

P-ADIC PROPERTIES OF MODULAR SCHEMES AND MODULAR FORMS

Nicholas M. Katz

International Summer School on Modular Functions  
ANTWERP 1972

## TABLE OF CONTENTS

Introduction	73
 Chapter 1: Moduli schemes and the q-expansion principle	 77
1.1 Modular forms of level 1	
1.2 Modular forms of level n	
1.3 Modular forms on $\Gamma_0(p)$	
1.4 The modular schemes $M_n$ and $\overline{M}_n$	
1.5 The invertible sheaf $\omega$ on $\overline{M}_n$ , and modular forms holomorphic at $\infty$	
1.6 The q-expansion principle	
1.7 Base-change for modular forms of level $n \geq 3$	
1.8 Base-change for modular forms of level 1 and 2	
1.9 Modular forms of level 1 and 2: q-expansion principle	
1.10 Modular schemes of level 1 and 2	
1.11 Hecke operators	
1.12 Applications to polynomial q-expansions; the strong q-expansion principle	
1.13 review of the modular scheme associated to $\Gamma_0(p)$	
 Chapter 2: p-adic modular forms	 97
2.0 The Hasse invariant as a modular form; its q-expansion	
2.1 Deligne's congruence $A \equiv E_{p-1} \pmod{p}$	
2.2 p-adic modular forms with growth conditions	
2.3 Determination of $M(R_0, r, n, k)$ when $p$ is nilpotent in $R_0$	
2.4 Determination of $S(R_0, r, n, k)$ when $p$ is nilpotent in $R_0$	
2.5 Determination of $S(R_0, r, n, k)$ in the limit	
2.6 Determination of a "basis" of $S(R_0, r, n, k)$ in the limit	
2.7 Banach norm and q-expansion for $r = 1$	
2.8 Bases for level 1 and 2	
2.9 Interpretation via formal schemes	
 Chapter 3: Existence of the canonical subgroup: applications	 112
3.1 The existence theorem : statement	
3.2 First principal corollary	
3.3 Second principal corollary	
3.4 Construction of the canonical subgroup in the case $r = 1$	
3.5 Hint for general $r$	
3.6 Lemmas on the formal group	

3.7	Construction of the canonical subgroup as a subscheme of the formal group	
3.8	The canonical subscheme is a subgroup	
3.9	Conclusion of the proof of 3.1	
3.10	Finiteness properties of the Frobenius endomorphism of p-adic modular functions	
3.11	Applications to the congruences of Atkin - the U operator	
3.12	p-adic Hecke operators	
3.13	Interpretation of Atkin's congruences on j	
<b>Chapter 4:</b>	<b>p-adic representations and congruences for modular forms</b>	<b>142</b>
4.1	p-adic representations and locally free sheaves	
4.2	Applications to modular schemes	
4.3	Igusa's theorem	
4.4	Applications to congruences between modular forms à la Serre	
4.5	Applications to Serre's "modular forms of weight X"	
<b>Appendix 1:</b>	<b>Motivations</b>	<b>158</b>
A1.1	Lattices and elliptic curves à la Weierstrass; the Tate curve	
A1.2	Modular forms and De Rham cohomology	
A1.3	The Gauss-Manin connection, and the function P: computations	
A1.4	The Gauss-Manin connection and Serre's $\partial$ operator	
A1.5	Numerical Formulae	
<b>Appendix 2:</b>	<b>Frobenius</b>	<b>175</b>
A2.1	Relation of the De Rham and p-adic modular Frobenii	
A2.2	Calculation at $\infty$	
A2.3	The "canonical direction" in $H_{\text{DR}}^1$	
A2.4	P as a p-adic modular function of weight two	
<b>Appendix 3:</b>	<b>Hecke Polynomials, coherent cohomology, and U</b>	<b>181</b>
A3.1	The Fredholm determinant of U	
A3.2	Relation to mod p étale cohomology and to coherent cohomology	
A3.3	Relation to the Cartier operator	

## List of Notations

1.0	$\omega_E/S$
1.1	Tate( $\mathbf{q}$ ), $\omega_{\text{can}}$ , $S(R_0, l, k)$
1.2	$n^E, \alpha_n$ ; $S(R_0, n, k)$
1.3	$r_0(\rho)$
1.4	$M_n, \bar{M}_n$
1.9	$S(K, n, k)$
1.11	$T_\ell$
2.0	$A$
2.1	$E_{p-1}, E_k$
2.2	$M(R_0, r, n, k)$ , $S(R_0, r, n, k)$
2.6	$B(n, k, j)$ , $B(R_0, n, k, j)$ , $B^{\text{rigid}}(R_0, r, n, k)$
2.8	$P, P_1$ (projectors)
2.9	$M_n(R_0, r)$ , $\bar{M}_n(R_0, r)$
3.1	$H, Y$
3.3	$\Phi$
3.4	$F, V$
3.11	$\text{tr } \Phi, U$
4.1	$w_n(k)$ , $\varphi$ , $S_n$
4.2	$S_m^\zeta$ , $\bar{S}_m^\zeta$
4.4	$G_x^*$ , Ramanujan's series $P$
A1.1	
A1.2	$H_{DR}^1$ ; $\omega, \eta$
A1.3	$\nabla$ , Weierstrass's $\zeta$
A1.4	$\theta, \partial$
A2.1	$F(\Phi)$
A2.2	$\omega_{\text{can}}, \eta_{\text{can}}$

(In 1)

Introduction

This exposé represents an attempt to understand some of the recent work of Atkin, Swinnerton-Dyer, and Serre on the congruence properties of the  $q$ -expansion coefficients of modular forms from the point of view of the theory of moduli of elliptic curves, as developed abstractly by Igusa and recently reconsidered by Deligne. In this optic, a modular form of weight  $k$  and level  $n$  becomes a section of a certain line bundle  $\underline{\omega}^{\otimes k}$  on the modular variety  $M_n$  which "classifies" elliptic curves with level  $n$  structure (the level  $n$  structure is introduced for purely technical reasons). The modular variety  $M_n$  is a smooth curve over  $\mathbb{Z}[1/n]$ , whose "physical appearance" is the same whether we view it over  $\mathbb{C}$  (where it becomes  $\varphi(n)$  copies of the quotient of the upper half plane by the principal congruence subgroup  $\Gamma(n)$  of  $SL(2, \mathbb{Z})$ ) or over the algebraic closure of  $\mathbb{Z}/p\mathbb{Z}$ , (by "reduction modulo  $p$ ") for primes  $p$  not dividing  $n$ . This very fact rules out the possibility of obtaining  $p$ -adic properties of modular forms simply by studying the geometry of  $M_n \otimes \mathbb{Z}/p\mathbb{Z}$  and its line bundles  $\underline{\omega}^{\otimes k}$ ; we can only obtain the reductions modulo  $p$  of identical relations which hold over  $\mathbb{C}$ .

The key is instead to isolate the finite set of points of  $M_n \otimes \mathbb{Z}/p\mathbb{Z}$  corresponding to supersingular elliptic curves in characteristic  $p$ , those whose Hasse invariant vanishes. One then considers various "rigid-analytic" open subsets of  $M_n \otimes \mathbb{Z}_p$  defined by removing  $p$ -adic discs of various radii around the supersingular points in characteristic  $p$ . This makes sense because the Hasse invariant is the reduction modulo  $p$  of a true modular form (namely  $E_{p-1}$ ) over  $\mathbb{Z}_p$ , so we can define a rigid analytic open subset of  $M_n \otimes \mathbb{Z}_p$  by taking only those  $p$ -adic elliptic curves on which  $E_{p-1}$  has  $p$ -adic absolute value greater than some  $\epsilon > 0$ . We may then define various sorts of truly  $p$ -adic modular forms as functions of elliptic curves on which  $|E_{p-1}| > \epsilon$ , or equivalently as sections of the line bundles  $\underline{\omega}^{\otimes k}$  restricted to the above-constructed

(In 2)

rigid analytic open sets of  $M_n \otimes \mathbb{Z}_p$ . [The role of the choice of  $\varepsilon$  is to specify the rate of growth of the coefficients of the Laurent series development around the "missing" supersingular points].

The most important tool in the study of these  $p$ -adic modular forms is the endomorphism they undergo by a "canonical lifting of the Frobenius endomorphism" from characteristic  $p$ . This endomorphism comes about as follows. Any elliptic curve on which  $|E_{p-1}| > \varepsilon$  for suitable  $\varepsilon$  carries a "canonical subgroup" of order  $p$ , whose reduction modulo  $p$  is the Kernel of Frobenius. The "canonical lifting" above is the endomorphism obtained by dividing the universal elliptic curve by its canonical subgroup (over the rigid open set of  $M_n \otimes \mathbb{Z}_p$  where it exists).

This endomorphism is related closely to Atkin's work. His operator  $U$  is simply ( $\frac{1}{p}$  times) the trace of the canonical lifting of Frobenius, and certain of his results on the  $q$ -expansion of the function  $j$  may be interpreted as statements about the spectral theory of the operator  $U$ .

The relation to the work of Swinnerton-Dyer and Serre is more subtle, and depends on the fact that the data of the action of the "canonical lifting of Frobenius" on  $\omega^{-1}$  over the rigid open set  $|E_{p-1}| \geq 1$  is equivalent to the knowledge of the representation of the fundamental group of the open set of  $M_n \otimes \mathbb{Z}/p\mathbb{Z}$  where the Hasse invariant is invertible on the  $p$ -adic Tate module  $T_p$  (which for a non-supersingular curve in characteristic  $p$  is a free  $\mathbb{Z}_p$ -module of rank one). Thanks to Igusa, we know that this representation is as non-trivial as possible, and this fact, interpreted in terms of the action of the canonical Frobenius on the  $\omega^{\otimes k}$ , leads to certain of the congruences of Swinnerton-Dyer and Serre.

In the first chapter, we review without proof certain aspects of the moduli of elliptic curves, and deduce various forms of the "q-expansion principle." This chapter owes much (probably its very existence) to discussions with Deligne. It is not " $p$ -adic", and may be read more or less independently

(In 3)

of the rest of the paper.

The second chapter develops at length various "p-adic" notions of modular form, in the spirit described above. A large part of it ( $r \neq 1$ ) was included with an eye to Dwork-style applications to Atkin's work, and may be omitted by the reader interested only in Swinnerton-Dyer and Serre style congruences. The idea of working at such "p-adic modular forms" is due entirely to Serre, who in his 1972 College de France course stressed their importance.

The third chapter develops the theory of the "canonical subgroup." This theory is due entirely to Lubin, who has unfortunately not published it except for a tiny hint [33]. The second half of the chapter interprets certain congruences of Atkin in terms of p-adic Banach spaces, the spectrum of the operator U, etc. The possibility of this interpretation is due to Dwork, through his realization that not only is  $pU$  integral, but U itself is "essentially" integral (cf[14]).

The fourth chapter explains the relation between the canonical Frobenius and certain congruences of Swinnerton-Dyer and Serre. It begins by recalling a "coherent sheaf" description of p-adic representations of the fundamental group of certain schemes on which  $p$  is nilpotent. This description is certainly well-known, and basically due to Hasse and Witt, but does not seem to be recorded elsewhere in the form we require. Using it, we show that the representation corresponding to  $\omega$  with its canonical Frobenius is that afforded by the (rank-one) p-adic Tate module  $T_p$  of non-supersingular elliptic curves. We then prove the extreme non-triviality of this representation in "canonical subgroup" style. This non-triviality is due to Igusa, whose proof is finally not so different from the one given. We then apply this result of non-triviality to deduce certain of the congruences of Swinnerton-Dyer and Serre.

In the first appendix, which is a sort of "chapter zero", we explain the relation between the classical approach to elliptic curves via their period

Ka-8

(In 4)

lattices and the "modern" one, the relation of DeRham cohomology of elliptic curves to modular forms, and the relation between the Gauss-Manin connection, Ramanujan's function  $P(q)$ , and Serre's  $\partial$ -operator on modular forms. The results are due to Weierstrass and Deligne. It is concluded by a "table" of formulas.

The second appendix explains the relation between the canonical Frobenius on  $p$ -adic modular forms and the Frobenius endomorphism of the DeRham cohomology of elliptic curves. It may also be read as an appendix to [25].

The third appendix relates Hecke polynomials mod  $p$  to L-series, coherent cohomology and the Fredholm determinant of  $U$ .

As should by now be obvious, this exposé owes its very existence to Lubin, Serre, Deligne, Atkin, and Dwork. It is a pleasure to acknowledge my debt to them, and to thank M. Rapoport for many helpful discussions.

Chapter 1: Moduli schemes and the q-expansion principle

In this chapter, we will recall some of the definitions and main results of the theory of moduli of elliptic curves, and deduce from them various forms of the "q-expansion principle" for modular forms.

1.0. By an elliptic curve over a scheme  $S$ , we mean a proper smooth morphism  $p: E \rightarrow S$ , whose geometric fibres are connected curves of genus one, together with a section  $e: S \rightarrow E$ .

$$\begin{array}{ccc} E & & \\ p \downarrow & \swarrow & \\ S & & \end{array} \quad e$$

We denote by  $\omega_{E/S}$  the invertible sheaf  $p_*(\Omega^1_{E/S})$  on  $S$ , which is canonically dual (Serre duality) to the invertible sheaf  $R^1 p_*(\mathcal{O}_E)$  on  $S$ .

1.1 Modular forms of level 1

A modular form of weight  $k \in \mathbb{Z}$  and level one is a rule  $f$  which assigns to any elliptic curve  $E$  over any scheme  $S$  a section  $f(E/S)$  of  $(\omega_{E/S})^{\otimes k}$  over  $S$  such that the following two conditions are satisfied.

1.  $f(E/S)$  depends only on the  $S$ -isomorphism class of the elliptic curve  $E/S$ .
2. The formation of  $f(E/S)$  commutes with arbitrary change of base  $g: S' \rightarrow S$  (meaning that  $f(E_{S'},/S') = g^* f(E/S)$ ).

We denote by  $M(\mathbb{Z}; 1, k)$  the  $\mathbb{Z}$ -module of such forms.

Equivalently, a modular form of weight  $k$  and level 1 is a rule  $f$  which assigns to every pair  $(E/R, \omega)$  consisting of an elliptic curve over (the spectrum of) a ring  $R$  together with a basis  $\omega$  of  $\omega_{E/R}$  (i.e., a nowhere vanishing section of  $\Omega^1_{E/R}$  on  $E$ ), an element  $f(E/R, \omega) \in R$ , such that the following three conditions are satisfied.

1.  $f(E/R, \omega)$  depends only on the  $R$ -isomorphism class of the pair  $(E/R, \omega)$ .
2.  $f$  is homogeneous of degree  $-k$  in the "second variable"; for any  $\lambda \in R^\times$  (the multiplicative group of  $R$ ),  

$$f(E, \lambda\omega) = \lambda^{-k} f(E, \omega).$$
3. The formation of  $f(E/R, \omega)$  commutes with arbitrary extension of scalars  $g: R \rightarrow R'$  (meaning  $f(E_{R'}, /R', \omega_{R'}) = g(f(E/R, \omega))$ ).

(The correspondence between the two notions is given by the formula

$$f(E/\text{Spec}(R)) = f(E/R, \omega) \cdot \omega^{\otimes k}$$

valid whenever  $S = \text{Spec}(R)$  and  $\omega_{E/S}$  is a free  $R$ -module, with basis  $\omega$ .)

If, in the preceding definitions we consider only schemes  $S$  (or rings  $R$ ) lying over a fixed ground-ring  $R_0$ , and only changes of base by  $R_0$ -morphisms, we obtain the notion of a modular form of weight  $k$  and level one defined over  $R_0$ , the  $R_0$ -module of which is noted  $M(R_0, l, k)$ .

A modular form  $f$  of weight  $k$  and level one defined over  $R_0$  can be evaluated on the pair  $(\text{Tate}(q), \omega_{\text{can}})_{R_0}$  consisting of the Tate curve and its canonical differential, viewed as elliptic curve with differential over  $\mathbb{Z}((q)) \otimes_{\mathbb{Z}} R_0$  (and not just over  $R_0((q))$ ).

The  $q$ -expansion of a modular form  $f$  is by definition the finite-tailed Laurent series

$$f((\text{Tate}(q), \omega_{\text{can}})_{R_0}) \in \mathbb{Z}((q)) \otimes_{\mathbb{Z}} R_0.$$

The modular form  $f$  is called holomorphic at  $\infty$  if its  $q$ -expansion lies in the subring  $\mathbb{Z}[[q]] \otimes_{\mathbb{Z}} R_0$ ; the module of all such is noted  $S(R_0; l, k)$ . Notice that the  $q$ -expansion lies in  $\mathbb{Z}((q)) \otimes_{\mathbb{Z}} R_0 \subset R_0((q))$ , i.e., it is finite  $R_0$ -linear combination of elements of  $\mathbb{Z}((q))$ . This implies, for example, that if  $R_0$  is the field of fractions of a discrete valuation ring, then the  $q$ -expansion coefficients of any modular form of weight  $k$  and level one over  $R_0$

have bounded denominators.

### 1.2. Modular forms of level n

For each integer  $n \geq 1$ , we denote by  $n^E$  the kernel of "multiplication by  $n$ " on  $E/S$ ; it is a finite flat commutative group-scheme of rank  $n^2$  over  $S$ , which is étale over  $S$  if and only if the integer  $n$  is invertible in  $\Gamma(S, \mathcal{O}_S)$  i.e., if and only if  $S$  is a scheme over  $\mathbb{Z}[\frac{1}{n}]$ . A level  $n$  structure on  $E/S$  is an isomorphism

$$\alpha_n: n^E \xrightarrow{\sim} (\mathbb{Z}/n\mathbb{Z})_S^2.$$

It cannot exist unless  $n$  is invertible on  $S$ , and in that case there always exists one on some finite étale covering  $S'$  of  $S$ . If a level  $n$  structure on  $E/S$  exists, and if  $S$  is connected, the set of all such is principal homogeneous under  $GL(2, \mathbb{Z}/n\mathbb{Z}) = \text{Aut}((\mathbb{Z}/n\mathbb{Z})_S^2)$ .

A modular form of weight  $k$  and level  $n$  is rule which assigns to each pair  $(E/S, \alpha_n)$  consisting of an elliptic curve together with a level  $n$  structure a section  $f(E/S, \alpha_n)$  of  $(\omega_{E/S})^{\otimes k}$  over  $S$ , in a way which depends only on the isomorphism class of  $(E/S, \alpha_n)$ , and which commutes with arbitrary base-change  $g: S' \rightarrow S$ . Equivalently, it is a rule which assigns to all triples  $(E/R, \omega, \alpha_n)$ , consisting of an elliptic curve over a ring  $R$  together with a base  $\omega$  of  $\omega_{E/R}$  and a level  $n$  structure  $\alpha_n$ , an element  $f(E/R, \omega, \alpha_n) \in R$  which depends only on the isomorphism class of  $(E/R, \omega, \alpha_n)$ , which commutes with arbitrary change of base, and which is homogeneous of degree  $-k$  in the "second variable", meaning that for any  $\lambda \in R^\times$ , we have  $f(E/R, \lambda\omega, \alpha_n) = \lambda^{-k} f(E/R, \omega, \alpha_n)$ . Exactly as for level one, we define the notion of a modular form of weight  $k$  and level  $n$  defined over a ring  $R_0$ . The  $R_0$ -module of all such is noted  $M(R_0, n, k)$ .

A modular form of weight  $k$  and level  $n$  defined over a ring  $R_0$  which contains  $1/n$  and a primitive  $n$ 'th root of unity  $\zeta_n$  may be evaluated on the triples  $(\text{Tate}(q^n), \omega_{\text{can}}, \alpha_n)_{R_0}$  consisting of the Tate curve  $\text{Tate}(q^n)$

with its canonical differential, viewed as defined over  $\mathbb{Z}((q)) \otimes_{\mathbb{Z}} R_0$ , together with any of its level n structures (all points of  $E_n$  are rational over  $\mathbb{Z}((q)) \otimes_{\mathbb{Z}} R_0$ ; in fact, being the canonical images of the points  $\zeta_n^{iq^j}$ ,  $0 \leq i, j \leq n-1$  from " $G_m$ ", they all have coordinates in  $\mathbb{Z}[[q]] \otimes_{\mathbb{Z}} \mathbb{Z}[\frac{1}{n}, \zeta_n]$ , and the non-constant q-coefficients of their  $(x, y)$  coordinates even lie in  $\mathbb{Z}[\zeta_n]$  (cf. [38]), as one sees using the explicit formulas of Jacobi-Tate.

The q-expansions of the modular form  $f$  are the finitely many finite-tailed Laurent series

$$1.2.1 \quad f((Tate(q^n), \omega_{can}, \alpha_n)_{R_0}) \in \mathbb{Z}((q)) \otimes_{\mathbb{Z}} R_0$$

obtained by varying  $\alpha_n$  over all the level n structures.

(NB Though it makes sense to speak of a modular form of weight k and level n defined over any ring  $R_0$ , we can speak of its q-expansions over  $R_0$  only when  $R_0$  contains  $1/n$  and a primitive n'th root  $\zeta_n$  of 1.)

A modular form defined over any ring  $R_0$  is said to be holomorphic at  $\infty$  if its inverse image on  $R_0[1/n, \zeta_n]$  has all its q-expansions in  $\mathbb{Z}[[q]] \otimes_{\mathbb{Z}} R_0[1/n, \zeta_n]$ . (If the ring  $R_0$  itself contains  $1/n$  and  $\zeta_n$ , this is equivalent to asking that all the q-expansions lie in  $\mathbb{Z}[[q]] \otimes_{\mathbb{Z}} R_0$ .) The module of such is denoted  $S(R_0; n, k)$ .

A modular form (resp: holo. at  $\infty$ ) of weight k and level n defined over a ring  $R_0$ , which does not depend on the "last variable"  $\alpha_n$  is a modular a modular form (resp: holo. at  $\infty$ ) of weight k and level one defined over  $R_0[1/n]$ .

### 1.3. Modular forms on $\Gamma_0(p)$

Analogously, for an integer  $n \geq 1$  and a prime number  $p \nmid n$ , a modular form of weight k and level n on  $\Gamma_0(p)$  is a rule  $f$  which assigns to each triple  $(E/S, \alpha_n, H)$  consisting of an elliptic curve, a level n structure, and a finite flat subgroup-scheme  $H \subset E$  of rank p, a section  $f(E/S, \alpha_n, H)$  of  $(\omega_{E/S})^{\otimes k}$  over S, which depends only on the isomorphism class of  $(E/S, \alpha_n, H)$ , and

whose formation commutes with arbitrary change of base  $S' \rightarrow S$ . Equivalently, it is a rule which assigns to each quadruple  $(E/R, \omega, \alpha_n, H)$  an element  $f(E/R, \omega, \alpha_n, H) \in R$ , which depends only on the isomorphism class of the quadruple, whose formation commutes with arbitrary change of base, and which is homogeneous of degree  $-k$  in the second variable. As before, we define the notion of a modular form of weight  $k$  and level  $n$  on  $\Gamma_0(p)$  being defined over a ring  $R_0$ .

A modular form of weight  $k$  and level  $n$  on  $\Gamma_0(p)$ , defined over a ring  $R_0$  which contains  $1/n$  and  $\zeta_n$  may be evaluated on each of the quadruples  $(\text{Tate}(q^n), \omega_{\text{can}}, \alpha_n, \mu_p)_{R_0}$ . We will call the values of  $f$  on these quadruples the  $q$ -expansions of  $f$  at the unramified cusps, and say that  $f$  is holomorphic at the unramified cusps if its  $q$ -expansions there all lie in  $\mathbb{Z}[[q]] \otimes_{\mathbb{Z}} R_0$ . We can also evaluate  $f$  on each of quadruples  $(\text{Tate}(q^{np}), \omega_{\text{can}}, \alpha_n, \{q^n\})$ , where  $\{q^n\}$  denotes the flat rank- $p$  subgroup scheme generated by (the image of)  $q^n$ . Its values there are called its  $q$ -expansions at the ramified cusps. We say that  $f$  is holomorphic at  $\infty$  if all of its  $q$ -expansions, at the ramified and unramified cusps, actually lie in  $\mathbb{Z}[[q]] \otimes_{\mathbb{Z}} R_0$ .

Remark. The distinction between ramified and unramified cusps on  $\Gamma_0(p)$  is quite a natural one - in the work of Atkin, one deals with modular functions (weight 0) of level one on  $\Gamma_0(p)$  which are holomorphic at the unramified cusp, but not at the ramified one.

#### 1.4. The modular schemes $M_n$ and $\bar{M}_n$

For each integer  $n \geq 3$ , the functor "isomorphism classes of elliptic curves with level  $n$  structure" is representable, by a scheme  $M_n$  which is an affine smooth curve over  $\mathbb{Z}[\frac{1}{n}]$ , finite and flat of degree =  $\#(\text{GL}_2(\mathbb{Z}/n\mathbb{Z})/\pm 1)$  over the affine  $j$ -line  $\mathbb{Z}[\frac{1}{n}, j]$ , and étale over the open set of the affine  $j$ -line where  $j$  and  $j-1728$  are invertible. The normalization of the projective

j-line  $\mathbb{P}_{\mathbb{Z}[1/n]}^1$  in  $M_n$  is a proper and smooth curve  $\bar{M}_n$  over  $\mathbb{Z}[1/n]$ , the global sections of whose structural sheaf are  $\mathbb{Z}[1/n, \zeta_n]$ . The curve  $M_n \otimes_{\mathbb{Z}[1/n]} \mathbb{Z}[1/n, \zeta_n]$  (resp.  $\bar{M}_n \otimes_{\mathbb{Z}[1/n]} \mathbb{Z}[1/n, \zeta_n]$ ) is a disjoint union of  $\phi(n)$  affine (resp. proper) smooth geometrically connected curves over  $\mathbb{Z}[1/n, \zeta_n]$ , the partitioning into components given by the  $\phi(n)$  primitive  $n$ 'th roots of one occurring as values of the e.m. pairing on the basis of  $E$  specified by the level  $n$  structure. The scheme  $\bar{M}_n - M_n$  over  $\mathbb{Z}[1/n]$  is finite and étale, and over  $\mathbb{Z}[1/n, \zeta_n]$ , it is a disjoint union of sections, called the cusps of  $\bar{M}_n$ , which in a natural way are the set of isomorphism classes of level  $n$  structures on the Tate curve  $\text{Tate}(q^n)$  viewed over  $\mathbb{Z}((q)) \otimes_{\mathbb{Z}} \mathbb{Z}[1/n, \zeta_n]$ . The completion of  $\bar{M}_n \otimes_{\mathbb{Z}} \mathbb{Z}[1/n, \zeta_n]$  along any of the cusps is isomorphic to  $\mathbb{Z}[1/n, \zeta_n][[q]]$ . The completion of the projective j-line  $\mathbb{P}_{\mathbb{Z}[1/n, \zeta_n]}^1$  along  $\infty$  is itself isomorphic to  $\mathbb{Z}[1/n, \zeta_n][[q]]$ , via the formula  $j(\text{Tate}(q)) = 1/q + 744 + \dots$ , and the endomorphism of  $\mathbb{Z}[1/n, \zeta_n][[q]]$  arising from the projection  $\bar{M}_n \longrightarrow \mathbb{P}^1$  is just given by  $q \mapsto q^n$ . In fact, for each cusp, the inverse image of the universal elliptic curve with level  $n$  structure  $(E/M_n, \alpha_n)$  over (the spectrum of)  $\mathbb{Z}[1/n, \zeta_n]((q))$  (viewed as a punctured disc around the cusp) is isomorphic to the inverse image over  $\mathbb{Z}[1/n, \zeta_n]((q))$  of the Tate curve  $\text{Tate}(q^n)$  with the level  $n$  structure corresponding to that cusp.

### 1.5. The invertible sheaf $\underline{\omega}$ on $\bar{M}_n$ , and modular forms holomorphic at $\infty$

There is a unique invertible sheaf  $\underline{\omega}$  on  $\bar{M}_n$  whose restriction to  $M_n$  is  $\underline{\omega}_{E/M_n} ((E/M_n, \alpha_n))$  (the universal elliptic curve with level  $n$  structure), and whose sections over the completion  $\mathbb{Z}[1/n, \zeta_n][[q]]$  at each cusp are precisely the  $\mathbb{Z}[1/n, \zeta_n][[q]]$  multiples of the canonical differential of the Tate curve. The Kodaira-Spencer style isomorphism (cf. A1.3.17 and [7])

$$\left( \underline{\omega}_{E/M_n} \right)^{\otimes 2} \simeq \Omega_{M_n/\mathbb{Z}[1/n]}^1$$

extends to an isomorphism

$$(\underline{\omega})^{\otimes 2} \simeq \Omega_{\overline{M}_n/\mathbb{Z}[1/n]}^1 (\log(\overline{M}_n - M_n)) ,$$

and, in fact, over  $\mathbb{Z}[1/n, \zeta_n][[q]]$ , the "square" of the canonical differential  $\omega_{\text{can}}$  on  $\text{Tate}(q^n)$  corresponds to  $n \cdot \frac{dq}{q}$ .

It follows that a modular form of level  $n$  and weight  $k$  holomorphic at  $\infty$  defined over any ring  $R_0 \ni 1/n$  is just a section of  $(\underline{\omega})^{\otimes k}$  on  $\overline{M}_n \otimes_{\mathbb{Z}[1/n]} R_0$ , or equivalently a section of the quasi-coherent sheaf  $(\underline{\omega})^{\otimes k} \otimes_{\mathbb{Z}[1/n]} R_0$  on  $\overline{M}_n$ .

### 1.6. The q-expansion principle

For any  $\mathbb{Z}[1/n]$ -module  $K$ , we define a modular form of level  $n$  and weight  $k$ , holomorphic at  $\infty$ , with coefficients in  $K$ , to be an element of  $H^0(\overline{M}_n, (\underline{\omega})^{\otimes k} \otimes_{\mathbb{Z}[1/n]} K)$ . At each cusp, such a modular form has a q-expansion in  $K \otimes_{\mathbb{Z}[1/n]} \mathbb{Z}[1/n, \zeta_n] \otimes_{\mathbb{Z}} \mathbb{Z}[[q]]$ .

Theorem 1.6.1. Let  $n \geq 3$ ,  $K$  a  $\mathbb{Z}[1/n]$ -module, and  $f$  a modular form of level  $n$  and weight  $k$ , holomorphic at  $\infty$ , with coefficients in  $K$ . Suppose that on each of the  $\varphi(n)$  connected components of  $\overline{M}_n \otimes_{\mathbb{Z}[1/n]} \mathbb{Z}[1/n, \zeta_n]$ , there is at least one cusp at which the q-expansion of  $f$  vanishes identically. Then  $f = 0$ .

Before proving it, we give the main corollary.

Corollary 1.6.2. (The q-expansion principle). Let  $n \geq 3$ ,  $K$  a  $\mathbb{Z}[1/n]$ -module,  $L \subset K$  a  $\mathbb{Z}[1/n]$ -submodule. Let  $f$  be a modular form of weight  $k$ , level  $n$ , holomorphic at  $\infty$ , with coefficients in  $K$ . Suppose that on each of the  $\varphi(n)$  connected components of  $\overline{M}_n \otimes_{\mathbb{Z}[1/n]} \mathbb{Z}[1/n, \zeta_n]$ , there is at least one cusp at which all the q-coefficients of  $f$  lie in  $L \otimes_{\mathbb{Z}[1/n]} \mathbb{Z}[1/n, \zeta_n]$ . Then  $f$  is a modular form with coefficients in  $L$ .

Proof of corollary. The exact sequence  $0 \rightarrow L \rightarrow K \rightarrow K/L \rightarrow 0$  of  $\mathbb{Z}[1/n]$ -modules gives an exact sequence of sheaves on  $\bar{M}_n$ ,

$$1.6.2.1 \quad 0 \rightarrow L \otimes (\underline{\omega})^{\otimes k} \rightarrow K \otimes (\underline{\omega})^{\otimes k} \rightarrow (K/L) \otimes (\underline{\omega})^{\otimes k} \rightarrow 0,$$

hence a cohomology exact sequence

$$1.6.2.2 \quad 0 \rightarrow H^0(\bar{M}_n, L \otimes \underline{\omega}^{\otimes k}) \rightarrow H^0(\bar{M}_n, K \otimes (\underline{\omega})^{\otimes k}) \rightarrow H^0(\bar{M}_n, (K/L) \otimes (\underline{\omega})^{\otimes k}).$$

The theorem (1.6.1) now applies to the image of  $f$  in  $H^0(\bar{M}_n, (K/L) \otimes \underline{\omega}^{\otimes k})$ , showing that image to be zero, whence  $f \in H^0(\bar{M}_n, L \otimes (\underline{\omega})^{\otimes k})$  by the cohomology exact sequence. QED

We now turn to the proof of the theorem. By considering the ring of dual numbers on  $K$ ,  $D(K) = \mathbb{Z}[1/n] \oplus K$ , [multiplication  $(a, k)(a', k') = (aa', ak' + a'k)$ ] we are reduced to the case where  $K$  is a ring over  $\mathbb{Z}[1/n]$ . Because the formation of the cohomology of quasi-coherent sheaves on quasi-compact schemes commutes with inductive limits, we are first reduced to the case where  $K$  is a finitely generated ring over  $\mathbb{Z}[1/n]$ , then to the case when  $K$  is a noetherian local ring. By faithful flatness of the completion, we further reduce to the case when  $K$  is a complete Noetherian local ring, then by Grothendieck's comparison theorem to the case when  $K$  is an artin local ring. By Krull's intersection theorem,  $f$  induces the zero-section of  $(\underline{\omega})^{\otimes k}$  over an open neighborhood of at least one cusp on each connected component of  $\bar{M}_n \otimes K \otimes \mathbb{Z}[1/n, \zeta_n]$ , hence on an open dense set in  $\bar{M}_n \otimes K$ . If  $f$  is not zero, there exists a non-void closed subset  $Z$  of  $\bar{M}_n \otimes K$ , containing no maximal point of  $\bar{M}_n \otimes K$ , on which  $f$  is supported. Over the local ring in  $\bar{M}_n \otimes K$  of any maximal point  $z$  of  $Z$ ,  $f$  becomes non-canonically a section of  $\mathcal{O}_{z, \bar{M}_n \otimes K}$  which is supported at the closed point, i.e. for any element  $g \in \mathcal{M}_z$  (the maximal ideal of  $\mathcal{O}_{z, \bar{M}_n \otimes K}$ ), there exists a power  $g^n$  of  $g$  such that  $g^n f = 0$ . Thus every element of  $\mathcal{M}_z$  is a zero-divisor, i.e. the point  $z \in \bar{M}_n \otimes K$  has depth zero. As  $\bar{M}_n \otimes K$

is smooth over an artin local ring  $K$ , it is Cohen-Macaulay, and hence only its maximal points have depth zero. Thus  $z$  must be a maximal point of  $\bar{M}_n \otimes K$ , a contradiction. Hence  $f$  must be zero. QED

### 1.7. Base-change of modular forms of level $n \geq 3$

Theorem 1.7.1. Let  $n \geq 3$ , and suppose either that  $k \geq 2$  or that  $k=1$  and  $n \leq 11$ . Then for any  $\mathbb{Z}[1/n]$ -module  $K$ , the canonical map

$$K \otimes H^0(\bar{M}_n, (\underline{\omega})^{\otimes k}) \longrightarrow H^0(\bar{M}_n, K \otimes (\underline{\omega})^{\otimes k})$$

is an isomorphism.

Proof. By standard base-changing theorems, it suffices to show that

$$H^1(\bar{M}_n, (\underline{\omega})^{\otimes k}) = 0. \quad \text{The isomorphism } (\underline{\omega})^{\otimes 2} \xrightarrow{\sim} \Omega_{\bar{M}_n/\mathbb{Z}[1/n]}^1(\log(\bar{M}_n - M_n)),$$

together with the fact that each connected component of  $\bar{M}_n \otimes \mathbb{Z}[1/n, \zeta_n]$  contains at least one cusp, shows that for  $k \geq 2$ , the restriction of  $(\underline{\omega})^{\otimes k}$  to each connected component of  $\bar{M}_n \otimes \mathbb{Z}[1/n, \zeta_n]$  has degree strictly greater than  $2g-2$ ,  $g$  the (common) genus of any of these components, and hence  $H^1(\bar{M}_n, (\underline{\omega})^{\otimes k}) = 0$  by Riemann-Roch. For  $3 \leq n \leq 11$ , explicit calculation shows that  $\underline{\omega}$  restricted to each connected component of  $\bar{M}_n \otimes \mathbb{Z}[1/n, \zeta_n]$  has degree strictly greater than  $2g-2$ , and we conclude as before. QED

Remark. When  $n \geq 12$ ,  $\underline{\omega}$  has degree  $\leq 2g-2$  on each connected component of  $\bar{M}_n \otimes \mathbb{Z}[1/n, \zeta_n]$ , and equality holds only for  $n = 12$ . The author does not know whether or not the formation of modular forms of weight one and level  $n \geq 12$  commutes with base change.

### 1.8. Base change of modular forms of level 1 and 2

Theorem 1.8.1. Let  $R_0$  be any ring in which 2 is invertible. For every integer  $k \geq 1$ , the canonical map  $S(\mathbb{Z}, 2, k) \otimes_{\mathbb{Z}} R_0 \longrightarrow S(R_0, 2, k)$  is an isomorphism.

Proof. First we should remark that there are no non-zero modular forms of level two and odd weight  $k$  over  $R_o$ , because the automorphism " $-1$ " of an elliptic curve transforms  $(E, \omega, \alpha_2)$  into  $(E, -\omega, -\alpha_2)$ , hence

$$f(E, \omega, \alpha_2) = f(E, -\omega, -\alpha_2), \text{ but } \alpha_2 = -\alpha_2, \text{ hence } f(E, -\omega, -\alpha_2) = f(E, \omega, \alpha_2) = (-1)^{-k} f(E, \omega, \alpha_2), \text{ hence } 2f(E, \omega, \alpha_2) = 0 \text{ for } k \text{ odd}.$$

In any case, modular forms of level two and weight  $k$ , holomorphic at infinity, over any ring  $R_o \ni 1/2$ , are precisely those modular forms of level four and weight  $k$  holomorphic at  $\infty$ , defined over  $R_o$ , which are invariant under the action of the subgroup of  $GL_2(\mathbb{Z}/4\mathbb{Z})$  consisting of the matrices  $\equiv I \pmod{2}$ . As this group has order 16, a power of two, we may simply apply the projector  $\frac{1}{16} \sum_{g \equiv 1 \pmod{2}} g$  to the base-changing isomorphism (1.7.1) in

level four to produce the desired isomorphism in level two.

Theorem 1.8.2. Let  $R_o$  be any ring in which 2 and 3 are invertible. For every integer  $k \geq 1$ , the canonical map

$$S(\mathbb{Z}, 1, k) \otimes_{\mathbb{Z}} R_o \longrightarrow S(R_o, 1, k)$$

is an isomorphism.

Proof. The proof is similar to the previous one. We view a modular form of level one over a ring  $R_o \ni 1/6$  as a modular form of level four (resp. three) invariant under  $GL(2, \mathbb{Z}/4\mathbb{Z})$  (resp.  $GL(2, \mathbb{Z}/3\mathbb{Z})$ ), defined over  $R_o$ . As  $GL(2, \mathbb{Z}/4\mathbb{Z})$  has order  $96 = 32 \times 3$  (resp.  $GL(2, \mathbb{Z}/3\mathbb{Z})$  has order  $48 = 16 \times 3$ ), the projection technique (1.8.1) shows that the canonical map

$$S(\mathbb{Z}[1/6], 1, k) \otimes_{\mathbb{Z}[1/6]} R_o \longrightarrow S(R_o, 1, k)$$

is an isomorphism. Thus it remains only to handle the passage from  $\mathbb{Z}[1/6]$ .

But for any ring  $R$ ,  $S(R, 1, k)$  is the fibre product of the diagram:

$$(1.8.2.1) \quad \begin{array}{ccc} H^0(\bar{M}_3 \otimes R, (\underline{\omega})^{\otimes k}) & & \\ \downarrow & & \\ H^0(\bar{M}_{12} \otimes R, (\underline{\omega})^{\otimes k}) & \longleftarrow & H^0(\bar{M}_4 \otimes R, (\underline{\omega})^{\otimes k}) \end{array}$$

(i.e. a modular form of level one over  $R$  is a modular form  $f_3$  of level three over  $R[1/3]$  together with a modular form  $f_4$  of level four over  $R[1/2]$ , such that  $f_3$  and  $f_4$  induce the same modular form of level 12 over  $R[1/12]$ ). As the formation of the diagram (1.8.2.1) and of its fibre product commutes with any flat extension of scalars  $R \rightarrow R'$ , taking  $R = \mathbb{Z}$ ,  $R' = \mathbb{Z}[1/6]$  gives the desired result.

Remark 1.8.2.2. The above theorem becomes false when we do not exclude the primes 2 and 3. For over the finite field  $\mathbb{F}_p$ , the Hasse invariant  $A$  is a modular form of level one and weight  $p-1$ , holomorphic at  $\infty$ . But over  $\mathbb{Z}$  there are no non-zero modular forms over  $\mathbb{Z}$  of level one, holomorphic at  $\infty$ , of weight either one or two. Similarly,  $A \cdot \Delta$  is a cusp form of level one and weight 13 (resp. 14) over  $\mathbb{F}_2$  (resp.  $\mathbb{F}_3$ ), which cannot be the reduction mod  $p$  of a modular form over  $\mathbb{Z}$ . See [9] for the full determination of modular forms over  $\mathbb{Z}$ .

### 1.9. Modular forms of level 1 and 2: q-expansion principle

For  $n = 1, 2$ , and any  $\mathbb{Z}[1/n]$ -module  $K$ , we define a modular form of level  $n$  and weight  $k$ , holomorphic at  $\infty$ , with coefficients in  $K$  to be  
for  $n = 1$ : an element of the fibre-product of the diagram

$$(1.9.0.0) \quad \begin{array}{ccc} H^0(\bar{M}_3, (\underline{\omega})^{\otimes k} \otimes_{\mathbb{Z}[1/3]} (K \otimes_{\mathbb{Z}} \mathbb{Z}[1/3])) & & \\ \downarrow & & \\ H^0(\bar{M}_{12}, (\underline{\omega})^{\otimes k} \otimes_{\mathbb{Z}[1/12]} (K \otimes_{\mathbb{Z}[1/12]} \mathbb{Z}[1/12])) & \longleftarrow & H^0(\bar{M}_4, (\underline{\omega})^{\otimes k} \otimes_{\mathbb{Z}[1/4]} (K \otimes_{\mathbb{Z}} \mathbb{Z}[1/4])) \end{array}$$

(1.9.0.1) for  $n=2$ : an element of  $H^0(\bar{M}_4, (\underline{\omega})^{\otimes k} \otimes_{\mathbb{Z}[1/4]} K)$  invariant by  
 the subgroup of  $GL_2(\mathbb{Z}/4 \mathbb{Z})$  consisting of matrices  
 $\equiv I \pmod{2}$ .

