Higher congruences between modular forms

By NICHOLAS M. KATZ

Introduction

The problem of determining all the congruences modulo a prime p that hold between the q-expansions of modular forms on SL(2, $\mathbf{Z}$) was solved by Swinnerton-Dyer [8], and the solution is one of the key ingredients in Serre's approach to the Kubota-Leopoldt zeta function via his p-adic modular forms [6], [7].

This paper gives an explicit solution to the problem of finding all congruences which hold modulo arbitrary powers of p. The key point is the *simultaneous* consideration of *all* congruences modulo *all* powers of p, in the form of the "ring of divided congruences", whose elements are those finite sums $\sum f_i$ of modular forms over $\mathbf{Q}_p$, f_i of weight i, such that the *sum* of the q-expansions $\sum f_i(q)$ has coefficients in $\mathbf{Z}_p$. It turns out (cf. 2.1) that the p-adic completion of *this* ring is in a natural way the coordinate ring of a certain "moduli problem", which we may loosely describe as that of elliptic curves over p-adic ground-rings together with isomorphisms of their formal groups with the formal multiplicative group.

The first part of the paper is devoted to working out this isomorphism, and to giving as a corollary an "abstract" set of generators for the relations modulo any power of p. In the second part we restrict ourselves to primes different from 2 and 3, and use the *Weierstrass* model of elliptic curves to give *explicit* generators for the relations modulo all powers of p (cf. 5.5). In a first appendix, we give the modular interpretation of our construction, and explain the *modular* meaning of Serre's "p-adic modular forms of weight χ". A second appendix spells out how to "transfer" congruences in q-expansion to congruences in the neighborhood of *any* ordinary elliptic curve. In a final appendix, we give Deligne's generalization to "false" modular forms of our interpretation of divided congruences by a moduli problem.

In the course of this work, we realized that the systematic consideration of the above-mentioned moduli problem led to an approach to the Kubota-Leopoldt zeta function which is a sort of "fibre product" of Serre's approach through constant terms of Eisenstein series and of Mazur's approach through his "p-adic measures". We hope to return to this question in a later paper.

A word about notation: When we write E_{p-1}, then for $p \geqq 5$ we mean the usual Eisenstein series

$$E_{p-1} = 1 - \frac{2(p-1)}{B_{p-1}} \sum_{n \geq 1} q^n \sum_{d \mid n} d^{p-2}$$

which is a modular form of weight $p-1$ over $\mathbf{Q} \cap \mathbf{Z}_p$, whose reduction mod p is the Hasse invariant. Unfortunately for $p = 2$ or $p = 3$ there are no modular forms over $\mathbf{Q} \cap \mathbf{Z}_p$ of level one and weight $p - 1$. In compensation, when $p = 2$ or 3, we will always consider modular forms of some fixed *level* $N \geqq 3$ prime to p, and simply denote by E_{p-1} *any* fixed level N modular form of weight $p - 1$ whose reduction modulo p is the Hasse invariant. For $p = 3$ and $N \geqq 3$ prime to p, such liftings always exist, while for $p = 2$, and N odd such liftings are only known to exist for $3 \leqq N \leqq 11$, and (hence) for any *multiples* of these N. (For example, when $p = 3$, the level two modular form whose value on $(y^2 = x(x-1)(x-\lambda), dx/y)$ is $-1 - \lambda$ provides such a lifting to all *even* levels, and for $p = 2$ the modular form of level-three "μ" on the level-3 curve $x^3 + y^3 + 1 = 3\mu xy$ provides such a lifting to odd levels divisible by three.)

(1.0) Fix a prime number p, and an integer $N \geqq 3$ prime to p, and if $p = 2$, assume further that N is a multiple of either 3, 5, 7, or 11. Let k be a perfect field of characteristic p, which contains a chosen primitive N^{th} root of unity ζ. For each integer $m \geqq 1$, write W_m for the Witt vectors $W_m(k)$ of length m, and denote $W_\infty(k)$ simply as W. The unique primitive N^{th} root of unity in W which lifts ζ, the "Teichmüller representative", will also be denoted ζ.

