and Fermat's Last Theorem (Gary Cornell, Joseph Silverman and Glenn Stevens, editors). Springer-Verlag, 1997. Pages 209–242.

[19] G. Faltings. *Crystalline cohomology and* p*-adic Galois representations.* In "Algebraic analysis, geometry and number theory", Proceedings of the JAMI inaugural conference (J. Igusa, ed.), John Hopkins Univ. Press, 1989.

[20] G. Faltings and B.W. Jordan. *Crystalline cohomology and* $\mathrm{GL}(2, \mathbb{Q})$. Israel Journal of Mathematics **90** (1995), 1–66.

[21] J-M. Fontaine and G. Laffaille. *Construction de représentations* p*-adiques.* Ann. scient. Éc. Norm. Sup. 4ème série, t. 15, 1982, 547–608.

[22] J-M. Fontaine and W. Messing. p*-adic periods and* p*-adic étale cohomology.* In "Current trends in arithmetical algebraic geometry (Arcata, Calif. 1985)", Contemp. Math 67, Amer. Math. Soc., Providence, 1987, 179–207.

[23] B.H. Gross. *A tameness criterion for Galois representations associated to modular forms (mod* p*).* Duke Mathematical Journal 61, No. 2, (1990).

[24] A. Herremans. *A combinatorial interpretation of Serre's conjecture on modular Galois representations.* Thesis, Leuven, 2001.

[25] K. Kato. *On* p*-adic vanishing cycles (application of ideas of Fontaine-Messing).* In "Algebraic Geometry, Sendai, 1985" , Adv. Stud. Pure Math. 10, North Holland, Amsterdam, 1987, 207–251.

[26] N. Katz. *p-adic properties of modular schemes and modular forms.* In Modular Functions of One Variable III. Springer Lecture Notes in Mathematics 350 (1973).

[27] N. Katz. *A result on modular forms in characteristic p.* Springer Lecture Notes in Mathematics 601, 53–61 (1976).

[28] N. Katz and B. Mazur. *Arithmetic moduli of elliptic curves.* Annals of Mathematics studies, study 108. Princeton University Press, 1985.

[29] L.J.P. Kilford. *Some non-Gorenstein Hecke algebras attached to space of modular forms.* Preprint, version of March 2002, available on `http://arXiv.org`. To appear in the Journal of Number Theory.

[30] I. Kiming. *On the experimental verification of the Artin conjecture for 2-dimensional odd Galois representations over $\mathbb{Q}$.* In "On Artin's conjecture for odd 2-dimensional representations", 1–36. Lecture Notes in Mathematics 1585, Springer, 1994.

[31] B. Mazur and K.A. Ribet. *Two-dimensional representations in the arithmetic of modular curves.* Astérisque 196–197, 215–255 (1991).

[32] K. McMurdy. *A splitting criterion for Galois representations associated to exceptional modular forms.* Preprint March 2002, available on `http://arXiv.org`.

[33] L. Merel. *Universal Fourier expansions of modular forms.* In "On Artin's conjecture for odd 2-dimensional representations", 59–94. Lecture Notes in Mathematics 1585, Springer, 1994.

[34] T. Oda. *The first De Rham cohomology group and Dieudonné modules.* Ann. Sc. Ecole Norm. Sup. (4) 2, 63–135 (1969).

[35] K.A. Ribet and W.A. Stein. *Lectures on Serre's conjectures.* In *Arithmetic Algebraic Geometry*, edited by Brian Conrad and Karl Rubin, AMS, 2001. Available on Stein's home page.

[36] A.J. Scholl. *Motives for modular forms.* Invent. math. **100** (1990), 419–430.

[37] J.-P. Serre. *Sur les représentations de degré 2 de $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.* Duke Mathematical Journal 54, No. 1, (1987), 179–230.

[38] J. Sturm. *On the congruence of modular forms.* Number Theory (New York, 1984–1985), 275–280, Lecture Notes in Mathematics 1240, Springer, 1987.