The module of all such is noted  $S(K, n, k)$ .

(In the case  $K$  is a ring, this notion coincides with that already introduced.) An exact sequence  $0 \rightarrow L \rightarrow K \rightarrow K/L \rightarrow 0$  gives an exact sequence (without the final 0) of modules of modular forms, analogous to (1.6.2.2).

As a corollary of (1.6.1), we have

Corollary 1.9.1. (q-expansion principle) Let  $n=1$  or  $2$ ,  $K$  a  $\mathbb{Z}[1/n]$ -module, and  $L \subset K$  a  $\mathbb{Z}[1/n]$  submodule. Let  $f$  be a modular form of weight  $k$ , level  $n$ , holomorphic at  $\infty$ , with coefficients in  $K$ . Suppose that one of the cusps (for  $n=1$ , there is only one,  $j=\infty$ , while for  $n=2$  there are three,  $\lambda = 0, 1, \infty$ ), the q-coefficients of  $f$  all lie in  $L$ . Then  $f$  is a modular form with coefficients in  $L$ .

### 1.10. Modular schemes of level 1 and 2

They don't exist, in the sense that the corresponding functors are not representable. However, for each  $n \geq 3$  we can form the quotients

$$\mathbb{M}_n/GL_2(\mathbb{Z}/n \mathbb{Z}) = \text{the affine } j\text{-line } \mathbb{A}_{\mathbb{Z}[1/n]}^1$$

$$\bar{\mathbb{M}}_n/GL_2(\mathbb{Z}/n \mathbb{Z}) = \text{the projective } j\text{-line } \mathbb{P}_{\mathbb{Z}[1/n]}^1$$

which fit together for variable  $n$  to form the affine and projective  $j$ -lines over  $\mathbb{Z}$ . We define  $M_1 = \mathbb{A}_{\mathbb{Z}}^1$ , the affine  $j$ -line, and  $\bar{M}_1 = \mathbb{P}_{\mathbb{Z}}^1$ . The invertible sheaf  $\underline{\omega}$  on  $\bar{M}_n$ ,  $n \geq 3$ , does not "descend" to an invertible sheaf on  $\bar{M}_1$ , but its 12<sup>th</sup> power  $\underline{\omega}^{\otimes 12}$  does descend, to  $\mathcal{O}(1)$ , the inverse of the ideal sheaf of  $\infty$ .

In particular, modular forms over any ring  $R$  of level one and weight  $12 \cdot k$  holomorphic at  $\infty$ , are just the elements of  $H^0(\mathbb{P}_R^1, \mathcal{O}(k))$ , and their formation does commute with arbitrary change of base.

Analogously for  $n=2$ , we define

$$M_2 = M_4 / \text{the subgroup of } GL_2(\mathbb{Z}/4\mathbb{Z}) \text{ of matrices } \equiv I \pmod{2}$$

$$\bar{M}_2 = \bar{M}_4 / \text{the subgroup of } GL_2(\mathbb{Z}/4\mathbb{Z}) \text{ of matrices } \equiv I \pmod{2}.$$

The scheme  $M_2$  is  $\text{Spec } \mathbb{Z}[\lambda][1/2\lambda(1-\lambda)]$ , and  $\bar{M}_2$  is the projective  $\lambda$ -line  $\mathbb{P}_{\mathbb{Z}[1/2]}^1$ . The invertible sheaf  $\omega$  does not descend to  $\bar{M}_2$ , but its square does descend, to  $\mathcal{O}(1) = \text{the inverse of the ideal sheaf of the cusp } \lambda = \infty$ . In particular, modular forms of level two over any ring  $R \ni 1/2$ , of (necessarily!) even weight  $2k$  and holomorphic at all three cusps, are just the elements of  $H^0(\mathbb{P}_R^1, \mathcal{O}(k))$ ; hence their formation commutes with arbitrary change of base.

### 1.11. Hecke operators

Let  $\ell$  be a prime number,  $R$  a ring in which  $\ell$  is invertible, and  $n$  an integer prime to  $\ell$ . For any elliptic curve  $E/R$ , the group-scheme  ${}_\ell E$  of points of order  $\ell$  is finite étale over  $R$ , and on a finite étale over-ring  $R'$  it becomes non-canonically isomorphic to  $(\mathbb{Z}/\ell\mathbb{Z})_{R'}^2$ . Thus over  $R'$ , the elliptic curve  $E_{R'}/R'$  has precisely  $\ell+1$  finite flat subgroups-(schemes) of rank  $\ell$ . For any such subgroup  $H$ , we denote by  $\pi: E_{R'} \longrightarrow E_{R'}/H$  the projection onto the quotient and by  $\tilde{\pi}: E_{R'}/H \longrightarrow E_{R'}$ , the dual map, which is also finite étale of degree  $\ell$ . The composition  $\tilde{\pi} \circ \pi$  is multiplication by  $\ell$  on  $E_{R'}/H$ , and the composition  $\tilde{\pi} \circ \pi$  is multiplication by  $\ell$  on  $E_{R'}$ .

If  $\omega$  is a nowhere vanishing differential on  $E/R$ , then  $\tilde{\pi}^*(\omega_{R'}) = \text{trace}_{\tilde{\pi}}(\omega_{R'})$  is a nowhere vanishing differential on  $E_{R'}/H$ . If  $\alpha_n: {}_n E \xrightarrow{\sim} (\mathbb{Z}/n\mathbb{Z})_{R'}^2$  is a level  $n$  structure on  $E/R$ , there is unique level  $n$

structure  $\pi(\alpha_n)$  on  $E_{R'}/H$  such that the diagram

$$(1.11.0.0) \quad \begin{array}{ccc} & (\mathbb{Z}/n\mathbb{Z})_R & \\ \alpha_n \nearrow & \uparrow & \nwarrow \pi(\alpha_n) \\ nE_R, & \xrightarrow{\pi} & n(E_R, / H) \end{array}$$

is commutative. (N.B. There is another "natural" choice of level  $n$  structure on  $E_{R'}/H$ , namely  $\alpha_n \circ \pi = \ell \cdot \pi(\alpha_n)$ , which we will not use.)

Given a modular form over  $R$  of level  $n$  and weight  $k$ , for each triple  $(E/R, \omega, \alpha_n)$  we may form the sum over the  $\ell+1$  subgroups  $H$  of order  $\ell+1$  of  $E_R$ ,

$$(1.11.0.1) \quad \sum_H f(E_R, / H, \pi^*(\omega), \pi(\alpha_n))$$

which, while apparently an element of  $R'$ , is in fact an element of  $R$ , and does not depend on the auxiliary choice of  $R'$ . Normalizing this sum by the factor  $\ell^{k-1}$ , we define the Hecke operator  $T_\ell$  on modular forms of level  $n$  and weight  $k$  by the formula

$$(1.11.0.2) \quad (T_\ell f)(E/R, \omega, \alpha_n) = \ell^{k-1} \sum_H f(E_R, / H, \pi^*(\omega), \pi(\alpha_n)),$$

the sum extended to the  $\ell+1$  subgroups of order  $\ell$ .

We now consider the effect on the  $q$ -expansions. The  $\ell$ -division points of the Tate curve  $\text{Tate}(q^n)$  over  $\mathbb{Z}((q)) \otimes_{\mathbb{Z}} \mathbb{Z}[1/n\ell]$  all become rational over  $\mathbb{Z}((q^{1/\ell})) \otimes_{\mathbb{Z}} \mathbb{Z}[1/n\ell, \zeta_\ell]$ , and the  $\ell+1$  subgroups of order  $\ell$  are the following:

$\mu_\ell$ , generated by  $\zeta_\ell$

$H_i$ , generated by  $(\zeta_\ell^i q^{1/\ell})^n$  for  $i = 0, 1, \dots, \ell-1$ .

For the subgroup  $\mu_\ell$ , the quotient  $\text{Tate}(q^n)/\mu_\ell$  is  $\text{Tate}(q^{n\ell})$  (the projection induced by the  $\ell$ 'th power map on  $G_m$ ) and the dual isogeny consists of dividing

$\text{Tate}(q^n)$  by the subgroup generated by  $q^n$ . For the subgroups  $H_i$ , the quotient  $\text{Tate}(q^n)/H_i$  is  $\text{Tate}((\zeta_\ell^i q^{1/\ell})^n)$ , and the dual isogeny consists of dividing  $(\text{Tate}((\zeta_\ell^i q^{1/\ell})^n))$  by its subgroup  $\mu_\ell$ .

Thus for the subgroup  $\mu_\ell$ , we have  $\pi^*(\omega_{\text{can}}) = \omega_{\text{can}}$  on  $\text{Tate}(q^{n\ell})$ , while for the subgroups  $H_i$ ,  $\pi^*(\omega_{\text{can}}) = \ell \cdot (\omega_{\text{can}})$  on  $\text{Tate}((\zeta_\ell^i q^{1/\ell})^n)$  (because in the latter case  $\pi$  is induced by the  $\ell$ 'th power mapping on  $G_m$ , on which  $\omega_{\text{can}}$  is  $dt/t$ ).

The quotient  $\text{Tate}(q^n)/\mu_\ell \xrightarrow{\sim} \text{Tate}(q^{n\ell})$  may be viewed as obtained from  $\text{Tate}(q^n)$  by the extension of scalars  $\phi_\ell: \mathbf{Z}((q)) \longrightarrow \mathbf{Z}((q))$  sending  $q \mapsto q^\ell$ . We denote by  $\alpha'_n$  the unique level  $n$  structure on  $\text{Tate}(q^n)$  such that  $\phi_\ell^*(\alpha'_n) = \pi_\ell(\alpha_n)$ ,  $\pi_\ell(\alpha_n)$  denoting the image of  $\alpha_n$  by the projection of  $\text{Tate}(q^n)$  onto  $\text{Tate}(q^n)/\mu_\ell \xrightarrow{\sim} \text{Tate}(q^{n\ell})$ .

The quotients  $\text{Tate}(q^n)/H_i \xrightarrow{\sim} \text{Tate}(q^{n/\ell} \zeta_\ell^{ni})$ ,  $i=0,\dots,\ell-1$  over  $\mathbf{Z}[1/n\ell, \zeta_{n\ell}]((q^{1/\ell}))$ , may each be viewed as obtained from  $\text{Tate}(q^n)/H_0 \xrightarrow{\sim} \text{Tate}(q^{n/\ell})$  by the extension of scalars  $\phi_i: \mathbf{Z}[1/n\ell, \zeta_{n\ell}]((q^{1/\ell})) \longrightarrow \mathbf{Z}[1/n\ell, \zeta_{n\ell}]((q^{1/\ell}))$  which sends  $q^{1/\ell} \mapsto \zeta_\ell^i q^{1/\ell}$ . Under this identification, we have (noting  $\pi_i: \text{Tate}(q^n) \longrightarrow \text{Tate}(q^n)/H_i$ ,  $i=0,\dots,\ell-1$  the projections) the relation  $\pi_i(\alpha_n) = \phi_i^*(\pi_0(\alpha_n))$ , as an immediate explicit calculation shows. We denote by  $\alpha''_n$  the level  $n$  structure  $\pi_\ell^*(\pi_0(\alpha_n))$  on  $\text{Tate}(q^n)$  obtained from  $\pi_0(\alpha_n)$  on  $\text{Tate}(q^{n/\ell})$  by the extension of scalars  $i_\ell: \mathbf{Z}[1/n\ell, \zeta_{n\ell}]((q^{1/\ell})) \xrightarrow{\sim} \mathbf{Z}[1/n\ell, \zeta_{n\ell}]((q))$  sending  $q^{1/\ell}$  to  $q$ .

Thus we have

$$(1.11.0.3) \quad \begin{aligned} f(\text{Tate}(q^n)/\mu_\ell, \pi_\ell^*(\omega_{\text{can}}), \pi_\ell(\alpha_n)) &= f(\text{Tate}(q^{n\ell}), \omega_{\text{can}}, \phi_\ell^*(\alpha'_n)) \\ &= \phi_\ell(f(\text{Tate}(q^n), \omega_{\text{can}}, \alpha'_n)). \end{aligned}$$

$$\begin{aligned}
 f(\text{Tate}(q^n)/H_i, \pi_i^*(\omega_{\text{can}}), \pi_i(\alpha_n)) &= f(\text{Tate}((\zeta^i q^{1/\ell})^n), \ell \cdot \omega_{\text{can}}, \varphi_i^*(\pi_o(\alpha_n))) \\
 &= \varphi_i(f(\text{Tate}(q^{n/\ell}), \ell \cdot \omega_{\text{can}}, \pi_o(\alpha_n))) \\
 (1.11.0.4) \quad &= \varphi_i \circ (i_\ell)^{-1}(f(\text{Tate}(q^n), \ell \cdot \omega_{\text{can}}, \alpha_n'')) \\
 &= \ell^{-1} \cdot \varphi_i \circ (i_\ell)^{-1}(f(\text{Tate}(q^n), \omega_{\text{can}}, \alpha_n'')) .
 \end{aligned}$$

Combining these, we have the following formula for  $T_\ell$ .

Formula 1.11.1. Let  $f$  be a modular form of level  $n$  and weight  $k$  over a ring  $R$ , and suppose  $\ell$  is a prime number not dividing  $n$  which is invertible in  $R$ . Let  $f$  be a modular form of level  $n$  and weight  $k$ , with  $q$ -expansions

$$(1.11.1.0) \quad f(\text{Tate}(q^n), \omega_{\text{can}}, \alpha_n) = \sum_{i>-\infty} a_i(\alpha_n) \cdot q^i .$$

Then

$$(1.11.1.1) \quad (T_\ell f)(\text{Tate}(q^n), \omega_{\text{can}}, \alpha_n) = \sum_{i>-\infty} b_i(\alpha_n) q^i ,$$

where the coefficients  $b_i(\alpha_n)$  are given by the formula

$$(1.11.1.2) \quad b_i(\alpha_n) = \ell^{k-1} a_{i/\ell}(\alpha_n') + a_{\ell i}(\alpha_n'')$$

(with the convention that  $a_{i/\ell} = 0$  unless  $\ell|i$ ).

Corollary 1.11.2. If  $f$  is holomorphic at  $\infty$ , so is  $T_\ell(f)$ . If  $f$  is a cusp-form (meaning that its  $q$ -expansions all start in degree  $\geq 1$ ), then so is  $T_\ell(f)$ . If all the  $q$ -expansions of  $f$  are polynomials in  $q$ , the same is true of  $T_\ell(f)$ .

Proof. These follow directly from the explicit formulae - we note that if  $f$  has polynomial  $q$ -expansions of  $\deg \leq n$ , then  $T_\ell(f)$  has expansions of degree  $\leq nl$ .

Proposition 1.11.3. Let  $n \geq 2$  and  $k \geq 2$ , or  $3 \leq n \leq 11$  and  $k \geq 1$ . For any prime  $\ell$  not dividing  $n$ , and any  $\mathbb{Z}[1/n]$ -module  $K$ , there is a necessarily unique endomorphism of the space of modular forms of weight  $k$  and

level  $n$ , holomorphic at  $\infty$ , with coefficients in  $K$ , whose effect on  $q$ -expansions is that given by the formulas (1.11.1.0-2).

Proof. By the base-changing theorem, we are reduced to the case  $K = \mathbb{Z}[1/n]$ .

For a modular form  $f$  over  $\mathbb{Z}[1/n]$ ,  $T_\ell$  exists à priori over  $\mathbb{Z}[1/n\ell]$ , but its  $q$ -expansions all have coefficients in  $\mathbb{Z}[1/n, \zeta_n]$ , so by (1.6.2) and (1.9.1),  $T_\ell(f)$  is in fact a modular form over  $\mathbb{Z}[1/n]$ . QED

Corollary 1.11.4. Let  $k \geq 2$ . For any prime  $\ell$ , and any  $\mathbb{Z}$ -module  $K$ , there is a necessarily unique endomorphism of the space of modular forms of weight  $k$  and level one, holomorphic at  $\infty$ , whose effect on the  $q$ -expansion is that given by the formulas (1.11.1.0-2).

Proof. Choose relatively prime integers  $n, m \geq 3$ , both prime to  $\ell$ , and view the module of level one modular forms as the fibre-product of the diagram

$$(1.11.4.1) \quad \begin{array}{ccc} H^0(\bar{M}_n, \underline{\omega}^{\otimes k} \otimes (K \otimes \mathbb{Z}[1/n])) & & \\ \downarrow & & \\ H^0(\bar{M}_{mn}, (\underline{\omega})^{\otimes k} \otimes (K \otimes \mathbb{Z}[1/mn])) & \longleftarrow & H^0(\bar{M}_m, (\underline{\omega})^{\otimes k} \otimes (K \otimes \mathbb{Z}[1/m])) . \end{array}$$

The desired  $T_\ell$  is the fibre product of the  $T_\ell$  constructed above on this diagram. QED

### 1.12. Applications to polynomial $q$ -expansions; the strong $q$ -expansion principle

In this section we will admit the following result, a special case of Swinnerton-Dyer's structure theorem (cf. [41], [43]), which will be proven later (cf. 4.4.1).

Result 1.12.0. Let  $n \geq 1$  be an integer,  $K$  a field of characteristic  $p \nmid n$ , and  $f$  a modular form over  $K$  of level  $n$  and weight  $k \geq 1$ , holomorphic at infinity. Suppose  $p-1 \nmid k$ . Then if all the  $q$ -expansions of  $f$  at the cusps

of  $\bar{M}_n \otimes K(\zeta_n)$  are constants,  $f = 0$ .

Using this result, we will now prove

Theorem 1.12.1. Let  $n, k \geq 1$  be integers, and suppose that  $f$  is a modular form of level  $n$  and weight  $k$ , holomorphic at  $\infty$ , with coefficients in a  $\mathbb{Z}[1/n]$ -module  $K$ . Suppose that for every prime  $p$  such that  $p-1|k$ , the endomorphism "multiplication by  $p$ " is injective on  $K$ . Then if all the  $q$ -expansions of  $f$  are polynomials in  $q$ ,  $f = 0$ .

Proof. We begin by reducing to the case  $n \geq 3$ , using the diagram (1.9.0.0) to handle the case  $n=1$ , and the interpretation (1.9.1.1) for  $n=2$ . We then reduce to the case in which  $n$  is divisible by  $a = \prod_{p-1|k} p$ ; by hypothesis  $K \subset K[1/a]$ , so we may replace  $K$  by  $K[1/a]$  (using the cohomology sequence (1.6.2.2)), then view  $f$  as a modular form of level  $a \cdot n$  with coefficients in  $K[1/a]$ . Next we reduce to the case in which  $K$  is an artin local ring over  $\mathbb{Z}[1/n]$ , as explained in the proof of (1.6.1). We will proceed by induction on the least integer  $b \geq 1$  such that  $M^b = 0$ ,  $M$  denoting the maximal ideal. Thus we begin with the case in which  $K$  is a field.

Consider the finite-dimensional  $K$ -space  $V$  of such modular forms, and choose a basis  $f_1, \dots, f_r$  of  $V$ . Let  $N$  be the maximum of the degrees of the  $q$ -expansions of the  $f_i$  at any of the cusps. At each cusp, record the

$q$ -expansion of  $F = \begin{pmatrix} f_1 \\ \vdots \\ f_r \end{pmatrix}$ :

$$F(Tate(q^n), \omega_{can}, \alpha_n) = \sum_{i=0}^N A_i(\alpha_n) q^i, \quad A_i = \begin{pmatrix} a_{i,1}(\alpha_n) \\ \vdots \\ a_{i,n}(\alpha_n) \end{pmatrix}$$

Let  $\ell$  be a prime number such that  $\ell \nmid n$ ,  $\ell > N$ . Because  $V$  is stable under the Hecke operator  $T_\ell$  (cf. 1.11), we have a matrix equation ( $C$  denoting an  $r \times r$  matrix with coefficients in  $K$ ),

$$T_\ell(F) = C \cdot F.$$

Passing to q-expansions gives the equation

$$\sum_i (A_{\ell i}(\alpha_n'') + \ell^{k-1} A_{i/\ell}(\alpha_n')) q^i = c \cdot \sum_i A_i(\alpha_n) q^i$$

whence, comparing coefficients of  $q^{i\ell}$ , we find the relation

$$A_{\ell^2 i}(\alpha_n'') + \ell^{k-1} A_i(\alpha_n') = c \cdot A_{i\ell}(\alpha_n) .$$

But for  $i \geq 1$ ,  $i\ell > N$  and  $i\ell^2 > N$ , hence  $A_{i\ell}(\alpha_n) = 0$  and  $A_{\ell^2 i}(\alpha_n'') = 0$  (by definition of  $N$ ). As  $\ell$  is invertible, we have  $A_i(\alpha_n') = 0$  for each level  $n$  structure  $\alpha_n$ . Hence each q-expansion of each  $f_i$  is a constant, hence by (1.12.0) each  $f_i = 0$ . This concludes the proof in case  $K$  is a field, and implies the case in which  $K$  is a vector space over a field, as vector spaces have bases.

Now consider the case of an Artin local ring  $K$  whose maximal ideal  $m$  satisfies  $m^{b+1} = 0$ . By induction,  $f$  becomes 0 in  $K/m^b$ , hence by the exact cohomology sequence (1.6.2.2) associated to the exact sequence of  $\mathbb{Z}[1/n]$ -modules  $0 \rightarrow m^b \rightarrow K \rightarrow K/m^b \rightarrow 0$ ,  $f$  comes from a form with coefficients in  $m^b$ . But as  $m^{b+1} = 0$ ,  $m^b$  is a (finite-dimensional!) vector space over the residue field  $K/m$ , and the previous case of a field applies. QED

Corollary 1.12.2. (Strong q-expansion principle) Let  $n, k \geq 1$ , and let  $a = \prod_{p=1}^k p$ . Let  $K$  be a  $\mathbb{Z}[1/an]$ -module of which  $L \subset K$  is a  $\mathbb{Z}[1/an]$ -submodule, and  $f$  a modular form of level  $n$  and weight  $k$ , holomorphic at  $\infty$ , such that at each cusp, all but finitely many of its q-expansion coefficients lie in  $L \otimes_{\mathbb{Z}[1/n]} \mathbb{Z}[1/n, \zeta_n]$ . Then  $f$  is a modular form with coefficients in  $L$ .

Proof. Apply the theorem to the image of  $f$  as modular form with coefficients in  $K/L$ . QED

### 1.13. Review of the modular scheme associated to $\Gamma_0(p)$

For each integer  $n \geq 3$  prime to  $p$ , the functor "isomorphism classes of elliptic curves with level  $n$  structure and a finite flat subgroup (scheme) of rank  $p$ " is representable, by a scheme  $M_{n,p}$ , which is an affine curve over  $\mathbb{Z}[1/n]$ ; it is a regular scheme, but it fails to be smooth over  $\mathbb{Z}[1/n]$  precisely at the finitely closed points on  $M_{n,p}$  corresponding to super-singular elliptic curves in characteristic  $p$ . The projection "forget the subgroup of rank  $p$ " makes  $M_{n,p}$  finite and flat over  $M_n$  of degree  $p+1$ .

We define  $\bar{M}_{n,p}$  to be the normalization of  $\bar{M}_n$  in  $M_{n,p}$ ; it is a regular scheme, proper and flat over  $\mathbb{Z}[1/n]$ . The difference  $\bar{M}_{n,p} - M_{n,p}$  is finite and étale over  $\mathbb{Z}[1/n]$ , and over  $\mathbb{Z}[1/n, \zeta_n]$  it is a disjoint union of sections, called the cusps of  $\bar{M}_{n,p}$ , two of which lie over each cusp of  $\bar{M}_n$ , and exactly one of which is étale over  $\bar{M}_n$ .

The completion of  $\bar{M}_{n,p} \otimes \mathbb{Z}[1/n, \zeta_n]$  along any of the cusps is isomorphic to  $\mathbb{Z}[1/n, \zeta_n][[q]]$ . The universal elliptic curve with level  $n$  structure and subgroup of order  $p$  over  $\mathbb{Z}[1/n, \zeta_n]((q))$ , viewed as a punctured disc around an unramified cusp, is the Tate curve  $\text{Tate}(q^n)$  with the level  $n$  structure corresponding to the underlying cusp of  $\bar{M}_n$ , and the subgroup  $\mu_p$ . Over one of the ramified cusps, the inverse image is the Tate curve  $(q^{np})$ , with the induced  $(q \mapsto q^p)$  level  $n$  structure from the cusp of  $\bar{M}_n$  below, and with the subgroup generated by  $q^n$ .

The automorphism of  $M_{n,p}$  given by  $(E, \alpha_n, H) \mapsto (E/H, \pi(\alpha_n), {}_p E/H)$  ( $\pi: E \rightarrow E/H$  denoting the projection, and  $\pi(\alpha_n)$  the level  $n$  structure explained in (1.11.0.0)) extends to an automorphism of  $\bar{M}_{n,p}$  which interchanges the two sorts of cusps.

## Chapter 2: p-adic modular forms

This chapter is devoted to the study of various properly p-adic generalizations of the notion of modular form, as "functions" of p-adic elliptic curves whose Hasse invariant is not too near zero.

### 2.0 The Hasse invariant A as a modular form; its q-expansion

Let  $R$  be any ring in which  $p = 0$  (i.e.,  $R$  is an  $\mathbb{F}_p$ -algebra) and consider an elliptic curve  $E/R$ . The  $p$ 'th power mapping  $F_{\text{abs}}$  is an additive  $p$ -linear endomorphism of  $\mathcal{O}_E$ , hence induces a  $p$ -linear endomorphism of the  $R$ -module  $H^1(E, \mathcal{O}_E)$ . If  $\omega$  is a base of  $\underline{\omega}_{E/R}$ , it determines the dual base  $\eta$  of  $H^1(E, \mathcal{O}_E)$ , and we define  $A(E, \omega) \in R$  by setting  $F_{\text{abs}}^*(\eta) = A(E, \omega) \cdot \eta$ . Replacing  $\omega$  by  $\lambda\omega$ ,  $\lambda \in R^\times$  has the effect of replacing  $\eta$  by  $\lambda^{-1}\eta$ , and  $F_{\text{abs}}^*(\lambda^{-1}\eta) = \lambda^{-p} F_{\text{abs}}^*(\eta) = \lambda^{-p} \cdot A(E, \omega) \cdot \eta = \lambda^{1-p} A(E, \omega) \cdot \lambda^{-1}\eta$ , whence  $A(E, \lambda\omega) = \lambda^{1-p} A(E, \omega)$ , which shows that  $A(E, \omega)$  is a modular form of level one and weight  $p-1$  defined over  $\mathbb{F}_p$ . More intrinsically, we may interpret  $F_{\text{abs}}^*$  as an  $R$ -linear homomorphism  $F_{\text{abs}}^*: F_{\text{abs}}^*(H^1(E, \mathcal{O}_E)) = (H^1(E, \mathcal{O}_E))^{\otimes p} \longrightarrow H^1(E, \mathcal{O}_E)$ , so as a section of  $(\underline{\omega}_{E/R})^{\otimes p-1}$ . In terms of the base  $\omega$  of  $\underline{\omega}$ , this section is  $A(E, \omega)^{\otimes p-1}$ . To see that  $A$  is holomorphic at  $\infty$ , we simply note that the Tate curve over  $\mathbb{F}_p((q))$  is the restriction of a plane curve  $C$  over  $\mathbb{F}_p[[q]]$ , and that its canonical differential  $\omega_{\text{can}}$  is the restriction of a base over  $\mathbb{F}_p[[q]]$  of the dualizing sheaf of  $C$ . Thus  $\omega_{\text{can}}$  determines the dual base  $\eta_{\text{can}}$  of  $H^1(C, \mathcal{O}_C)$  as  $\mathbb{F}_p[[q]]$ -module, and  $A(\text{Tate}(q), \omega_{\text{can}})$  is just the matrix of  $F_{\text{abs}}^*$  on  $H^1(C, \mathcal{O}_C)$  with respect to the base  $\eta_{\text{can}}$ . In particular,  $A(\text{Tate}(q), \omega_{\text{can}}) \in \mathbb{F}_p[[q]]$ .

An alternative method of establishing holomorphy is to use the fact that for any elliptic curve  $E/R$  over any base ring  $R$ ,  $H^1(E, \mathcal{O}_E)$  is the tangent space of  $E/R$  at the origin, which is to say the  $R$ -module of all translation-invariant derivations of  $E/R$ , and that when  $R$  is an  $\mathbb{F}_p$ -algebra, the action of  $F_{\text{abs}}^*$  on  $H^1(E, \mathcal{O}_E)$  consists of taking the  $p$ 'th iterate of an invariant

derivation. Now we use the fact that there is a local parameter  $t$  on the completion of the Tate curve along its identity section in terms of which  $\omega_{\text{can}} = dt/(1+t)$ . Let  $D$  be the invariant derivation dual to  $\omega_{\text{can}}$ . Then  $D(t) = 1+t$ , hence  $D(1+t) = 1+t$ , hence  $D^n(1+t) = 1+t$  for all  $n \geq 1$ . Over  $\mathbb{F}_p$ ,  $D^p$  is an invariant derivation, and it agrees with  $D$  on  $\omega_{\text{can}}$ , hence  $D^p = D$ , hence  $F_{\text{abs}}^*(\eta_{\text{can}}) = \eta_{\text{can}}$ , and  $A(\text{Tate}(q), \omega_{\text{can}}) = 1$ .

### 2.1 Deligne's congruence $A \equiv E_{p-1} \pmod{p}$

For any even integer  $k \geq 4$ , the Eisenstein series  $E_k$  is the modular form over  $\mathbb{C}$  of level one and weight  $k$  whose  $q$ -expansion is

$$1 - \frac{2k}{b_k} \sum \sigma_{k-1}(n) q^n, \quad \sigma_{k-1}(n) = \sum_{\substack{d|n \\ d \geq 1}} d^{k-1}.$$

As its  $q$ -expansion coefficients all lie in  $\mathbb{Q}$ ,  $E_k$  is defined over  $\mathbb{Q}$  (by 1.9.1). For  $k = p-1$ ,  $p \geq 5$ , the  $p$ -adic ordinal of  $\frac{-2(p-1)}{b_{p-1}}$  is 1, hence  $E_{p-1}$  has  $q$ -expansion coefficients in  $\mathbb{Q} \cap \mathbb{Z}_p$ . Thus it makes sense to reduce  $E_{p-1}$  modulo  $p$ , obtaining a modular form over  $\mathbb{F}_p$ , whose  $q$ -expansion is the constant 1. Hence  $A = E_{p-1} \pmod{p}$ , because both are modular forms of the same weight with the same  $q$ -expansions.

For  $p = 2$  and 3, it is not possible to lift  $A$  to a modular form of level one, holomorphic at  $\infty$ , over  $\mathbb{Q} \cap \mathbb{Z}_p$ . However, for  $p = 2$  and  $3 \leq n \leq 11$ ,  $2 \nmid n$  we may lift  $A$  to a modular form of level  $n$  and weight 1, holomorphic at  $\infty$ , over  $\mathbb{Z}[1/n]$  (by 1.7.1). For  $p = 3$  and any  $n \geq 3$ ,  $3 \nmid n$  we may lift  $A$  to a modular form of level  $n$  and weight 2, holomorphic at  $\infty$ , over  $\mathbb{Z}[1/n]$  (by 1.7.1).

For  $p = 2$  and  $3 \leq n \leq 11$ ,  $n$  odd (resp. for  $p = 3$  and  $n \geq 2$ ,  $3 \nmid n$ ), we choose a modular form  $E_{p-1}$  of weight  $p-1$  and level  $n$ , holomorphic at  $\infty$ , defined over  $\mathbb{Z}[1/n]$ , which lifts  $A$ .

Remark. For  $p=2$ , there exists a lifting of  $A$  to a modular form of level  $n$  over  $\mathbb{Z}[1/n]$  for  $n = 3, 5, 7, 9, 11$ , and hence for any  $n$  divisible by one of  $3, 5, 7, 11$ . But the author does not know whether  $A$  lifts to a form of level  $n$  for other  $n$  (even for  $n=13!$ ). An alternative approach to the difficulties caused by  $p=2$  and  $3$  might be based on the observation that the Eisenstein series  $E_4 = 1 + 240 \sum \sigma_3(n)q^n$  provides a level 1 lifting to  $\mathbb{Z}$  of  $A^4$  if  $p=2$  (resp. of  $A^2$  if  $p=3$ ).

## 2.2 $p$ -adic modular forms with growth conditions

2.2.0 Let  $R_o$  be a  $p$ -adically complete ring (i.e.  $R_o \cong \varprojlim R_o/p^N R_o$ ), and choose an element  $r \in R_o$ . For any integer  $n \geq 1$ , prime to  $p$ , (resp.  $3 \leq n \leq 11$  for  $p=2$ , and  $n \geq 2$  for  $p=3$ ) we define the module  $M(R_o, r, n, k)$  of  $p$ -adic modular forms over  $R_o$  of growth  $r$ , level  $n$  and weight  $k$ : An element  $f \in M(R_o, r, n, k)$  is a rule which assigns to any triple  $(E/S, \alpha_n, Y)$  consisting of:

(2.2.1) an elliptic curve  $E/S$ , where  $S$  is a  $R_o$ -scheme on which  $p$  is nilpotent (i.e.  $p^N = 0$  for  $N \gg 0$ );

(2.2.2) a level  $n$  structure  $\alpha_n$ ;

(2.2.3) a section  $Y$  of  $\omega_{E/S}^{\otimes(1-p)}$  satisfying  $Y \cdot E_{p-1} = r$ ;

a section  $f(E/S, \alpha_n, Y)$  of  $(\omega_{E/S})^{\otimes k}$  over  $S$ , which depends only on the isomorphism class of the triple, and whose formation commutes with arbitrary change of base of  $R_o$ -schemes  $S' \rightarrow S$ .

Equivalently, we may interpret  $f$  as a rule which attaches to each quadruple  $(E/R, \omega, \alpha_n, Y)$  consisting of:

(2.2.4) an elliptic curve  $E/R$ ,  $R$  an  $R_o$ -algebra in which  $p$  is nilpotent;

(2.2.5) a base  $\omega$  of  $\omega_{E/R}$ ;

(2.2.6) a level  $n$ -structure;

(2.2.7) an element  $Y \in R$  satisfying  $Y \cdot E_{p-1}(E, \omega) = r$ ,

an element  $f(E/R, \omega, \alpha_n, Y)$  in  $R$ , which depends only on isomorphism class of the quadruple, whose formation commutes with extension of scalars of  $V$ -algebras, and which satisfies the functional equation:

$$(2.2.8) \quad f(E/R, \lambda\omega, \alpha_n^{p-1}Y) = \lambda^{-k} f(E/R, \omega, \alpha_n, Y) \quad \text{for } \lambda \in R^X.$$

By passage to the limit, we can allow  $R$  to be a  $p$ -adically complete  $R_0$ -algebra in the above definition.

(2.2.9) We say that  $f$  is holomorphic at  $\infty$  if for each integer  $N \geq 1$ , its value on  $(\text{Tate}(q^n), \omega_{\text{can}}, \alpha_n, r(E_{p-1}(\text{Tate}(q^n), \omega_{\text{can}}))^{-1})$ , considered over  $\mathbb{Z}((q)) \otimes (R_0/p^N R_0)[\zeta_n]$  lies in  $\mathbb{Z}[[q]] \otimes (R_0/p^N R_0)[\zeta_n]$ , for each level  $n$  structure  $\alpha_n$ . We denote by  $S(R_0, r, n, k)$  the submodule of  $M(R_0, r, n, k)$  consisting of forms holomorphic at  $\infty$ .

As formal consequence of the definitions, we have

$$2.2.10 \quad M(R_0, r, n, k) = \varprojlim M(R_0/p^N R_0, r, n, k).$$

$$2.2.11 \quad S(R_0, r, n, k) = \varprojlim S(R_0/p^N R_0, r, n, k).$$

### 2.3 Determination of $M(R_0, r, n, k)$ when $p$ is nilpotent in $R_0$

2.3.0 We begin by determining the universal triple  $(E/S, \alpha_n, Y)$  supposing that  $p$  is nilpotent in  $R_0$ , and  $n \geq 3$ . For notational convenience, let's denote  $\omega^{\otimes 1-p}$  by  $\mathcal{L}$ . By the definition of  $M_n$ , the functor

$\mathcal{F}_{R_0, r, n}: S \longrightarrow S\text{-isomorphism classes of triples } (E/S, \alpha_n, Y)$  is the functor  
 $\mathcal{F}_{R_0, r, n}: S \longrightarrow \begin{cases} R_0\text{-morphisms } g: S \rightarrow M_n \otimes R_0, \text{ together with a section} \\ Y \text{ of } g^*(\mathcal{L}) \text{ verifying } Y \cdot g^*(E_{p-1}) = r \end{cases}$

which we may view as a sub-functor of the functor

$$\mathcal{F}_{R_0, n}: S \longrightarrow \{R_0\text{-morphisms } g: S \rightarrow M_n, \text{ plus a section } Y \text{ of } g^*(\mathcal{L})\}.$$

This last functor is representable, by the  $M_n \otimes R_0$ -scheme

$$\begin{array}{c} \text{Spec}_{M_n \otimes R_o}(\text{Symm}(\check{\mathcal{L}})) \\ \downarrow \\ M_n \otimes R_o \end{array}$$

Indeed, we may cover  $M_n \otimes R_o$  by affine opens  $\text{Spec}(B_i)$  over which  $\check{\mathcal{L}}$  admits an invertible section  $\check{\ell}_i$ , and cover  $S$  by affine opens  $\text{Spec}(A_{ij})$  such that  $g|_{\text{Spec}(A_{ij})}$  factors through  $\text{Spec}(B_i)$ . Over  $\text{Spec}(B_i)$ ,  $\text{Spec}(\text{Symm}(\check{\mathcal{L}}))$  is  $\text{Spec}(B_i[\check{\ell}_i])$ . A section  $Y$  of  $g^*(\check{\mathcal{L}})$  determines an element  $Y \cdot g^*(\check{\ell}_i)$  of  $A_{ij}$ , and then a lifting of the given homomorphism  $g: B_i \rightarrow A_{ij}$  to a homomorphism  $\tilde{g}_{ij}: B_i[\check{\ell}_i] \rightarrow A_{ij}$  by the formula

$$\tilde{g}_{ij}(\sum b_k (\check{\ell}_i)^k) = \sum g(b_k)(Y \cdot g^*(\check{\ell}_i))^k.$$

These  $\tilde{g}_{ij}$  piece together to define a morphism from  $S$  to  $\text{Spec}(\text{Symm}(\check{\mathcal{L}}))$ .

The subfunctor  $\mathcal{F}_{R_o, r, n}$  is then represented by the closed subscheme of  $\text{Spec}(\text{Symm}(\check{\mathcal{L}}))$  defined by the vanishing of  $E_{p-1} - r$ . Thus the universal triple  $(E/S, \alpha_n, Y)$  is just the inverse image on  $\text{Spec}(\text{Symm}(\check{\mathcal{L}}))$  of the universal elliptic curve with level  $n$  structure over  $M_n \otimes R_o$ , hence

Proposition 2.3.1. When  $p$  is nilpotent in  $R_o$ , and  $n \geq 3$  is prime to  $p$ , there is a canonical isomorphism

$$M(R_o, r, n, k) = H^0(\text{Spec}_{M_n \otimes R_o}(\text{Symm}(\check{\mathcal{L}})(E_{p-1} - r)), \omega^{\otimes k})$$

$$\begin{aligned} &= H^0(M_n \otimes R_o, \bigoplus_{j \geq 0} (\omega^{\otimes (k+j(p-1))}) / (E_{p-1} - r)) \\ (\text{because } M_n \text{ is affine}) &= H^0(M_n \otimes R_o, \bigoplus_{j \geq 0} (\omega^{\otimes (k+j(p-r))}) / (E_{p-1} - r)) \\ &= \bigoplus_{j \geq 0} M(R_o, n, k+j(p-1)) / (E_{p-1} - r). \end{aligned}$$

## 2.4 Determination of $S(R_o, r, n, k)$ when $p$ is nilpotent in $R_o$

Proposition 2.4.1. Let  $n \geq 3$ ,  $p \nmid n$ . Under the isomorphism (2.3.1), the submodule  $S(R_o, r, n, k) \subset M(R_o, r, n, k)$  is the submodule  $H^0(\text{Spec } \bar{M}_n \otimes R_o, (\text{Symm}(\check{\mathcal{L}})/(E_{p-1} - r)), \underline{\omega}^{\otimes k})$  of  $H^0(\text{Spec } \bar{M}_n \otimes R_o, (\text{Symm}(\check{\mathcal{L}})/(E_{p-1} - r)))$ .

Proof. It suffices to treat the case in which  $R_o \ni \zeta_n$ . Then the ring of the completion of  $\bar{M}_n \otimes R_o$  along  $\infty$  is a finite number of copies of  $R_o[[q]]$ , hence the ring of the completion of  $\text{Spec } \bar{M}_n \otimes R_o, (\text{Symm}(\check{\mathcal{L}})/(E_{p-1} - r))$  along the inverse image of  $\infty$  is isomorphic to a finite number of copies of

$$R_o[[q]] \cong R_o[[q]][Y]/(Y \cdot E_{p-1}(\text{Tate}(q^n), \omega_{\text{can}}, \alpha_n) - r)$$

(an isomorphism because  $E_{p-1}(\text{Tate}(q^n), \omega_{\text{can}}, \alpha_n)$  is invertible in  $R_o[[q]]$ ). Thus the condition that an element  $f \in H^0(\text{Spec } \bar{M}_n \otimes R_o, (\text{Symm}(\check{\mathcal{L}})/(E_{p-1} - r)), \underline{\omega}^{\otimes k})$  have holomorphic  $q$ -expansions is precisely the condition that it extend to a section of  $\underline{\omega}^{\otimes k}$  over  $\text{Spec } \bar{M}_n \otimes R_o, (\text{Symm}(\check{\mathcal{L}})/(E_{p-1} - r), \underline{\omega}^{\otimes k})$ . QED

Remark 2.4.1.1. Analogously to (2.3.1), we have

$$\begin{aligned} H^0(\text{Spec } \bar{M}_n \otimes R_o, (\text{Symm}(\check{\mathcal{L}})/(E_{p-1} - r)), \underline{\omega}^{\otimes k}) \\ = H^0(\bar{M}_n \otimes R_o, \underline{\omega}^{\otimes k} \otimes \text{Symm}(\check{\mathcal{L}})/(E_{p-1} - r)) \\ = H^0(\bar{M}_n \otimes R_o, \bigoplus_{j \geq 0} \underline{\omega}^{k+j(p-1)} / (E_{p-1} - r)). \end{aligned}$$

## 2.5 Determination of $S(R_o, r, n, k)$ in the limit

Theorem 2.5.1. Let  $n \geq 3$ , and suppose either that  $k \geq 2$  or that  $k=1$  and  $n \leq 11$ , or that  $k=0$  and  $p \neq 2$ , or that  $k=0$ ,  $p=2$ , and  $n \leq 11$ . Let  $R_o$  be any  $p$ -adically complete ring ( $R_o \xrightarrow{\sim} \lim_{\leftarrow} R_o/p^N R_o$ ), and suppose  $r \in R_o$  is not a zero divisor in  $R_o$ . Then the homomorphism

$$\begin{array}{c}
 \lim_{\leftarrow} H^0(\bar{M}_n, \bigoplus_{j \geq 0} \underline{\omega}^{k+j(p-1)}) \otimes_{\mathbb{Z}[1/n]} (R_o/p^N R_o)/(E_{p-1} - r) \\
 \downarrow \\
 2.5.1.0 \quad S(R_o, r, n, k) = \lim_{\leftarrow} S(R_o/p^N R_o, r, n, k)
 \end{array}$$

is an isomorphism.