Let M^0 be the moduli scheme over W which classifies isomorphism classes of elliptic curves over W-algebras together with a level-N structure of determinant ζ, and let M be its canonical compactification. Thus M is a proper smooth curve over W with geometrically connected fibres, and the difference $M - M^0$ is a disjoint union of sections, the "cusps", the completion along each of which "is" $W[[q]]$; over the "punctured disc" $W((q))$ around each cusp, the universal curve with level-N structure becomes a "Tate curve" Tate (q^N), with one of its level-N structures. For each integer $m \geqq 1$, we put $M_m^0 = M^0 \otimes_W W_m$, $M_m = M \otimes_W W_m$. Let S_m^0 (resp. S_m) denote the open subscheme of M_m^0 (resp. M_m) where the Hasse invariant mod p (or equivalently E_{p-1}) is *invertible*. The schemes S_m^0 and S_m are *affine* smooth curves over W_m, with geometrically irreducible special fibre. We have

$$S_m = S_{m+1} \otimes_{W_{m+1}} W_m , \qquad S_m^0 = S_{m+1}^0 \otimes_{W_{m+1}} W_m .$$

(1.1) Let $E \to S_m^0$ be the inverse image on S_m^0 of the universal elliptic curve. Because the Hasse invariant is invertible, it follows that for each integer $n \geqq 1$, the kernel of multiplication by p^n on E, noted ${}_{p^n}E$, is an extension

(1.1.1) $$0 \longrightarrow {}_{p^n}\hat{E} \longrightarrow {}_{p^n}E \longrightarrow {}_{p^n}E^{et} \longrightarrow 0$$

where

(1.1.2) ${}_{p^n}\hat{E}$ is the kernel of p^n in the *formal group* $\hat{E}$ of E; it is a finite flat group-scheme over S_m^0 which locally for the etale topology on S_m^0 is isomorphic to μ_{p^n} and where ${}_{p^n}E^{et}$ is the Cartier dual of ${}_{p^n}\hat{E}$, locally for the etale topology on S_m^0 isomorphic to $\mathbf{Z}/p^n\mathbf{Z}$.

Thus the group-scheme ${}_{p^n}E^{et}$, as a "twisted" version of $\mathbf{Z}/p^n\mathbf{Z}$, is described by an element of $H^1_{et}(S_m^0, \operatorname{Aut}(\mathbf{Z}/p^n\mathbf{Z})) = \operatorname{Hom}(\pi_1(S_m^0), (\mathbf{Z}/p^n\mathbf{Z})^x)$, i.e., it is described by a *character* χ_n of $\pi_1(S_m^0) = \pi_1(S_1^0)$ with values in $(\mathbf{Z}/p^n\mathbf{Z})^x$. (For m variable, the shemes S_m^0 are deduced one from another by reduction modulo a nilpotent ideal, hence have canonically isomorphic fundamental groups.) For variable n, the characters χ_n fit together to give a character χ of $\pi_1(S_m^0) = \pi_1(S_1^0)$ with values in $\mathbf{Z}_p^\times$, such that $\chi_n = \chi \bmod p^n$.

(1.2) We now recall the fundamental facts (proven in [3, Ch. 4]) about the characters χ_n and the coverings they define.

(1.2.1) The characters χ_n, χ on $\pi_1(S_m^0)$ extend to characters still noted χ_n, χ on $\pi_1(S_m)$, which are *trivial* on the decomposition groups at the cusps (which are the points of $S_m - S_m^0$).

(1.2.2) The characters $\chi_n\colon \pi_1(S_m) \to (\mathbf{Z}/p^n\mathbf{Z})^\times$ are surjective (for any non-void Zariski open set $U \subset S_m$, the composite $\chi_m\colon \pi_1(U) \to (\mathbf{Z}/p^n\mathbf{Z})^\times$ remains surjective simply because $\pi_1(U) \to \pi_1(S_m)$ is surjective!).