Proof. Let  $\mathcal{S}$  denote the quasicoherent sheaf  $\bigoplus_{j \geq 0} \underline{\omega}^{k+j(p-1)}$  on  $\bar{M}_n$ , and put  $\mathcal{S}_N = \mathcal{S} \otimes R_o/p^N R_o$ . The inverse system of exact sequences

$$2.5.1.1 \quad 0 \longrightarrow \mathcal{S}_N \xrightarrow{E_{p-1} - r} \mathcal{S}_N \longrightarrow \mathcal{S}_N/(E_{p-1} - r) \longrightarrow 0$$

gives an inverse system of six-term cohomology sequences

$$\begin{array}{ccccccc}
 0 \longrightarrow H^0(\bar{M}_n, \mathcal{S}_N) & \xrightarrow{E_{p-1} - r} & H^0(\bar{M}_n, \mathcal{S}_N) & \longrightarrow & H^0(\bar{M}_n, \mathcal{S}_N/(E_{p-1} - r)) & \longrightarrow & H^1(\bar{M}_n, \mathcal{S}_N) = \\
 2.5.1.2 & & & & & & \\
 & \xrightarrow{E_{p-1} - r} & H^1(\bar{M}_n, \mathcal{S}_N) & \longrightarrow & H^1(\bar{M}_n, \mathcal{S}_N/(E_{p-1} - r)) & \longrightarrow & 0.
 \end{array}$$

Suppose first that  $k > 0$ . Under our hypotheses, the base-changing theorem (1.7.1) applies, according to which  $H^0(\bar{M}_n, \mathcal{S}_N) = H^0(\bar{M}_n, \mathcal{S}) \otimes (R_o/p^N R_o)$ , and  $H^1(\bar{M}_n, \mathcal{S}_N) = 0$ . Thus the  $H^0$  terms in (2.5.1.2) form a short exact sequence of inverse systems, the first of which has surjective transition morphisms.

Hence the inverse limits of these inverse systems form the desired short exact sequence.

In case  $k=0$  and  $p \neq 2$  or  $k=0$ ,  $p=2$  and  $n \leq 11$ , we have  $H^1(\bar{M}_n, \underline{\omega}^{\otimes k}) = 0$  for  $k \geq 1$ , hence  $H^1(\bar{M}_n, \mathcal{S}) = H^1(\bar{M}_n, \mathcal{O})$ , and by (1.7.1)),  $H^0(\bar{M}_n, \mathcal{S}_N) = H^0(\bar{M}_n, \mathcal{S}) \otimes R_o/p^N R_o$ . The exact sequence (2.5.1.2) becomes

$$\begin{aligned}
 0 \longrightarrow H^0(\bar{M}_n, \mathcal{S}) \otimes R_o/p^N R_o & \longrightarrow H^0(\bar{M}_n, \mathcal{S}) \otimes R_o/p^N R_o \longrightarrow H^0(\bar{M}_n, \mathcal{S}_N/(E_{p-1} - r)) \longrightarrow \\
 & \rightarrow H^1(\bar{M}_n, \mathcal{O}) \otimes R_o/p^N R_o \xrightarrow{-r} H^1(\bar{M}_n, \mathcal{O}) \otimes R_o/p^N R_o \longrightarrow H^0(\bar{M}_n, \mathcal{O}) \otimes R_o/(p^N, r) \longrightarrow 0.
 \end{aligned}$$

For variable  $N$ , these form a six-term exact sequence of inverse systems. If the sequence of their inverse limits were exact, the theorem would follow, because the map  $\lim_{\leftarrow} H^0(\bar{M}_n, \mathcal{O}) \otimes R_o/p^N R_o \xrightarrow{-r} \lim_{\leftarrow} H^0(\bar{M}_n, \mathcal{O}) \otimes R^o/p^N R_o$  is injective (this because  $H^0(\bar{M}_n, \mathcal{O})$  is a finite free  $\mathbb{Z}[1/n]$ -module, and  $r$  is not a zero divisor in  $R_o \xrightarrow{\sim} \lim_{\leftarrow} R_o/p^N R_o$ ). To prove the exactness we apply a general lemma.

Lemma 2.5.2. Let  $0 \longrightarrow K^0 \longrightarrow K^1 \longrightarrow K^2 \longrightarrow \dots$  be a (long) exact sequence in the category of projective systems of abelian groups indexed by the positive integers. Suppose that for all  $i \neq i_o$ , the projective system  $K^i$  has surjective transition morphisms, and that the sequence

$$\lim_{\leftarrow}^{i+1} K^o \longrightarrow \lim_{\leftarrow}^{i+2} K^o \longrightarrow \lim_{\leftarrow}^{i+3} K^o \text{ is exact. Then the sequence}$$

$$0 \longrightarrow \lim_{\leftarrow} K^0 \longrightarrow \lim_{\leftarrow} K^1 \longrightarrow \lim_{\leftarrow} K^2 \longrightarrow \dots$$

is exact.

Proof. Consider the 2 spectral sequences of hypercohomology for the functor  $\lim_{\leftarrow}$ .

$$I_2^{p,q} = H^p(R^q(\lim_{\leftarrow})(K^\bullet)) \implies \mathbb{R}^{p+q}(\lim_{\leftarrow})(K^\bullet)$$

$$II_2^{p,q} = R^p(\lim_{\leftarrow}(H^q(K^\bullet))) \implies \mathbb{R}^{p+q}(\lim_{\leftarrow})(K^\bullet)$$

By hypothesis, we have  $II_2^{p,q} = 0$  for all values of  $q$ , hence  $\mathbb{R}^n(\lim_{\leftarrow})(K^\bullet) = 0$  for all  $n$ . According to ([48]), we have  $R^i(\lim_{\leftarrow}) = 0$  for  $i \geq 2$ , hence  $I_2^{p,q} = 0$  for  $q \geq 2$ . By ([48]), we have  $R^1(\lim_{\leftarrow})(K^i) = 0$  for  $i \neq i_o$ , hence

$$I_2^{p,q} = 0 \text{ unless } q=0 \text{ or } q=1 \text{ and } p=i_o.$$

As we have also supposed that  $I_2^{i+2,0} = 0$ , we have degeneration:  $E_2^{p,q} = E_\infty^{p,q}$  for all  $p,q$ . As  $E_\infty^{p,q} = 0$  for all  $p,q$ , we get in particular  $I_2^{p,0} = 0$  for all  $p$ , which is the desired conclusion. QED

## 2.6 Determination of a "basis" of $S(R_o, r, n, k)$ in the limit

Lemma 2.6.1. Under the numerical hypotheses of theorem (2.5.1), for each  $j \geq 0$  the injective homomorphism

$$2.6.1.1 \quad H^0(\bar{M}_n \otimes \mathbb{Z}_p, \underline{\omega}^{\otimes k+j(p-1)}) \xrightarrow{E_{p-1}} H^0(\bar{M}_n \otimes \mathbb{Z}_p, \underline{\omega}^{\otimes k+(j+1)(p-1)})$$

admits a section.

Proof. We must show that the cokernel of (2.6.1.1) is a finite free  $\mathbb{Z}_p$ -module. By the base-changing theorem (1.7.1), we have for each  $j \geq 0$  an exact sequence of finite free  $\mathbb{Z}_p$ -modules

$$2.6.1.1.1 \quad 0 \longrightarrow H^0(\bar{M}_n \otimes \mathbb{Z}_p, \underline{\omega}^{\otimes k+j(p-1)}) \xrightarrow{E_{p-1}} H^0(\bar{M}_n \otimes \mathbb{Z}_p, \underline{\omega}^{k+(j+1)(p-1)}) \longrightarrow \\ \longrightarrow H^0(\bar{M}_n \otimes \mathbb{Z}_p, \underline{\omega}^{\otimes k+(j+1)(p-1)} / E_{p-1} \underline{\omega}^{\otimes k+j(p-1)}) \longrightarrow H^1(\bar{M}_n \otimes \mathbb{Z}_p, \underline{\omega}^{k+j(p-1)}) \longrightarrow 0$$

whose formation commutes with arbitrary change of base (for  $\underline{\omega}^{\otimes k+(j+1)(p-1)} / E_{p-1} \underline{\omega}^{\otimes k+j(p-1)}$ , remark that it's  $\mathbb{Z}_p$ -flat by Igusa's theorem (cf[17])), and modulo  $p$ , it becomes a skyscraper sheaf on  $M_n \otimes \mathbb{F}_p$ , hence has vanishing  $H^1$ . Hence the cokernel of the map (2.6.1.1) is the kernel of a surjective map of finite free  $\mathbb{Z}_p$ -modules, hence is itself a finite free  $\mathbb{Z}_p$ -module. QED

For each  $n, k$  satisfying the hypotheses of (2.5.1), and each  $j \geq 0$  we choose once and for all a section of (2.6.1.1), and denote its image by  $B(n, k, j+1)$ . Thus for  $j \geq 0$ , we have a direct sum decomposition

$$2.6.1.2 \quad H^0(\bar{M}_n, \underline{\omega}^{\otimes k+(j+1)(p-1)}) \simeq_{E_{p-1}} H^0(\bar{M}_n, \underline{\omega}^{k+j(p-1)}) \oplus B(n, k, j+1)$$

and

$$2.6.1.3 \quad H^0(\bar{M}_n, \underline{\omega}^{\otimes k}) \stackrel{\text{dfn}}{=} B(n, k, 0).$$

We define  $B(R_o, n, k, j) = B(n, k, j) \otimes R_o$ . Iterating the  $R_o$ -analogue of (2.6.1.2) gives a direct sum decomposition

$$S(R_o, n, k+j(p-1)) \xleftarrow{\sim} \bigoplus_{a=0}^j B(R_o, n, k, a)$$

2.6.1.3

$$\sum E_{p-1}^{j-a} b_a \xleftarrow{\sim} \sum b_a.$$

Let  $B^{\text{rigid}}(R_o, r, n, k)$  denote the  $R_o$ -module consisting of all formal sums

$$\sum_{a=0}^{\infty} b_a, \quad b_a \in B(R, n, k, a)$$

whose terms tend to zero in the sense that given any  $N > 0$ ,  $\exists M > 0$  such that  $b_a \in p^N \cdot B(R, n, k, a)$  for  $a \geq M$ , the  $M$  allowed to depend both upon  $N$  and upon the series  $\sum b_a$ . (Notice that  $B^{\text{rigid}}(R_o, r, n, k)$  does not depend upon  $r$ !)

Proposition 2.6.2. Hypotheses as in (2.5.1), the inclusion of  $B^{\text{rigid}}(R_o, r, n, k)$  in the  $p$ -adic completion of  $H^0(\bar{M}_n, \bigoplus_{j \geq 0} \omega^{k+j(p-1)})$  induces (via (2.6.1.3)) an isomorphism

$$B^{\text{rigid}}(R_o, r, n, k) \longrightarrow S(R_o, r, n, k)$$

2.6.2.1

$$\sum b_a \longrightarrow " \sum_{a \geq 0} \frac{r^a \cdot b_a}{(E_{p-1})^a} "$$

where " $\sum_{a \geq 0} \frac{r^a \cdot b_a}{(E_{p-1})^a}$ " has the value  $\sum_{a \geq 0} b_a(E/S, \alpha_n) \cdot Y^a$  on  $(E/S, \alpha_n, Y)$ .

Proof. For injectivity, we must show that if  $\sum_{a \geq 0} b_a \in B^{\text{rigid}}(R, n, k)$  can be written  $(E_{p-1} - r) \cdot \sum_{a \geq 0} s_a$  with  $s_a \in S(R, n, k+a(p-1))$ , and  $s_a$  tending to zero as  $a \rightarrow \infty$ , then all  $b_a = 0$ . It suffices to show that for any  $N > 0$ ,  $b_a \equiv 0 \pmod{p^N}$ . But  $\pmod{p^N}$ , both  $\sum b_a$  and  $\sum s_a$  become finite sums. To fix ideas, suppose  $b_a \equiv s_a \equiv 0 \pmod{p^N} \forall a > M$ . Let's show  $b_M \equiv s_M \equiv 0 \pmod{p^N}$ . As  $0 \equiv b_{M+1} \equiv E_{p-1} s_M \pmod{p^N}$ ,  $s_M \equiv 0 \pmod{p^N}$ , hence  $b_M \equiv E_{p-1} s_{M-1} \pmod{p^N}$ , hence  $b_M \equiv 0 \pmod{p^N}$  by (2.6.1.3). Now start again with  $M-1 \dots$ .

For surjectivity, we just use the decomposition (2.6.1.3). Given  $\sum s_a$ ,  $s_a \in S(R, n, k+a(p-1))$  tending to zero, we may decompose  $s_a = \sum_{i+j=a} (E_{p-1})^i b_j(a)$ , with  $b_j(a) \in B(R, n, k, j)$ , and  $b_j(a)$  tends to zero as  $a \rightarrow \infty$ , uniformly in  $j$ .

Then  $\sum_a s_a = \sum_a \sum_{i+j=a} (E_{p-1})^i b_j(a) = \sum_a \sum_{i+j=a} r^i b_j(a) +$   
 $+ (E_{p-1} - r) \sum_a \sum_{i+j=a} b_j(a) \sum_{u+v=i-1} (E_{p-1})^u \cdot r^v$ , hence  $\sum_a s_a$  and  $\sum_a \sum_{i+j=a} r^i b_j(a)$   
have the same image in  $S(R_o, r, n, k)$ . But for each  $j$ ,  $\sum_i r^i b_j(i+j)$  converges  
to an element  $b_j^* \in B(R, n, k, j)$ , and  $b_j^*$  tends to zero as  $j \rightarrow \infty$ , and  
 $\sum_{j \geq 0} b_j^*$  has the same image in  $S(R_o, r, n, k)$  as  $\sum_a s_a$ . QED

Corollary 2.6.3. Hypotheses as in (2.5.1), the canonical mapping

$S(R_o, r, n, k) \rightarrow S(R_o, l, n, k)$  defined modularly by composition with the trans-  
formation of functors:  $(E/S, \alpha_n, Y) \rightarrow (E/S, \alpha_n, rY)$ , is injective; the corre-  
sponding map  $B^{rigid}(R_o, r, n, k) \rightarrow B^{rigid}(R_o, l, n, k)$

is given by

$$\sum_a b_a \rightarrow \sum_a r^a b_a.$$

## 2.7 Banach norm and q-expansion for $r=1$

Proposition 2.7.1. Hypotheses as in (2.5.1), let  $x \in R_o$  be any element which  
divides a power  $p^N$ ,  $N \geq 1$ , of  $p$ . Then the following conditions on an ele-  
ment  $f \in S(R_o, l, n, k)$  are equivalent, for  $k \geq 0$ :

- (1)  $f \in x \cdot S(R_o, l, n, k)$ ,
- (2) the q-expansions of  $f$  all lie in  $x \cdot R_o[[\zeta_n]]$ ,
- (3) on each of the  $\phi(n)$  connected components of  $\bar{M}_n \otimes_{\mathbb{Z}[1/n]} \mathbb{Z}[1/n, \zeta_n]$ ,

there is at least one cusp where the q-expansion of  $f$  lies in

$$x \cdot R_o[[\zeta_n]].$$

Proof. Clearly (1)  $\Rightarrow$  (2)  $\Rightarrow$  (3). We will prove (3)  $\Rightarrow$  (1). Because  
 $r=1$ , we have

$$S(R_o/xR_o, l, n, k) \cong B^{rigid}(R_o/xR_o, l, n, k) \cong B^{rigid}(R_o, l, n, k)/x \cdot B^{rigid}(R_o, l, n, k),$$

so replacing  $R_o$  by  $R_o/xR_o$ , we are reduced to the case  $x=0$ , and  $p$  nilpotent in  $R_o$ . In that case  $f \in B^{\text{rigid}}(R_o, l, n, k)$  is a finite sum  $\sum_{a=0}^M b_a$ ,  $b_a \in B(R_o, n, k, a)$ , and its  $q$ -expansion at  $(\text{Tate}(q^n), \omega_{\text{can}}, \alpha_n, (E_{p-1})^{-1})$  is that of

$$\sum_{a=0}^N b_a \cdot (E_{p-1})^{-a} = \frac{\sum_{a=0}^N b_a \cdot (E_{p-1})^{N-a}}{(E_{p-1})^N},$$

hence by hypothesis,  $\sum_{a=0}^N b_a (E_{p-1})^{N-a}$  has  $q$ -expansion zero at one or more cusps on each geometric connected component of  $\bar{M}_n$ , hence by the  $q$ -expansion principle (1.6.2),  $\sum_{a=0}^N b_a (E_{p-1})^{N-a} = 0$ . By (2.6.1.3), each  $b_a = 0$ . QED

Proposition 2.7.2. Let  $n, k, R$  satisfy the hypotheses of (2.5.1). Suppose given for each cusp  $\alpha$  of  $\bar{M}_n$  a power series  $f_\alpha(q) \in R_o[[t_n]][[q]]$ . The following conditions are equivalent:

1. The  $f_\alpha$  are the  $q$ -expansions of an (necessarily unique) element  $f \in S(R_o, l, n, k)$ .
2. For every power  $p^N$  of  $p$ , there exists a positive integer  $M \equiv 0 \pmod{p^{N-1}}$ , and a "true" modular form  $g_N \in S(R_o, n, k+M(p-1))$  whose  $q$ -expansions are congruent  $\pmod{p^N}$  to the given  $f_\alpha$ .

Proof. (1)  $\implies$  (2). Replacing  $R_o$  by  $R_o/p^N R_o$ , we may suppose  $p$  nilpotent in  $R_o$ . We must show that the  $q$ -expansion of  $f$  is the  $q$ -expansions of a true modular form of level  $n$  and weight  $k' \geq k$ ,  $k' \equiv k \pmod{p^{N-1}(p-1)}$ . But as we saw above [cf(2.7.1)], for  $M \gg 0$ , and  $p$  nilpotent in  $R_o$ ,  $f$  has the same  $q$ -expansions as  $g/(E_{p-1})^M$ ,  $g$  truly modular of weight  $k+M(p-1)$ . Multiplying top and bottom by a suitable power of  $E_{p-1}$ , we may suppose  $M \equiv 0 \pmod{p^{N-1}}$ . Then the  $q$ -expansion congruence  $E_{p-1}(q) \equiv 1 \pmod{p}$  at each cusp gives  $(E_{p-1})^{p^{N-1}}(q) \equiv 1 \pmod{p^N}$ , hence  $(E_{p-1})^M(q) \equiv 1 \pmod{p^N}$ , and hence  $f \pmod{p^N}$  has the same  $q$ -expansion as  $g$ .

(2)  $\implies$  (1). Multiplying necessary  $g_N$  by a power of  $(E_{p-1})^{p^{N-1}}$ , we may assume that the weights  $k + M_N(p-1)$  of the  $g_N$  are increasing with  $N$ . Let  $\Delta_N = M_{N+1} - M_N$ . Then  $(g_{N+1} - g_N \cdot (E_{p-1})^{\Delta_N})$  lies in  $p^N \cdot S(R_o, n, k + M_{N+1}(p-1))$  by the  $q$ -expansion principle (1.6.2), hence  $\sum_N (g_{N+1} - g_N \cdot (E_{p-1})^{\Delta_N})$  "converges" to an element of  $S(R_o, 1, n, k)$ , whose  $q$ -expansions are congruent modulo  $p^N$  to those of  $g_N$ . QED

## 2.8. Bases for levels one and two

Suppose  $p \neq 2, 3$ . Then  $E_{p-1}$  is a modular form of level one which lifts the Hasse invariant, and hence for any  $p$ -adically complete ring  $R_o \ni r$  and integer  $n \geq 3$  prime to  $p$ , the group  $GL_2(\mathbb{Z}/n\mathbb{Z})$  acts on the functor  $\mathcal{F}_{R_o, r, n}$  [by  $g(E/S, \alpha_n, Y) = (E/S, g\alpha_n, Y)$  on the set  $\mathcal{F}_{R_o, r, n}(S)$ ], hence on  $M(R_o, r, n, k)$  and on  $S(R_o, r, n, k)$ . Clearly  $M(R_o, r, 1, k)$  is just the submodule  $M(R_o, r, n, k)^{GL_2(\mathbb{Z}/n\mathbb{Z})}$  of invariants under this action, and  $S(R_o, r, 1, k)$  is the submodule  $S(R_o, r, n, k)^{GL_2(\mathbb{Z}/n\mathbb{Z})}$  of  $S(R_o, r, n, k)$ . Now suppose  $n=3$  or  $n=4$ . This choice has the advantage that  $GL_2(\mathbb{Z}/n\mathbb{Z})$  then has order prime to  $p$  (because  $p \neq 2, 3$ ), and  $P = \frac{1}{\#GL_2(\mathbb{Z}/n\mathbb{Z})} \sum g$  is then a projection onto the invariants. Using  $P$  we may also make the chosen section of (2.6.1.1) invariant by  $GL_2(\mathbb{Z}/3\mathbb{Z})$ , and define  $B(1, k, j) = B(n, k, j)^{GL_2(\mathbb{Z}/n\mathbb{Z})} = P(B(n, k, j))$ ,  $B(R_o, 1, k, j) = B(1, k, j) \otimes_{\mathbb{Z}[1/n]} R_o = B(R_o, n, k, j)^{GL_2(\mathbb{Z}/n\mathbb{Z})}$ . Similarly, we define  $B^{\text{rigid}}(R_o, r, 1, k) = P(B^{\text{rigid}}(R_o, r, n, k)) = (B^{\text{rigid}}(R_o, r, n, k))^{GL_2(\mathbb{Z}/n\mathbb{Z})}$ ; it is the subspace of  $B^{\text{rigid}}(R_o, r, n, k)$  consisting of the elements  $\sum b_a$  each of whose terms  $b_a$  is invariant by  $GL_2(\mathbb{Z}/n\mathbb{Z})$ .

Applying the projector  $P$  to (2.6.2) gives:

Proposition 2.8.1. Let  $p \neq 2,3$ ,  $R_o$  a  $p$ -adically complete ring and  $r \in R_o$  not a zero-divisor. Then for each  $k \geq 0$ , the canonical mapping

$$2.8.1.0 \quad \begin{aligned} {}^B\text{rigid}(R_o, r, 1, k) &\longrightarrow S(R_o, r, 1, k) \\ \sum b_a &\longrightarrow " \sum \frac{r^{a_b} a}{(E_{p-1})^a} " \end{aligned}$$

is an isomorphism.

Now suppose  $p \neq 2$ , and consider level two. Let  $E_{p-1} \in S(\mathbb{Z}[\frac{1}{2}], 2, p-1)$  a lifting of the Hasse invariant. Because the subgroup  $G_1$  has order prime to  $p$ ,  $G_1 = \text{Kernel: } GL(\mathbb{Z}/4\mathbb{Z}) \longrightarrow GL(2, \mathbb{Z}/2\mathbb{Z})$ , considerations similar to the above provide a projector  $P_1 = \frac{1}{\#G_1} \sum g_1$  from level 4 to level 2. We have  $M(R_o, r, 2, k) = M(R_o, r, 4, k)^{G_1} = P_1(M(R_o, r, 4, k))$ ,  $S(R_o, r, 2, k) = S(R_o, r, 4, k)^{G_1} = P_1(S(R_o, r, 4, k))$ ,  ${}^B\text{rigid}(R_o, r, 2, k) = {}^B\text{rigid}(R_o, r, 4, k)^{G_1}$ , the subspace of  ${}^B\text{rigid}(R_o, r, 4, k)$  of elements  $\sum b_a$  with each  $b_a$  invariant by  $G_1$ . Applying  $P_1$  to (2.6.2) we get:

Proposition 2.8.2. Let  $p \neq 2$ ,  $R_o$  a  $p$ -adically complete ring and  $r \in R_o$  not a zero-divisor. For each  $k \geq 0$ , the canonical mapping

$$2.8.2.0 \quad \begin{aligned} {}^B\text{rigid}(R_o, r, 2, k) &\longrightarrow S(R_o, r, 2, k) \\ \sum b_a &\longrightarrow " \sum \frac{r^{a_b} a}{(E_{p-1})^a} " \end{aligned}$$

is an isomorphism.

Applying the projectors  $P$  or  $P_1$  to (2.7.1) gives

Proposition 2.8.3. Let  $R_o$  be a  $p$ -adically complete ring. Suppose either that  $p \neq 2$  and  $n=2$  or that  $p \neq 2,3$  and  $n=1$ . Let  $x \in R_o$  be any element which divides a power  $p^N$ ,  $N \geq 1$  of  $p$ . The following conditions on an element  $f \in S(R_o, 1, n, k)$  are equivalent:

- (1)  $f \in x \cdot S(R_o, 1, n, k)$ ,
- (2) the  $q$ -expansions of  $f$  all lie on  $xR_o[[q]]$ .

### 2.9. Interpretation via formal schemes

Let  $n \geq 3$ ,  $p \nmid n$ ,  $R_o$  a  $p$ -adically complete ring, and  $r \in R_o$ .

We denote by  $M_n(R_o, r)$  (resp.  $\bar{M}_n(R_o, r)$ ) the formal scheme over  $R_o$  given the compatible family of  $R_o/p^N R_o$ -schemes  $\underline{\text{Spec}}_{M_n \otimes R_o/p^N R_o}(\text{Symm}(\check{Z})/(E_{p-1} - r))$  (resp.  $\underline{\text{Spec}}_{\bar{M}_n \otimes R_o/p^N R_o}(\text{Symm}(\check{Z})/(E_{p-1} - r))$ ). We have

$$\begin{aligned} M(R_o, r, n, k) &= H^0(M_n(R_o, r), \underline{\omega}^{\otimes k}) \\ S(R_o, r, n, k) &= H^0(\bar{M}_n(R_o, r), \underline{\omega}^{\otimes k}). \end{aligned}$$

Equivalently, we may view  $M_n(R_o, r)$  (resp.  $\bar{M}_n(R_o, r)$ ) as the completion along  $p=0$  of the usual scheme  $\underline{\text{Spec}}_{M_n \otimes R_o}(\text{Symm}(\check{Z})/(E_p - r))$  (resp.  $\underline{\text{Spec}}_{\bar{M}_n \otimes R_o}(\text{Symm}(\check{Z})/(E_{p-1} - r))$ ). For any  $r$ , the first of these schemes is affine, because  $M_n$  is, and when  $r=1$  both schemes are affine. The  $p$ -adic completions of their coordinate rings are just the rings  $M(R, r, n, 0)$  and  $S(R_o, 1, n, 0)$  respectively.

Chapter 3. Existence of the Canonical Subgroup: Applications

In this chapter we study the "canonical subgroup" of an elliptic curve whose Hasse invariant is "not too near zero." For simplicity, we assume throughout this chapter that the groundring  $R_{\circ}$  is a complete discrete valuation ring of residue characteristic  $p$  and generic characteristic zero. We normalize the ordinal function by requiring that  $\text{ord}(p) = 1$ .

Theorem 3.1. (Lubin) I. Let  $r \in R_{\circ}$  have  $\text{ord}(r) < p/p+1$ . There is one and only one way to attach to every  $r$ -situation  $(E/R, \alpha_n, Y)$  ( $R$  a  $p$ -adically complete  $R_{\circ}$ -algebra,  $p \nmid n$ ,  $n \geq 1$  if  $p \neq 2,3$ ,  $n \geq 3$  if  $p = 2,3$ ,  $Y \cdot E_{p-1} = r$ ) a finite flat rank  $p$  subgroup scheme  $H \subset E$ , called the canonical subgroup of  $E/R$ , such that:

$H$  depends only on the isomorphism class of  $(E/R, \alpha_n, Y)$ , and only on that of  $(E/R, Y)$  if  $p \neq 2,3$ .

The formation of  $H$  commutes with arbitrary change of base

$R \rightarrow R'$  of  $p$ -adically complete  $R_{\circ}$ -algebras.

If  $p/r = 0$  in  $R$ ,  $H$  is the kernel of Frobenius:  $E \rightarrow E^{(p)}$ .

If  $E/R$  is the Tate curve  $\text{Tate}(q^n)$  over  $R_{\circ}/p^N R_{\circ}((q))$ , then  $H$  is the subgroup  $\mu_p$  of  $\text{Tate}(q^n)$ .

II. Suppose  $r \in R_{\circ}$  has  $\text{ord}(r) < 1/p+1$ . Then there is one and only one way to attach to every  $r$ -situation  $(E/R, \alpha_n, Y)$  ( $R$  a  $p$ -adically complete  $R_{\circ}$ -algebra,  $p \nmid n$ ,  $n \geq 1$  if  $p \neq 2,3$ ,  $n \geq 3$  if  $p = 2,3$ ,  $Y \cdot E_{p-1} = r$ ) an  $r^p$ -situation  $(E'/R, \alpha'_n, Y')$ , where

$$\begin{cases} E' = E/H \\ \alpha'_n = \pi(\alpha_n), \quad \pi: E \rightarrow E' \text{ denoting the projection} \\ Y' \cdot E_{p-1}(E'/R, \alpha'_n) = r^p \end{cases}$$

such that

$Y'$  depends only on the isomorphism class of  $(E/R, \alpha_n, Y)$ ,  
and only on that of  $(E/R, Y)$  if  $p \neq 2, 3$ .

The formation of  $Y'$  commutes with arbitrary change of  
base  $R \rightarrow R'$  of  $p$ -adically complete  $\mathbb{R}_o$ -algebras.

If  $p/r = 0$  in  $R$ ,  $Y'$  is the inverse image  $y^{(p)}$  of  
 $Y$  on  $E^{(p)} = E'$ .

Before giving the proof, we give some applications.

Theorem 3.2. Suppose  $n \geq 3$ ,  $p \nmid n$ . Let  $f$  be a modular form of level  $n$  and weight  $k$  on  $\Gamma_o(p)$ , defined over  $\mathbb{R}_o$ , and which is holomorphic at the unramified cusps of  $\bar{M}_{n,p}$ . There exists a (necessarily unique) element  $\tilde{f} \in S(R_o, l, n, k)$  whose  $q$ -expansions at each cusp of  $\bar{M}_n$  is that of  $\tilde{f}$  at the overlying unramified cusp of  $\bar{M}_{n,p}$ . Furthermore, if  $r \in \mathbb{R}_o$  has  $\text{ord}(r) < p/p+1$ , then in fact  $\tilde{f} \in S(R_o, r, n, k)$ .

Proof. Simply define  $\tilde{f}(E/R, \omega, \alpha_n, Y) = f(E/R, \omega, \alpha_n, H)$ .

Theorem 3.3. Suppose  $n \geq 3$ ,  $p \nmid n$ , and that either  $k \geq 2$  or  $k=1$  and  $n \leq 11$ , or that  $k=0$ ,  $p \neq 2$ , or that  $k=0$ ,  $p=2$  and  $n \leq 11$ . Let  $r \in \mathbb{R}_o$  have  $\text{ord}(r) < 1/p+1$ . For any  $f \in S(R_o, r^p, n, k)$ , there is a unique element  $\phi(f) \in S(R_o, l, n, k)$  whose  $q$ -expansions are given by

$$\phi(f)(\text{Tate}(q^n), \omega_{\text{can}}, \alpha_n) = f(\text{Tate}(q^{np}), \omega_{\text{can}}, \pi(\alpha_n))$$

[where  $\pi: \text{Tate}(q^n) \rightarrow \text{Tate}(q^{np})$  is the map "dividing by  $\mu_p$ ", and  $\pi(\alpha_n)$  is the induced level  $n$ -structure]. Furthermore,  $\phi(f) \cdot (E_{p-1})^k \in S(R_o, r, n, pk)$ .

Proof. Define  $\phi(f)(E/R, \omega, \alpha_n, Y) = f(E'/R, \pi^*(\omega), \alpha'_n, Y')$ , [ $E' = E/H$ ,  $\pi: E \rightarrow E'$  is the projection]. This makes sense if  $Y \cdot E_{p-1} = 1$ , for then  $\pi$  is étale and so  $\pi^*(\omega)$  is a nowhere vanishing differential on  $E' = E/H$ . To see that  $E_{p-1}^k \cdot \phi(f)$  actually lies in  $S(R_o, r, n, kp)$ , notice that its value on

$(E/R, \omega, \alpha_n, Y)$ ,  $Y \cdot E_{p-1} = r^p$ , is given formally by  $(E_{p-1}(E/R, \omega, \alpha_n))^k \cdot f(E'/R, \pi^*(\omega), \alpha'_n, Y')$ . [In fact this expression has no meaning, because  $\pi^*(\omega)$  may well fail to be nowhere-vanishing on  $E'$ .] However, if we write  $\pi^*(\omega) = \lambda \cdot \omega'$  with  $\lambda \in R$  and  $\omega'$  nowhere-vanishing on  $E'$ , then  $((E_{p-1})^k \cdot \phi(f))(E/R, \omega, \alpha_n, Y) = \left( \frac{E_{p-1}(E/R, \omega, \alpha_n)}{\lambda} \right)^k \cdot f(E'/R, \omega', \alpha'_n, Y')$ . But a simple tangent calculation (cf. 3.6.5) shows that  $\lambda$  and  $E_{p-1}$  are essentially equal; they differ multiplicatively by a unit of  $R$ . By "reduction to the universal case", in which  $R$  is flat over  $\mathbb{Z}_p$ , we can make sense of the ratio  $E_{p-1}/\lambda$ , and interpret it as a unit in any  $R$ ; this permits us to define  $((E_{p-1})^k \cdot \phi(f))(E/R, \omega, \alpha_n, Y) = \left( \frac{E_{p-1}(E/R, \omega, \alpha_n)}{\lambda} \right)^k f(E', \omega', \alpha'_n, Y')$ . QED

### 3.4 Construction of the canonical subgroup in case $r=1$

Let us first note that for  $r=1$  the theorem is very simple. Given  $(E/R, \alpha_n)$  with  $E_{p-1}(E/R, \alpha_n)$  invertible, the curve  $E \otimes R/pR$  over  $R/pR$  has invertible Hasse invariant, hence  $\text{Ker}(F: E \otimes R/pR \longrightarrow (E \otimes R/pR)^{(p)})$  is a finite flat subgroup-scheme of  $E \otimes R/pR$  of rank  $p$  whose Cartier dual, the kernel of Verschiebung, is étale. Since  $R$  is  $p$ -adically complete, Hensel's lemma allows us to uniquely lift  $\text{Ker } F$  to the desired subgroup-scheme  $H$  of  $E/R$  (by taking for  $H$  the Cartier dual of the unique lifting of its étale dual). Since the Tate curve  $\text{Tate}(q^n)$  over  $\mathbb{F}_p((q))$  has  $\ker F = \mu_p$ , the above argument shows that the canonical subgroup of  $\text{Tate}(q^n)$  over  $R_0/p^N R_0((q))$  is  $\mu_p$ . This concludes the proof of part I of the Theorem. For part II, still only in the case  $r=1$ , we simply note that  $E' = E/H$  reduces mod  $p$  to  $(E \otimes R/pR)/\text{Ker } F \cong (E \otimes R/pR)^{(p)}$ , which certainly has invertible Hasse invariant if  $E \otimes R/pR$  does - indeed  $E_{p-1}((E \otimes R/pR)^{(p)}, \omega^{(p)}, \alpha_n^{(p)}) = ((E_{p-1}(E \otimes R/pR, \omega, \alpha_n))^p$ . Hence  $E_{p-1}(E', \alpha'_n)$  is invertible in  $R$ . This concludes the proof of (3.1) in the case  $r=1$ .

3.5.0 The "general case" is unfortunately more difficult, and involves a somewhat detailed study of the formal group of an elliptic curve. Our method of constructing the canonical subgroup will be to first construct a finite flat subscheme of the formal group, then to show that it is in fact a subgroup which has the desired properties. We begin with some lemmas on the formal group.

### 3.6 Lemmas on the formal group

Lemma 3.6.1. Let  $R$  be an  $\mathbb{F}_p$ -algebra,  $E/R$  an elliptic curve, and  $\omega$  a nowhere vanishing differential. Let  $X$  be a parameter for the formal group of  $E/R$  (i.e., the completion of  $E$  along the identity section), which is dual to  $\omega$  in the sense that the expansion of  $\omega$  along the formal group is

$$\omega = (1 + \sum_{n \geq 1} a_n X^n) dX .$$

Let  $A(E, \omega)$  denote the Hasse invariant. Then we have the identities

$$a_{\frac{p^n - 1}{p-1}} = (A(E, \omega))^{p-1} \quad \text{for } n=1, 2, \dots .$$

Proof. Let  $C: \Omega^1_{E/R} \longrightarrow (\Omega^1_{E/R})^{(p)}$  denote the Cartier operator, "dual" to the endomorphism  $D \longrightarrow D^p$  of  $T^1_{E/R}$ . We have  $C(\omega) = A(E, \omega) \cdot \omega^{(p)}$ , but we may calculate  $C$  "locally":

$$C(a_n X^n dX) = \begin{cases} 0, & p \nmid n+1 \\ a_{\frac{n+1}{p-1}-1} (X^{\frac{n+1}{p-1}} dX)^{(p)} & \text{if } p \mid n+1 \end{cases}$$

Hence  $C(\omega) = \sum_{m \geq 0} a_{p(m+1)-1} (X^m dX)^{(p)}$ , and

$$C(\omega) = A(E, \omega) \cdot \omega^{\otimes p} = \sum A(E, \omega) (a_m)^p (X^m dX)^{(p)}, \text{ whence}$$

$$a_{p(m+1)-1} = A(E, \omega) \cdot (a_m)^p . \text{ As } a_0 = 1, \text{ the result follows easily.} \quad \text{QED}$$

Lemma 3.6.2. Let  $R$  be any  $\mathbb{Z}_p$ -algebra, and let  $G$  be a one-parameter formal group over  $R$ . Then

$$(1) \quad \text{End}_R(G) \supset \mathbb{Z}_p \quad \text{and} \quad \mathbb{Z}_p \text{ lies in the center of } \text{End}_R(G) .$$

(2) Given any parameter  $X_0$ , there exists a (non-unique!) parameter  $X = X_0 + \text{higher terms}$  such that for any  $p\text{-l}'\text{st root of unity}$   $\zeta \in \mathbb{Z}_p$ , we have  $[\zeta](X) = \zeta X$ .

Proof. Thanks to Lazard, we're reduced to the universal situation, which has  $R$  flat over  $\mathbb{Z}_p$ . So we may use log, exp, and continuity to get (1). As for (2), it is proven directly in ([31], lemma 4.12), or we can remark that any choice of a "p-typical coordinate"  $X$  (cf.[5], [6]) which is congruent to  $X_0 \pmod{\text{degree two terms}}$  will do the job.

Lemma 3.6.3. Let  $R$  be an  $\mathbb{F}_p$ -algebra,  $G$  a one-parameter formal group over  $R$ . In terms of any parameter  $X$ ,  $[p](X)$  is a function of  $X^p$ : i.e.

$$3.6.3.0 \quad [p](X) = V(X^p) = \sum_{n \geq 1} v_n X^{np}.$$

Proof. In  $\text{End}_R(G)$ ,  $p = V \circ F$ ,  $F: G \rightarrow G^{(p)}$ ,  $V: G^{(p)} \rightarrow G$ . QED

Lemma 3.6.4. Let  $R$  be a  $\mathbb{Z}_p$ -algebra,  $G$  a one-parameter formal group over  $R$ ,  $X$  a parameter on  $G$  such that  $[\zeta](X) = \zeta X$  for any  $p\text{-l}'\text{st root of unity}$   $\zeta \in \mathbb{Z}_p$ . Then  $[p](X) = X \cdot (\text{a series in } X^{p-1})$ .

Proof.  $[p](\zeta)(X) = [\zeta]([p](X))$  because  $p \cdot \zeta = \zeta \cdot p$  in  $\mathbb{Z}_p$ . Thus  $[p](\zeta X) = \zeta \cdot ([p](X))$ , so writing  $[p](X) = \sum e_n X^n$ , we have  $e_n \zeta^n = e_n \zeta$ , hence  $(\zeta - \zeta^n)e_n = 0$ . But for  $n \not\equiv 1 \pmod{p-1}$ ,  $\zeta - \zeta^n$  is invertible in  $\mathbb{Z}_p$ , hence  $e_n = 0$ . QED

Lemma 3.6.5. Let  $R$  be a  $\mathbb{Z}_p$ -algebra,  $G$  a one-parameter formal group over  $R$ ,  $X$  a parameter,  $\omega = (1 + \sum_{n \geq 1} a_n X^n) dX$  the dual invariant differential. Then we have

$$3.6.5.0 \quad [p](X) \equiv a_{p-1} \cdot X^p + \text{higher terms} \pmod{p}.$$

Proof. [In the application to elliptic curves, we have  $a_{p-1} = A(E, \omega)$ , and  $[p](X) = V(X^p) = \text{tangent}(V) \cdot X^p + \text{higher terms}$ , so the assertion is that  $A(E, \omega) = \text{tangent}(V) = \text{action of } F \text{ on } H^1(E, \mathcal{O})$ , which is true!]

By Lazard, we are reduced to the universal case, in which  $R$  is flat over  $\mathbb{Z}_p$ . Over  $R[1/p]$ , we have  $\omega = d\phi(X)$ ,  $\phi(X) \in R[1/p][[X]]$ ,  $\phi(X) = X + \sum_{n=2}^{p-2} a_n \frac{X^{n+1}}{n+1} + a_{p-1} \frac{X^p}{p} + \text{higher terms}$ . Let  $\psi(X)$  be the inverse series to  $\phi$ :  $\psi(X) = X + \dots, \psi(\phi(X)) = X$ . Then  $[p](X) = \psi(p \cdot \phi(X))$ .

Because  $\phi(X) \bmod p$  lies in  $X + X^2 R[[X]]$ , for each  $n \geq 2$ ,  $\phi(X)^n \bmod p$  lies in  $X^n + X^{n+1} R[[X]]$ . If we write  $\psi(X) = X + \sum_{i \geq 2} b_i X^i$ , we see from this and the requirement  $\psi(\phi(X)) = X$  that  $b_2, \dots, b_{p-1} \in R$ , while  $b_p \equiv -a_{p-1}/p$  modulo  $R$ . Now the term of degree  $p$  in  $[p](X) = \psi(p\phi(X))$  is given by

$$\sum_{i=1}^p b_i p^i \cdot (\text{coef of } X^p \text{ in } (\phi(X))^i) = a_{p-1} + \sum_{i=2}^{p-1} b_i p^i \cdot (\text{coef of } X^p \text{ in } \phi(X)^i) + b_p \cdot p^p,$$

and as  $p b_p \in R$ , we see that all the terms save  $a_{p-1}$  lie in  $pR$ . QED

We may summarize our findings in a proposition.

Proposition 3.6.6. Let  $R$  be a  $\mathbb{Z}_p$ -algebra,  $G$  a one-parameter formal group over  $R$ ,  $X$  a coordinate on  $G$  which satisfies  $[\zeta](X) = \zeta X$  for every  $p-1$ 'st root of unity  $\zeta \in \mathbb{Z}_p$ , and  $\omega$  the "dual" differential. Then

$$3.6.6.0 \quad [p](X) = pX + aX^p + \sum_{m=2}^{\infty} c_m \cdot X^{m(p-1)+1}$$

where  $a, c_2, c_3, \dots \in R$ , and  $c_r \in pR$  unless  $m(p-1)+1 \equiv 0(p)$ , i.e.,  $c_m \in pR$  unless  $m \equiv 1(p)$ . Further, if  $G$  is the formal group of an elliptic curve  $E/R$ , then  $a \equiv A(E, \omega) \bmod pR$ .

Proof. By (3.6.4),  $[p](X) = X \cdot (a \text{ series in } X^{p-1})$ , but modulo  $pR$ ,  $[p](X)$  is also a series in  $X^p$ , by (3.6.3). The congruence for  $a$  is by (3.6.1).

### 3.7 Construction of the canonical subgroup as a subscheme of the formal group

Suppose we are given  $(E/R, \alpha_n, Y)$  with  $R$  a  $p$ -adically complete  $\mathbb{R}_o$ -algebra,  $n \geq 1$  if  $p \neq 2, 3$ ,  $n \geq 3$  for  $p = 2, 3$ ,  $Y \cdot E_{p-1} = r$ ,  $\text{ord}(r) < p/p+1$ . Because it suffices to treat the case when  $r$  is nilpotent in  $R$ , we may, by ordinary localization on  $R$ , suppose that the formal group of  $E/R$  is given by a one-parameter formal group law over  $R$ , with formal parameter  $X$ ; we denote by  $\omega$  the "dual" differential. By reduction to the universal case, we may now reduce to the case when  $R$  is a flat  $\mathbb{Z}_p$ -algebra. By (3.6.2), we may suppose that  $[\zeta](X) = \zeta X$  for all  $p-1$ 'st roots of unity  $\zeta \in \mathbb{Z}_p$ . By (3.6.6), the endomorphism  $[p]$  on the formal group looks like

$$(3.7.0) \quad [p](X) = pX + aX^p + \sum_{m \geq 2} c_m X^{m(p-1)+1}$$

$$\text{with } \begin{cases} a \equiv E_{p-1}(E/R, \omega, \alpha_n) \pmod{pR} \\ c_m \equiv 0 \pmod{pR} \text{ unless } m \equiv 1 \pmod{p} \end{cases}.$$

We first give a heuristic for the method to be used.

Naively speaking, the kernel of  $[p]$  is an  $\mathbb{F}_p$ -vector space, and the canonical subgroup is just a nice choice of a line in this  $\mathbb{F}_p$ -space, i.e., it is an orbit of  $\mathbb{F}_p^X$  in this vector space. But the action of  $\mathbb{F}_p^X$  on  $\text{Ker}([p])$  is induced by the action of  $\mu_{p-1} \subset \mathbb{Z}_p^\times$  on the formal group. Thus we must write down the equation for the orbits of the action of  $\mu_{p-1}$  on  $\text{Ker}([p])$ , and somehow solve this equation in a "canonical" way. Because  $\zeta \in \mu_{p-1}$  acts on  $X$  by  $[\zeta](X) = \zeta X$ , it is natural to take  $T \stackrel{\text{dfn}}{=} X^{p-1}$  as a parameter for the space of orbits of the action of  $\mathbb{F}_p^*$  on  $\text{Ker}([p])$ . The formal identity (obtained from (3.6.6.0) by substituting  $T = X^{p-1}$ )

$$(3.7.1) \quad [p](X) = X \cdot (p + aT + \sum_{m \geq 2} c_m T^m)$$

suggests that in fact the equation for the orbits is

$$(3.7.2) \quad g(T) \stackrel{\text{dfn}}{=} p + aT + \sum_{m \geq 2} c_m T^m = 0,$$

and that the canonical subgroup is nothing more than a canonical zero of  $g(T)$ .

We now implement the above heuristically-motivated procedure. Let  $r_1 \in R_o$  be the element  $-p/r$ ; we have  $\text{ord}(r_1) = 1 - \text{ord}(r) > 1/p+1$ , (because  $\text{ord}(r) < p/p+1$  by hypothesis). Let  $Y = Y(E/R, \omega, \alpha_n) \in R$ ; we have  $Y \cdot E_{p-1}(E/R, \omega, \alpha_n) = r$ . Because  $a \equiv E_{p-1}(E/R, \omega, \alpha_n)$  modulo  $pR$ , we may write  $E_{p-1}(E/R, \omega, \alpha_n) = a + pb$ ,  $b \in R$ . Thus  $Y \cdot (a + pb) = r$ , and an immediate calculation shows that if we put

$$(3.7.4) \quad t_o = \frac{r_1 Y}{1 + r_1 b Y}$$

(which makes sense, because  $r_1$  is topologically nilpotent in  $R$ ), then  $p + at_o = 0$ .

Let's define  $g_1(T) = g(t_o T)$ ;

$$(3.7.5) \quad \begin{aligned} g_1(T) &= p + at_o T + \sum_{m \geq 2} c_m (t_o)^m T^m \\ &= p - pT + \sum_{r \geq 2} c_r (t_o)^m T^m. \end{aligned}$$

Let  $r_2 = (r_1)^{p+1}/p$ , an element of  $R_o$  having  $\text{ord}(r_2) > 0$ . Let  $r_3 \in R_o$  be any generator of the ideal  $(r_2, (r_1)^2)$  of  $R_o$ .

Lemma 3.7.6. We may write  $g_1(T) = p \cdot g_2(T)$ , with

$$(3.7.6.1) \quad \begin{aligned} g_2(T) &= 1 - T + \sum_{m \geq 2} d_m T^m, \\ \text{with } d_m &\in r_3 R, \text{ and } d_m \rightarrow 0 \text{ as } m \rightarrow \infty. \end{aligned}$$

Proof. We have  $d_m = c_m (t_o)^m / p$ . Because  $c_m / p$  lies in  $R$  if  $m \not\equiv 1 \pmod{p}$ , and because  $(t_o)^{p+1}/p$  lies in  $r_2 R$ , we have  $d_m \in r_3 R$  for all  $m \geq 2$ , and  $d_m \rightarrow 0$  as  $m \rightarrow \infty$ . We next apply Newton's lemma to  $R$ ,  $I = r_3 R$  and  $h = g_2$ .

Lemma 3.7.7. (Newton) Let  $R$  be a ring complete and separated with respect to powers of an ideal  $I \subset R$ . Let  $h(T) = 1 - T + \sum_{m=2}^{\infty} d_m T^m$ , with  $d_m \in I$ ,

and  $d_m \rightarrow 0$  as  $m \rightarrow \infty$ . By "substitution",  $h$  gives rise to a continuous function  $h: R \rightarrow R$ . There exists a unique element  $t_\infty \in T$  such that  $h(1 - t_\infty) = 0$ .

Proof. Making the substitution  $T = 1 - S$ , we introduce

$h_1(S) = h(1 - S) = e_0 + (1 + e_1)S + \sum_{m \geq 2} e_m S^m$ , with coefficients  $e_i \in I$ . For  $s \in I$ ,  $h_1(s) = h(1 - s)$ , so our problem is to show that  $h_1$  has a unique zero  $s_\infty$  in  $I$ . For any  $s \in I$ ,  $h_1'(s) \in 1 + I$ , hence is invertible in  $R$ , while  $h_1(s) \in I$ . The Newton process of successive approximations:

$s_0 = 0, \dots, s_{n+1} = s_n - h_1(s_n)/h_1'(s_n)$  is easily seen to converge to a zero of  $h_1$ . If  $s$  and  $s + \Delta$  are two zeros of  $h_1$  in  $I$ , we have  $0 = h_1(s + \Delta) = h_1(s) + h_1'(s) \cdot \Delta + (\Delta^2) = h_1'(s) \cdot \Delta + (\Delta^2)$ , hence as  $h_1'(s)$  is invertible, we have  $\Delta \in (\Delta^2)$ . Because  $\Delta \in I$  and  $R$  is  $I$ -adically separated, this implies  $\Delta = 0$ . QED

Tracing back our steps, we have constructed a zero  $t_{\text{can}} = t_0(1 - t_\infty)$  of  $g(T)$ . Because  $t_{\text{can}}$  lies in  $r_1 R$ , we may expand  $g$  in powers of  $T - t_\infty$ , and conclude that  $g(T)$  is divisible by  $T - t_{\text{can}}$  in  $R[[T]]$ . We define the canonical subscheme to be the finite flat rank  $p$  subscheme of  $\text{Ker}([p])$  defined by the equation  $x^p - t_{\text{can}} X$ . (It may be verified that this subscheme is independent of the choice of coordinate  $X$  on the formal group satisfying  $[\zeta](x) = \zeta X$  for all  $p$ -1'st roots of unity  $\zeta \in \mathbb{Z}_p^\times$ .)

### 3.8 The canonical subscheme is a subgroup

Let's begin by remarking that if  $E/R$  modulo  $p$  has invertible Hasse invariant, then  $[p](X) = pX + (\text{unit}) X^p + \dots$ . By the formal version of the Weierstrass Preparation Theorem, we see that in  $R[[X]]$ , we have  $[p](X) = (X^p - t_{\text{can}} X) \cdot (\text{a unit in } R[[X]])$ . Thus when Hasse is invertible mod  $p$ , the canonical subscheme is all of  $\text{Ker}([p])$  in the formal group, hence in particular it's a subgroup-scheme of the formal group.

In the general case, the condition that the subscheme of equation  $x^p - t_{\text{can}} X$  be a subgroup-scheme of the formal group is that, noting by  $G(X, Y)$  the group law, we have

$$(3.8.1) \quad G(X, Y)^p - t_{\text{can}} G(X, Y) = 0 \quad \text{in} \quad R[[X, Y]]/(x^p - t_{\text{can}} X, Y^p - t_{\text{can}} Y).$$

Because  $t_{\text{can}}$  lies in  $r_1 R$ , it is topologically nilpotent in  $R$ , hence the  $R$ -algebra  $\mathbb{A} = R[[X, Y]]/(x^p - t_{\text{can}} X, Y^p - t_{\text{can}} Y)$  is finite and free of rank  $p^2$  with basis  $X^i Y^j$ ,  $0 \leq i, j \leq p-1$ . The condition that  $G(X, Y)^p - t_{\text{can}} G(X, Y)$  vanish in  $\mathbb{A}$  is simply that the  $p^2$  "coefficients"  $g_{ij} \in R$  defined by the equation

$$(3.8.2) \quad G(X, Y)^p - t_{\infty} G(X, Y) = \sum_{0 \leq i, j \leq p-1} g_{ij} X^i Y^j \quad \text{in} \quad \mathbb{A}$$

all vanish in  $R$ . Thus it suffices to find a  $p$ -adically complete  $R_o$ -algebra  $R' \supset R$  such that, over  $R'$ , the canonical subscheme is a subgroup (for then the  $g_{ij}$  vanish in  $R'$ , hence vanish in  $R$ ). But in the universal situation,  $R = M(R_o, r, n, o) \subset R' = M(R_o, l, n, o)$ , and over  $R'$ ,  $E_{p-1}$  is invertible, hence Hasse mod  $p$  is invertible, and so as noted above the canonical subscheme is a subgroup over  $R'$ . This concludes the proof of part I of the main theorem (3.1).

(3.9) We now turn to proving part II of 3.1, by constructing  $Y'$ . As before we may suppose  $R$  flat over  $\mathbb{Z}_p$ . Let  $r \in R_o$  have  $\text{ord}(r) < 1/p+1$ . Then  $r_1 = p/r$  has  $\text{ord}(r_1) > p/p+1$ , and hence  $r_1$  is divisible by  $r^p$ , and  $r_4 = r_1/r^p$  has  $\text{ord}(r_4) > 0$ . Since  $t_{\text{can}} \in r_1 R$ , modulo  $r_1 R$  the canonical subgroup is just the kernel of  $F: E \rightarrow E^{(p)}$ . Hence  $E' \bmod r_1 R$  is  $E^{(p)}$ . Let  $\omega'$  be any nowhere vanishing one-form on  $E'$  which reduces modulo  $r_1 R$  to  $\omega^{(p)}$  on  $E^{(p)}$ . Hence we have the congruence

$$(3.9.1) \quad E_{p-1}(E'/R, \omega', \alpha'_n) \equiv (E_{p-1}(E, \omega, \alpha_n))^p \bmod r_1 R.$$

Because  $r_1 = r_4 \cdot r^p$ , we may write

$$(3.9.2) \quad E_{p-1}(E'/R, \omega', \alpha'_n) = (E_{p-1}(E/R, \omega, \alpha_n))^p + r^p r_4 j, \quad j \in R.$$

Using the equation

$$(3.9.3) \quad Y(E/R, \omega, \alpha_n) \cdot E_{p-1}(E/R, \omega, \alpha_n) = r$$

one immediately checks that if we define

$$(3.9.4) \quad Y'(E'/R, \omega', \alpha'_n) = (Y(E/R, \omega, \alpha_n))^p / l + r_4 j \cdot (Y(E/R, \omega, \alpha_n))^p,$$

then  $Y'(E'/R, \omega', \alpha'_n) \cdot E_{p-1}(E'/R, \omega', \alpha'_n) = r^p$ . This concludes the proof of part II. QED

### 3.10 Finiteness properties of the Frobenius endomorphism of p-adic modular functions.

Throughout the rest of this chapter, we denote by  $R_o$  a complete discrete valuation ring of mixed characteristic with perfect residue field  $R_o/m$ . The Frobenius endomorphism  $\varphi$  of  $S(R_o, l, n, k)$  is defined by  $\varphi(f)(E, \omega, \alpha_n, Y = (E_{p-1})^{-1}) = f(E/H, \pi^*(\omega), \pi(\alpha_n), Y' = l/E_{p-1})$ , where  $H$  denotes the canonical subgroup of  $E$ ,  $\pi: E \rightarrow E/H$  denotes the projection. As we have seen above, for  $r \in R_o$  having  $\text{ord}(r) < l/p+1$ , the composite  $(E_{p-1})^k \cdot \varphi$  "extends" to give a commutative diagram

$$\begin{array}{ccc} S(R_o, l, n, k) & \xrightarrow{\varphi} & S(R_o, l, n, k) \xrightarrow{(E_{p-1})^k} S(R_o, l, n, pk) \\ \downarrow & & \downarrow \\ S(R_o, r^p, n, k) & \dashrightarrow & S(R_o, r, n, pk) \end{array}$$

For  $k=0$ , we find simply that the endomorphism  $\varphi$  maps  $S(R_o, r^p, n, 0)$  to  $S(R_o, r, n, 0)$  for any  $r \in R_o$  having  $\text{ord}(r) < l/p+1$ .

Theorem 3.10.1. Suppose  $n \geq 3$  and  $p \nmid n$ , and  $n \leq 11$  if  $p=2$ . Then

I. For  $r \in R_o$  with  $\text{ord}(r) < 1/p+1$ , the Frobenius morphism

$\phi: S(R_o, r^p, n, 0) \longrightarrow S(R_o, r, n, 0)$  is a finite morphism (but not in general flat).

II. If  $r=1$ , then  $\phi$  is a finite flat morphism of degree  $p$ .

III. For any  $r$  with  $\text{ord}(r) < 1/p+1$ , the homomorphism ( $K$  the fraction field of  $R_o$ )

$$\phi \otimes K: S(R_o, r^p, n, 0) \otimes K \longrightarrow S(R_o, r, n, 0) \otimes K$$

is finite and etale of rank  $p$ .

Proof. (I). Because the ring  $S(R_o, r, n, 0)$  is complete and separated in the  $p$ -adic topology, to prove finiteness of  $\phi$  it suffices to prove that the induced homomorphism

$$3.10.2 \quad \phi \otimes R_o/\underline{m}: S(R_o, r^p, n, 0) \otimes R_o/\underline{m} \longrightarrow S(R_o, r, n, 0) \otimes R_o/\underline{m}$$

is finite. Interpreting  $S(R_o, r, n, 0)$  as  $H^0(\bar{M}_n(R_o, r), \mathcal{O})$  (cf. 2.9), and noting that  $\bar{M}_n(R_o, r)$  is flat over  $R_o$ , we see (by "universal coefficients") that the canonical homomorphism  $S(R_o, r, n, 0) \otimes R_o/\underline{m} \longrightarrow S(R_o/\underline{m}, r, n, 0)$  is injective, with cokernel of finite dimension over  $R_o/\underline{m}$ . Thus  $S(R_o/\underline{m}, r, n, 0)$  is a finite module over  $S(R_o, r, n, 0) \otimes R_o/\underline{m}$ , and we have a commutative diagram of ring homomorphisms

$$3.10.3 \quad \begin{array}{ccc} S(R_o/\underline{m}, r^p, n, 0) & \xrightarrow{\phi} & S(R_o/\underline{m}, r, n, 0) \\ \uparrow & & \uparrow \\ S(R_o, r^p, n, 0) \otimes R_o/\underline{m} & \xrightarrow{\phi \otimes R_o/\underline{m}} & S(R_o, r, n, 0) \otimes R_o/\underline{m} \end{array}$$

in which the vertical arrows are finite. Thus the finiteness of the lower horizontal arrow (which is what we wish to prove) follows from the finiteness of the upper horizontal arrow.

Notice that if  $r=1$ , both  $S(R_{\mathcal{O}}/\underline{m}, r, n, 0)$  and  $S(R_{\mathcal{O}}/\underline{m}, r^p, n, 0)$  are  $S(R_{\mathcal{O}}/\underline{m}, 1, n, 0)$ , while if  $0 < \text{ord}(r)$ , both  $S(R_{\mathcal{O}}/\underline{m}, r, n, 0)$  and  $S(R_{\mathcal{O}}/\underline{m}, r^p, n, 0)$  are  $S(R_{\mathcal{O}}/\underline{m}, 0, n, 0)$ . Because  $\text{ord}(r) < 1/p+1$ , both  $p/r$  and  $p/r^p$  lie in  $\underline{m}$ , and hence over  $R_{\mathcal{O}}/\underline{m}$  the canonical subgroup over  $\bar{M}_n(R_{\mathcal{O}}/\underline{m}, r)$  and over  $\bar{M}_n(R_{\mathcal{O}}/\underline{m}, r^p)$  is just the kernel of Frobenius. It follows immediately that in either case (i.e.,  $r=1$  or  $0 < \text{ord}(r) < 1/p+1$ ), the endomorphism  $\phi$  of  $S(R_{\mathcal{O}}/\underline{m}, r, n, 0)$  is precisely the  $p$ 'th power mapping (because  $\phi(f)(E, \omega, \alpha_n, Y) = f(E^{(p)}, \omega^{(p)}, \alpha_n^{(p)}, Y^p) = (f(E, \omega, \alpha_n, Y))^p$ ). But  $\bar{M}_n(R_{\mathcal{O}}/\underline{m}, r)$  is a scheme of finite type over  $R_{\mathcal{O}}/\underline{m}$ , hence  $S(R_{\mathcal{O}}/\underline{m}, r, n, 0)$  is a finitely generated  $R_{\mathcal{O}}/\underline{m}$ -algebra, hence finite over itself by the  $p$ 'th power endomorphism, which proves (I).

For (II), we remark that when  $r=1$ , the scheme  $\bar{M}_n(R_{\mathcal{O}}/\underline{m}, 1)$  is simply the open set of  $\bar{M}_n \otimes R_{\mathcal{O}}/\underline{m}$  where  $E_{p-1}$  is invertible, hence is a smooth affine curve over  $R_{\mathcal{O}}/\underline{m}$ . Hence the  $p$ 'th power endomorphism of its coordinate ring  $S(R_{\mathcal{O}}/\underline{m}, 1, n, 0)$  makes that ring finite and flat over itself of rank  $p$ . Because  $S(R_{\mathcal{O}}, 1, n, 0)$  is  $p$ -adically complete and flat over  $R_{\mathcal{O}}$ , it follows that  $\phi$  makes  $S(R_{\mathcal{O}}, 1, n, 0)$  into a finite flat module over itself of degree  $p$ .

The proof of (III) is more difficult, and requires Tate's theory of rigid analytic spaces. The ring  $S(R_{\mathcal{O}}, r, n, 0)$  is the  $p$ -adic completion of  $H^0(\bar{M}_n \otimes R_{\mathcal{O}}, \text{Symm}(\underline{\omega}^{\otimes p-1}))/(\underline{E}_{p-1} - r)$ , and this last algebra is finitely generated over  $R_{\mathcal{O}}$  (because  $\underline{\omega}$  has positive degree, hence is ample). Thus noting by  $K$  the fraction field of  $R_{\mathcal{O}}$ , we see that  $S(R_{\mathcal{O}}, r, n, 0) \otimes K$  is a rigid algebra in the sense of Tate, and contains as dense subalgebra the  $K$ -algebra  $H^0(\bar{M}_n \otimes K, \text{Symm}(\underline{\omega}^{\otimes p-1}))/(\underline{E}_{p-1} - r) \cong H^0(\bar{M}_n \otimes K, \text{Symm}(\underline{\omega}^{\otimes p-1}))/(\underline{E}_{p-1} - 1) \cong H^0(\bar{M}_n \otimes K, \text{Symm}(\underline{\omega}^{\otimes p-1})/(\underline{E}_{p-1} - 1))$ , which is precisely the coordinate ring  $D_n \otimes K$  of the open subset of  $\bar{M}_n \otimes K$  where  $\underline{E}_{p-1}$  is invertible. Thanks to Tate, the ideals of  $S(R_{\mathcal{O}}, r, n, 0) \otimes K$  are all closed, hence are the closures of their intersections with  $D_n \otimes K$ . But as  $D_n \otimes K$  is the coordinate ring of a smooth affine curve over  $K$ , its prime ideals are either minimal (corresponding

to irreducible components) or maximal (corresponding to conjugacy classes of points with values in finite extensions of  $K$ ). Indeed, the closed points of  $S(R_o, r, n, 0) \otimes K$  are conjugacy classes of homomorphisms  $\pi: S(R_o, r, n, 0) \rightarrow K'$ ,  $K'$  a finite extension of  $K$ , or equivalently they are homomorphisms  $\pi: D_n \otimes K \rightarrow K'$  which satisfy the continuity conditions  $|\pi(D_n)| \leq 1$ ,  $1 \geq |\pi(E_{p-1})| \geq |r|$  (i.e., that the images of  $E_{p-1}$  and of  $Y = r/E_{p-1}$  be "power bounded"). Further, the completions of the local rings at corresponding closed points are isomorphic, hence are regular local rings of dimension one, hence  $S(R_o, r, n, 0) \otimes K$  is a regular ring of dimension one. Thus the map

$$3.10.4 \quad S(R_o, r^p, n, 0) \otimes K \xrightarrow{\phi \otimes K} S(R_o, r, n, 0) \otimes K$$

is a finite morphism between regular rings of the same dimension, hence (cf. EGA IV, 17.3.5.2) is flat. To see that it has rank  $p$ , it suffices to note that by (II), it has rank  $p$  over the dense open set where  $|E_{p-1}| = 1$ . It remains only to see that (3.10.4) is étale. For this, it suffices to show that the fibre over each point with values in  $\Omega$ , the completion of the algebraic closure of  $K$ , consists of  $p$  distinct points. Over a point at infinity, corresponding to  $\text{Tate}(q^n)$  over  $K((q))$ , the fibre consists of the  $p$  curves  $\text{Tate}(\zeta_p^{q^{n/p}})$  over  $K((q))$ , each of which gives rise to  $\text{Tate}(q^n)$  upon division by its canonical subgroup  $\mu_p$ . A finite point is an elliptic curve  $E/\Omega$  [with level  $n$  structure  $\alpha_n$ ] having good reduction, such that for any differential  $\omega$  which extends to a nowhere vanishing differential over the valuation ring of  $\Omega$ , we have  $1 \geq |E_{p-1}(E/K, \omega)| \geq |r|^p$ . The curve  $E$  has  $p+1$  subgroups of order  $p$ , say  $H_0, H_1, \dots, H_p$ , of which  $H_0$  is the canonical subgroup.

Let  $E^{(i)} = E/H_i$ . The points lying over  $E$  are among the  $p+1$  curves  $E^{(i)}$ , ( $E^{(i)}$  carrying the induced level  $n$  structure); indeed,  $E^{(i)}$  lies over if and only if  $E^{(i)}$  is a point of  $S(R_o, r, n, 0) \otimes \Omega$  whose canonical subgroup is  $p/E_i$ .

Consider first the case in which  $|E_{p-1}(E/K, \omega)| = 1$ , i.e., a formal group of height one. Then  $H_0$  is the kernel of  $p$  in the formal group, while the  $H_i$ ,  $i \geq 1$ , meet the formal group only in  $\{0\}$ . The quotient  $E^{(0)} = E/H_0$  again has a formal group of "height one" hence its canonical subgroup is the kernel of  $p$  in its formal group, while the image of  $p^E$  in  $E^{(0)}$  meets the formal group only in  $\{0\}$ . Thus  $E^{(0)}$  does not lie over  $E$ . For  $i \geq 1$ , the quotient  $E^{(i)}$  also has a formal group of height one, but now the image of  $H_0$  in  $E^{(i)} = E/H_i$  is the kernel of  $p$  in the formal group, i.e., it is the canonical subgroup, and hence the  $E^{(i)}$ ,  $i=1,\dots,p$ , do lie over.

It remains to treat the case of "supersingular reduction", which we do by Lubin's original method, and show (part 5 of theorem 3.10.7) that again only  $E^{(1)}, \dots, E^{(p)}$  lie over.

(3.10.5) Let  $\Omega$  be an algebraically closed complete (under a rank one valuation) field of characteristic zero and residue characteristic  $p$ . Let  $R \subset K$  be the valuation ring, and let  $E/R$  be an elliptic curve over  $R$ , and  $X$  a parameter for the formal group of  $E/R$ , normalized by the condition  $[\zeta](X) = \zeta X$  for every  $p-1$ 'st root of unity in  $\mathbb{Z}_p$ . Suppose that the Hasse invariant of the special fibre vanishes. Then in the formal group, we have

$$(3.10.6) \quad [p](X) = pX + aX^p + \sum_{m=2}^p c_m X^{m(p-1)+1} + c_{p+1} X^{p^2} + \sum_{m \geq p+2} c_m X^{m(p-1)+1}$$

with  $\text{ord}(a) > 0$ ,  $\text{ord}(c_m) \geq 1$  for  $m \not\equiv 1 \pmod{p}$ , and  $\text{ord}(c_{p+1}) = 0$ , (this last because we suppose height two for the special fibre). [If  $\text{ord}(a) < 1$ , we have  $\text{ord}(a) = \text{ord } E_{p-1}(E/R, \omega)$  for any nowhere vanishing differential  $\omega$  on  $E/R$ , by (2.1).]

Theorem 3.10.7. (Lubin)

1. If  $\text{ord}(a) < p/p+1$ , the canonical subgroup  $H_0$  consists of  $\{0\}$  and the  $p-1$  solutions  $X$  of (3.10.6) whose ordinal is  $\frac{1-\text{ord}(a)}{p-1}$ . The  $p^2-p$  other solutions of (3.10.6) all have ordinal  $\frac{\text{ord}(a)}{p^2-p}$  (which is  $< \frac{1-\text{ord}(a)}{p-1}$ ). If  $\text{ord}(a) \geq p/p+1$ , then all non-zero solutions of (3.10.6) have ordinal  $1/p^{2-1}$ .

2. If  $\text{ord}(a) < 1/p+1$ , then the quotient  $E' = E/H_0$  has as normalized coordinate for its formal group  $X' = \prod_{x \in H_0} G(X, x)$ , where  $G(X, Y)$  denotes the formal group law on  $E$ . The expression of  $[p]$  on  $E/H_0$  is

$$[p](X') = pX' + a'(X')^p + \dots$$

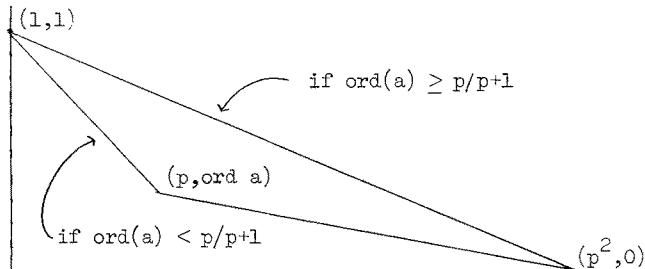
with  $\text{ord}(a') = p \text{ ord}(a)$ .

3. If  $1/p+1 < \text{ord}(a) < p/p+1$ , then  $\text{ord}(a') = 1 - \text{ord}(a)$ , and the canonical subgroup of  $E/H_0$  is  $pE/H_0$ , and  $(E/H_0)/H_0(E/H_0)$  is just  $E$ , (but a level  $n$  structure  $\alpha_n$  becomes  $p^{-1}\alpha_n$  after two divisions by the canonical subgroup - (compare Dwork [11], 8.11)).

4. If  $\text{ord}(a) \geq p/p+1$ , there exist  $p+1$  curves  $E^{(i)}$ , each having  $\text{ord}(a^{(i)}) = 1/p+1$ , such that  $E = E^{(i)}/H_0(E^{(i)})$ , where  $H_0(E^{(i)})$  denotes the canonical subgroup of  $E^{(i)}$ . These curves are  $E^{(i)} = E/H_i$ ,  $i = 0, 1, \dots, p$ .

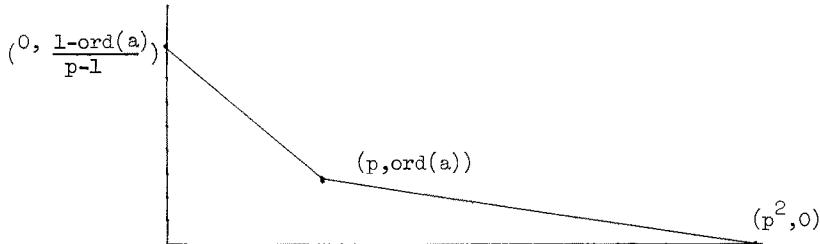
5. If  $0 < \text{ord}(a) < p/p+1$ , there exist precisely  $p$  curves  $E^{(i)}$  having  $\text{ord}(a_i) < 1/p+1$  such that  $E = E^{(i)}/H_0(E^{(i)})$ , namely the curves  $E^{(i)} = E/H_i$ ,  $i = 1, \dots, p$  (cf. 3.10.4ff), and  $\text{ord}(a_i) = \frac{1}{p} \text{ ord}(a)$ .

Proof. 1. follows from looking at the Newton polygon of  $[p](X)$ , which is



and remarking that the construction of the canonical subgroup as subscheme of the formal group consisted precisely of isolating the factor of  $[p](X)$  corresponding to the first slope, when there is a first slope.

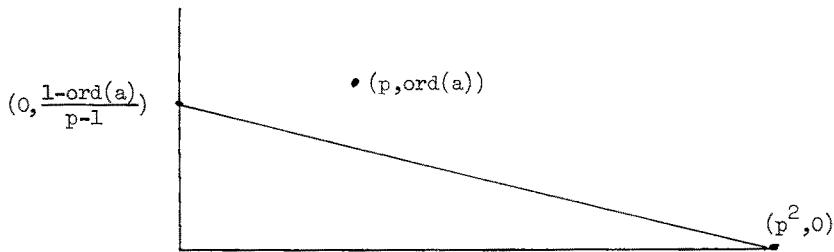
2. By Lubin ([32]), we know that if  $H$  is any finite subgroup of a one-parameter formal group over  $R_O$ , then  $X \rightarrow \prod_{x \in H} G(X, x)$  is the projection onto the quotient. Thus the non-zero points of order  $p$  on  $E/H_O$  are of two sorts, the points  $\prod_{x \in H_O} G(y, x)$  with  $[p](y) = 0$ ,  $\text{ord}(y) = \frac{\text{ord}(a)}{p^2-p}$ , and the points  $\prod_{x \in H_O} G(z, x)$  where  $[p](z) \in H_O$ ,  $[p](z) \neq 0$ . The first sort of point has ordinal given by  $\sum_{x \in H_O} \text{ord}(G(y, x))$ , and as  $\text{ord}(y) < \text{ord}(x)$  for any  $x \in H_O$ , this sum is just  $p(\text{ord } y) = \frac{\text{ord}(a)}{p-1}$ . The second sort of point has ordinal  $\sum_{x \in H_O} \text{ord}(G(z, x))$ . From the equation  $[p](z) \in H_O - \{0\}$ , we see that  $\text{ord}([p](z)) = \frac{1-\text{ord}(a)}{p-1}$ . The Newton polygon of  $[p](z) = z \in H_O - \{0\}$  is thus



and hence  $z$  has either ordinal  $\text{ord}(a)/p^2-p$  or  $\frac{1-p}{p-1} \text{ord}(a)$ . In either case,  $\text{ord}(z) < \text{ord}(x)$  for any  $x \in H_O$ . Hence the second sort of point has ordinal either  $\text{ord}(a)/p-1$  or  $(1-p \text{ord}(a))/p-1$ . Thus among the non-zero points of order  $p$  on  $E/H_O$ , there are two distinct ordinals which occur, namely  $\text{ord}(a)/p-1$  and  $(1-p \text{ord}(a))/p-1$ , of which the greater is  $(1-p \text{ord}(a))/p-1$ .

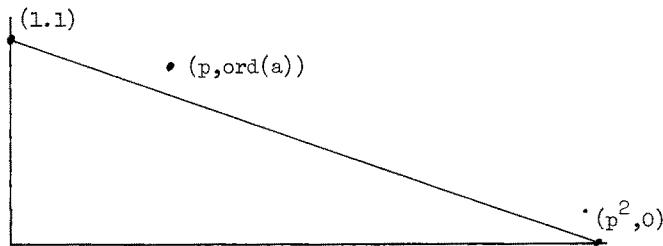
Thus by 1,  $E/H_O$  has  $\text{ord}(a') < p/p+1$ , and  $\frac{1-\text{ord}(a')}{p-1} = \frac{1-p \text{ord}(a)}{p-1}$ , which proves 2. We note that the image of  $\frac{E}{p}$  is not the canonical subgroup.

3. If we suppose  $1/p+1 < \text{ord}(a) < p/p+1$ , then on  $E/H_0$  the first sort of points of order  $p$  are the points  $\prod_{x \in H_0} G(y, x)$  for each  $y$  such that  $[p](y) = 0$ ,  $y \notin H_0$ . As in 2, these points have ordinal  $\text{ord}(a)/p-1$ . The second sort are the points  $\prod_{x \in H_0} G(z, x)$  where  $[p](z) \in H_0 - \{0\}$ , hence  $[p](z)$  has ordinal  $\frac{1-\text{ord}(a)}{p-1}$ . Their hypothesis  $\text{ord}(a) > 1/p+1$  insures that the Newton polygon of  $[p](Z) = x \in H_0 - \{0\}$  is



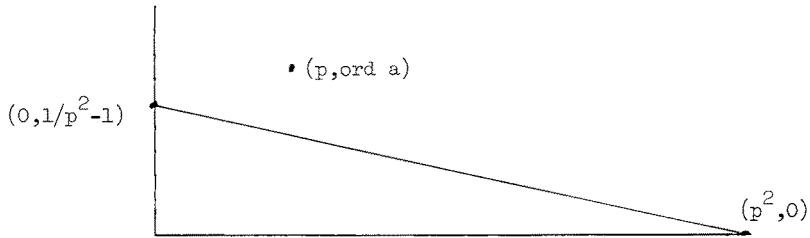
hence  $\text{ord}(z) = \frac{1-\text{ord}(a)}{p^2(p-1)} < \text{ord}(x)$  for any  $x \in H_0$ , hence the second sort of point has ordinal  $1 - \text{ord}(a)/p(p-1)$ . Thus  $E/H_0$  has a canonical subgroup, namely its points of order  $p$  of largest ordinal =  $\text{ord}(a)/p-1$ . Hence  $\frac{1-\text{ord}(a')}{p-1} = \text{ord}(a)/p-1$ , whence  $\text{ord}(a') = 1 - \text{ord}(a)$ , and the canonical subgroup is the image of all the points of order  $p$  on  $E$ .

4. If  $\text{ord}(a) \geq p/p+1$ , the Newton polygon of  $[p](X)$  is



Hence all non-zero points of order  $p$  have the same ordinal  $1/p^2-1$ . The points  $z$  such that  $[p](z) = x$ ,  $[p](x) = 0$ ,  $x \neq 0$ , have ordinal  $1/p^2(p^2-1)$ ,

because the Newton polygon of  $[p](Z) = x$ ,  $\text{ord}(x) = 1/p^2 - 1$ , is



Thus for any subgroup  $H_i$  of order  $p$  of  $E$ , the first sort of point of order  $p$  has  $\text{ord} = \sum_{x \in H_i} \text{ord}(G(y, x)) \geq p \text{ord}(y) = p/p^2 - 1$  (since  $\text{ord}(y) = \text{ord}(x)$  if  $x \neq 0$ ). The second sort of point has ordinal  $p \cdot \text{ord}(z) = 1/p(p^2 - 1)$ , (because  $\text{ord}(z) < \text{ord}(x)$  for any  $x \in H_i$ ). But  $p/p^2 - 1 > 1/p(p^2 - 1)$ , hence each  $E/H_i$  has a canonical subgroup, which is the image of  $\frac{p}{p}E$ . Looking at the ordinals of the non-canonical points of order  $p$  on  $E/H_i$ , we have by (3.10.7.1) the equality  $\text{ord}(a')/p^2 - p = 1/p(p^2 - 1)$ , hence  $\text{ord}(a') = 1/p + 1$ .

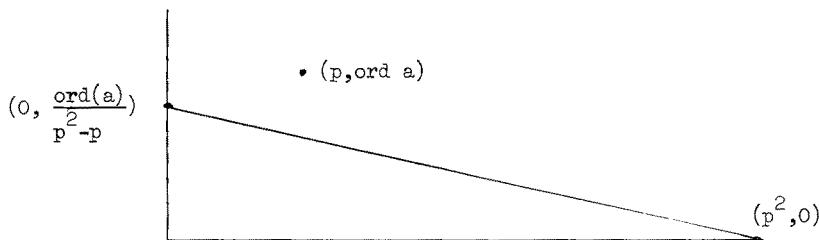
5. We first remark that if  $\text{ord}(a) < p/p+1$ , then  $E' = E/H$  either has  $\text{ord}(a') > 1/p+1$ , or its canonical subgroup is not the image of  $\frac{p}{p}E$  and hence  $E'/H(E') \neq E$ . Indeed, if  $\text{ord}(a) < 1/p+1$ , then as noted in the proof of 2., the canonical subgroup is not the image of  $\frac{p}{p}E$ . If  $\text{ord}(a) = 1/p+1$ , then as proven in 4.,  $\text{ord}(a') \geq p/p+1$ . If  $\text{ord}(a) > 1/p+1$ , then  $\text{ord}(a') = 1 - \text{ord}(a)$ , and  $1 - \text{ord}(a) > 1/p+1$  because  $\text{ord}(a) < p/p+1$ . It remains to see that for each non-canonical subgroup  $H_i$ ,  $i = 1, \dots, p$ ,  $E^{(i)} = E/H_i$  has  $\text{ord}(a^{(i)}) = \frac{1}{p} \text{ord}(a_i)$ , and its canonical subgroup is the image of  $\frac{p}{p}E$ .

Again we calculate the ordinals of the points of order  $p$  on  $E/H_i$ . The first sort of points are all images of points of the canonical subgroup  $H_0$  of  $E$  (because  $\frac{p}{p}E = H_0 \oplus H_i$  for  $i = 1, \dots, p$ ). For  $y \in H_0 - \{0\}$ ,  $\text{ord } G(y, 0) = \text{ord } y = \frac{1 - \text{ord}(a)}{p-1}$ , while  $\text{ord}(G(y, x)) = \text{ord } x = \frac{\text{ord}(a)}{p^2 - p}$  because  $\text{ord}(y) > \text{ord } x$  if  $x \in H_i - \{0\}$ . Hence the image of  $y \in H_0 - \{0\}$  has

$$\text{ordinal} = \text{ord}(y) + \sum_{x \in H_i - \{0\}} \text{ord}(x) = \frac{1-\text{ord}(a)}{p-1} + p-1 \cdot \frac{\text{ord}(a)}{p^2-p} = \frac{1-\text{ord}(a)}{p-1} + \frac{\text{ord}(a)}{p}.$$

What about the image of a point  $z$  such that  $[p](z) \in H_i - \{0\}$ ?

The Newton polygon of  $[p](z) = x$ ,  $x \in H_i - \{0\}$ , is



hence  $\text{ord}(z) = \text{ord}(a)/p^2(p^2-p) = \text{ord}(x)/p^2$  for  $x \in H_i - \{0\}$ . Thus  $\text{ord}(z) < \text{ord}(x)$ , hence the second sort of points of order  $p$  on  $E^{(i)}$  have  $\text{ordinal} = p \cdot \text{ord}(z) = \text{ord}(a)/p(p^2-p)$ . But  $\frac{1-\text{ord}(a)}{p-1} + \frac{\text{ord}(a)}{p} > \text{ord}(a)/p(p^2-p)$  (because  $\text{ord}(a) < p/p+1 < p^2/p+1$ ), hence  $E^{(i)}$  has a canonical subgroup, and  $\frac{1-\text{ord}(a^{(i)})}{p-1} = \frac{1-\text{ord}(a)}{p-1} + \frac{\text{ord}(a)}{p}$ , hence  $\text{ord}(a^{(i)}) = \text{ord}(a)/p$ . This concludes the proof of 5., and also of theorem (3.10.7).

### 3.11 Applications to the congruences of Atkin - the U operator

We maintain the notations of the previous section. As we have seen, for each  $r \in R_0$  having  $\text{ord}(r) < 1/p+1$ , the homomorphism  $\varphi: S(R_0, r^p, n, 0) \longrightarrow S(R_0, r, n, 0)$  is finite, and becomes finite and flat of degree  $p$  when we tensor with  $K$ . Thus there is defined the trace morphism

$$3.11.1 \quad \text{tr}_\varphi: S(R_0, r, n, 0) \otimes K \longrightarrow S(R_0, r^p, n, 0) \otimes K.$$

For  $r=1$ ,  $\varphi$  is itself finite flat of degree  $p$ , hence there is defined

$$3.11.2 \quad \text{tr}_\varphi: S(R_0, 1, n, 0) \longrightarrow S(R_0, 1, n, 0).$$

In terms of  $q$ -expansion, we have

$$3.11.3 \quad (\text{tr}_\varphi(f))(\text{Tate}(q^n), \omega_{\text{can}}, \alpha_n) = \sum_{\zeta^p=1} f(\text{Tate}(\zeta q^{n/p}), \omega_{\text{can}}, \frac{1}{p} \pi_\zeta(\alpha_n))$$

where  $\pi_\zeta(\alpha_n)$  denotes the induced level  $n$  structure on  $\text{Tate}(\zeta q^{n/p})$ , viewed as a quotient of  $\text{Tate}(q^n)$ . Equivalently, if we write

$$3.11.3.1 \quad f(\text{Tate}(q^n), \omega_{\text{can}}, \alpha_n) = \sum A_i(\alpha_n) q^i$$

then we have the formula (in which  $\alpha''_n$  is the level  $n$  structure on  $\text{Tate}(q^n)$  obtained as the inverse image of  $\pi_o(\alpha_n)$  on  $\text{Tate}(q^{n/p})$  by the extension of scalars  $q^{1/p} \rightarrow q$ , compare pp.32-33)

$$3.11.3.2 \quad (\text{tr}_\varphi(f))(\text{Tate}(q^n), \omega_{\text{can}}, \alpha_n) = p \cdot \sum A_{pi} \left( \frac{1}{p} \alpha''_n \right) q^i.$$

Notice that we have the relation, for any  $f \in S(R_o, r, n, 0) \otimes K$ ,

$$3.11.3.3 \quad p \cdot T_p(f) = \text{tr}_\varphi(I_p^*(f)) + \varphi(f)$$

(where  $I_p^*(f)(E/R, \omega, \alpha_n) \stackrel{\text{dfn}}{=} f(E/R, \omega, p \cdot \alpha_n)$ ), which should be viewed as the "canonical  $p$ -adic lifting" of the Eichler-Shimura congruence relation (compare Deligne [7]).

Integrality Lemma 3.11.4. For any  $r \in R_o$  with  $\text{ord}(r) < 1/p+1$ , we have  $\text{tr}_\varphi(S(R_o, r, n, 0)) \subset S(R_o, r^p, n, 0)$  (although  $\varphi: S(r_o, r^p, n, 0) \rightarrow S(R_o, r, n, 0)$  is finite but not flat if  $\text{ord}(r) > 0$ !).

Proof. We may suppose  $\text{ord}(r) > 0$ , the case  $r=1$  being trivial. It follows (from Tate [45]) that for any finite flat morphism  $\varphi: A \rightarrow B$  of rigid algebras over  $K$ , we have  $\text{tr}_\varphi$  (power-bounded elements of  $B$ )  $\subset$  power-bounded elements of  $A$ . Thus we must show that the power-bounded elements of  $S(R_o, r, n, 0) \otimes K$  are precisely  $S(R_o, r, n, 0)$ . For this, we introduce the finitely generated  $R_o$ -algebra  $B = H^0(\bar{M}_n \otimes R_o, \underline{\text{Symm}}(\underline{\omega}^{\otimes p-1})) / (E_{p-1} - r)$ . Its  $p$ -adic completion  $\hat{B} \stackrel{\text{dfn}}{=} \lim_{\leftarrow} B/p^N B$  is  $S(R_o, r, n, 0)$ , and indeed via the

isomorphism (2.6.2.1),  $B$  corresponds to the  $R_{\circ}$ -submodule of  $B^{\text{rigid}}(R_{\circ}, r, n, 0)$  consisting of all finite sums, which shows incidentally that  $B$  is a (free and hence) flat  $R_{\circ}$ -module, and that  $B/\underline{m}B \cong \hat{B}/\underline{m}\hat{B}$ . The fact that  $E_{p-1}$  modulo  $\underline{m}$  has simple zeros implies that  $B/\underline{m}B$  is reduced. (Indeed,  $B/\underline{m}B$  is  $H^0(M_n \otimes R_{\circ}/\underline{m}, \text{Symm}(\omega^{\otimes p-1})/(E_{p-1}))$ , and if  $\sum_0^N f_i$  represents a nilpotent element, with minimal  $N$ , then a power of  $f_N$  is divisible by  $E_{p-1}$ , hence  $f_N$  is divisible by  $E_{p-1}$ , which contradicts the minimality of  $N$ .) We may thus conclude by the following lemma.

Lemma 3.11.5. Let  $R_{\circ}$  be a complete discrete valuation ring,  $B$  a flat finitely-generated  $R_{\circ}$ -algebra such that  $\hat{B}/\underline{m}\hat{B}$  is reduced. Then the set of power-bounded elements of  $\hat{B} \otimes K$  is  $\hat{B}$ .

Proof. Since  $\hat{B}$  is flat over  $B$ , hence over  $R_{\circ}$ , we have  $\hat{B} \subset \hat{B} \otimes K$ , so the statement makes sense. By Tate, we know that any power-bounded element of  $\hat{B} \otimes K$  is integral over  $\hat{B}$ , so we must show that  $\hat{B}$  is integrally closed in  $\hat{B} \otimes K$ . Let  $\pi$  be a uniformizing parameter of  $R_{\circ}$ . If  $f \in \hat{B}$  and  $f/\pi$  is integral over  $\hat{B}$ , then clearing the denominators in the equation shows that  $f$  is a nilpotent element of  $\hat{B}/\underline{m}\hat{B}$ , hence  $f \in \underline{m}\hat{B} = \pi\hat{B}$ . QED

3.11.6. We now define Atkin's operator  $U: S(R_{\circ}, r^p, n, 0) \otimes K \longrightarrow S(R_{\circ}, r^p, n, 0)$  to be the composite

$$S(R_{\circ}, r^p, n, 0) \otimes K \xrightarrow{\quad} S(R_{\circ}, r, n, 0) \otimes K \xrightarrow{\frac{1}{p} \text{tr} \Phi} S(R_{\circ}, r^p, n, 0) \otimes K.$$

Thus if  $f \in S(R_{\circ}, r^p, n, 0)$  has  $q$ -expansions

$$3.11.6.1 \quad f(\text{Tate}(q^n), \omega_{\text{can}}, \alpha_n) = \sum_i A_i (\alpha_n) q^i$$

then  $Uf \in S(R_{\circ}, r^p, n, 0) \otimes K$  has  $q$ -expansions

$$3.11.6.2. \quad (Uf)(\text{Tate}(q^n), \omega_{\text{can}}, \alpha_n) = \sum_i A_{pi} \left( \frac{1}{p} \alpha_n^i \right) \cdot q^i.$$

[This formula shows that  $U(S(R_{\circ}, 1, n, 0)) \subset S(R_{\circ}, 1, n, 0)$ ]. It is not true in

general that  $U(S(R_0, r^p, n, 0)) \subset S(R_0, r^p, n, 0)$ , but the situation is as good as if it were true, as Dwork was the first to realize.

Lemma 3.11.7. (Dwork) Suppose  $p \geq 7$ , and suppose  $r \in R_0$  satisfies the inequality

$$\frac{2}{3(p-1)} < \text{ord}(r) < \frac{1}{p+1} .$$

Then the  $R_0$ -submodule  $S(R_0, r^p, n, 0) + U(S(R_0, r^p, n, 0))$  of  $S(R_0, r^p, n, 0) \otimes K$  is U-stable.

Remark 3.11.8. The point is that the submodule  $S(R_0, r^p, n, 0) + U(S(R_0, r^p, n, 0))$  contains  $S(R_0, r^p, n, 0)$  and is contained in  $\frac{1}{p} S(R_0, r^p, n, 0)$ , hence it defines the same topology on  $S(R_0, r^p, n, 0) \otimes K$  as  $S(R_0, r^p, n, 0)$ . Thus in an equivalent norm on  $S(R_0, r^p, n, 0) \otimes K$ ,  $U$  has operator norm  $\leq 1$ .

Proof. Let's use the representation (2.6.2.1) of elements of  $S(R_0, r^p, n, 0)$  in the form  $f = \sum_{a \geq 0} \frac{r^{pa} \cdot b_a}{(E_{p-1})^a}$ . The hypothesis insures that for  $a \geq 2$ ,  $\text{ord}(r^{pa}/p \cdot r^a) > 0$ , and hence

$$3.11.9. \quad f = b_0 + \frac{r^p \cdot b_1}{E_{p-1}} + p \cdot (\text{an element of } \frac{r^{2(p-1)}}{p} S(R_0, r, n, 0)) .$$

Because  $pU = \text{tr}_\varphi$  maps  $S(R_0, r, n, 0)$  to  $S(R_0, r^p, n, 0)$ , we have

$$3.11.10. \quad U(f) = U(b_0) + U\left(\frac{r^p b_1}{E_{p-1}}\right) + \text{an element of } \frac{r^{2(p-1)}}{p} S(R_0, r^p, n, 0) .$$

Since  $b_0$  is just a constant, we have  $U(b_0) = b_0$ , and hence it suffices to show that for any  $b_1 \in H^0(\bar{M}_n \otimes R_0, \underline{\omega}^{\otimes p-1})$ , we have

$$3.11.11. \quad U^2\left(\frac{r^p b_1}{E_{p-1}}\right) \subset S(R_0, r^p, n, 0) + U(S(R_0, r^p, n, 0)) .$$

For this, notice that  $rb_1/E_{p-1}$  lies in  $S(R_0, r, n, 0)$ , hence

$$3.11.12. \quad \text{tr}_{\varphi} \left( \frac{r^p b_1}{E_{p-1}} \right) = \sum_{a \geq 1} \frac{r^{pa} b_a'}{(E_{p-1})^a} .$$

The hypotheses insure that  $\text{ord}(\frac{r^{p-1}}{p} \cdot r^{pa}/p \cdot r^a) > 0$  if  $a \geq 2$ , and hence

$$3.11.13. \quad U \left( \frac{r^p b_1}{E_{p-1}} \right) = \frac{r^{p-1}}{p} \text{tr}_{\varphi} \left( \frac{r^p b_1}{E_{p-1}} \right) = \frac{r^{p-1}}{p} \left( b_0' + \frac{r^p b_1'}{E_{p-1}} \right) + \\ + p \text{ (an element of } \frac{r^{3(p-1)}}{p^2} S(R_o, r, n, 0)) .$$

Notice that  $U \left( \frac{r^p b_1}{E_{p-1}} \right)$  has q-expansions divisible by  $r^p$ , as does

$p \cdot (\text{any element of } S(R_o, r^p, n, 0))$ , and hence so does

$$(r^{p-1}/p) \left( b_0' + \frac{r^p b_1'}{E_{p-1}} \right) = \frac{r^{p-1}}{p} \left( \frac{b_0' E_{p-1} + r^p b_1'}{E_{p-1}} \right) ,$$

and hence so does  $\frac{r^{p-1}}{p} (b_0' E_{p-1} + r^p b_1')$ . By the q-expansion principle, there exists an element  $b_1'' \in H^0(\bar{M}_n \otimes R_o, \omega^{\otimes p-1})$  such that

$$\frac{r^{p-1}}{p} (b_0' E_{p-1} + r^p b_1') = r^p b_1'', \text{ hence } \frac{r^{p-1}}{p} \left( b_0' + \frac{r^p b_1'}{E_{p-1}} \right) = \frac{r^p b_1''}{E_{p-1}} , \text{ hence}$$

$$U \left( \frac{r^p b_1}{E_{p-1}} \right) = \frac{r^p b_1''}{E_{p-1}} + p \cdot (\text{an element of } \frac{r^{3(p-1)}}{p^2} S(R_o, r, n, 0)) .$$

Again using the fact that  $pU = \text{tr}_{\varphi}$  maps  $S(R_o, r, n, 0)$  to  $S(R_o, r^p, n, 0)$ ,

we find

$$U^2 \left( \frac{r^p b_1}{E_{p-1}} \right) = U \left( \frac{r^p b_1''}{E_{p-1}} \right) + \text{an element of } S(R_o, r^p, n, 0) ,$$

which proves (3.11.11) and the lemma.

QED

3.12 p-adic Hecke operators

For any prime number  $\ell$  which is prime to both  $p$  and to the level  $n$ , we may define  $T_\ell$  on  $S(R_0, r, n, 0)$  by the usual formula

$$3.12.1 \quad (T_{\ell f})(E/R, \omega, \alpha_n, Y) = \ell^{k-1} \sum f(E_R, /K, \check{\pi}^*(\omega), \pi(\alpha_n), \check{\pi}^*(Y))$$

the sum extended to the  $\ell+1$  subgroups  $K$  of order  $\ell$ . The various  $T_\ell$  commute with each other, and for  $k=0$  they all commute with  $U$ .

We may consider the "spectral decomposition" of the  $K$ -Banach space  $S(R_0, r^p, n, 0) \otimes K$  with respect to  $U$  (which is completely continuous, because the inclusion  $S(R_0, r^p, n, 0) \otimes K$  into  $S(R_0, r, n, 0) \otimes K$  is). For any rational number  $v$ , the subspace

$$3.12.3 \quad \bigcup_{m \geq 1} \bigcup_{\alpha \in K^{\text{alg. cl.}} \text{ of ordinal } v} \text{Ker}(U - \alpha)^m$$

of  $S(R_0, r^p, n, 0) \otimes K$  is finite-dimensional, and is stable by  $U$  and the  $T_\ell$ . By Dwork's lemma (3.11.7), this subspace is reduced to  $\{0\}$  unless  $v \geq 0$ . The first interesting case is thus to take  $v=0$ , the so-called "unit-root subspace" of  $S(R_0, r^p, n, 0) \otimes K$ . [Notice that this unit root subspace is independent of the choice of  $r \in R_0$  with  $1/p+1 > \text{ord}(r) > 0$ , because  $U$  maps  $S(R_0, r, n, 0) \otimes K$  to  $S(R_0, r^p, n, 0) \otimes K$ , i.e. it improves growth conditions. Thus if  $f \in S(R_0, r, n, 0) \otimes K$  is annihilated by  $(U - \alpha)^m$ , and  $\alpha \neq 0$ , then  $f$  is a  $K(\alpha)$ -linear combination of  $U(f), U^2(f), \dots, U^m(f)$ , hence in fact  $f \in S(R_0, r^p, n, 0) \otimes K, \dots$ .]

Lemma 3.12.4. (Dwork) Hypotheses as in (3.11.7), the dimension of the unit root subspace of  $S(R_0, r^p, n, 0) \otimes K$  is at most  $\dim_K H^0(\bar{M}_n \otimes K, \omega^{\otimes p-1})$ .

Proof. The dimension of the unit root subspace is the number of unit zeros of the Fredholm determinant of  $U$ , which by (3.11.8) lies in  $R_0[[T]]$ , hence this dimension is also the degree of this Fredholm determinant reduced modulo  $\underline{m}$ , which is to say the degree of the determinant of  $U$  on  $(S(R_0, r^p, n, 0) + U(S(R_0, r^p, n, 0))) \otimes_{R_0} R_0/\underline{m}$ .

But for  $f \in S(R_0, r^p, n, 0)$ ,  $f = \sum_{a \geq 0} \frac{r^{pa} b_a}{(E_{p-1})^a}$ , we have  
 $U(f) = b_0 + U(\frac{r^{p_b}}{E_{p-1}})$  modulo  $\underline{m} \cdot S(R_0, r^p, n, 0)$  and  
 $U^2(f) = U(\frac{r^{p_b''}}{E_{p-1}})$  modulo  $\underline{m} \cdot S(R_0, r^p, n, 0)$ . Thus the image of  $U$  on  
 $(S(R_0, r^p, n, 0) + U(S(R_0, r^p, n, 0)) \otimes R/\underline{m}$  is spanned by the images under  $U$  of  
all elements  $b_0 \in H^0(\bar{M}_n \otimes R_0, \mathcal{O})$  and  $\frac{r^{p_b}}{E_{p-1}}$  with  
 $b_1 \in B(R_0, n, k, 1) \xrightarrow{\sim} H^0(\bar{M}_n \otimes R_0, \underline{\omega}^{\otimes p-1})/E_{p-1} H^0(\bar{M}_n \otimes R_0, \mathcal{O})$ . Thus the rank  
of  $U$  on  $(S(R_0, r^p, n, 0) + U(S(R_0, r^p, n, 0)) \otimes R_0/\underline{m}$  is at most the K-dimension  
of  $H^0(\bar{M}_n \otimes K, \underline{\omega}^{\otimes p-1})$ .

### 3.13 Interpretation of Atkin's congruences on $j$

We denote by  $j$  the absolute  $j$ -invariant, viewed as a modular function of level one, defined over  $\mathbb{Z}$ , having a first order pole at infinity. As is well known,  $p \cdot T_p(j)$  lies in  $\mathbb{Z}[j]$ . By inverse image we may view both  $j$  and  $p \cdot T_p(j)$  as elements of  $M(R_0, r, n, 0)$  for any  $r \in R$ . We may also view  $\phi(j)$  as an element of  $M(R_0, r, n, 0)$ , for any  $r \in R_0$  having  $\text{ord}(r) < p/p+1$  [indeed,  $\phi(j)(E, Y) = j(E/H)$ ,  $H$  the canonical subgroup]. Subtracting, we define  $p \cdot U(j) = p \cdot T_p(j) - \phi(j) \in M(R_0, r, n, 0)$ . Because  $j$  has only a first order pole at  $\infty$ ,  $U(j)$  is holomorphic at infinity, indeed its  $q$ -expansion is

$$3.13.1 \quad U(j)(\text{Tate}(q)) = \sum_{n \geq 0} c(pn) q^n, \quad \text{where}$$

$$3.13.2 \quad j(\text{Tate}(q)) = \sum_{n \geq -1} c(n) q^n = \frac{1}{q} + 744 + \dots.$$

Thus  $U(j)$  lies in  $S(\mathbb{Z}_p, 1, n, 0)$ , and  $p \cdot U(j)$  lies in  $S(R_0, r, n, 0)$  for any  $r \in R_0$  having  $\text{ord}(r) < p/p+1$ . Combining this observation with the

remark (3.11.8), we see that for every  $m \geq 1$ , we have

$$U^m(j) \in S(\mathbb{Z}_p, l, n, 0) \cap p^{-2} \cdot S(R_0, r, n, 0).$$

Let us examine explicitly the congruence consequences of the innocuous statement " $U(j) \in S(\mathbb{Z}_p, l, n, 0) \cap p^{-1} S(R_0, r, n, 0)$  whenever  $\text{ord}(r) < p/p+1$ ". Suppose that  $p \neq 2, 3$ , so that we may work directly with  $S(R_0, r, l, 0)$  via its basis as constructed in (2.6.2.1). We may write

$$3.13.3.0 \quad U(j) = \sum_{a \geq 0} \frac{b_a}{(E_{p-1})^a}, \quad b_a \in B(\mathbb{Z}_p, l, 0, a).$$

For  $r \in R_0$  with  $\text{ord}(r) < p/p+1$ , we have  $p \cdot b_a \in r^a B(R_0, l, 0, a)$ , hence we have  $p b_a \in p^{\{ap/p+1\}} B(\mathbb{Z}_p, l, 0, a)$ , where  $\{ap/p+1\}$  denotes the least integer  $\geq ap/p+1$ . Thus  $b_0 \in \mathbb{Z}_p$ ,  $b_1 \in B(\mathbb{Z}_p, l, 0, 1)$ ,  $b_a \in p^{a-1} B(\mathbb{Z}_p, l, 0, a)$  for  $2 \leq a \leq p$ ,  $b_{p+1} \in p^{p-1} B(\mathbb{Z}_p, l, 0, a), \dots$ , certainly  $b_a \in p^{n+1} B(\mathbb{Z}_p, l, 0, a)$  if  $a > p^n$ , for  $n \geq 1$ . Thus

$$3.13.3.1 \quad U(j) \equiv \sum_{a=0}^{p^n} \frac{b_a}{(E_{p-1})^a} \pmod{p^{n+1} S(\mathbb{Z}_p, l, 1, 0)}$$

$$3.13.3.2 \quad U(j) \equiv \frac{\sum_{a=0}^{p^n} b_a \cdot (E_{p-1})^{p^n-a}}{(E_{p-1})^p} \pmod{p^{n+1} S(\mathbb{Z}_p, l, 1, 0)}.$$

Using the fact that  $E_{p-1}$  has q-expansion  $\equiv 1(p)$ , and hence that  $(E_{p-1})^p$  has q-expansion  $\equiv 1(p^{n+1})$ , we deduce that for  $p \neq 2, 3$ , the q-expansion of  $U(j)$  is congruent mod  $p^{n+1}$  to the q-expansion of a true modular form of level one, defined over  $\mathbb{Z}$ , holomorphic at  $\infty$ , of weight  $p^n(p-1)$ . In fact, using  $(E_{p-1})^p$  to kill the constant term, we find that  $U(j) - 744$  has q-expansion congruent mod  $p^{n+1}$  to the q-expansion of a cusp form of level one and weight  $p^n(p-1)$ , defined over  $\mathbb{Z}$ , a result obtained independently by Koike [28].

We now return to the properly Atkin-esque aspects of the  $U^n(j)$ , and their interpretation.

Lemma 3.13.4. Suppose there exists a  $p$ -adic unit  $a \in \mathbb{Z}_p^\times$  such that for every  $m \geq 1$ , we have the  $q$ -expansion congruences

$$U^{m+1}(j-744) \equiv a U^m(j-744) \pmod{p^m} \text{ in } q\text{-expansion}$$

$$\text{i.e., } c(p^{m+1} i) \equiv ac(p^m i) \pmod{p^m} \text{ for all } m \geq 1.$$

Let  $c_\infty(i) = \lim_m a^{-m} c(p^m i)$ . Then for  $r \in R_0$  having  $\text{ord}(r) < p/p+1$ , there is a unique element " $\lim$ "  $a^{-m} U^m(j-744) \in S(\mathbb{Z}_p, 1, n, 0) \cap p^{-2} S(R_0, r, n, 0)$  which is of level one (i.e., invariant under  $\text{GL}_2(\mathbb{Z}/n\mathbb{Z})$ ), whose  $q$ -expansion is  $\sum_{m \geq 1} c_\infty(i) q^i$ , and which is fixed by  $a^{-1} U$ .

Proof. By (2.7), the hypothesis is in fact equivalent to the congruences

$$3.13.4.1 \quad (a^{-1} U)^{m+1}(j-744) \equiv (a^{-1} U)^m(j-744) \pmod{p^m S(\mathbb{Z}_p, 1, n, 0)}.$$

Let's write the expression of  $(a^{-1} U)^m(j-744)$  in terms of the base of  $S(\mathbb{Z}_p, 1, n, 0)$ :

$$3.13.4.2 \quad (a^{-1} U)^m(j-744) = \sum_{a \geq 0} \frac{b_a(m)}{(E_{p-1})^a}, \quad b_a(m) \in B(\mathbb{Z}_p, n, 0, a).$$

Then we have the congruences  $b_a(n+1) \equiv b_a(n) \pmod{p^n B(\mathbb{Z}_p, n, 0, a)}$ , we may define  $b_a(\infty) = \lim_m b_a(m) \in B(\mathbb{Z}_p, n, 0, a)$ . But for any  $r \in R_0$  with  $\text{ord}(r) < 1/p+1$ , we have  $p^2 b_a(m) \in r^a B(R_0, n, 0, a)$ , hence  $p^2 b_a(\infty) \in r^a B(R_0, n, 0, a)$ . Varying  $(R_0, r)$ , we see that in fact  $p^2 b_a(\infty)$  lies in  $p^{\lfloor ap/p+1 \rfloor} B(\mathbb{Z}_p, n, 0, a)$ , where  $\lfloor x \rfloor$  denotes the least integer  $\geq x$ , (i.e.,  $\lfloor x \rfloor = -[-x]$ ). Hence  $\sum \frac{b_a(\infty)}{(E_{p-1})^a} \stackrel{\text{def}}{=} \text{"lim"}(a^{-1} U)^m(j-744)$  lies in  $S(\mathbb{Z}_p, 1, n, 0) \cap p^{-2} S(R_0, r, n, 0)$ , and in  $S(\mathbb{Z}_p, 1, n, 0)$  it is the limit (in the Banach space topology of  $(a^{-1} U)^m(j-744)$ ).

The last two assertions are obviously true for  $r=1$ , by passage to the limit, and follow for any  $r$  of  $\text{ord}(r) < p/p+1$  because the canonical map  $S(R_0, r, n, 0) \longrightarrow S(R_0, 1, n, 0)$  is injective. QED

Remark 3.13.5. The hypotheses of the lemma are in fact satisfied for  $p = 13$ , a striking result due to Atkin.

(3.13.6) Using the fact that the twelfth power  $\underline{\omega}^{\otimes 12}$  of  $\underline{\omega}$  descends to the invertible sheaf  $\mathcal{O}(1)$  on the projective  $j$ -line over  $\mathbb{Z}$ , one can copy the construction of a basis of  $S(R_o, r, n, 0)$ ,  $n \geq 3$ , to get a basis of  $S(R_o, r, 1, 0) \xrightarrow{\text{dfn}} S(R_o, r, n, 0)^{GL_2(\mathbb{Z}/n\mathbb{Z})}$  for primes  $p \equiv 1 \pmod{12}$ . Then one can copy the proof given in ([14]) to show that the dimension of the unit root subspace of  $S(R_o, r, 1, 0) \otimes K$  is at most  $\dim H^0(\mathbb{P}^1, \underline{\omega}^{\otimes p-1}) = \dim H^0(\mathbb{P}^1, \mathcal{O}(\frac{p-1}{12})) = 1 + \frac{p-1}{12}$ , for  $p \equiv 1 \pmod{12}$ . In particular, for  $p = 13$ , the unit root space has a base consisting of the constant function and the function "lim"  $(a^{-1}U)^m(j-744)$ , and this latter function is necessarily the unique "unit root cusp form" in  $S(R_o, r, 1, 0)$ . This unicity, together with the stability of the space of unit root cusp forms under the Hecke operators  $T_\ell$ ,  $\ell \neq 13$ , gives a startling result of Atkin.

Theorem 3.13.7. (Atkin) The 13-adic modular function

"lim"  $(a^{-1}U)^m(j-744) = \sum_{i \geq 1} c_\infty(i)q^i$  is a simultaneous eigenfunction of all the Hecke operators  $T_\ell$ ,  $\ell \neq 13$ .

(3.13.8) Using the fact that  $\underline{\omega}^{\otimes 2}$  descends to the invertible sheaf  $\mathcal{O}(1)$  on the projective  $\lambda$ -line  $\bar{M}_2$  over  $\mathbb{Z}[1/2]$ , one may construct as above a base of  $S(R_o, r, 2, 0)$ , and prove as above that the unit root subspace of  $S(R_o, r, 2, 0) \otimes K$  has dimension at most  $\dim H^0(\bar{M}_2, \underline{\omega}^{\otimes p-1}) = \dim H^0(\mathbb{P}^1, \mathcal{O}(\frac{p-1}{2})) = 1 + \frac{p-1}{2}$ , for  $p$  odd. In fact, Dwork has proven that in this case the dimension is exactly  $1 + \frac{p-1}{2}$ , (cf. his exposé in this volume).

(3.13.9) Dwork's result implies that for  $p \equiv 1 \pmod{12}$ , the dimension of the unit root subspace of  $S(R_o, r, 1, 0)$  is precisely  $1 + \frac{p-1}{12}$ , and hence that there are precisely  $\frac{p-1}{12}$  independent unit root cusp forms in  $S(R_o, r, 1, 0)$ .

For  $p = 13$ , this fact together with the "accident"  $c(13) \not\equiv 0 \pmod{13}$ , implies Atkin's result that  $a$  and " $\lim_m (a^{-1}U)^m$ " ( $j=744$ ) exist.

Chapter 4.  $p$ -adic representations and congruences for modular forms4.1  $p$ -adic representations and locally free sheaves

Let  $q$  be a power of  $p$ ,  $k$  a perfect field containing  $\mathbb{F}_q$ ,  $W_n(k)$  its ring of Witt vectors of length  $n$ , and  $S_n$  a flat affine  $W_n(k)$ -scheme whose special fibre is normal, reduced and irreducible. Suppose that  $S_n$  admits an endomorphism  $\phi$  which induces the  $q$ -th power mapping on the special fibre. [If  $S_n$  is affine and smooth over  $W_n(k)$ , then such a  $\phi$  always exists.]

Proposition 4.1.1 There is an equivalence of categories between the category of finite free  $W_n(\mathbb{F}_q)$ -modules  $M$  on which  $\pi_1(S_n)$  acts continuously, and the category of pairs  $(H, F)$  consisting of a locally free sheaf of finite rank  $H$  on  $S_n$  together with an isomorphism  $F: \phi^*(H) \xrightarrow{\sim} H$ .

Construction-proof. Given a representation  $M$  of  $\pi_1(S_n)$ , let  $T_n$  be a finite étale Galois  $S_n$ -scheme such that the representation factors through  $\text{Aut}(T_n/S_n)$ . Because  $T_n$  is étale over  $S_n$ , there is a unique  $\phi$ -linear endomorphism of  $T_n$  which induces the  $q$ -th power endomorphism of  $T_n \times_{W_n(k)} k$ , which we denote by  $\phi_T$ . By unicity,  $\phi_T$  commutes with  $\text{Aut}(T_n/S_n)$ . Let  $H_T$  be the  $T_n$ -module  $M \otimes_{W_n(\mathbb{F}_q)} \mathcal{O}_{T_n}$ , and let  $F_T$  be the  $\phi_T$ -linear endomorphism of  $H_T$  defined by  $F_T(m \otimes f) = m \otimes \phi_T(f)$ . For each  $g \in \text{Aut}(S_n)$ , we define  $g(m \otimes f) = g(m) \otimes (g^{-1})^*(f)$ , thus defining an action of  $\text{Aut}(T_n/S_n)$  on  $(H_T, F_T)$ . By descent, it follows that there is a unique  $(H, F)$  on  $S_n$  whose inverse image on  $T_n$  is  $\text{Aut}(T_n/S_n)$ -isomorphic to  $(H_T, F_T)$ . The construction  $M \rightsquigarrow (H, F)$  defines the functor we will prove to be an equivalence. Notice that we can recover  $M$  as the fixed points of  $F_T$  acting as  $\phi$ -linear endomorphisms of the module of global sections of  $H_T$ , hence our functor is fully faithful. To show that it is an equivalence, we must show that any  $(H, F)$  arises in this way, or, in concrete terms, we must show that given  $(H, F)$ , there exists a finite étale covering  $T_n$  of  $S_n$  over which  $H$  admits a basis

of  $F$ -fixed points. We proceed by induction on the integer  $n$ .

Suppose first  $n=1$ . Then  $S$  is a  $k$ -scheme, and  $(H, F)$  is a locally free finite rank  $S$ -module  $H$  together with a  $q$ -linear endomorphism  $F$  of  $H$  which gives an isomorphism  $F : H^{(q)} \rightarrow H$ . For any  $S$ -scheme  $T$ , the inverse image module  $H_T$  carries the inverse image  $q$ -linear map  $F_T$ , defined by  $(F_T(h \otimes t)) = F(h) \otimes t^q$ , which gives an isomorphism  $F_T : H_T^{(q)} \rightarrow H_T$ .

Notice that the functors on  $S$ -schemes

$$\left\{ \begin{array}{l} X(T) = \text{global sections of } H_T \\ Y(T) = \text{bases of } H_T \text{ } (\mathcal{O}_T\text{-isomorphisms } (\mathcal{O}_T)^r \rightarrow H_T \text{, where } r = \text{rank}(H)) \\ Z(T) = \text{bases of } H_T \text{ consisting of fixed points of } F_T \end{array} \right.$$

are all representable, the first by  $\text{Spec}_S(\text{Symm}(H))$ , the second by the open subset of the  $r = \text{rank}(H)$ -fold product  $X_{(r/S)} = X \times_S X \dots \times_S X$  over which the tautological map  $(\mathcal{O}_{X(r/S)})^r \rightarrow H_{X(r/S)}$  is an isomorphism, the third by the closed subscheme of  $Y$  over which the universal basis is fixed by  $F_Y$ . We must show that  $Z$  is finite and étale over  $S$ . This problem is local on  $S$ , hence we may assume  $S$  affine and  $H$  free. Choose a basis  $h_1, \dots, h_r$  of  $H$ , and let  $(a_{ij})$  be the invertible matrix of  $F : F(h_i) = \sum_j a_{ji} h_j$ .

Consider the functor on  $S$ -schemes

$$Y'(T) = \text{sections of } H_T \text{ fixed by } F_T.$$

It is representable by a scheme finite and étale of rank  $q^r$  over  $S$ , because a section  $\sum_i x_i h_i$  of  $H$  is  $F$ -fixed if and only if  $\sum_j x_j h_j = \sum_i (x_i)^q \sum_j a_{ji} h_j$ , thus  $Y'$  is the closed subscheme of  $\mathbb{A}_S^r$  defined by the equation

$$x_j = \sum_i a_{ji} (x_i)^q, \quad j=1, \dots, r.$$

Because the matrix  $(a_{ij})$  is invertible, if we denote by  $(b_{ij})$  its inverse, the equations are the same as the equations

$$(x_i)^q = \sum_j b_{ij} x_j \quad i=1, \dots, r,$$

which define a finite étale  $S$ -scheme of rank  $q^r$ .

The scheme  $Z$  is the open subscheme of  $Y^{(r/S)} = Y' \times_S \dots \times_Y'$  where the universal  $r$ -tuple of  $F$ -fixed sections form a base of  $H$ , and hence  $Z$  is étale over  $S$ . It remains to check that  $Z$  is proper over  $S$ , and non-void. By the valuative criterion, we must show that for any valuation ring  $V$  over  $S$ , any  $F$ -fixed basis of  $H_K$  ( $K$  the fraction field of  $V$ ) prolongs to an  $F$ -fixed basis of  $H_V$ . Because the scheme  $Y'$  of fixed points is finite over  $S$ , each basis element prolongs to a unique  $F$ -fixed section of  $H_V$ . To see that the corresponding map  $V^r \rightarrow H_V$  is an isomorphism, we look at its determinant, which reduces us to the case of a rank one module. Then the matrix of  $F$  is  $F(h_1) = ah_1$ , with  $a$  invertible in  $V$ , and an  $F$ -fixed basis of  $H_K$  is a vector  $k \cdot h_1$ , with  $k \in K$  satisfying  $k = ak^p$ . As  $a \in V$  is invertible in  $V$ , any such  $k$  is an invertible element of  $V$ , hence  $k \cdot h_1$  "is" an  $F$ -fixed base of  $H_V$ .

It remains to see that  $Z$  is non-empty. As its formation commutes with arbitrary change of base  $S' \rightarrow S$ , it's enough to check the case when  $S$  is the spectrum of an algebraically closed field. But a finite-dimensional vector space over an algebraically closed field with a  $q$ -linear automorphism is always spanned by its fixed points (Lang's trick; cf. [23]) and the set of fixed bases is a  $GL_r(\mathbb{F}_q)$ -torsor. Thus  $Z$  is finite étale of rank  $= \#GL_r(\mathbb{F}_q)$  over  $S$ , and the action of  $GL_r(\mathbb{F}_q)$  on  $Z$  (induced by its action on the functor of  $F$ -fixed bases) makes  $Z$  into a  $GL_r(\mathbb{F}_q)_S$ -torsor. The cohomology class of this torsor is an element of  $H_{et}^1(S, GL_r(\mathbb{F}_q)) = \text{Hom}(\pi_1(S), GL_r(\mathbb{F}_q))$  which is none other than the desired representation. This concludes the construction-proof for  $n=1$ .

Suppose the result known for  $n-1$ . Then there is a finite étale covering  $T_{n-1}$  of  $S_{n-1} = S_n \times_{W_n(k)} W_{n-1}(k)$  over which  $H/p^{n-1}H$  admits a

basis of  $F$ -fixed points. There is a unique finite étale covering  $T_n$  of  $S_n$  such that  $T_n \times_{S_n} S_{n-1}$  is  $T_{n-1}$ , and replacing  $S_n$  by  $T_n$  we may suppose that  $H/p^{n-1}H$  admits a basis of  $F$ -fixed points. Let  $h_1, \dots, h_r$  be a basis of  $H$  which lifts an  $F$ -fixed basis of  $H/p^{n-1}H$  ( $S_n$  is affine!). Writing  $\underline{h} = \begin{pmatrix} h_1 \\ \vdots \\ h_r \end{pmatrix}$ , we have  $F(\underline{h}) = (1 + p^{n-1}\Delta)\underline{h}$ . In order for  $(1 + p^{n-1}E) \cdot \underline{h}$  to be an  $F$ -fixed basis, we must have

$$(1 + p^{n-1} \cdot \phi(E)) \cdot (1 + p^{n-1}\Delta)\underline{h} = (1 + p^{n-1}E)\underline{h}$$

or equivalently ( $S_n$  being flat over  $W_n(k)$ )

$$\phi(E) + \Delta \equiv E \pmod{(p)},$$

which is a set of  $r^2$  Artin-Schreier equations  $(e_{ij})^q - e_{ij} = -\Delta_{ij}$  over  $S_1 = S_n \times_{W_n(k)} k$ . On a finite étale covering  $T_1$  of  $S_1$ , these equations admit solutions, and hence on the unique finite étale covering  $T_n$  of  $S_n$  such that  $T_n \times_{S_n} S_1 = T_1$ , the module  $H_{T_n}$  admits an  $F$ -fixed basis. QED

Remarks 4.1.2.1 The operation "tensor product" in the category of representations of  $\pi_1(S_n)$  in finite free  $W_n(\mathbb{F}_q)$  modules corresponds to the tensor product  $(H, F) \otimes (H', F') = (H \otimes H, F \otimes F')$ , defined by  $(F \otimes F)(h \otimes h') = F(h) \otimes F'(h')$ .

(4.1.2.2) The "internal Hom" in the category of representations corresponds to the internal Hom defined by  $\underline{\text{Hom}}((H, F), (H_1, F_1)) = (\underline{\text{Hom}}_{\mathcal{O}}(H, H_1), F_2)$  where  $F_2$  is the unique  $\phi$ -linear endomorphism of  $\underline{\text{Hom}}_{\mathcal{O}}(H, H_1)$  such that for  $h \in H, f \in \underline{\text{Hom}}(H, H_1)$ , we have  $F_2(f)(F(h)) = F_1(f(h))$ . In particular,  $\underline{\text{Hom}}((H, F), (\mathcal{O}, \phi))$  is the "contragredient"  $(\check{H}, \check{F})$ , defined by the requirement that for  $h \in H, \check{h} \in \check{H}$ , we have  $\langle F(h), \check{F}(\check{h}) \rangle = \phi(\langle h, \check{h} \rangle)$ .

(4.1.2.3) Because  $S_1$  is normal, reduced and irreducible, a representation of  $\pi_1(S_m) = \pi_1(S_1)$  is just a suitably unramified representation of the Galois group of the function field of  $S_1$ . Thus for any non-void open set  $U \subset S_n$ ,

the functor "restriction" from the category of representations of  $\pi_1(S_n)$  to the category of representations of  $\pi_1(U)$  is fully faithful. Hence the functor "restriction" from the category of  $(H, F)$ 's over  $S_n$  to the category of those over  $U$  is fully faithful.

#### 4.2. Application to modular schemes

4.2.0. Let  $n \geq 3$ ,  $p$  a prime not dividing  $n$ ,  $q$  a power of  $p$  such that  $q \equiv 1 \pmod{n}$ , and choose an isomorphism between  $\mu_n$  and  $\mathbb{Z}/n\mathbb{Z}$  over  $W(\mathbb{F}_q)$ , i.e. choose a primitive  $n$ 'th root of unity  $\zeta$ . Let  $S_m^\zeta$  (resp.  $\bar{S}_m^\zeta$ ) be the open subset of  $M_n \otimes W_m(\mathbb{F}_q)$  (resp. of  $\bar{M}_n \otimes W_m(\mathbb{F}_q)$ ) where  $E_{p-1}$  is invertible and where the e.m. pairing on the basis of  ${}_n E$  has the value  $\zeta$ , i.e. where the determinant of the level  $n$  structure is the chosen isomorphism of  $\mathbb{Z}/n\mathbb{Z}$  with  $\mu_n$ . The schemes  $S_m^\zeta$  (resp.  $\bar{S}_m^\zeta$ ) are smooth affine  $W_m(\mathbb{F}_q)$  schemes with geometrically connected fibres. In the notation of (2.9), we have  $M_n(W_m(\mathbb{F}_q), 1) = \cup S_m^\zeta$ , the union taken over the primitive  $n$ 'th roots of unity, and  $\bar{M}_n(W_m(\mathbb{F}_q), 1) = \cup \bar{S}_m^\zeta$ .

Let  $\sigma$  denote the Frobenius automorphism of  $W_m(\mathbb{F}_q)$ . We have  $\sigma(\zeta) = \zeta^p$ , and hence  $S_m^{\zeta^p} = (S_m^\zeta)^{(\sigma)}$ ,  $\bar{S}_m^{\zeta^p} = (\bar{S}_m^\zeta)^{(\sigma)}$ . The endomorphism  $\phi$  of  $M_n(W_m(\mathbb{F}_q), 1)$  defined by "division by the canonical subgroup" does not respect the various  $\bar{S}_m^\zeta$ , but rather it maps  $\bar{S}_m^\zeta$  to  $\bar{S}_m^{\zeta^p}$  (because modulo  $p$ , the canonical subgroup is the kernel of absolute Frobenius). As  $\bar{S}_m^{\zeta^p} = (\bar{S}_m^\zeta)^{(\sigma)}$ , we may and will view  $\phi$  as a  $\sigma$ -linear endomorphism of each  $S_m^\zeta$ , which modulo  $p$  becomes the  $p$ 'th power mapping. In a similar fashion, the endomorphism  $\phi$  of the invertible sheaf  $\underline{\omega}^{\otimes k}$  on  $\bar{M}_n(W_m(\mathbb{F}_q), 1)$ , defined by  $\phi(f)(E, \omega, \alpha_n) = f(E/H, \pi^*(\omega), \pi(\alpha_n))$  [where  $H$  denotes the canonical subgroup and  $\pi: E \rightarrow E/H$  the projection], may be viewed as a  $\phi$ -linear endomorphism of  $\underline{\omega}^{\otimes k}|_{\bar{S}_m^\zeta}$ , for each primitive  $n$ 'th root of unity  $\zeta$ . [Notice that  $\underline{\omega}^{\otimes k}$  is generated by  $\phi(\underline{\omega}^{\otimes k})$  as a sheaf; indeed for a local section  $f$  of  $\underline{\omega}^{\otimes k}$ , a glance at  $q$ -expansions shows that  $\phi(f) \equiv f^p/(E_{p-1})^k$ , hence  $\phi(f)$  is an

invertible section wherever  $f$  is.]

We wish to determine which representation of  $\pi_1(\bar{S}_m^\zeta)$  in a free  $\mathbb{Z}/p^m\mathbb{Z} = W_m(\mathbb{F}_p)$ -module of rank one corresponds via (4.1.1) to  $(\underline{\omega}^{\otimes k}, \varphi)$  on  $\bar{S}_m^\zeta$ . Of course it suffices to do this for  $k=1$ , by (4.1.2.1). There is an obvious candidate, namely the representation of  $\pi_1(\bar{S}_m^\zeta)$  on the étale quotient of the kernel of  $p^m$  on the universal curve  $E$ . [Noting by  $\pi: E \xrightarrow{(\varphi)} E/H$  the projection onto the quotient by the canonical subgroup, the composite  $\pi_m: E \xrightarrow{\pi^m} E/\ker(\pi^m)$  induces an isomorphism of the étale quotient  $\frac{E}{p^m} = \frac{E}{p^m} / \ker(\pi^m) \xrightarrow{\cong} \ker(\pi)^m$  in  $E^{(\varphi^m)}$ .] If this candidate is to "work", we must have:

Lemma 4.2.1. The representation of  $\pi_1(\bar{S}_m^\zeta)$  on  $\ker(\pi)^m$  extends to a representation of  $\pi_1(\bar{S}_m^\zeta)$ , i.e., it is "unramified at  $\infty$ ".

Proof. Since the étale topology cannot distinguish  $\bar{S}_m^\zeta$  and  $\bar{S}_1^\zeta$ , it is equivalent to show that the representation of  $\pi_1(\bar{S}_1^\zeta)$  on  $\ker(\pi^m)$  extends to a representation of  $\pi_1(\bar{S}_1^\zeta)$  on  $\ker(\pi^m)$ . Let  $K$  denote the function field of  $\bar{S}_1^\zeta$ ; we must see that the inertia group of  $\text{Gal}(K^{\text{sep}}/K)$  at each cusp acts trivially on  $\ker(\pi^m)$  in  $E_K^{(p^m)}(K^{\text{sep}})$ . To decide, we may replace  $K$  by its completion at each cusp, which is just  $k((q))$ ,  $k = \mathbb{F}_q!$ , and the inverse image of  $E$  over this completion is the Tate curve  $\text{Tate}(q^n)/k((q))$ . The curve  $E^{(p^m)}$  becomes  $\text{Tate}(q^{np^m})$ , and  $(\pi)^m$  is the map  $\text{Tate}(q^{np^m}) \rightarrow \text{Tate}(q^n)$  given by "division by the subgroup generated by  $q^{n^m}$ ". As this subgroup consists entirely of rational points, the inertial group (and even the decomposition group) at each cusp acts trivially.

Theorem 4.2.2. The representation of  $\pi_1(\bar{S}_m^\zeta)$  on  $\ker(\pi)^m$  ( $\cong$  to the étale quotient of  $\ker p^m$  on the universal curve) corresponds, via the equivalence (4.1.1), to  $(\underline{\omega}, \varphi)$ .

Proof. By the "full-faithfulness" of restriction to open sets, it suffices to prove this over  $S_m^\zeta$ . Let's take a finite étale covering  $T$  of  $S_m$  which

trivializes the representation - in concrete terms, we adjoin the coordinates of a point of  $\text{Ker}(\check{\pi})^m$  of order precisely  $p^m$ . Over  $T$ , each point of  $\text{Ker}(\check{\pi})^m$  gives a morphism  $(\mathbb{Z}/p^m\mathbb{Z})_T \xrightarrow{\sim} (\text{Ker}(\check{\pi})^m)_T$ , whose Cartier dual is a morphism  $(\text{Ker } p^m \text{ in } \hat{E})_T = (\text{Ker } \pi^m)_T \longrightarrow (\mu_{p^m})_T \hookrightarrow (\mathbb{G}_m)_T$ . The inverse image of the invariant differential  $dt/t$  on  $(\mathbb{G}_m)_T$  furnishes an invariant differential on the kernel of  $p^m$  in  $\hat{E}$ . Since  $T$  is killed by  $p^m$ , the first infinitesimal neighborhood of the identity section of  $E$  lies in the kernel of  $p^m$  in  $\hat{E}$ , and hence there is a unique invariant differential on  $E$  whose restriction to the kernel of  $p^m$  in  $\hat{E}$  is the given one. Thus we have defined a morphism from  $(\text{Ker}(\check{\pi})^m)_T$  to  $\omega_T$ . Further, if we take a point of  $\text{Ker}(\check{\pi})^m$  of order precisely  $p^m$ , the map  $(\mathbb{Z}/p^m\mathbb{Z})_T \longrightarrow (\text{Ker}(\check{\pi})^m)_T$  is an isomorphism, hence the Cartier dual is an isomorphism, and hence the inverse image of  $dt/t$  on  $\text{Ker } p^m$  in  $\hat{E}$  is nowhere vanishing. Thus the induced map  $(\text{Ker}(\check{\pi})^m)_T \otimes_{\mathbb{Z}/p^m\mathbb{Z}} \mathcal{O}_T \longrightarrow \omega_T$  is an isomorphism of invertible sheaves on  $T$ . It is clear that this map commutes with the obvious action of  $\text{Aut}(T/S_m^\zeta)$ . [In concrete terms, and locally on  $S$ ,  $\text{Ker}(p^m)$  in  $\hat{E}$  has coordinate ring free on  $1, X, \dots, X^{p^m-1}$ , a point  $P$  of  $(\text{Ker}(\check{\pi})^m)_T$  gives rise to a map  $\mu_{p^n}$  defined by  $f(X) = \sum a_i(P)X^i$ , the corresponding differential is  $\omega_p = df/f$ , and for any  $g \in \text{Aut}(T/S_m)$ , we have  $a_i(g(P)) = g(a_i(P))$ , and hence  $\omega_g(P) = g(\omega_P)$ .] By descent, we have constructed an isomorphism between  $\underline{\omega}$  and the invertible sheaf on  $S_m^\zeta$  associated to the étale quotient of  $p^m E$ .

It remains to see that this isomorphism is compatible with the  $\phi$ -linear endomorphisms. Tensoring one with the inverse of the other, we obtain a  $\phi$ -linear endomorphism on  $\mathcal{O}_{S_m^\zeta}$ ; we must show that it carries "1" to "1". To check this, it suffices to do so in a "punctured disc at  $\infty$ ", over  $W_m(\mathbb{F}_q)((q))$  when we look at the Tate curve  $\text{Tate}(q^n)$ . The morphism  $\check{\pi}: \text{Tate}(q^n \cdot p^m) \longrightarrow \text{Tate}(q^n)$  has kernel the subgroup generated by  $q^n$ . The point  $q^n$  is a rational point of  $\text{Ker}(\check{\pi})^m$ , and the corresponding differential

is precisely the Tate differential  $\omega_{\text{can}} = dt/t$ . As  $q^n$  is a rational point, the section  $[q^n] \otimes 1$  of  $\text{Ker}(\pi)^\text{m} \otimes_{\mathbb{Z}/p^n\mathbb{Z}} \mathcal{O}$  is fixed by the canonical  $F$ , and the corresponding section  $\omega_{\text{can}}$  of  $\underline{\omega}$  is fixed by  $\varphi$  (because  $\omega_{\text{can}}$  has  $q$ -expansion identically "1"). Hence our isomorphism respects the  $\varphi$ -linear endomorphisms in a punctured disc around  $\infty$ , and hence respects it everywhere.

Remark 4.2.2.1. One may prove this theorem in a non-constructive way by showing that both of the associated  $p$ -adic characters  $x_i: \pi_1(S_m^\zeta) \rightarrow (\mathbb{Z}/p^m\mathbb{Z})^\times$  have the same value on all Frobenius elements, namely the reciprocal of the "unit root" of the ordinary elliptic curve which is the fibre over the corresponding closed point of  $S_m^\zeta$ .

Theorem 4.3. (Igusa [21]) The homomorphism

$\pi_1(\bar{S}_m^\zeta) \rightarrow \text{Aut}(\text{Ker}(\pi)_T^\text{m}) \xrightarrow{\sim} (\mathbb{Z}/p^m\mathbb{Z})^\times$  is surjective, and for every non-void open set  $U \subset \bar{S}_m^\zeta$ , the composite  $\pi_1(U) \rightarrow \pi_1(\bar{S}_m^\zeta) \rightarrow (\mathbb{Z}/p^m\mathbb{Z})^\times$  remains surjective.

Proof. It suffices to show that, denoting by  $K$  the function field of  $S_m^\zeta \times_{W_m(\mathbb{F}_q)} \mathbb{F}_q$ , the homomorphism  $\text{Gal}(K^{\text{sep}}/K) \rightarrow \text{Aut}(\text{Ker } V^m \text{ in } E^{(p^m)}(K^{\text{sep}}))$  is surjective. In fact, we will prove that the inertial group of  $\text{Gal}(K^{\text{sep}}/K)$  at any supersingular elliptic curve already maps surjectively. Let  $\mathcal{P}$  be any closed point of  $S_1^\zeta$  where  $E_{p-1}$  vanishes; replacing  $\mathbb{F}_q$  by its algebraic closure  $k$ , we may assume  $\mathcal{P}$  is a rational point. The completion of  $S_1^\zeta \otimes k$  at  $\mathcal{P}$  is isomorphic to  $\text{Spec}(k[[A]])$ , and the inverse image of the universal curve over  $k[[A]]$  admits a nowhere vanishing differential  $\omega$  such that  $E_{p-1}(E, \omega) = A$ . (This is just Igusa's theorem that the Hasse invariant has only simple zeros.) So we must prove

Theorem 4.3 bis (Igusa). Let  $E, \omega$  be an elliptic curve over  $k[[A]]$  with Hasse invariant  $A$ ,  $k$  being an algebraically closed field of characteristic  $p$ . Then the extension of  $k((A))$  obtained by adjoining the points of  $\text{Ker } V^m: E^{(p^m)} \rightarrow E$  is fully ramified of degree  $p^{m-1}(p-1)$ , with Galois group

canonically isomorphic to  $\text{Aut}(\mathbb{Z}/p^m\mathbb{Z})$ .

Proof. The first statement implies the second, since  $\text{Ker } V^m$  is cyclic of order  $p^m$  over  $k((A))^{sep}$ . In terms of a normalized parameter  $X$  for the formal group (i.e.  $[\zeta](X) = \zeta X$  for any  $p-1$ st root of unity  $\zeta \in \mathbb{Z}_p^\times$ ), the endomorphism  $[p]$  has the shape

$$4.3.1 \quad [p](X) = V(X^p) = AX^p + \alpha X^{p^2} + \dots$$

with  $\alpha$  invertible in  $k[[A]]$  (because modulo  $A$ , we have a supersingular curve by hypothesis, hence its formal group is of height two). Thus  $V(X) = AX + \alpha X^p + \dots$ , and the composite  $V^m: E^{(p^m)} \rightarrow E$  is the composite

$$E^{(p^m)} \xrightarrow{V^{(p^{m-1})}} E^{(p^{m-1})} \xrightarrow{V^{(p^{m-2})}} \dots \xrightarrow{V^{(p)}} E^{(p)} \xrightarrow{V} E.$$

The expression of  $V^{(p^m)}$  is  $V^{(p^m)}(X) = A^{p^m}X + \alpha^{p^m}X^p + \dots$ . A point of  $\text{Ker } V^m$  with values in  $k((A))^{sep}$  of order precisely  $p^m$  may be viewed as a sequence  $y_0, \dots, y_{m-1}$  of elements of the maximal ideal of  $k((A))^{sep}$  which satisfy the successive equations

$$\left\{ \begin{array}{l} 0 = V(y_0) = Ay_0 + \alpha(y_0)^p + \dots \\ y_0 = V^{(p)}(y_1) = A^p y_1 + \alpha^p (y_1)^p + \dots \\ y_{m-2} = V^{(p^{m-1})}(y_{m-1}) = A^{p^{m-1}} y_{m-1} + \alpha^{p^{m-1}} (y_{m-1})^p + \dots . \end{array} \right.$$

But a glance at the Newton polygons of these equations shows successively that the ordinals of  $y_0, \dots, y_{m-1}$  are given by (noting by  $\text{ord}$  the ordinal normalized so that  $\text{ord}(A) = 1$ ):

$$\left\{ \begin{array}{l} \text{ord}(y_0) = 1/p-1 \\ \text{ord}(y_1) = 1/p(p-1) \\ \vdots \\ \text{ord}(y_{m-1}) = 1/p^{m-1}(p-1) . \end{array} \right.$$

QED

#### 4.4. Applications to congruences between modular forms à la Serre

Corollary 4.4.1. Let  $k$  be an integer, and suppose  $m \geq 1$ . The following conditions are equivalent:

- 1)  $k \equiv 0 \pmod{(p-1) \cdot p^{m-1}}$  if  $p \neq 2$ , and  $k \equiv 0 \pmod{2^{\alpha(m)}}$  if  $p=2$ ,  
where  $\alpha(1) = 0$ ,  $\alpha(2) = 1$ , and  $\alpha(m) = m-2$  if  $m \geq 3$ .
- 2) The  $k$ 'th (tensor) power of the representation of  $\pi_1(\overline{S}_m^\zeta)$  on the étale quotient of  $p^{mE}$  is trivial.
- 3) The sheaf  $\underline{\omega}^{\otimes k}$  on  $\overline{S}_m^\zeta$  admits a nowhere vanishing section fixed by  $\phi$ .
- 4) Over a non-void open set  $U \subset \overline{S}_m^\zeta$ ,  $\underline{\omega}^{\otimes k}$  admits a nowhere vanishing section fixed by  $\phi$ .
- 5) Over  $\overline{S}_m^\zeta$ ,  $\underline{\omega}^{\otimes k}$  admits a section whose  $q$ -expansion at one of the cusps of  $\overline{S}_m^\zeta$  is identically 1.
- 6) Over a non-void open set  $U \subset \overline{S}_m^\zeta$  which contains a cusp,  $\underline{\omega}^{\otimes k}$  admits a section whose  $q$ -expansion at that cusp is identically 1.

Further, if 1) holds, then any section verifying either 4) or 6) extends uniquely to a section over all of  $\overline{S}_m^\zeta$  verifying 3) and 5), and is in fact the  $k/(p-1)$ 'st power of  $E_{p-1}$ .

Proof. 1)  $\iff$  2), because the image of  $\pi_1(\overline{S}_m^\zeta)$  is all of  $\text{Aut}(\mathbb{Z}/p^m\mathbb{Z}) \cong (\mathbb{Z}/p^m\mathbb{Z})^*$ , a group of exponent  $p^{m-1}(p-1)$  for  $p \neq 2$  and of exponent  $2^{\alpha(m)}$  for  $p=2$ . By (4.3), 2)  $\iff$  3) equivalence 3)  $\iff$  4) is by full-faithfulness of "restriction to  $U$ ", cf. (4.1.2.3). By the explicit formula for  $\phi$  and the  $q$ -expansion principle, we have 3)  $\iff$  5) and 4)  $\iff$  6). When 1) holds, the unicity of the section satisfying 4) or 6) or 3) or 5) follows from the full-faithfulness of restriction to  $U$ ; that this section is  $(E_{p-1})^{k/p-1}$  follows from the  $q$ -expansion principle.

Corollary 4.4.2. (Serre) Suppose  $f_i$ ,  $i=1,2$  are elements of  $S(W(\mathbb{F}_q), l, n, k_i)$ ,  $i=1,2$ , and that  $k_1 \geq k_2$ . Suppose that the  $q$ -expansions of  $f_1$  and  $f_2$  at at least one cusp of  $\bar{M}_m(W(\mathbb{F}_q), l)$  are congruent modulo  $p^m$ , and that  $f_1(q) \not\equiv 0 \pmod{p}$  at that cusp. Then  $k_1 \equiv k_2$  modulo  $p^{m-1}(p-1)$  if  $p \neq 2$ , and  $k_1 \equiv k_2$  modulo  $2^{\alpha(m)}$  if  $p=2$ , where  $\alpha(1)=0$ ,  $\alpha(2)=1$ , and  $\alpha(m)=m-2$  for  $m \geq 3$ . If these congruences hold at at least one cusp on each irreducible component, then  $f_2 \equiv f_1 \cdot (E_{p-1})^{k_2-k_1/p-1} \pmod{p^m S(W(\mathbb{F}_q), l, n, k_2)}$ .

Proof. Once we prove the congruence on the  $k_i$ , the final assertion results from the  $q$ -expansion principle. To prove the congruence on the weights, we reduce the situation modulo  $p^m$ . Then  $f_1$  and  $f_2$  are sections of  $\underline{\omega}^{\otimes k_1}$  and  $\underline{\omega}^{\otimes k_2}$  respectively over  $\bar{S}_m^\zeta$ . By hypothesis,  $f_1$  and hence  $f_2$  are invertible on a non-void open set  $U$  of  $\bar{S}_m^\zeta$ , and the ratio  $f_2/f_1$  is thus an invertible section of  $\underline{\omega}^{k_2-k_1}$  over  $U$ , and by hypothesis  $f_2/f_1$  has  $q$ -expansion identically one at at least one cusp on each  $\bar{S}_m^\zeta$ . By (4.4.1), we have the desired congruence on  $k_1 - k_2$ . QED

Corollary 4.4.3. (Serre) Let  $f$  be a true modular form of level  $n$  and weight  $k$  on  $\Gamma_0(p)$ , holomorphic at the unramified cusps, and defined over the fraction field  $K$  of  $W(\mathbb{F}_q)$ . Suppose that at each unramified cusp, the  $q$ -expansion has all its non-constant  $q$ -coefficients in  $W(\mathbb{F}_q)$ . Then the constant terms of the  $q$ -expansions lie in  $p^{-m} \cdot W(\mathbb{F}_q)$ , where, for  $p \neq 2$ ,  $m$  is the largest integer such that  $\phi(p^m) = \#(\mathbb{Z}/p^m \mathbb{Z})^X$  divides  $k$ , and for  $p=2$ ,  $m=1$  if  $k$  is odd, and  $m = \text{ord}_2(k) + 2$  if  $k$  is even.

Proof. For  $N \gg 0$ ,  $p^N f$  is a true modular form of level  $n$  and weight  $k$  on  $\Gamma_0(p)$ , defined over  $W(\mathbb{F}_q)$ . By (3.2), there is a unique element  $g$  of  $S(W(\mathbb{F}_q), l, n, k)$  whose  $q$ -expansions are those of  $p^N f$  at the corresponding unramified cusps. If  $-m_0$  denotes the minimum of the ordinals of the constant terms of these  $q$ -expansions, then  $g$  is divisible by  $p^{N-m_0}$  in  $S(W(\mathbb{F}_q), l, n, k)$ , by (2.7). Thus we may write  $g = p^{N-m_0} h$ , with  $h \in S(W(\mathbb{F}_q), l, n, k)$  having the

same  $q$ -expansions as does  $p^{m_0} f$  at the corresponding unramified cusps. Then  $h$  has integral  $q$ -expansions, and at least one of them is congruent modulo  $p^{m_0}$  to a constant which is a unit on  $W(\mathbb{F}_q)$ . Multiplying  $f$  by the reciprocal of this unit, we get a  $q$ -expansion which is congruent mod  $p^N$  to "1". As the constant function "1" is modular of weight zero, we must have

$$k \equiv 0 \pmod{p^{m_0-1}(p-1)} \text{ if } p \neq 2, \quad k \equiv 0 \pmod{2^{\alpha(m_0)}} \text{ for } p=2. \quad \text{QED}$$

Remark 4.4.4. If we apply these estimates to the constant terms of the classical level one Eisenstein series  $E_k$ , we get precisely the correct bounds for the denominators of the Bernoulli numbers (cf. [42], [43] for more on Bernoulli numbers).

#### 4.5. Applications to Serre's "modular forms of weight $X$ "

4.5.0. Let  $X \in \text{End}(\mathbb{Z}_p^X)$ . For each power  $p^m$  of  $p$ ,  $X$  induces an endomorphism of  $(\mathbb{Z}/p^m\mathbb{Z})^X$ . For any primitive  $n$ 'th root of unity  $\zeta$ , and for any representation  $\rho$  of  $\pi_1(S_m^\zeta)$  in a free  $\mathbb{Z}/p^m\mathbb{Z}$  module of rank one, we may define the representation  $\rho^X \stackrel{\text{dfn}}{=} X \circ \rho$ . Taking for  $\rho$  the representation given by the étale quotient of  $p^m E$ , we denote by  $(\underline{\omega}^X, \varphi)$  the invertible sheaf with  $\varphi$ -linear endomorphism which corresponds to  $\rho^X$ . For variable  $m$ , the sheaves  $\underline{\omega}^X$  on  $S_m^\zeta$  are compatible, and we define a compatible family of global sections to be a  $p$ -adic modular form of weight  $X$  and level  $n$ , holomorphic at  $\infty$ , defined over  $W(\mathbb{F}_q)$ . If  $X = k \in \mathbb{Z} \subset \text{End}(\mathbb{Z}_p^X)$ , we just recover the elements of  $S(W(\mathbb{F}_q), 1, n, k)$ . For  $p \neq 2$ ,  $\mathbb{Z}$  is dense in  $\text{End}(\mathbb{Z}_p^X)$ , and indeed  $\text{End}(\mathbb{Z}_p^X) \xleftarrow{\sim} \varprojlim \mathbb{Z}/\varphi(p^m)\mathbb{Z}$ ; for  $p=2$ ,  $\mathbb{Z}_2$  has index four in the (non-commutative) ring  $\text{End}(\mathbb{Z}_2^X)$ . If  $p \neq 2$ , then for any  $X$  (resp. if  $p=2$ , for any  $X \in \mathbb{Z}_2$ ), the pair  $(\underline{\omega}^X, \varphi)$  on  $S_m^\zeta$  is isomorphic to  $(\underline{\omega}^{\otimes k_m}, \varphi)$  for any  $k_m \in \mathbb{Z}$  such that  $k_m \equiv X \pmod{\varphi(p^m)}$  (resp. if  $p=2$ , modulo  $2^0$  if  $m=1$ ,  $2^1$  if  $m=2$ , and  $2^{m-2}$  if  $m \geq 3$ ). The isomorphism between  $(\underline{\omega}^{\otimes k_m}, \varphi)$  and  $(\underline{\omega}^{\otimes k'_m}, \varphi)$  for different choices  $k_m, k'_m \in \mathbb{Z}$  approximating  $X$  is given

by multiplication by  $(E_{p-1})^{(k'_m - k_m)/(p-1)}$ . As this isomorphism leaves invariant the  $q$ -expansion modulo  $p^m$  (resp. modulo  $2^{m-1}$  for  $p=2$ ), it follows that a  $p$ -adic modular form of weight  $X$  and level  $n$ , holomorphic at  $\infty$ , defined over  $W(\mathbb{F}_q)$ , has a well defined  $q$ -expansion in  $W[[q]]$  at each cusp, and that for given  $X$ ,  $f$  is uniquely determined by its  $q$ -expansions.

Theorem 4.5.1. Let  $X \in \text{End}(\mathbb{Z}_p^X)$ , and suppose  $X \in \mathbb{Z}_2$  if  $p=2$ . Let  $f$  be a modular form of weight  $X$  and level  $n$ , holomorphic at  $\infty$ , defined over  $W(\mathbb{F}_q)$ . Then there exists a sequence of integers  $0 \leq k_1 \leq k_2 \leq k_3 \leq \dots$ , satisfying

$$\begin{cases} k_m \equiv X \pmod{\varphi(p^m)} & \text{if } p \neq 2 \\ k_m \equiv X \pmod{2^{m-2}} & \text{if } p=2 \text{ and } m \geq 3 \end{cases}$$

and a sequence of true modular forms  $f_i$  of weight  $k_i$  and level  $n$ , holomorphic at  $\infty$ , defined over  $W(\mathbb{F}_q)$ , such that

$$\begin{cases} f_m \equiv f \pmod{p^m} \text{ in } q\text{-expansion, if } p \neq 2 \\ f_m \equiv f \pmod{2^{m-1}} \text{ in } q\text{-expansion if } p=2, m \geq 3. \end{cases}$$

Conversely. Let  $\{k_m\}_{m \geq 1}$  be an arbitrary sequence of integers, and suppose given a sequence  $f_m \in S(W(\mathbb{F}_q), 1, n, k_m)$  of  $p$ -adic modular forms of integral weights  $k_i$  such that

$$\begin{cases} f_{m+1} \equiv f_m \pmod{p^m} \text{ in } q\text{-expansion at each cusp} \\ f_m \not\equiv 0 \pmod{p^m} \text{ in } q\text{-expansion.} \end{cases}$$

Then the sequence of weights  $k_m$  converges to an element  $X \in \text{End}(\mathbb{Z}_p^X)$ , and there is a unique modular form  $f = \text{"lim"} f_m$  of weight  $X$  and level  $n$ , holomorphic at  $\infty$ , defined over  $W(\mathbb{F}_q)$ , such that

$$f_m \equiv f \pmod{p^m} \text{ in } q\text{-expansion.}$$

Corollary 4.5.2. (Serre) If a collection of elements of  $W[[q]]$  is the set of  $q$ -expansions of a  $p$ -adic modular form  $f$  of weight  $\chi \in \text{End}(\mathbb{Z}_p^\chi)$  (resp.  $\chi \in \mathbb{Z}_2$  if  $p=2$ ) and level  $n$ , holomorphic at  $\infty$  and defined over  $W(\mathbb{F}_q)$ , then both  $f$  and  $\chi$  are uniquely determined.

Proof of the theorem. The first part follows directly from the definitions.

For the second part, we will reduce to the case in which the  $f_m$  are all true modular forms, whose weights satisfy  $0 \leq k_1 \leq k_2 \leq \dots$ . Indeed, if we replace  $f_m$  by  $f'_m = f_m \cdot (E_{p-1})^{(p^{n-1})N_m}$  with  $N_m \gg 0$ , then we may suppose all  $k_m \geq 0$ , and by (2.7.2), for  $N_m \gg 0$ ,  $f'_m$  has  $q$ -expansion mod  $p^m$  of a true modular form. Rechoosing the  $N_m$  to be sufficiently increasing with  $m$ , we have the desired reduction. Now consider the limit  $q$ -expansions. We may and will work on each irreducible component of  $\bar{M}_n \otimes W(\mathbb{F}_q)$  separately. If on a given component, the limit  $q$ -expansion is identically zero at any cusp, it is so at every cusp, hence each  $f_m$  is  $\equiv 0 \pmod{p^m}$  on that component, and there is nothing to prove. In the contrary case, the limit  $q$ -expansion is divisible by  $p^{m_0}$  but not by  $p^{m_0+1}$  at each cusp ( $m_0$  is independent of the choice of cusp on each irreducible component: cf.(2.7.1)). Then for  $m > m_0$ ,  $f_m = p^{m_0} g_m$  where  $g_m$  is a true modular form with  $q$ -expansions  $\not\equiv 0 \pmod{p}$ . So replacing the sequence  $f_m$  by the sequence  $\{f'_m\} = \{g_{m_0+m}\}$ , we may suppose that each  $f_m$  has all  $q$ -expansions  $\not\equiv 0 \pmod{p}$ . Then by (4.4.1), the congruence  $f_{m+1} \equiv f_m \pmod{p^m}$  in  $q$ -expansion implies that  $k_{m+1} \equiv k_m$  modulo  $\phi(p^m)$  for  $p \neq 2$ , and modulo  $2^{m-2}$  if  $p=2$  and  $m \geq 3$ , and that  $f_{m+1} = f_m \cdot (E_{p-1})^{(k_{m+1}-k_m)/(p-1)}$  modulo  $p^m$ . Hence  $\chi = \lim k_m$  exists in  $\text{End}(\mathbb{Z}_p^\chi)$ , and  $\{f_m \pmod{p^m}\}_{m \geq 1}$  define a compatible family of sections of the sheaves  $\underline{\omega}^\chi$  on the schemes  $\bar{S}_m^\chi$ .

QED

Corollary 4.5.3. (Serre) Let  $\chi \in \text{End}(\mathbb{Z}_p^\chi)$ , and suppose  $\chi \in \mathbb{Z}_2$  if  $p=2$ . Let  $0 \leq k_1 \leq k_2 \leq \dots$  be a sequence of integers such that  $k_m \equiv \chi \pmod{\phi(p^m)}$  if  $p \neq 2$ , and modulo  $2^{m-2}$  if  $p=2$  and  $m \geq 3$ . Let  $\{f_m\}$  be a sequence of true modular forms of weight  $k_m$  and level  $n$  on  $\Gamma_0(p)$ , holomorphic at

the unramified cusps, and defined over the fraction field  $K$  of  $W(\mathbb{F}_q)$ . Suppose that the non-constant terms of all the  $q$ -expansions of the  $f_m$  are in  $W(\mathbb{F}_q)$ , and that at each cusp,

$$f_{m+1}(q) - f_{m+1}(0) \equiv f_m(q) - f_m(0) \pmod{p^m}.$$

Then if  $x \neq 0$ , let  $m_0$  be the largest integer such that  $x \equiv 0 \pmod{p^{m_0}}$  if  $p \neq 2$ , for  $p=2$ ,  $m_0=1$  if  $x$  is invertible in  $\mathbb{Z}_2$ , and  $m_0=2+\text{ord}_2(x)$  if  $x$  is not invertible in  $\mathbb{Z}_2$ . Then for  $m \geq m_0$ ,  $p^m f_m$  has integral ( $\in W(\mathbb{F}_q)$ )  $q$ -expansions, and at each cusp we have the congruence on constant terms:  $p^m f_{m+1}(0) \equiv p^m f_m(0) \pmod{p^{m-m_0}}$  for all  $m > m_0$  if  $p \neq 2$ , and  $2^m f_m(0) \equiv 2^m f_m(0) \pmod{2^{m-1-m_0}}$  if  $m \geq 3$  and  $m \geq m_0$ .

Proof. The integrality of the  $q$ -expansions of the  $p^m f_m$  follows from (4.4.3).

Let  $g_m = p^m f_m$ , which has integral  $q$ -expansions. Then  $g_m$  and  $h_m \stackrel{\text{dfn}}{=} g_m \cdot (\mathbb{E}_{p-1}^{(k_{m+1}-k_m)/(p-1)})$  have  $q$ -expansions which are congruent modulo  $p^m$  if  $p \neq 2$ , (resp. modulo  $2^{m-1}$  if  $p=2$ ) and  $g_m(0) = h_m(0)$ . Thus  $g_{m+1} - h_m$  has  $q$ -expansions congruent to the constants  $g_{m+1}(0) - h_m(0)$  modulo  $p^m$  if  $p \neq 2$ , (resp. modulo  $2^{m-1}$  if  $p=2$ ). Applying (4.4.3) to the function  $(g_{m+1} - h_m)/p^m$  for  $p \neq 2$ , (resp. to  $g_{m+1} - h_m/2^{m-1}$  for  $p=2$ ) we find that its constant term has denominator at most  $p^m$ . Thus  $g_{m+1}(0) \equiv h_m(0) \pmod{p^{m-m_0}}$  if  $p \neq 2$ , and  $2^{m-1-m_0}$  if  $p=2$ . QED

Example 4.5.4. (Serre) Take  $f_m = G_{k_m}$ , the classical Eisenstein series of level 1, whose  $q$ -expansions are given by  $-(b_{k_m})/2k_m + \sum_{n \geq 1} \sigma_{k_m-1}(n)q^n$ . Choose the  $k_m$  to be strictly increasing with  $m$ , so that they tend archimedeanly to  $\infty$ . One checks immediately that the hypotheses of (4.5.3) are verified. The limit "lim"  $p^m f_m \stackrel{\text{dfn}}{=} p^m G_X^*$  is thus a modular form of weight  $X = \lim k_m$ , whose  $q$ -expansion is given by

$$G_X^*(q) = \mathcal{L}^*(X) + \sum_{n \geq 1} q^n \sum_{d|n, p \nmid d} X(d)/d$$

where  $\zeta^*(x)$  is the (prime to  $p$  part of the) Kubota-Leopoldt zeta function, in the notation of Serre [42]. We hasten to point out that even if the character  $x$  is an even positive integer  $2k \geq 4$ , the above defined  $G_{2k}^*$  is a  $p$ -adic modular form of weight  $2k$ , but it is not the usual Eisenstein series  $G_{2k}$ . Indeed, the  $q$ -expansion of  $G_{2k}^*$  is given by

$$G_{2k}^*(q) = \frac{1}{2}(1-p^{2k-1})\zeta(1-2k) + \sum_{n \geq 1} q^n \sum_{d|n, p \nmid d} d^{2k-1}$$

while the  $q$ -expansion of  $G_{2k}$  is given by

$$G_{2k}(q) = \frac{1}{2}\zeta(1-2k) + \sum_{n \geq 1} q^n \sum_{d|n} d^{2k-1}.$$

Both  $G_{2k}$  and  $G_{2k}^*$  are  $p$ -adic modular forms of weight  $2k$ , which, as Serre explained to me, are related as follows:

$$\begin{cases} G_{2k}^* = G_{2k} - p^{2k-1}\phi(G_{2k}) \\ G_{2k} = \sum_{n \geq 0} (p^{2k-1} \cdot \phi)^n(G_{2k}^*) \end{cases}.$$

Taking  $k=1$ , we obtain a  $p$ -adic modular form  $G_2^*$  of weight 2, and we may define  $G_2$  as a  $p$ -adic modular form by setting

$$G_2 \stackrel{\text{dfn}}{=} \sum_{n \geq 0} p^n \phi^n(G_2^*).$$

An immediate calculation gives the  $q$ -expansion of  $G_2$  (cf. A1.3 for the series  $P$ )

$$G_2(q) = \frac{-1}{2^4} + \sum_{n \geq 1} q^n \sum_{d|n} d = \frac{-1}{2^4} P(q)$$

and shows that, for any prime  $p$ , the series  $P(q)$  is the  $q$ -expansion of a  $p$ -adic modular form of weight two and level one. We refer the reader to A2.4 for an "intrinsic" proof of this fact for  $p \neq 2, 3$ , based on the classical interpretation of  $P$  as a ratio of periods (cf. A1.3).

Appendix 1: Motivations

In this "motivational" appendix we will first recall the relation between complex elliptic curves and lattices in  $\mathbb{C}$ , then the relation between modular forms and the de Rahm cohomology of elliptic curves, and finally the relation between the Gauss-Manin connection and Serre's  $\partial$  operator on modular forms. These relations are due to Weierstrass and Deligne.

A1.1 Lattices and elliptic curves

Given a lattice  $L \subset \mathbb{C}$ , we may form the quotient  $\mathbb{C}/L$ , a one-dimensional complex torus, and endow it with the translation-invariant one-form  $\omega = dz$  ( $z$  the coordinate on  $\mathbb{C}$ ). Thanks to Weierstrass, we know that  $\mathbb{C}/L$  "is" an elliptic curve, given as a cubic  $\mathbb{P}^2$  by the inhomogeneous equation

$$\text{A1.1.1} \quad y^2 = 4x^3 - g_2x - g_3,$$

such that  $\omega$  is the differential  $dx/y$ . The isomorphism from  $\mathbb{C}/L$  to this curve is explicitly given by the  $\wp$ -function:

$$\text{A1.1.2} \quad z \in \mathbb{C}/L \longrightarrow (x = \wp(z; L), y = \wp'(z; L))$$

where

$$\text{A1.1.2.1} \quad \wp(z; L) = \frac{1}{z^2} + \sum_{\ell \in L - \{0\}} \left( \frac{1}{(z-\ell)^2} - \frac{1}{\ell^2} \right),$$

$$\text{A1.1.2.2} \quad \wp'(z; L) = \frac{d\wp(z; L)}{dz} = \frac{-2}{z^3} + \sum_{\ell \in L - \{0\}} \frac{-2}{(z-\ell)^3},$$

$$\text{A1.1.2.3} \quad g_2 = 60 \sum_{\ell \in L - \{0\}} 1/\ell^4, \quad g_3 = 140 \sum_{\ell \in L - \{0\}} 1/\ell^6.$$

Conversely, given an elliptic curve  $E$  over  $\mathbb{C}$  together with a non-zero everywhere holomorphic differential  $\omega$ , it arises in the above way from the lattice of periods of  $\omega$ ,

$$\text{A1.1.2.4} \quad L(E, \omega) = \left\{ \int_{\gamma} \omega \mid \gamma \in H_1(E; \mathbb{Z}) \right\} \subset \mathbb{C}.$$

Under this correspondence, the effect of replacing  $(E, \omega)$  by  $(E, \lambda\omega)$ ,  $\lambda \in \mathbb{C}^*$ , is to replace  $L$  by  $\lambda \cdot L$ :

$$\text{Al.1.2.5} \quad L(E, \lambda\omega) = \lambda \cdot L(E, \omega) .$$

Recall that classically, a complex modular form of weight  $k$  (and level 1) is a holomorphic function on the upper-half plane  $f(\tau)$  which satisfies the transformation equation

$$\text{Al.1.3} \quad f\left(\frac{a\tau + b}{c\tau + d}\right) = f(\tau) \cdot (c\tau + d)^k \quad \forall \begin{pmatrix} ab \\ cd \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) .$$

As explained in [42<sup>1</sup>], there is associated to  $f$  a unique function of lattices  $F(L)$  such that  $f(\tau) = F(\mathbb{Z}\tau + \mathbb{Z})$ , and which is homogeneous of degree  $-k$  in  $L$ :  $F(\lambda L) = \lambda^{-k} F(L)$  for  $\lambda \in \mathbb{C}^*$ . (Explicitly,  $F(L) = \omega_2^{-k} f(\omega_1/\omega_2)$  if  $L = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$  and  $\mathrm{Im}(\omega_1/\omega_2) > 0$ .)

By Weierstrass, we may now associate to  $f$  a "holomorphic" function  $\mathbb{F}$  of pairs  $(E, \omega)$  consisting of an elliptic curve/ $\mathbb{C}$  together with a nowhere-vanishing differential which is homogeneous of degree  $-k$  in the second variable:  $\mathbb{F}(E, \lambda\omega) = \lambda^{-k} \mathbb{F}(E, \omega)$ , defined by  $\mathbb{F}(E, \omega) = F(L(E, \omega))$ . This is the point of view taken in the text.

### Al.2 Homomorphy at $\infty$ and the Tate curve

Recall further that a complex modular form  $f(\tau)$  is said to be meromorphic (resp. holomorphic) at  $\infty$ , if the periodic function  $f(\tau) = f(\tau+1)$ , when viewed as a function of  $q = \exp(2\pi i\tau)$ , holomorphic for  $0 < |q| < 1$ , in fact extends to a meromorphic (resp. holomorphic) function of  $q$  in  $|q| < 1$ . In terms of  $\mathbb{F}$ , we are asking about the behavior of

$$\mathbb{F}(\mathbb{C}/2\pi i\mathbb{Z} + 2\pi i\tau\mathbb{Z}, 2\pi i dz) = \mathbb{F}(\mathbb{C}^*/q^{\mathbb{Z}}, dt/t)$$

(where  $t = \exp(2\pi i z)$  is the parameter on  $\mathbb{C}^*$ , and  $q^{\mathbb{Z}}$  denotes the subgroup of  $\mathbb{C}^*$  generated by  $q$ ), as  $q$  tends to zero. By standard calculations (cf. [38]), the curve  $\mathbb{C}/L$ ,  $L = 2\pi i\mathbb{Z} + 2\pi i\tau\mathbb{Z}$  with differential  $2\pi i dz$  is given

as the plane cubic

$$Y^2 = 4X^3 - \frac{E_4}{12}X + \frac{E_6}{216}, \text{ with differential } dX/Y$$

A1.2.1

$$(X = \mathcal{P}(2\pi iz, L), \quad Y = \mathcal{F}'(2\pi iz, L))$$

with coefficients the Eisenstein series

$$\begin{aligned} A1.2.2 \quad & \left\{ \begin{array}{l} 12 \cdot (2\pi i)^4 g_2(\tau) = E_4 = 1 + 240 \sum \sigma_3(n) q^n \\ 216 \cdot (2\pi i)^6 g_3(\tau) = E_6 = 1 - 504 \sum \sigma_5(n) q^n \end{array} ; \quad \sigma_k(n) = \sum_{\substack{d|n \\ d \geq 1}} d^k \right. \end{aligned}$$

Thus to ask that the modular form  $f$  be meromorphic (resp. holomorphic) at  $\infty$  is to ask that  $F\left(Y^2 = 4X^3 - \frac{E_4}{12}X + \frac{E_6}{216}, dX/Y\right)$  lie in the ring  $\mathbb{C}((q))$  of finite-tailed Laurent series (resp., that it lie in  $\mathbb{C}[[q]]$ , the ring of formal power series in  $q$ ).

The equation A1.2.1 in fact defines an elliptic curve over the ring  $\mathbb{Z}[1/6]((q))$ ; in fact, if we introduce

$$X = x + \frac{1}{12}, \quad Y = x + 2y$$

then we may rewrite the equation in the form

$$A1.2.3 \quad y^2 + xy = x^3 + B(q)x + C(q)$$

with coefficients

$$\begin{aligned} A1.2.4 \quad & \left\{ \begin{array}{l} B(q) = -5 \left( \frac{E_4 - 1}{240} \right) = -5 \sum_{n \geq 1} \sigma_3(n) q^n \\ C(q) = \frac{-5 \left( \frac{E_4 - 1}{240} \right) - 7 \left( \frac{E_6 - 1}{504} \right)}{12} = \sum_{n \geq 1} \left( \frac{-5\sigma_3(n) - 7\sigma_5(n)}{12} \right) q^n \end{array} . \right. \end{aligned}$$

This last equation defines an elliptic curve over  $\mathbb{Z}((q))$  whose restriction to  $\mathbb{Z}[\frac{1}{6}]((q))$  is the above curve, and the nowhere vanishing differential  $dx/2y+x$  restricts to give  $dX/Y$  over  $\mathbb{Z}[\frac{1}{6}]((q))$ .

By definition, the Tate curve  $\text{Tate}(q)$  with its canonical differential  $\omega_{\text{can}}$  is the elliptic curve over  $\mathbf{Z}((q))$  defined by (A1.2.3), with differential  $\omega_{\text{can}} = dx/2y+x$ . For each integer  $n \geq 1$ , the Tate curve  $\text{Tate}(q^n)$  with its canonical differential  $\omega_{\text{can}}$  is deduced from  $(\text{Tate}(q), \omega_{\text{can}})$  by the extension of scalars  $\mathbf{Z}((q)) \rightarrow \mathbf{Z}((q))$  given by  $\sum a_i q^i \mapsto \sum a_i q^{ni}$ . Explicitly,  $(\text{Tate}(q^n), \omega_{\text{can}})$  is given by

$$\text{A1.2.5} \quad y^2 + xy = x^3 + B(q^n) \cdot x + C(q^n); \quad \omega_{\text{can}} = dx/2y+x.$$

Let  $\zeta_n$  be a primitive  $n$ 'th root of unity. The points of order  $n$  on  $\mathbf{C}^*/q^{n\mathbf{Z}}$  are clearly the (images of the)  $n^2$  points

$$\text{A1.2.6} \quad (\zeta_n)^i q^j, \quad 0 \leq i, j \leq n-1.$$

Using the explicit expressions for  $x$  and  $y$  as functions of  $t = \exp(2\pi iz)$

$$\left\{ \begin{array}{l} x(t) = \sum_{k \in \mathbb{Z}} \frac{q^{nk} t}{(1-q^{nk} t)^2} - 2 \sum_{k=1}^{\infty} \frac{q^{nk}}{1-q^{nk}} \\ y(t) = \sum_{k \in \mathbb{Z}} \frac{(q^{nk} t)^2}{(1-q^{nk} t)^3} + \sum_{k=1}^{\infty} \frac{q^{nk}}{1-q^{nk}}, \end{array} \right.$$
A1.2.7

one sees that each of the  $n^2-1$  points  $(\zeta_n)^i q^j$ ,  $0 \leq i, j \leq n-1$ ,  $(i,j) \neq (0,0)$  has  $x$  and  $y$  coordinates in  $\mathbf{Z}[[q]] \otimes_{\mathbf{Z}} \mathbf{Z}[\zeta_n, 1/n]$ . Hence all level  $n$  structures on  $\text{Tate}(q^n)$  over  $\mathbf{Z}((q))$  are defined over  $\mathbf{Z}((q)) \otimes \mathbf{Z}[\zeta_n, 1/n]$  (rather than just over  $\mathbf{Z}[\zeta_n, 1/n]((q))$ ). This implies that the  $q$ -expansions of a modular form of level  $n$  have bounded denominators (cf. 1.2.1).

## A1.2 Modular forms and de Rham cohomology

We can now give a purely algebraic definition of modular forms of weight  $k$ , (meromorphic at  $\infty$ ) as being certain "functions"  $f(E, \omega)$  defined whenever

$$\begin{matrix} E & ; & \omega \\ \pi \downarrow & & \\ R & & \end{matrix}$$

is any elliptic curve over any ring  $R$ , and  $\omega \in \Gamma(E, \Omega_{E/R}^1)$  is a nowhere vanishing differential on  $E$ , whose values  $f(E, \omega)$  are elements of the ground-ring  $R$ . The conditions to be satisfied are

- 0)  $f(E, \lambda\omega) = \lambda^{-k} f(E, \omega)$  for all  $\lambda \in R^\times$ ;
- 1)  $f(E, \omega)$  depends only on the isomorphism class of  $(E, \omega)$  over  $R$ ;
- 2) if  $\phi: R \rightarrow R'$  is a ring homomorphism, then, denoting by  $(E_\phi, \omega_\phi)$  the curve with differential over  $R'$  deduced by extension of scalars, we have  $f(E_\phi, \omega_\phi) = \phi(f(E, \omega))$ .

{Such modular forms are automatically meromorphic at infinity, simply because the Tate curve  $\text{Tate}(q)$  is an elliptic curve over  $\mathbb{Z}((q))$ .}

Given a modular form  $f$  of weight  $k$ , we may form the  $k$ -ple differential  $f(E, \omega) \cdot \omega^{\otimes k}$  on  $E$ , which is independent of the choice of  $\omega$ , and view it as a global section over  $R$  of the (invertible) sheaf  $(\underline{\omega}_{E/R})^{\otimes k}$ , where

$$\underline{\omega}_{E/R} \stackrel{\text{dfn}}{=} \pi_*(\Omega_{E/R}^1).$$

This permits us to interpret a (meromorphic at  $\infty$ ) modular form of weight  $k$  as a function  $f(E)$ , defined on any elliptic curve  $E$  over any ring  $R$ , with values in the global sections of  $(\underline{\omega}_{E/R})^{\otimes k}$ , which satisfies

- 1) if  $\alpha: E \rightarrow E'$  is an isomorphism of elliptic curves over  $R$ , then  $\alpha^*(f(E')) = f(E)$ ;
- 2) if  $\phi: R \rightarrow R'$  is a ring homomorphism, then  $f(E_\phi) = \phi^*(f(E))$ .

Why bother to look at the de Rham cohomology? Over any base ring  $R$ , the (1<sup>st</sup>) de Rham cohomology of an elliptic curve  $E/R$ , noted  $H_{DR}^1(E/R)$  and defined as  $H^1(E, \Omega_{E/R}^1)$ , sits in a short exact sequence, its "Hodge filtration") of  $R$ -modules

$$\begin{array}{ccccccc}
 0 & \longrightarrow & \underline{\omega}_{E/R} & \longrightarrow & H^1_{DR}(E/R) & \longrightarrow & \underline{\text{Lie}}(E/R) \longrightarrow 0 \\
 & & & & " & & \\
 \text{Al.2.1} & & & & H^1(E, \mathcal{O}_E) & & \\
 & & & & " & & \\
 & & & & (\underline{\omega}_{E/R})^{\otimes -1} & & 
 \end{array}$$

Furthermore, when the integer 6 is invertible in R, this sequence has a canonical (but not functorial) splitting,

$$H^1_{DR}(E/R) \longrightarrow \underline{\omega}_{E/R} \oplus (\underline{\omega}_{E/R})^{\otimes -1}$$

which may be obtained as follows. Given  $(E, \omega)$  over R,  $R \ni 1/6$ , then there are unique meromorphic functions with poles only along the identity section, of orders 2 and 3 respectively, X and Y on E such that  $\omega = dX/Y$  and such that E is defined by (inhomogeneous) equation

$$Y^2 = 4X^3 - g_2 X - g_3, \quad g_2, g_3 \in R$$

(when  $R = C$ , we have  $X = \tilde{\mathcal{P}}(z; L)$ ,  $Y = \tilde{\mathcal{P}}'(z; L)$ , L the lattice of periods of  $\omega$ ). To specify the dependence on  $\omega$ , let's write  $X(E, \omega)$ ,  $Y(E, \omega)$ ,  $g_2(E, \omega)$ ,  $g_3(E, \omega)$ . By uniqueness, we necessarily have

$$\text{Al.2.2} \quad \left\{ \begin{array}{l} X(E, \lambda \omega) = \lambda^{-2} \cdot X(E, \omega) \\ Y(E, \lambda \omega) = \lambda^{-3} \cdot Y(E, \omega) \\ g_2(E, \lambda \omega) = \lambda^{-4} g_2(E, \omega) \\ g_3(E, \lambda \omega) = \lambda^{-6} g_3(E, \omega) \end{array} \right.$$

But over any base-ring R, the first de Rham cohomology of an elliptic curve  $E/R$  is nothing other than the module of differentials on  $E/R$  having at worst double poles at  $\infty$  (i.e. along the identity section). More precisely, the inclusion of the de Rham complex  $\mathcal{O}_E \longrightarrow \Omega^1_{E/R}(\infty)$  in the complex

$$\mathcal{O}_E(\infty) \longrightarrow \Omega^1_{E/R}(2\infty)$$

induces an isomorphism on  $H^1(E, \mathcal{O}_E(\infty))$ . Because  $H^1(E, \mathcal{O}_E(\infty)) = 0 = H^1(E, \Omega_{E/R}^1(2\infty)) = 0$  for  $i > 0$ , we have

$$\begin{aligned} H^1(E, \mathcal{O}_E(\infty)) &\longrightarrow \Omega_{E/R}^1(2\infty) = \text{Coker}(H^0(E, \mathcal{O}_E(\infty)) \longrightarrow H^0(E, \Omega_{E/R}^1(2\infty))) \\ \text{Al.2.3} \qquad \qquad \qquad &= \text{Coker}(R \xrightarrow{\circ} H^0(E, \Omega_{E/R}^1(2\infty))) \\ &= H^0(E, \Omega_{E/R}^1(2\infty)). \end{aligned}$$

If we suppose  $\delta$  to be invertible in  $R$ , then as soon as we choose a nowhere vanishing differential  $\omega$  on  $E$ , we may canonically specify a basis of  $H^1(E, \Omega_{E/R}^1(2\infty))$ , namely

$$\text{Al.2.4} \qquad \omega = \frac{dX(E, \omega)}{Y(E, \omega)} \quad \text{and} \quad \eta = X(E, \omega) \cdot \omega = \frac{X(E, \omega) \cdot dX(E, \omega)}{Y(E, \omega)}.$$

Replacing  $\omega$  by  $\lambda\omega$ ,  $\lambda \in R^\times$ , has the effect of replacing this basis by

$$\text{Al.2.5} \qquad \lambda\omega = \frac{dX(E, \lambda\omega)}{Y(E, \lambda\omega)} \quad \text{and} \quad \lambda^{-1}\eta = \frac{X(E, \lambda\omega) dX(E, \lambda\omega)}{Y(E, \lambda\omega)},$$

which is to say that we have defined an isomorphism

$$\text{Al.2.6} \qquad H_{DR}^1(E/R) \xleftarrow{\sim} \underline{\omega}_{E/R} \oplus \underline{\omega}_{E/R}^{-1}$$

given locally on  $R$  in terms of the choice of a nowhere vanishing  $\omega$  by

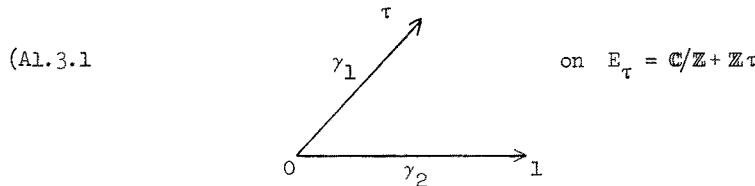
$$a\omega + b\eta \longleftrightarrow a\omega \oplus b\omega^{-1}.$$

For every integer  $k \geq 1$ , the  $k$ 'th symmetric power of this isomorphism provides an isomorphism

$$\text{Al.2.7} \qquad \text{Symm}^k(H_{DR}^1(E/R)) \cong (\underline{\omega}_{E/R})^{\otimes k} \oplus (\underline{\omega}_{E/R})^{\otimes k-2} \oplus \dots \oplus (\underline{\omega}_{E/R})^{\otimes -k}.$$

A1.3 The Gauss-Manin connection, and the function P

We begin by computing the Gauss-Manin connection on  $H_{DR}^1(E/R)$  in the case where  $R$  is the ring of holomorphic functions of  $\tau$ , and  $E$  is the relative elliptic curve defined by the lattice  $\mathbb{Z} + \mathbb{Z}\tau$ . The dual  $H_1(E/R)$  of  $H_{DR}^1(E/R)$  is  $R$ -free on the two families of paths  $\gamma_1$  and  $\gamma_2$ :



The Gauss-Manin connection in this context is the action  $\nabla_\tau = \nabla \left( \frac{d}{d\tau} \right)$  of  $\frac{d}{d\tau}$  on  $H_{DR}^1(E/R)$  given by the formula (cf.[26], 4.1.2)

$$(A1.3.2) \quad \int_{\gamma_i} \nabla_\tau(\xi) = \frac{d}{d\tau} \int_{\gamma_i} \xi \quad \text{for } \xi \in H_{DR}^1(E/R), \text{ and } i=1,2$$

(i.e., it is the dual of the connection on  $H_1(E/R)$  for which  $\gamma_1$  and  $\gamma_2$  are the horizontal sections).

To actually compute, let's note by  $\omega$  (resp.  $\eta$ ) the cohomology classes of  $\frac{dx}{y}$  and  $\frac{xdx}{y}$  respectively, and denote by  $\omega_i$ ,  $i=1,2$  and  $\eta_i$ ,  $i=1,2$  the periods  $\int_{\gamma_i} \omega$  and  $\int_{\gamma_i} \eta$ , which we view simply as elements of  $R$ . We will also denote by  $\gamma_1$  and  $\gamma_2$  the elements of  $H_{DR}^1(E/R)$  defined by Poincaré duality and the requirement that for any  $\xi \in H_{DR}^1(E/R)$ ,  $\int_{\gamma_i} \xi = \langle \xi, \gamma_i \rangle$ . Thus  $\langle \gamma_2, \gamma_1 \rangle = 1 = -\langle \gamma_1, \gamma_2 \rangle$ , and  $\langle \gamma_1, \gamma_1 \rangle = \langle \gamma_2, \gamma_2 \rangle = 0$ . We have  $\omega_i = \langle \omega, \gamma_i \rangle$  and  $\eta_i = \langle \eta, \gamma_i \rangle$  for  $i=1,2$ . Hence we necessarily have

$$(A1.3.3) \quad \begin{cases} \omega = \omega_1 \gamma_2 - \omega_2 \gamma_1 \\ \eta = \eta_1 \gamma_2 - \eta_2 \gamma_1 \end{cases}; \quad \begin{pmatrix} \omega_1 & -\omega_2 \\ \eta_1 & -\eta_2 \end{pmatrix} \begin{pmatrix} \gamma_2 \\ \gamma_1 \end{pmatrix} = \begin{pmatrix} \omega \\ \eta \end{pmatrix}$$

(because both sides have the same periods over both  $\gamma_1$  and  $\gamma_2$ ).

But the classical "period relation" of Legendre

$$\text{Al.3.4} \quad \eta_1 \omega_2 - \eta_2 \omega_1 = 2\pi i$$

[which expresses that the topological cup-product  $\langle \omega, \eta \rangle$  is  $2\pi i$ , or equivalently that the DR-cup-product  $\langle \omega, \eta \rangle_{\text{DR}} = 1$ ]. This allows us to express  $\omega$  and  $\eta$  in terms of  $\gamma_1$  and  $\gamma_2$ :

$$\text{Al.3.5} \quad 2\pi i \begin{pmatrix} \gamma_2 \\ \gamma_1 \end{pmatrix} = \begin{pmatrix} -\eta_2 & \omega_2 \\ -\eta_1 & \omega_1 \end{pmatrix} \begin{pmatrix} \omega \\ \eta \end{pmatrix}.$$

Applying  $\nabla_\tau$ , we annihilate  $\gamma_1$  and  $\gamma_2$ , hence, noting  $\frac{d}{d\tau}$  by a prime ' ,

$$\text{Al.3.6} \quad 0 = \begin{pmatrix} -\eta'_2 & \omega'_2 \\ -\eta'_1 & \omega'_1 \end{pmatrix} \begin{pmatrix} \omega \\ \eta \end{pmatrix} + \begin{pmatrix} -\eta_2 & \omega_2 \\ -\eta_1 & \omega_1 \end{pmatrix} \begin{pmatrix} \nabla'_\tau(\omega) \\ \nabla'_\tau(\eta) \end{pmatrix}$$

an equation we may solve using Legendre's relation:

$$\begin{aligned} \begin{pmatrix} \nabla'_\tau(\omega) \\ \nabla'_\tau(\eta) \end{pmatrix} &= \frac{-1}{2\pi i} \begin{pmatrix} \omega_1 & -\omega_2 \\ \eta_1 & -\eta_2 \end{pmatrix} \begin{pmatrix} -\eta'_2 & \omega'_2 \\ -\eta'_1 & \omega'_1 \end{pmatrix} \begin{pmatrix} \omega \\ \eta \end{pmatrix} \\ \text{Al.3.7} \quad &= \frac{-1}{2\pi i} \begin{pmatrix} \eta'_1 \omega_2 - \eta'_2 \omega_1 & \omega_1 \omega'_2 - \omega_2 \omega'_1 \\ \eta_2 \eta'_1 - \eta'_1 \eta_2 & \eta_1 \omega'_2 - \eta_2 \omega'_1 \end{pmatrix} \begin{pmatrix} \omega \\ \eta \end{pmatrix}. \end{aligned}$$

At this point we must recall that  $\omega_1 = \tau$ ,  $\omega_2 = 1$  and Legendre's relation becomes:  $\eta_1 - \tau \eta_2 = 2\pi i$ . Fed back into (Al.3.7), this information gives

$$\text{Al.3.8} \quad \begin{pmatrix} \nabla'_\tau(\omega) \\ \nabla'_\tau(\eta) \end{pmatrix} = \frac{-1}{2\pi i} \begin{pmatrix} \eta_2 & -1 \\ (\eta_2)^2 - 2\pi i \eta'_2 & -\eta_2 \end{pmatrix} \begin{pmatrix} \omega \\ \eta \end{pmatrix}.$$

Lemma Al.3.9.  $\eta_2 = -\sum_m \sum_n' \frac{1}{(m\tau+n)^2} = \frac{-\pi^2}{3} P$ , where  $\Sigma'$  means that the term  $(m=0, n=0)$  is omitted, and  $P$  is the function of  $q = e^{2\pi i \tau}$  given by

$$P(q) = 1 - 24 \sum_{n \geq 1} \sigma_1(n) q^n, \text{ where } \sigma_1(n) = \sum_{d \geq 1, d|n} d.$$

Proof. The first follows from the definition of  $\eta_2$  as a period of  $\eta = XdX/Y = \mathcal{P}(z)dz$ , and the fact that  $\eta = -d\zeta$ , where  $\zeta$  is the Weierstrass  $\zeta$ -function

$$(Al.3.10) \quad \zeta(z) = \frac{1}{z} + \sum_m \sum_n' \left\{ \frac{1}{z-m\tau-n} + \frac{1}{m\tau+n} + \frac{z}{(m\tau+n)^2} \right\}.$$

Indeed  $\eta_2 = \int_{\gamma_2} \eta = \int_0^1 (-d\zeta(z)) = \int_z^{z+1} (-d\zeta(z)) = \zeta(z) - \zeta(z+1)$ , and hence

$$\eta_2 = \frac{1}{z} - \frac{1}{z+1} + \sum_m \sum_n' \left\{ \frac{1}{z-m\tau-n} - \frac{1}{z-m\tau-n+1} - \frac{1}{(m\tau+n)^2} \right\}$$

$$(Al.3.11) \quad = \frac{1}{z} - \frac{1}{z+1} + \sum_{m \neq 0} \sum_n \frac{-1}{(m\tau+n)^2} + \sum_{n \neq 0} \left\{ \frac{-1}{n^2} + \frac{1}{z-n} - \frac{1}{z+1-n} \right\}$$

$$= \sum_m \sum_n' \frac{1}{(m\tau+n)^2} .$$

The second equality is ubiquitous (cf. [42<sup>1</sup>], pp. 154-155).

Remark Al.3.12. A similar calculation, based on the fact that the  $\zeta$  is an absolutely convergent double sum, hence also given by function

$$(Al.3.12.1) \quad \zeta(z) = \frac{1}{z} + \sum_n \sum_m' \left\{ \frac{1}{z-m\tau-n} + \frac{1}{m\tau+n} + \frac{z}{(m\tau+n)^2} \right\}$$

shows that  $\eta_1 = \zeta(z) - \zeta(z+\tau) = -\sum_m \sum_n' \frac{\tau}{(m\tau+n)^2}$ . Comparing these two formulas,

we see that  $\eta_2(-1/\tau) = \tau\eta_1(\tau)$ , and hence Legendre's formula  $\eta_1(\tau) - \tau\eta_2(\tau) = 2\pi i$  is equivalent to the transformation formula

$$(Al.3.12.2) \quad \frac{\eta_2(-1/\tau)}{\tau} - \tau\eta_2(\tau) = 2\pi i ,$$

$$\text{i.e.} \quad \eta_2(-1/\tau) = \tau^2 \eta_2(\tau) + 2\pi i \tau$$

$$\text{or equivalently } P(-1/\tau) = \tau^2 P(\tau) - \frac{6i\tau}{\pi} .$$

Remark (Al.3.13). Viewing Legendre's relation as saying that  $\langle \omega, \eta \rangle_{\text{DR}} = 1$ , one can prove it easily using Serre's cup-product formula, valid on any complete nonsingular curve over  $\mathbb{C}$ : for any d.f.k  $\omega$  and any d.s.k  $\eta$ , the cup-product  $\langle \eta, \omega \rangle_{\text{DR}}$  is given by the sum  $\sum_P \text{res}_P(f_P \cdot \omega)$ , where at each point  $P$ ,  $f_P$  is an element of the  $P$ -adic completion of the function field such that  $\eta = df_P$ . If one bears in mind that, analytically, we have  $\eta = -d\zeta$ , then the usual proof of Legendre's relation on an elliptic curve (cf. [46], 20.4.11) just becomes an analytic proof of Serre's cup-product formula in that particular case.

Returning to the relative elliptic curve  $\mathbb{C}/\mathbb{Z} + \mathbb{Z}\tau$  over  $\mathbb{R}$ , we have

$$(Al.3.14) \quad \begin{pmatrix} \nabla_t(\omega) \\ \nabla_t(\eta) \end{pmatrix} = \frac{1}{2\pi i} \begin{pmatrix} \frac{\pi^2 P}{3} & 1 \\ \frac{\pi^4}{9} (P^2 - \frac{12}{2\pi i} P) & -\frac{\pi^2}{3} P \end{pmatrix} \begin{pmatrix} \omega \\ \eta \end{pmatrix}$$

Consider now the differentials  $\omega_{\text{can}} = 2\pi i \omega$ ,  $\eta_{\text{can}} = \frac{1}{2\pi i} \eta$ , and let  $\theta = \frac{1}{2\pi i} \frac{d}{dt} = q \frac{d}{dq}$ . Then  $\omega_{\text{can}}$  is the canonical differential  $dt/t$  on the Tate curve  $\text{Tate}(q)$  over  $\mathbb{C}((q))$ ,  $\eta_{\text{can}}$  is the d.s.k. "dual" to  $\omega_{\text{can}}$  in the sense of the splitting (Al.2.6), and the Gauss-Manin connection on  $H^1_{\text{DR}}(\text{Tate}(q)/\mathbb{C}((q)))$  is given in terms of  $\omega = \frac{1}{2\pi i} \omega_{\text{can}}$  and  $\eta = 2\pi i \eta_{\text{can}}$  by

$$(Al.3.15) \quad \begin{aligned} \nabla(\theta) \begin{pmatrix} \omega \\ \eta \end{pmatrix} &= \frac{1}{2\pi i} \begin{pmatrix} \nabla_t(\omega) \\ \nabla_t(\eta) \end{pmatrix} = \frac{-1}{4\pi^2} \begin{pmatrix} \frac{\pi^2 P}{3} & 1 \\ \frac{\pi^4}{9} (P^2 - 12\theta P) & -\frac{\pi^2 P}{3} \end{pmatrix} \begin{pmatrix} \omega \\ \eta \end{pmatrix} \\ &= \begin{pmatrix} \frac{-P}{12} & \frac{-1}{4\pi^2} \\ \frac{\pi^2}{36} (P^2 - 12\theta P) & \frac{P}{12} \end{pmatrix} \begin{pmatrix} \omega \\ \eta \end{pmatrix} \end{aligned}$$

and hence is given in terms of  $\omega_{\text{can}}$ ,  $\eta_{\text{can}}$  by

$$(Al.3.16) \quad \nabla(\theta) \begin{pmatrix} \omega_{\text{can}} \\ \eta_{\text{can}} \end{pmatrix} = \begin{pmatrix} \frac{-P}{12} & 1 \\ \frac{P^2 - 12\theta P}{144} & \frac{P}{12} \end{pmatrix} \begin{pmatrix} \omega_{\text{can}} \\ \eta_{\text{can}} \end{pmatrix}.$$

(A1.3.17) The isomorphism  $\Omega^1 \cong \underline{\omega}^{\otimes 2}$ .

Let  $T$  be an arbitrary scheme,  $S$  a smooth  $T$ -scheme, and  $E/S$  an elliptic curve. For any derivation  $D \in \underline{\text{Der}}(S/T)$  and any nowhere vanishing invariant one-form  $\omega$  on  $E/S$ , we may apply  $\nabla(D)$  to  $\omega$ , view  $\nabla(D)$  as an element of  $H_{\text{DR}}^1(E/S)$ , and compute the cup-product  $\langle \omega, \nabla(D)\omega \rangle \in \mathcal{O}_S$ . We view this construction as defining a pairing between  $\underline{\text{Der}}(S/T)$  and  $\underline{\omega}^{\otimes 2}$ ,  $\underline{\omega}$  denoting the line bundle  $f_*\Omega_{E/S}^1$  on  $S$ , or equivalently as a morphism from  $\underline{\omega}^{\otimes 2}$  to  $\Omega_{S/T}^1$ . The dual mapping  $\underline{\text{Der}}(S/T) \rightarrow (R^1f_*(\mathcal{O}_E))^{\otimes 2}$  is precisely the tangent mapping of the classifying map from  $S$  to the modular stack (or to the modular scheme  $M_n$ , if we rigidify the situation with a level  $n$  structure). When this map is an isomorphism, the classifying map is étale, and we say that  $E/S$  is "almost modular".

Corollary A1.3.18. Consider the Tate curve  $\text{Tate}(q)$  over  $\mathbb{Z}((q))$ . The image of  $\omega_{\text{can}}^{\otimes 2}$  is the differential  $dq/q$  on  $\mathbb{Z}((q))$ .

Proof. The assertion is that  $\langle \omega_{\text{can}}, \nabla(\theta)\omega_{\text{can}} \rangle = 1$ . It suffices to check this over  $\mathbb{C}((q))$ , where we have  $\nabla(\theta)(\omega_{\text{can}}) = \frac{-P}{12}\omega_{\text{can}} + \eta_{\text{can}}$ . As  $\langle \omega_{\text{can}}, \omega_{\text{can}} \rangle = 0$ , and  $\langle \omega_{\text{can}}, \eta_{\text{can}} \rangle = 1$ , QED.

#### A1.4 The Gauss-Manin connection and Serre's $\partial$ operator ([41]): d'après Deligne

A series  $f(q) \in \mathbb{C}[[q]]$  is (the  $q$ -expansion of) a modular form of weight  $k$  if and only if  $f(q) \cdot (\omega_{\text{can}})^{\otimes k}$  extends to a "global" section of  $\underline{\omega}^{\otimes k}$ , i.e. one which is "defined" for all families of elliptic curves  $/\mathbb{C}$ , or equivalently if there exist integers  $a, b$  with  $a-b=k$  such that  $f(q) \cdot (\omega_{\text{can}})^{\otimes a} \cdot (\eta_{\text{can}})^{\otimes b}$  extends to a "global" section of  $\text{Symm}^{a+b}(H_{\text{DR}}^1)$ , in the same sense.

We now view the Gauss-Manin connection on  $H_{\text{DR}}^1(E/S)$ , where  $S$  is a smooth  $T$ -scheme, as an arrow  $\nabla: H_{\text{DR}}^1(E/S) \rightarrow H_{\text{DR}}^1(E/S) \otimes \Omega_{S/T}^1$ . Its  $k$ 'th symmetric power is a connection on  $\text{Symm}^k(H_{\text{DR}}^1)$ , so an arrow

$\text{Symm}^k(H^1) \longrightarrow \text{Symm}^k(H^1) \otimes_{S/T} \Omega_{S/T}^1$ . If  $E/S$  is "almost" modular, we have isomorphism  $\Omega_{S/T}^1 \sim \underline{\omega}^{\otimes 2}$ , so we may view this last arrow as an arrow  $\text{Symm}^k(H^1) \longrightarrow \text{Symm}^k(H^1) \otimes \underline{\omega}^{\otimes 2}$ . Suppose now that  $6 = 2 \cdot 3$  is invertible in  $S$ . Then we have a splitting  $H_{\text{DR}}^1(E/S) \sim \underline{\omega} \oplus \underline{\omega}^{-1}$ , whose  $k$ 'th symmetric power is a splitting  $\text{Symm}^k(H_{\text{DR}}^1(E/S)) \sim \sum_{j=0}^k \underline{\omega}^{\otimes k-2j}$ , and we may interpret

the Gauss-Manin connection as an arrow

$$\text{Al.4.1} \quad \sum_{j=0}^k \underline{\omega}^{\otimes k-2j} \longrightarrow \sum_{j=0}^k \underline{\omega}^{\otimes k-2j} \otimes \underline{\omega}^{\otimes 2} = \sum_{j=0}^k \underline{\omega}^{\otimes k+2-2j}.$$

Suppose that  $f$  is the  $q$ -expansion of a modular form of weight  $k$ . Then for any integers  $a$  and  $b$  such that  $a-b=k$ ,  $f \cdot (\omega_{\text{can}})^{\otimes a} \otimes (\eta_{\text{can}})^{\otimes b}$  extends to a global section of  $\text{Symm}^{a+b}(H^1)$ . Hence its image under the Gauss-Manin connection extends to a global section of  $\text{Symm}^{a+b}(H^1) \otimes \underline{\omega}^{\otimes 2}$ . But its image under Gauss-Manin is

$$\begin{aligned} & \theta(f) \cdot (\omega_{\text{can}})^{\otimes 2} \cdot (\omega_{\text{can}})^{\otimes a} \cdot (\eta_{\text{can}})^{\otimes b} \\ & + f \cdot a \cdot (\omega_{\text{can}})^{\otimes a-1} \left( \frac{-P}{12} \omega_{\text{can}} + \eta_{\text{can}} \right) \otimes (\omega_{\text{can}})^{\otimes 2} \otimes (\eta_{\text{can}})^b \\ & + f \cdot (\omega_{\text{can}})^{\otimes a} \cdot b \cdot (\eta_{\text{can}})^{\otimes b-1} \left( \frac{P^2 - 120P}{144} \omega_{\text{can}} + \frac{P}{12} \eta_{\text{can}} \right) \cdot (\omega_{\text{can}})^{\otimes 2} \end{aligned}$$

which we group according to the decomposition  $\text{Symm}^{a+b}(H^1) \otimes \underline{\omega}^2 \simeq \sum_{j=0}^{a+b} \underline{\omega}^{a+b+2-2j}$ ,

$$\begin{aligned} & = \left\{ \theta(f) - (a-b) \cdot f \cdot \frac{P}{12} \right\} \cdot (\omega_{\text{can}})^{\otimes a+2} \cdot (\eta_{\text{can}})^{\otimes b} \\ & + \{af\} \cdot (\omega_{\text{can}})^{\otimes a+1} \cdot (\eta_{\text{can}})^{\otimes b+1} \\ & + \left\{ bf \cdot \frac{P^2 - 120P}{144} \right\} (\omega_{\text{can}})^{\otimes a+3} \cdot (\eta_{\text{can}})^{\otimes b-1}. \end{aligned}$$

Thus we conclude that if  $f$  is modular of weight  $k=a-b$ , then

$$\text{Al.4.2} \quad \begin{cases} \theta(f) - kf \cdot \frac{P}{12} & \text{is modular of weight } k+2 = a+2-b \\ af & \text{is modular of weight } k = a-b \\ bf \cdot \left[ \frac{P^2 - 120P}{144} \right] & \text{is modular of weight } k+4 = a+3 - (b-1). \end{cases}$$

[Serre's  $\delta$  operator is  $\delta(f) = 12 \theta(f) - k \cdot P \cdot f$  for  $f$  modular of weight  $k$ , hence  $\delta f$  is modular of weight  $k+2$ .]

Corollary Al.4.3.  $P^2 - 12 \theta P$  is modular of weight 4, hence

$$\underline{P^2 - 12 \theta P = E_4} \stackrel{\text{dfn}}{=} Q.$$

Proof. Take  $f=1$  which is modular of weight  $0 = 1-1$ , to see that  $P^2 - 12 \theta P$  is modular of weight 4. As it has constant term 1, it is necessarily  $E_4$ .

Corollary Al.4.4. (Deligne)  $P = \frac{\theta \Delta}{\Delta}$ , where  $\Delta$  denotes the unique normalized cusp form of weight 12, the discriminant  $(E_4^3 - E_3^4)/1728$ .

Proof.  $\theta(\Delta) - \Delta \cdot P$  is a cusp form of weight 14 and level 1, and there are none save zero. QED

Corollary Al.4.5. The Gauss-Manin connection on  $H_{DR}^1$  of  $\text{Tate}(q)$  over  $\mathbb{Z}[1/6]((q))$  is given by

$$(Al.4.6) \quad \begin{pmatrix} \nabla(\theta)(\omega_{can}) \\ \nabla(\theta)(\eta_{can}) \end{pmatrix} = \begin{pmatrix} -P & 1 \\ Q & P/12 \end{pmatrix} \begin{pmatrix} \omega_{can} \\ \eta_{can} \end{pmatrix}.$$

Proof.  $\omega_{can}, \eta_{can}$  give a base of  $H_{DR}^1$  over  $\mathbb{Z}(\frac{1}{6})((q)) \subset \mathbb{C}((q))$ , and we have the desired assertion by transcendental means over  $\mathbb{C}((q))$ .

#### Remarks.

1. The value at 0 of the connection matrix is  $\begin{pmatrix} -1/12 & 1 \\ 1/44 & 1/12 \end{pmatrix}$ , which is a nilpotent matrix. This shows that the canonical extension (in the sense of [8]) of  $H_{DR}^1$  with its Gauss-Manin connection to  $\infty$  is given by the free module with base  $\omega_{can}, \eta_{can}$ .

2. We have  $(\nabla(\theta))^2(\omega_{can}) = 0$  (because the periods of  $\omega$  are 1 and  $\tau$  both killed by  $(\frac{d}{d\tau})^2$ ), hence by Igusa [17], the Hasse-invariant has a  $q$ -expansion  $f(q) \in \mathbb{F}_p[[q]]$  which satisfies  $\theta^2 f = 0$ , so writing  $f = \sum a_n q^n$ , we have  $(a_n)^2 = 0$ , hence  $a_n = 0$ , hence  $f = a_0 + a_p q^p + \dots$ . By direct

calculation (of the coefficient of  $x^{p-1}$  in the  $\frac{p-1}{2}$ -th power of  
 $4x^3 - \frac{E_4(0)}{12}x + \frac{E_6(0)}{216}$ ) =  $4x^3 - \frac{x}{12} + \frac{1}{216}$ , (cf.[26], 2.3.7.14), we compute  
 $a_0 = 1$ , hence  $f \equiv 1 \pmod{q^p}$ . As the same is also true for the reduction  
 $\pmod{p}$  of  $E_{p-1}$ , we have  $E_{p-1} \equiv f \pmod{(p, q^p)}$ , hence  $E_{p-1} - f$  is a cusp form  
 $\pmod{p}$  of weight  $p-1$  and level 1 with a zero of order  $\geq p$ , hence vanishes  
 $\pmod{p}$ . Thus  $E_{p-1} \pmod{p}$  is the Hasse invariant, and  $f(q)$  is identically 1.  
 (We gave Deligne's original and more conceptual proof of this fact in 2.1.)

(A1.5)

Formulas

(A1.5.0) For  $n \geq 3$ ,  $\bar{M}_n$  is proper and smooth over  $\mathbb{Z}[1/n]$ , and its inverse image over  $\mathbb{Z}[1/n, \zeta_n]$  is the disjoint union of  $\phi(n)$  proper smooth schemes with geometrically connected fibres  $\bar{M}_n^\zeta$ , one for each primitive  $n$ 'th root of unity  $\zeta$  (corresponding to the value of the e.m. pairing on the given basis of points of order  $n$ ). The  $\mathbb{Z}[1/n, \zeta_n]$  schemes  $\bar{M}_n^\zeta$  are non-canonically isomorphic to each other. We give below the formulas for their (common) genus, the (common) number of their cusps, and the degree of the invertible sheaf  $\omega$ .

The method of deducing such relations is very simple: one notes that by flatness, the fact that  $\bar{M}_n^\zeta - M_n^\zeta$  is a disjoint union of sections, and the isomorphism  $\omega^{\otimes 2} \cong \bigcap_{\bar{M}_n^\zeta / \mathbb{Z}[1/n, \zeta_n]}^1$  (log "cusps"), it suffices to calculate these

invariants for any geometric fibre  $\bar{M}_n^\zeta \otimes k$  [ $k$  any algebraically closed field containing  $1/n$ ]. One then applies the standard Hurwitz formula to the mor-

phism  $\bar{M}_n^\zeta \otimes k \rightarrow \mathbb{P}_k^1$  provided by the  $j$ -invariant. A closed point of  $\mathbb{P}_k^1$

other than  $\infty$  "is" an elliptic curve  $E$  over  $k$ , up to isomorphism. The

points of  $\bar{M}_n^\zeta \otimes k$  lying over it are the set of all level  $n$  structures on  $E$

such that the value of the e.m. pairing on the given basis of  $_n E$  is  $\zeta$ ,

modulo the natural action of  $\text{Aut}(E)$  of  $_n E$ . The cardinality of the fibre

over the point " $E$ " is thus  $\#SL_2(\mathbb{Z}/n\mathbb{Z})/\# \text{Aut}(E)$ . For  $j(E) \neq 0, 1728$ ,

$\text{Aut}(E) = \pm 1$ , and hence over  $\mathbb{P}_k^1 - \{0, 1728, \infty\}$ , the projection is étale of

degree  $\#SL_2(\mathbb{Z}/n\mathbb{Z})/2$ . The fibre over  $0$  has  $\#SL_2(\mathbb{Z}/n\mathbb{Z})/6$  points, and that

over  $1728$  has  $\#SL_2(\mathbb{Z}/n\mathbb{Z})/4$  points. The points over  $\infty$  are the cusps, each

of which is ramified of degree  $n$ , hence the number of cusps is  $\#SL_2(\mathbb{Z}/n\mathbb{Z})/2n$ .

Letting  $X$  denote the topological Euler characteristic, we thus have the formula:

$$X(\bar{M}_n^\zeta \otimes k) = \#SL_2(\mathbb{Z}/n\mathbb{Z}) \left[ \frac{1}{6} + \frac{1}{4} + \frac{1}{2n} \right] + \#SL_2(\mathbb{Z}/n\mathbb{Z})[1/2] \cdot X(\mathbb{P}_k^1 - \{0, 1728, \infty\}),$$

$$\text{i.e., } X(\bar{M}_n^\zeta \otimes k) = \#SL_2(\mathbb{Z}/n\mathbb{Z}) \left[ \frac{1}{6} + \frac{1}{4} + \frac{1}{2n} - \frac{1}{2} \right] = \#SL_2(\mathbb{Z}/n\mathbb{Z}) \cdot \left[ \frac{6-n}{12n} \right]. \text{ Now}$$

$\#SL_2(\mathbb{Z}/n\mathbb{Z}) = n^3 \prod_{p|n} (1 - \frac{1}{p^2})$ , so we have finally

(A1.5.1) Formulas

$$(A1.5.2) \quad 1 - \text{genus}(\bar{M}_n^\circ) = \frac{6-n}{24n} \#SL_2(\mathbb{Z}/n\mathbb{Z}) = \frac{n^2(6-n)}{24} \prod_{p|n} (1 - \frac{1}{p^2}) ;$$

$$(A1.5.3) \quad \# \text{ cusps on } \bar{M}_n^\circ = \frac{1}{2n} \#SL_2(\mathbb{Z}/n\mathbb{Z}) = \frac{n^2}{2} \prod_{p|n} (1 - \frac{1}{p^2}) ;$$

$$(A1.5.4) \quad \text{degree}(\underline{\omega}) \text{ on } \bar{M}_n^\circ = \frac{1}{2} \deg(\Omega^1(\log \text{cusps})) = \frac{1}{2}(2g-2 + \# \text{ cusps}) \\ = (\frac{n-6}{24n} + \frac{1}{4n}) \#SL_2(\mathbb{Z}/n\mathbb{Z}) \\ = \frac{1}{24} \#SL_2(\mathbb{Z}/n\mathbb{Z}) .$$

(A1.5.5) Sample consequences

$\bar{M}_n^\circ$  has genus zero only for  $n = 3, 4, 5$ , and genus one only for  $n = 6$ . We always have  $\deg(\underline{\omega}^{\otimes 2}) > 2g-2$ , but  $\deg(\underline{\omega}) > 2g-2$  only for  $3 \leq n \leq 11$ . For  $n = 3, 4, 5$ ,  $\bar{M}_n^\circ$  is a  $\mathbb{P}^1$ , hence  $\underline{\omega}$  is uniquely determined by its degree;  $\underline{\omega} = \mathcal{O}(1)$  on  $\bar{M}_3^\circ$ ,  $\underline{\omega} = \mathcal{O}(2)$  on  $\bar{M}_4^\circ$ ,  $\underline{\omega} = \mathcal{O}(5)$  on  $\bar{M}_5^\circ$ .

Appendix 2 - Frobenius

In this appendix we will explain the relation between the Frobenius endomorphism on  $p$ -adic modular forms and the action of Frobenius on the de Rham cohomology of "the" universal elliptic curve.

(A2.0) Let  $R$  be a  $p$ -adically complete ring,  $E/R$  an elliptic curve which modulo  $p$  has invertible Hasse invariant, and  $H \subset E$  its canonical subgroup. Let  $E' = E/H$ , and let  $\pi: E \rightarrow E'$  denote the projection. Then  $\pi$  induces an  $R$ -morphism  $\pi^*: H_{DR}^1(E'/R) \rightarrow H_{DR}^1(E/R)$ . Suppose now that  $R = M(W(\mathbb{F}_q), 1, n, 0)$ , the ring of  $p$ -adic modular functions of level  $n$  defined over  $W(\mathbb{F}_q)$ , where  $q$  is a power of  $p$  such that  $q \equiv 1 \pmod{n}$ . Let  $E/R$  be the universal curve with level  $n$  structure, such that Hasse is invertible mod  $p$ . As  $E' = E/H$  is a curve over  $R$  with level  $n$  structure and Hasse invertible mod  $p$ , it is "classified" by a unique homomorphism  $\phi: R \rightarrow R$  such that  $E' = E^{(\phi)}$ . This homomorphism  $\phi$  is precisely the Frobenius endomorphism of the ring  $M(W(\mathbb{F}_q), 1, n, 0)$  defined in [11] (the "Deligne-Tate mapping"). The induced homomorphism  $\pi^*: H_{DR}^1(E'/R) = H_{DR}^1(E^{(\phi)})/R = (H^1(E/R))^{(\phi)} \rightarrow H_{DR}^1(E/R)$  gives a  $\phi$ -linear endomorphism of  $H_{DR}^1(E/R)$ , which we denote  $F(\phi) = \pi^* \circ \phi^{-1}$  (to be compatible with the notations of [25]). Because  $\pi^*$  is induced by an  $R$ -morphism  $E \rightarrow E'$ , the endomorphism  $F(\phi)$  respects the Hodge filtration  $0 \rightarrow \underline{\omega} \rightarrow H_{DR}^1(E/R) \rightarrow \underline{\omega}^{-1} \rightarrow 0$ , and thus induces  $\phi$ -linear endomorphisms (still noted  $F(\phi)$ ) of  $\underline{\omega}$  and of  $\underline{\omega}^{-1}$ .

Lemma (A2.1). On  $\underline{\omega}$ ,  $F(\phi) = p\phi$ ; on  $\underline{\omega}^{-1}$ ,  $F(\phi) = \phi$ .

Proof. (We will suppress the level  $n$  structures, for simplicity.) Let  $f$  be a section of  $\underline{\omega}$ . Then  $f(E, \omega) \cdot \omega$  is a section of  $\Omega_{E/R}^1$ . By definition,  $\phi(f)$  is the section  $f(E/H, \tilde{\pi}^*(\omega)) \cdot \omega$  of  $\Omega_{E/R}^1$ . Because  $\tilde{\pi}$  is étale and  $E/H = E^{(\phi)}$ , we have  $\tilde{\pi}^*(\omega) = \lambda \cdot \omega^{(\phi)}$  with  $\lambda$  invertible in  $R$ . Thus  $f(E/H, \tilde{\pi}^*(\omega)) \cdot \omega = f(E^{(\phi)}, \lambda \omega^{(\phi)}) \cdot \omega = \lambda^{-1} \cdot \phi(f(E, \omega)) \cdot \omega$ . On the other hand,

$F(\phi)(f(E, \omega)) \stackrel{\text{dfn}}{=} \pi^*((f(E, \omega) \cdot \omega^{(\phi)})) = \phi(f(E, \omega)) \cdot \pi^*(\omega^{(\phi)}) = \phi(f(E, \omega)) \cdot \frac{p\omega}{\lambda}$ , [the last equality because  $p\omega = [p]^*(\omega) = \pi^*(\pi^*(\omega)) = \pi^*(\lambda \cdot \omega^{(\phi)}) = \lambda \cdot \pi^*(\omega^{(\phi)})$ ].

Thus  $F(\phi) = p\phi$  as  $\phi$ -linear endomorphism.

Similarly, for  $\omega^{-1}$ , a section  $f$  is a section  $f(E, \omega) \cdot \omega^{-1}$  of  $H^1(E, \mathcal{O}_E)$ , and  $\phi(f)$  is the section  $f(E/H, \pi^*(\omega)) \cdot \omega^{-1}$  of  $H^1(E, \mathcal{O}_E)$ . But as before  $E/H = E^{(\phi)}$ ,  $\pi^*(\omega) = \lambda\omega$  with  $\lambda$  invertible in  $R$ , and so  $\phi(f)$  is the section  $\lambda \cdot \phi(f(E, \omega)) \cdot \omega^{-1}$ . But  $F(\phi)(f(E, \omega) \cdot \omega^{-1}) = \pi^*(\phi(f(E, \omega) \cdot (\omega^{-1})^{(\phi)})) = \phi(f(E, \omega)) \cdot \pi^*(\omega^{-1})^{(\phi)}$ . So we must show that  $\pi^*(\omega^{-1})^{(\phi)} = \lambda \cdot \omega^{-1}$ , or by Serre duality, that  $\pi^*(\omega^{(\phi)}) = \lambda \cdot \omega$ , which was the definition of  $\lambda$ . QED

## A2.2 Calculation at $\infty$

The canonical subgroup of  $\text{Tate}(q)$  over  $\mathbb{Z}((q))$  is  $\mu_p$ , and the quotient is  $\text{Tate}(q^p) = \text{Tate}(q)^{(\phi)}$ , where  $(\phi f)(q) = f(q^p)$ . Thus we also have a  $\phi$ -linear endomorphism of  $H_{\text{DR}}^1(\text{Tate}(q)/\mathbb{Z}((q)))$ . Passing to  $\mathbb{C}((q))$  and viewing the situation analytically,  $\omega_{\text{can}}$  becomes the differential  $2\pi i dz$  on  $\mathbb{C}/\mathbb{Z} + \mathbb{Z}\tau$ , and the canonical subgroup becomes  $\frac{1}{p}\mathbb{Z}/\mathbb{Z}$ . The quotient is  $\mathbb{C}/\frac{1}{p}\mathbb{Z} + \mathbb{Z}\tau \xrightarrow{p} \mathbb{C}/\mathbb{Z} + \mathbb{Z}\cdot p\tau$ . In terms of the bases  $\gamma_i(\tau)$ ,  $i=1,2$  and  $\gamma_i(p\tau)$ ,  $i=1,2$  of  $H_1$ , we have  $\pi\gamma_1(\tau) = \gamma_1(p\tau)$ ,  $\pi(\gamma_2(\tau)) = p\gamma_2(p\tau)$ . It follows that  $\pi^*(\omega_{\text{can}}(q^p)) = \pi^*((\omega_{\text{can}}(q))^{(\phi)}) = p \cdot \omega_{\text{can}}(q)$  because both have the same periods:

$$\begin{aligned} \text{A2.2.1} \quad & \left\{ \begin{array}{l} \int_{\gamma_1(\tau)} \pi^*(\omega_{\text{can}}(q^p)) = \int_{\pi\gamma_1} \omega_{\text{can}}(q^p) = \int_{\gamma_1(p\tau)} \omega_{\text{can}}(q^p) = p\tau \\ \int_{\gamma_2(\tau)} \pi^*(\omega_{\text{can}}(q^p)) = \int_{\pi\gamma_2} \omega_{\text{can}}(q^p) = \int_{p\cdot\gamma_2(p\tau)} \omega_{\text{can}}(q^p) = p \cdot \tau \end{array} \right. \end{aligned}$$

By functionality,  $F(\phi)$  respects the Gauss-Manin connection, and  $\nabla(\theta)(\omega_{\text{can}}) = \frac{-p}{12}\omega_{\text{can}} + \eta_{\text{can}}$  is the unique (up to scalars) element of  $H_{\text{DR}}^1(\text{Tate}(q)/\mathbb{Z}((q)))$  killed by  $\nabla(\theta)$  (as a direct calculation shows - indeed

by (A14.6), this rank two differential equation over  $\mathbb{C}$  has non-trivial (unipotent) monodromy around  $q = 0$ , hence has at most one solution which is single-valued at  $q = 0$ . It follows that

$$(A2.2.2) \quad F(\phi)(\nabla(\theta)(\omega_{can})) = a \cdot \nabla(\theta)\omega_{can} \text{ for some } a \in \mathbb{Z}; \text{ explicitly,}$$

$$(A2.2.3) \quad \frac{-\phi(P)}{12} \pi^*(\omega_{can}^{(\phi)}) + \pi^*(\eta_{can}^{(\phi)}) = \frac{-aP}{12} \omega_{can} + a \cdot \eta_{can}, \text{ whence}$$

$$(A2.2.4) \quad F(\phi)(\eta_{can}) = \frac{p \cdot \phi(P) - aP}{12} \omega_{can} + a \cdot \eta_{can}.$$

Because  $\omega_{can}$  and  $\nabla(\theta)\omega_{can}$  give a base of  $H^1$  such that  $\omega_{can} \wedge \nabla(\theta)\omega_{can}$  is a constant base of  $H^2$ , the fact that  $\pi$  has degree  $p$  shows that  $a=1$ , so

$$(A2.2.5) \quad F(\phi)(\eta_{can}) = \frac{p \cdot \phi(P) - P}{12} \omega_{can} + \eta_{can}.$$

Thus the matrix of  $F(\phi)$  on  $H^1(\mathrm{Tate}(q)/\mathbb{Z}[1/6]((q)))$  is given by

$$(A2.2.6) \quad \begin{pmatrix} F(\phi)(\omega_{can}) \\ F(\phi)(\eta_{can}) \end{pmatrix} = \begin{pmatrix} p & 0 \\ \frac{p \cdot \phi(P) - P}{12} & 1 \end{pmatrix} \begin{pmatrix} \omega_{can} \\ \eta_{can} \end{pmatrix}.$$

To give formulas valid over  $\mathbb{Z}((q))$ , we use the base  $\omega_{can}, \nabla(\theta)(\omega_{can})$  of  $H^1_{DR}(\mathrm{Tate}(q)/\mathbb{Z}((q)))$ ; we have

$$(A2.2.7) \quad \begin{pmatrix} F(\phi)(\omega_{can}) \\ F(\phi)(\nabla(\theta)(\omega_{can})) \end{pmatrix} = \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} \omega_{can} \\ \nabla(\theta)(\omega_{can}) \end{pmatrix}.$$

### A2.3 The "canonical direction" in $H^1_{DR}$ (a special case of [25], [13])

We return to the universal situation  $R = M(W(\mathbb{F}_q), 1, n, 0)$ ,  $E/R$  universal. In terms of a base  $\omega, \eta$  of  $H^1_{DR}(E/R)$  adopted to the Hodge filtration, the matrix of  $F(\phi)$  has the shape:

$$(A2.3.1) \quad F(\phi) \begin{pmatrix} \omega \\ \eta \end{pmatrix} = \begin{pmatrix} p/\lambda & 0 \\ c & \lambda \end{pmatrix} \begin{pmatrix} \omega \\ \eta \end{pmatrix} \quad \text{with } \begin{cases} \lambda \in R \text{ invertible} \\ c \in R \end{cases} .$$

An argument of successive approximation shows that there is a unique element  $f \in R$  such that  $F(\phi)(\eta + f\omega) \in R \cdot (\eta + f\omega)$ ; indeed

$$(A2.3.2) \quad F(\phi)(\eta + f\omega) = c\omega + \lambda\eta + \phi(f)\frac{p}{\lambda} \cdot \omega = [c + \frac{p}{\lambda}\phi(f)]\omega + \lambda\eta ,$$

so we want  $f \in R$  to satisfy

$$(A2.3.3) \quad \begin{cases} \text{i.e.} & c + \frac{p}{\lambda}\phi(f) = \lambda f \\ & f = \frac{c}{\lambda} + \frac{p}{\lambda^2}\phi(f) \end{cases} .$$

Let us define a mapping  $T: R \rightarrow R$  by  $T(f) = \frac{c}{\lambda} + \frac{p}{\lambda^2}\phi(f)$ . It is immediate that  $T$  is a contraction mapping of  $R$  in its  $p$ -adic topology, so has a unique fixed point  $\lim T^n(0)$ , which is explicitly given by

$$(A2.3.4) \quad f = \frac{c}{\lambda} + \sum_{n \geq 1} \frac{\frac{p^n}{2} \frac{n(n-1)}{2} (1/\lambda) \cdot \phi^n(c)}{\phi \frac{n(n+1)}{2}(\lambda)} .$$

Of course, the choice of base is not canonical, nor need there exist a global basis (over all of  $R$ ), but the given construction does construct an  $F(\phi)$ -splitting of the Hodge filtration

$$(A2.3.5) \quad 0 \longrightarrow \underline{\omega} \longrightarrow H_{DR}^1(E/R) \xrightarrow{\quad} \underline{\omega}^{-1} \longrightarrow 0 .$$

Looking at  $\infty$ , we see that in terms of the base  $\omega_{can}, \nabla(\theta)(\omega_{can})$  of  $H_{DR}^1(Tate(q)/\mathbb{Z}(q))$ , we have simply "constructed" the vector  $\nabla(\theta)(\omega_{can})$ , which is indeed fixed by  $F(\phi)$ . Hence we have proven

Theorem A2.3.6. (Dwork) Let  $\bar{M}_n(W(\mathbb{F}_q), 1)$  denote the formal scheme over  $W(\mathbb{F}_q)$  which mod  $p^m$  is the open subset of  $\bar{M}_n \otimes_{W_m} W_m(\mathbb{F}_q)$  where  $E_{p-1}$  is invertible. The locally free rank two module on  $M_n(W(\mathbb{F}_q), 1)$  given by

$H_{DR}^1(E/M_n(W(\mathbb{F}_q), 1))$  admits a locally free extension  $H_{DR}^1(E/\bar{M}_n(W(\mathbb{F}_q), 1))$  which along any cusp is the  $W(\mathbb{F}_q)[[q]]$  submodule of  $H^1(\text{Tate}(q^n)/W(\mathbb{F}_q)((q)))$  spanned by  $\omega_{\text{can}}$  and by  $\nabla(\theta)(\omega_{\text{can}})$ . The Gauss-Manin connection over  $M_n(W(\mathbb{F}_q), 1)$  extends to a "connection with logarithmic poles" over  $\bar{M}_n(W(\mathbb{F}_q), 1)$ , and the  $\varphi$ -linear endomorphism  $F(\varphi)$  over  $M_n(W(\mathbb{F}_q), 1)$  extends to a  $\varphi$ -linear endomorphism, still noted  $F(\varphi)$ , over all of  $\bar{M}_n(W(\mathbb{F}_q), 1)$  (cf(A2.2.6) and (A2.2.7) for the explicit formulas defining these extensions). There is a canonical  $F(\varphi)$ -stable splitting of the Hodge filtration

$$0 \longrightarrow \underline{\omega} \longrightarrow H_{DR}^1(E/\bar{M}_n(W(\mathbb{F}_q), 1)) \xrightarrow{\quad} \underline{\omega}^{-1} \longrightarrow 0, \quad (\text{the } \underline{\omega} \text{ of which we denote } U \subset H_{DR}^1(E/\bar{M}_n(W(\mathbb{F}_q), 1)); \text{ it is a horizontal (by unicity!) } F(\varphi)\text{-stable rank one submodule}).$$

#### A2.4. P as a p-adic modular form of weight 2

Suppose now that  $p \neq 2, 3$ . Let  $R$  be any ring in which  $p$  is nilpotent,  $E/R$  an elliptic curve whose Hasse invariant modulo  $p$  is invertible, and  $U \subset H_{DR}^1(E/R)$  the inverse image of the canonical rank one submodule constructed above. (Strictly speaking, we must first choose a level  $n$  structure for some  $n \geq 3$  prime to  $p$  defined over an étale over-ring  $R'$  of  $R$ , and check that the  $U$  obtained in  $H_{R'}^1(E_{R'}/R')$  descends to a  $U \subset H_{DR}^1(E/R)$  which is independent of choices.) Let  $\omega$  be a nowhere-vanishing differential on  $E/R$  (which in any case exists locally on  $R$ ), and let  $\eta$  be the corresponding differential of the second kind (i.e.  $\omega = \frac{dX}{Y}$ ,  $\eta = \frac{XdX}{Y}$  as explained in (A1.2.4)). Because  $H^1 = R \cdot \omega + U$ , we see that if  $u \in U$  is a base of  $U$  (which in any case exists locally on  $R$ ) then the de Rham cup-product  $\langle \omega, u \rangle$  is invertible on  $R$ . We may then define a "function"  $\tilde{P}$  by the formula

$$(A2.4.1) \quad \tilde{P}(E/R, \omega) = 12 \frac{\langle \eta, u \rangle}{\langle \omega, u \rangle} \quad \text{for any base } u \text{ of } U.$$

Clearly the right-hand expression is independent of the choice of base  $u$  of  $U$ , and the effect of replacing  $\omega$  by  $\lambda\omega$ ,  $\lambda \in R^\times$  is to replace  $\eta$  by  $\lambda^{-1}\eta$ ,

hence  $\tilde{P}(E/R, \lambda\omega) = \lambda^{-2}\tilde{P}(E/R, \omega)$ . Hence  $\tilde{P}$  is a p-adic modular form of weight two and level one. Its q-expansion is

$$A2.4.2 \quad \tilde{P}(\text{Tate}(q), \omega_{\text{can}}) = 12 \frac{\langle \eta_{\text{can}}, u \rangle}{\langle \omega_{\text{can}}, u \rangle} = 12 \frac{\langle \eta_{\text{can}}, \nabla(\theta)(\omega_{\text{can}}) \rangle}{\langle \omega_{\text{can}}, \nabla(\theta)(\omega_{\text{can}}) \rangle}$$

because, formally at  $\infty$ ,  $U$  is spanned by  $\nabla(\theta)(\omega_{\text{can}})$ . If we denote by  $P(q)$  the series  $1 - 24 \sum \sigma_1(n)q^n$ , then by (A1.3.16) we have

$$\nabla(\theta)(\omega_{\text{can}}) = \frac{-P(q)}{12} \omega_{\text{can}} + \eta_{\text{can}}. \text{ Substituting into (A2.4.2) gives}$$

$$(A2.4.3) \quad \tilde{P}(\text{Tate}(q), \omega_{\text{can}}) = 12 \frac{\langle \eta_{\text{can}}, \frac{-P(q)}{12} \omega_{\text{can}} + \eta_{\text{can}} \rangle}{\langle \omega_{\text{can}}, \frac{-P(q)}{12} \omega_{\text{can}} + \eta_{\text{can}} \rangle} = \frac{12 \cdot P(q)}{12} \frac{\langle \eta_{\text{can}}, -\omega_{\text{can}} \rangle}{\langle \omega_{\text{can}}, \eta_{\text{can}} \rangle} = P(q).$$

This provides a modular proof that  $P$  is p-adically modular.

Appendix 3: Hecke polynomials, coherent cohomology, and U

In this final appendix, we explain the relation between Hecke polynomials mod  $p$ , coherent cohomology, and the endomorphism  $U$  of  $S(R, r, n, 0) \otimes K$  (notations as in (3.11)).

(A3.1.0) Let us begin by computing the trace of  $U^n$ , using the Dwork-Monsky fixed point formula. For simplicity, we take  $R$  to have residue field  $\mathbb{F}_p$ . Let  $R_m$  be its unramified extension of degree  $m$ , and  $K_m$  the fraction field of  $R_m$ . The endomorphism  $\varphi$  acts on the points of  $\bar{M}_n(\mathbb{F}_p, 1)$  with values in the algebraic closure  $\bar{\mathbb{F}}_p$  of  $\mathbb{F}_p$  as the relative Frobenius. For each integer  $m \geq 1$  we denote by  $T_m^O$  the set of  $\bar{\mathbb{F}}_p$ -valued points of  $\bar{M}_n(\mathbb{F}_p, 1)$  which are fixed by the  $m$ 'th iterate  $\varphi^m$ , i.e.,  $T_m^O$  is the set of  $\mathbb{F}_p$ -valued points of  $\bar{M}_n(\mathbb{F}_p, 1)$ . It is known (cf.[36]) that each element of  $T_m^O$  lifts to a unique  $R_m$ -valued point of the formal scheme  $\bar{M}_n(R, 1)$  which is fixed by  $\varphi$ . We denote by  $T_m$  the set of such  $\varphi$ -fixed  $R_m$ -valued points of  $\bar{M}_n(R, 1)$  (so  $T_m \cong T_m^O$  by reduction mod  $p$ ). The tangent space to  $\bar{M}_n(R, 1)$  at a point  $t \in T_m$  is a free  $R_m$ -module of rank one, on which  $\varphi^m$  acts as an  $R_m$ -linear endomorphism. We denote by  $d\varphi^m(t) \in R_m$  its "matrix". The Dwork-Monsky trace formula [36] is as follows:

$$(A3.1.1) \quad \text{trace}(U^n) = \sum_{t \in T_m} \frac{-1}{p^m} \frac{d\varphi^m(t)}{1-d\varphi^m(t)} .$$

It remains to determine the "local terms" in this formula. We begin with the cusps, i.e., the points  $t \in T_m$  whose image  $t_0 \in T_m^O$  is a cusp of  $\bar{M}_n(\mathbb{F}_q, 1)$ . Then, as we have seen, the overlying point  $t \in T_m$  is itself a cusp of  $\bar{M}_n(R_m, 1)$ , the completion of its local ring is  $R_m[[q]]$ , and the action of  $\varphi^m$  is given by  $q \mapsto q^{p^m}$ , whose linear term is zero. Hence  $d\varphi^m(t) = 0$  at the cusps.

Now suppose  $t \in T_m$  is not a cusp. Then the corresponding elliptic curve  $E_t$  is the so-called canonical lifting of its reduction  $E_{t_0}$  (because

the  $m'$ 'th iterate of the Frobenius endomorphism of  $E_{t_0}$  lifts to an endomorphism of  $E_t$ , namely  $m$ -fold division by the canonical subgroup - (cf. Messing [34]).

In this case it is known that the completion of the local ring at  $t$  is isomorphic to  $R_m[[X]]$ , where  $1+X$  is the Serre-Tate parameter (cf. ft note, p.186). Let  $\alpha \in \mathbb{Z}_p^X = \alpha(m, t_0)$  be the "matrix" of the action of the automorphism " $p^m$ -th power" acting on the Tate module  $T_p(E_{t_0}(\bar{\mathbb{F}}_p))$  of the reduced curve. Then (cf. Messing [34]), the action of  $\phi^m$  on  $R_m[[X]]$  is the one sending  $1+X \mapsto (1+X)^{p^m/\alpha^2}$ , hence  $d\phi^m(t) = p^m/\alpha(m, t_0)^2$ . Combining all this, we find the formula

$$(A3.1.2) \quad \text{trace}(U^m) = \sum_{\substack{t \in T_m \\ t \text{ not a cusp}}} \frac{1}{p^m - \alpha(m, t_0)^2} .$$

Denoting by  $T_m^\infty$  the set of  $\mathbb{F}_{p^m}$ -valued points of  $M_n(\mathbb{F}_p, 1)$ , i.e. the set of ordinary elliptic curves over  $\mathbb{F}_{p^m}$  with level  $n$  structure, we have

$$(A3.1.3) \quad \text{trace}(U^m) = \sum_{t_0 \in T_m^\infty} \frac{1}{p^m - \alpha(m, t_0)^2} .$$

The next step is to assemble this data into an expression for the Fredholm determinant  $\det(1-tU)$  as a product of L-series on  $M_n(\mathbb{F}_p, 1)$ . For any closed point  $x$  of  $M_n(\mathbb{F}_p, 1)$  (i.e., an orbit of  $\text{Gal}(\mathbb{F}_p/\mathbb{F}_p)$  acting on the  $\bar{\mathbb{F}}_p$ -valued points of  $M_n(\mathbb{F}_p, 1)$ ), we define  $\alpha(x) = \alpha(\deg(x), \tilde{x})$ , where  $\tilde{x}$  is any  $\mathbb{F}_{p^{\deg(x)}}$ -valued point of  $M_n(\mathbb{F}_p, 1)$  lying over  $x$ . For each integer  $r$ , the L-series  $L(M_n(\mathbb{F}_p, 1); \alpha^r; t)$  is the element of  $\mathbb{Z}_p[[t]]$  given by the infinite product over all closed points  $x$  of  $M_n(\mathbb{F}_p, 1)$

$$(A3.1.4) \quad \prod_x (1 - \alpha^r(x) \cdot t^{\deg(x)})^{-1} .$$

An elementary calculation now yields the following identity.

#### Identity A3.1.5

$$\det(1-tU) = \prod_{r \geq 0} L(M_n(\mathbb{F}_p, 1), \alpha^{-2(r+1)}, p^r t) \quad (\text{which is the key point})$$

of [12]). It shows independently of (3.11.7) that  $\det(1 - tU)$  lies in  $\mathbf{Z}_p[[t]]$ , and gives as a corollary the following congruence formula.

Corollary A3.1.6.  $\det(1 - tU) \equiv L(M_n(\mathbb{F}_p, 1), \alpha^{p-3}, t)$  modulo  $p \cdot \mathbf{Z}_p[[t]]$ .

Proof. the term with  $r=0$  remains modulo  $p$ , and modulo  $p$  the characters  $\alpha^{-2}$  and  $\alpha^{p-3}$  are equal, hence give L-series which coincide mod  $p$ .

But the character  $\alpha_0 = \alpha \bmod p$  is the one associated to the locally constant rank-one  $\mathbb{F}_p$ -étale sheaf  $R^1 f_* \mathbb{F}_p$ , and the L-series  $L(M_n(\mathbb{F}_p, 1), \alpha_0^{p-3}, t)$  is just the L-series  $L(M_n(\mathbb{F}_p, 1), (R^1 f_* \mathbb{F}_p)^{\otimes p-3}, t)$  associated to  $(R^1 f_* \mathbb{F}_p)^{\otimes p-3}$  in (4.1.1).

[NB the apparent inversion is due to the fact that  $\alpha$  describes the action of the arithmetic Frobenius on the étale quotient of  $\text{Ker } p$ , and hence by duality it is the action of the geometric Frobenius on its dual  $R^1 f_* \mathbb{F}_p$ .]

Furthermore, the sheaf  $R^1 f_* \mathbb{F}_p$  extends to a locally constant rank-one  $\mathbb{F}_p$ -étale sheaf on  $\bar{M}_n(\mathbb{F}_p, 1)$ , and the value of the extended character (still denoted  $\alpha_0$ ) is 1 at each cusp (cf. (4.2.1)). Thus we have

$$(A3.1.7) \quad L(M_n(\mathbb{F}_p, 1), \alpha_0^{p-3}, t) = [\prod_{\substack{x \text{ closed} \\ \text{point among} \\ \text{the cusps}}} (1 - t^{\deg x})] \cdot L(\bar{M}_n(\mathbb{F}_p, 1), (R^1 f_* \mathbb{F}_p)^{\otimes p-3}, t).$$

(A3.2.) Let  $H_{\text{comp}}^1$  denote the étale cohomology groups with compact supports  $H_{\text{comp}}^1(\bar{M}_n(\mathbb{F}_p, 1), (R^1 f_* \mathbb{F}_p)^{\otimes p-3})$ , which are  $\text{Gal}(\bar{\mathbb{F}}_p / \mathbb{F}_p)$ -modules over  $\mathbb{F}_p$ . Only  $H_{\text{comp}}^1$  is  $\neq 0$ . Let  $F_{\text{geom}} \in \text{Gal}(\bar{\mathbb{F}}_p / \mathbb{F}_p)$  denote the inverse of the automorphism  $x \mapsto x^p$ . According to ([47]), we have the formula

$$(A3.2.1) \quad L(\bar{M}_n(\mathbb{F}_p, 1), (R^1 f_* \mathbb{F}_p)^{\otimes p-3}, t) = \det(1 - t F_{\text{geom}}|_{H_{\text{comp}}^1}).$$

By (4.2.2), the invertible sheaf with  $p$ -linear "automorphism" corresponding to  $(R^1 f_* \mathbb{F}_p)^{\otimes p-3}$  is  $(\underline{\omega}^{3-p}, \phi)$  over  $\bar{M}_n(\mathbb{F}_p, 1)$ . But the pair  $(\underline{\omega}^{\otimes 3-p}, \phi)$  extends to an invertible sheaf with  $p$ -linear endomorphism on all of  $\bar{M}_n \otimes \mathbb{F}_p$ , namely to the invertible sheaf  $\underline{\omega}^{\otimes 3-p}$  on  $\bar{M}_n \otimes \mathbb{F}_p$ , with  $p$ -linear endomorphism

$$\bar{\varphi}: \underline{\omega}^{\otimes 3-p} \longrightarrow \underline{\omega}^{\otimes 3-p}$$

given by

$$\bar{\varphi}: g \longrightarrow A^{p-3} \cdot g^p$$

where  $A = E_{p-1} \bmod p$  denotes the Hasse invariant  $\in \Gamma(\bar{M}_n \otimes \mathbb{F}_p, \underline{\omega}^{\otimes p-1})$ ,  
(compare q-expansions!)

Because this extended endomorphism vanishes at the fibres outside  
 $\bar{M}_n(\mathbb{F}_p, 1)$ , we have an isomorphism

$$(A3.2.2) \quad H^1_{\text{comp}} \xrightarrow{\sim} \text{the fixed points of } \bar{\varphi} \text{ acting } p\text{-linearly on} \\ H^1(\bar{M}_n \otimes \mathbb{F}_p, \underline{\omega}^{\otimes 3-p})$$

under which the action of the arithmetic Frobenius on  $H^1_{\text{comp}}$  is its obvious action on the fixed points of  $\bar{\varphi}$ . It follows formally that we have the identity

$$(A3.2.3) \quad \det(1 - t F_{\text{geom}}|H^1_{\text{comp}}) = \det(1 - t \bar{\varphi}|H^1(\bar{M}_n \otimes \mathbb{F}_p, \underline{\omega}^{\otimes 3-p})) .$$

Putting this all together, we have the following congruence relation modulo  $p \mathbb{Z}_p[[t]]$ .

$$(A3.2.4) \quad \det(1 - t U) = \left[ \prod_{\substack{x \text{ closed} \\ \text{point lying} \\ \text{among the cusps}}} (1 - t^{\deg X}) \right] \cdot \det(1 - t \bar{\varphi}|H^1(\bar{M}_n \otimes \mathbb{F}_p, \underline{\omega}^{\otimes 3-p})) .$$

(A3.3) We now wish to calculate the determinant of  $\bar{\varphi}$  on  $H^1(\bar{M}_n \otimes \mathbb{F}_p, \underline{\omega}^{\otimes 3-p})$  by using Serre duality and the Cartier operator. For this it is convenient to abstract the situation slightly in the following lemma - in which  $X$  is  $\bar{M}_n \otimes \mathbb{F}_p$ ,  $\mathcal{L}$  is  $\underline{\omega}^{\otimes p-3}$ , and  $B$  is  $A^{p-3}$ .

Lemma A3.3.1. Let  $X$  be a projective smooth curve over  $\mathbb{F}_p$ ,  $\mathcal{L}$  an invertible sheaf, and  $B$  a section of  $\mathcal{L}^{\otimes p-1}$ . The composition

$$(A3.3.2) \quad \mathcal{L} \otimes \mathcal{O}_X^1 \xrightarrow{B} \mathcal{L}^{\otimes p} \otimes \mathcal{O}_X^1 \xrightarrow{C} \mathcal{L} \otimes \mathcal{O}_X^1$$

(where  $C$  is the Cartier operation, defined locally by  $C(\ell^p \otimes \omega) = \ell \otimes C(\omega)$ ) induces an endomorphism of  $H^0(X, \mathcal{L} \otimes \Omega^1_X)$  which is dual to the endomorphism of  $H^1(X, \mathcal{L}^{-1})$  induced by the endomorphism  $\check{\ell} \rightarrow B(\check{\ell})^p$  of  $\mathcal{L}^{-1}$ .

Proof. We begin by remarking that although  $X \hookrightarrow \mathbb{P}^n$  need not be geometrically connected, Serre duality on  $\mathbb{P}^n$  gives a perfect pairing between  $H^i(X, \mathcal{F})$  and  $\text{Ext}_{\mathcal{O}_X}^{1-i}(\mathcal{F}, \Omega_X^1)$  with values in  $H^n(\mathbb{P}^n, \Omega_{\mathbb{P}^n}^m) \cong \mathbb{F}_p$  for any coherent  $\mathcal{F}$  on  $X$ , which just as in the usual case may be computed via repartitions and residues. The desired duality now follows from the fact that if  $x \in X$  is a closed point, and  $\check{\ell}$  and  $\xi$  are meromorphic sections of  $\mathcal{L}^{-1}$  and  $\mathcal{L} \otimes \Omega^1_X$ , then  $\text{residue}_x(B \cdot (\check{\ell})^p \cdot \xi) = (\text{residue}_x(\check{\ell} \cdot C(B\xi)))^p$ , (the usual Cartier formula applied to the one-form  $B(\check{\ell})^p \xi$ ). QED

Lemma A3.3.3. Take  $X = \bar{M}_n \otimes \mathbb{F}_p$ ,  $\mathcal{L} = \underline{\omega}^{\otimes 2k}$ ,  $k \geq 0$ , and  $B = A^{2k}$  in the previous lemma. Under the isomorphism

$H^0(\bar{M}_n \otimes \mathbb{F}_p, \underline{\omega}^{\otimes 2k} \otimes \Omega^1_X) \cong H^0(\bar{M}_n \otimes \mathbb{F}_p, \underline{\omega}^{\otimes 2k+2} \otimes I(\text{cusps})) \cong$  the space of cusp forms of level  $n$  and weight  $2k+2$  over  $\mathbb{F}_p$ , the endomorphism  $\xi \rightarrow C(A^{2k}\xi)$  is the Hecke operator  $T_p$ .

Proof. It suffices to check the  $q$ -expansions. But in terms of  $q$ -expansions and the isomorphism  $\Omega_X^1(\log \text{cusps}) \cong \underline{\omega}^{\otimes 2}$ , if  $\xi$  in  $q$ -expansion is  $f(q)(\frac{dq}{q})^{k+1}$  then  $C(A^k \xi)$  in  $q$ -expansion is  $C(f(q) \cdot (\frac{dq}{q})^{\otimes (2kp+2)/2}) = C(f(q) \frac{dq}{q}) \cdot (\frac{dq}{q})^{\otimes k}$ . But if  $f(q) = \sum a_n q^n$ ,  $C(f(q) \frac{dq}{q}) = \sum (a_n q^n)^{1/p} \cdot q^n \frac{dq}{q}$ . Comparing this with the explicit formula (1.11.1.2) for  $T_p$  gives the desired result (because  $p^{2k-1} \equiv 0 \pmod{p!}$ ). QED

Putting this all together, we obtain the congruence relation  
 $\pmod{p} \mathbb{Z}_p[[t]] :$

$$(A3.3.3) \left\{ \begin{array}{l} \det(1-tU) \equiv [\prod_{\substack{x \text{ closed} \\ \text{point lying} \\ \text{among the cusps}}} (1-t^{\deg x})] \cdot \det \left( 1-tT_p \middle| \begin{array}{l} \text{cusp forms of weight } p-1 \\ \text{and level } n \end{array} \right) \\ \det \left( 1-tT_p \middle| \begin{array}{l} \text{cusp forms of weight } p-1 \\ \text{and level } n \end{array} \right) \equiv \det \left( 1-t \cdot C \circ A^{p-3} \middle| H^0(\bar{M}_n \otimes \mathbb{F}_p, \omega^{\otimes p-3} \otimes \mathbb{1}) \right) \end{array} \right.$$

This formula is the starting point for recent work of Adolphson [0].

FOOTNOTE : the first new sentence on page 182 is incorrect, though the tangent calculation we deduce from it is correct. The difficulty is that the Serre-Tate parameter is not "rational" over  $R_m$ , but only over  $R_\infty$ , the completion of the maximal unramified extension of  $R$ . However, if we view  $t$  as defining, by extension of scalars, a rational point of  $\bar{M}_n(R_\infty, 1)$ , then the completion of its local ring is indeed isomorphic to  $R_\infty[[X]]$ , where  $1+X$  is the Serre-Tate parameter (cf. Messing [34]). Further, the  $R_\infty$ -linear endomorphism of  $R_\infty[[X]]$  deduced from  $\phi^m$  by extension of scalars is given by  $1+X \mapsto (1+X)^{p^m/\alpha^2}$ , in the notation of page 182, and the formula (A3.1.2) remains true.

References

- O. Adolphson, A.: Thesis, Princeton University 1973.
1. Atkin, A. O. L.: Congruence Hecke operators, Proc. Symp. Pure Math., vol. 12,
2. ----- : Congruences for modular forms. Proceedings of the IBM Conference on Computers in Mathematical Research, Blaricum, 1966. North-Holland (1967).
3. ----- , and J. N. O'Brien: Some properties of  $p(n)$  and  $c(n)$  modulo powers of 13. TAMS 126, (1967), 442-459.
4. Cartier, P.: Une nouvelle opération sur les formes différentielles, C. R. Acad. Sci. Paris 244, (1957), 426-428.
5. ----- : Modules associés à un groupe formel commutatif. Courbes typiques. C. R. Acad. Sci. Paris 256, (1967), 129-131.
6. ----- : Groupes formels, course at I.H.E.S., Spring, 1972. (Notes by J. F. Boutot available (?) from I.H.E.S., 91-Bures-sur-Yvette, France.)
7. Deligne, P.: Formes modulaires et représentations  $\ell$ -adiques. Exposé 355. Séminaire N. Bourbaki 1968/1969. Lecture Notes in Mathematics 179, Berlin-Heidelberg-New York: Springer 1969.
8. ----- : Equations Différentielles à Points Singuliers Réguliers. Lecture Notes in Mathematics 163. Berlin-Heidelberg-New York: Springer 1970.
9. ----- : Courbes Elliptiques: Formulaire (d'après J. Tate). Multigraph available from I.H.E.S., 91-Bures-sur-Yvette, France, 1968.
10. ----- , and M. Rapoport: Article in preparation on moduli of elliptic curves.
11. Dwork, B.:  $p$ -adic cycles, Pub. Math. I.H.E.S. 37, (1969), 27-115.
12. ----- : On Hecke Polynomials, Inventiones Math. 12(1971), 249-256.
13. ----- : Normalized Period Matrices I, II. Annals of Math. 94, 2nd series, (1971), 337-388, and to appear in Annals of Math.
14. ----- : Article in this volume.
15. Grothendieck, A.: Fondements de la Géométrie Algébrique, Secrétariat Mathématique, 11 rue Pierre Curie, Paris 5<sup>e</sup>, France, 1962.
- 15 bis -----: Formule de Lefschetz et rationalité des fonctions L, Exposé 279, Séminaire Bourbaki 1964/1965.

16. Hasse, H. : Existenz separabler zyklischer unverzweigter Erweiterungskörper vom Primzahlgrade über elliptischen Funktionenkörpern der Charakteristik  $p$ . J. Reine angew. Math. 172, (1934), 77-85.
17. Igusa, J. : Class number of a definite quaternion with prime discriminant, Proc. Natl. Acad. Sci. 44, (1958), 312-314.
18. -----: Kroneckerian model of fields of elliptic modular functions, Amer. J. Math. 81, (1959), 561-577.
19. -----: Fibre systems of Jacobian varieties III, Amer. J. Math. 81, (1959), 453-476.
20. -----: On the transformation theory of elliptic functions, Amer. J. Math. 81, (1959), 436-452.
21. -----: On the algebraic theory of elliptic modular functions, J. Math. Soc. Japan 20, (1968), 96-106.
22. Ihara, Y.: An invariant multiple differential attached to the field of elliptic modular functions of characteristic  $p$ . Amer. J. Math. 78, (1971), 137-147.
23. Katz, N.: Une formule de congruence pour la fonction zeta. Exposé 22, SGA 7, 1969, to appear in Springer Lecture Notes in Mathematics. (Preprint available from I.H.E.S., 91-Bures-sur-Yvette, France.)
24. -----: Nilpotent connections and the monodromy theorem - applications of a result of Tjurittin, Pub. Math. I.H.E.S. 39, (1971), 355-412.
25. -----: Travaux de Dwork. Exposé 409, Séminaire N. Bourbaki 1971/72, Springer Lecture Notes in Mathematics, 317, (1973), 167-200.
26. -----: Algebraic solutions of differential equations ( $p$ -curvature and the Hodge filtration). Invent. Math. 18, (1972), 1-118.
27. -----, and T. Oda: On the differentiation of de Rham cohomology classes with respect to parameters, J. Math. Kyoto Univ. 8, (1968), 199-213.
28. Koike, M.: Congruences between modular forms and functions and applications to a conjecture of Atkin, to appear.
29. Lehner, J.: Lectures on modular forms. National Bureau of Standards, Applied Mathematics Series 61, Washington, D.C., 1969.
30. Lubin, J., J.-P. Serre and J. Tate: Elliptic curves and formal groups, Woods Hole Summer Institute 1964 (mimeographed notes).

31. Lubin, J.: One-parameter formal Lie groups over p-adic integer rings,  
Ann. of Math. 80, 2nd series (1964), 464-484.
32. -----: Finite subgroups and isogenies of one-parameter formal groups,  
Ann. of Math. 85, 2nd series (1967), 296-302.
33. -----: Newton factorizations of polynomials, to appear.
- 33.bis -----: Canonical subgroups of formal groups, secret notes.
34. Messing, W.: The crystals associated to Barsotti-Tate groups: with  
applications to abelian schemes. Lecture Notes in Mathematics 264,  
Berlin-Heidelberg-New York: Springer 1972.
35. -----: Two functoriality, to appear.
36. Monsky, P.: Formal cohomology III - Trace Formulas. Ann. of Math. 93,  
2nd series (1971), 315-343.
37. Newman, M.: Congruences for the coefficients of modular forms and for  
the coefficients of  $j(\tau)$ . Proc. A.M.S. 9, (1958), 609-612.
38. Roquette, P.: Analytic theory of elliptic functions over local fields.  
Göttingen: Vanderhoeck und Ruprecht, 1970.
39. Serre, J.-P.: Endomorphismes complètement continus des espaces de Banach  
p-adiques. Pub. Math. I.H.E.S. 12, (1962).
40. -----: Course at Collège de France, spring 1972.
41. -----: Congruences et formes modulaires. Exposé 416, Séminaire N.  
Bourbaki, 1971/72, Lecture Notes in Math. 317, (1973), Springer, 319-338.
42. -----: Formes modulaires et fonctions zêta p-adiques, these Proceedings.
- 42<sup>1</sup>. -----: Cours d'arithmétique. Paris: Presses Univ. de France 1970.
43. Swinnerton-Dyer, H. P. F.: On  $\ell$ -adic representations and congruences for  
coefficients of modular forms, these Proceedings.
44. Tate, J.: Elliptic curves with bad reduction. Lecture at the 1967  
Advanced Science Summer Seminar, Bowdoin College, 1967.
45. -----: Rigid analytic spaces. Inventiones Math. 12, (1971), 257-289.
46. Whittaker, E. T. and G. N. Watson: A course of modern analysis,  
Cambridge, Cambridge University Press, 1962.

47. Deligne, P., Cohomologie à Supports Propres, Exposé 17, SGA 4, to appear in Springer Lecture Notes in Mathematics.
48. Roos, J. E., Sur les foncteurs dérivés de  $\lim_{\leftarrow}$ . Applications, C. R. Acad. Sci. Paris, tome 252, 1961, pp. 3702-04.