(1.2.3) Let $T_{m,n} \to S_m$ be the etale covering of S_m defined by (kernel of the) character $\chi_n\colon \pi_1(S_m) \to (\mathbf{Z}/p^n\mathbf{Z})^\times$. The scheme $T_{m,n}$ is a smooth affine W_m-scheme with geometrically connected special fibre. For fixed n, we have

(1.2.3.1) $$T_{m+1,n} \otimes W_m \simeq T_{m,n}$$

and for fixed m we have

(1.2.3.2) $$T_{m,n+1} \xrightarrow{pr_{m,n+1}} T_{m,n} \longrightarrow \cdots \longrightarrow T_{m,1} \longrightarrow S_m .$$

The inverse image of any cusp of S_m is the disjoint unit of $\varphi(p^n) = (p-1)p^{n-1} = \#((\mathbf{Z}/p^n\mathbf{Z})^\times)$ W_m-sections of $T_{m,n}$ called the *cusps* of $T_{m,n}$, and the completion of $T_{m,n}$ along any of its cusps is isomorphic to the completion of S_m along the corresponding cusp (both being isomorphic to $W_m[[q]]$). (This last fact is simply because χ_n is trivial on the decomposition group at each cusp: In down-to-earth terms, a cusp of S_m is represented by a Tate curve Tate (q^N) with one of its level-N structures. Now the formal group of the Tate curve *is* isomorphic to $\hat{\mathbf{G}}_m$, hence the etale quotient of the kernel of p^n on the Tate curve isomorphic to $\mathbf{Z}/p^n\mathbf{Z}$ over $W_m[[q]]$; the $\varphi(p^n)$ cusps of $T_{m,n}$ lying over the chosen cusp of S_m are simply the possible choices of this last isomorphism. For fixed m, the schemes $\{T_{m,n}\}$ form a "pro-algebraic" etale covering of S_m with galois group $\mathbf{Z}_p^\times$.)

(1.2.4) There exists on $T_{m,m}$ an invertible section ω_{can} of the (inverse image from S_m of the) invertible sheaf $\underline{\omega}$ whose q-expansion at each cusp of $T_{m,n}$ is a constant $\alpha \in (\mathbf{Z}/p^m\mathbf{Z})^\times \subset W_m^\times \subset W_m[[q]]$. The constant varies with the cusp, but when we fix a cusp of S_m, the q-expansions of ω_{can} at the $\varphi(p^m)$ cusps lying over run exactly once over the elements of $(\mathbf{Z}/p^m\mathbf{Z})^\times$. The set of possible ω_{can} on $T_{m,m}$ is principally homogeneous under (multiplication by) $(\mathbf{Z}/p^m\mathbf{Z})^\times$. (In fact, according to the main result of [3, Ch. 4] the scheme $T_{m,m}$ is defined by "adjoining" to S_m such a section ω_{can}.)

The $\varphi(p^m)$ various ω_{can} are obtained "explicitly" as follows: Over $T_{m,m}$ the kernel of p^m in the formal group $\hat{E}$ admits $\varphi(p^m)$ isomorphisms to μ_{p^m}. We may pull back the canonical differential $dT/(1+T)$ on $\mu_{p^m} = \operatorname{Spec}(\mathbf{Z}[T]/(1+T)^{p^m}-1)$ by each of these isomorphisms, and obtain $\varphi(p^m)$ invariant differentials on ${}_{p^m}\hat{E}$. Because we are in "characteristic p^m", invariant differentials on ${}_{p^m}\hat{E}$ extend uniquely to invariant differentials on $\hat{E}$; these in turn extend uniquely to invariant differentials on E over the open set $T^0_{m,m} = T_{m,m} \mid S^0_m$ which when viewed as sections of $\underline{\omega}$ over $T^0_{m,m}$ are precisely the restrictions to $T^0_{m,m}$ of the sections ω_{can}.

(1.3) We *fix* once and for all a compatible system of choices $\{\omega_{\text{can}}(m)\}_m$ of the ω_{can} on the various $T_{m,m}$, the compatibility being that under the diagram

$$\begin{array}{l} T_{m,m+1} \simeq T_{m+1,m+1} \otimes W_m \hookrightarrow T_{m+1,m+1} \\ \Big\downarrow pr_{m,m+1} \\ T_{m,m} \end{array}$$

we have

$$\omega_{\text{can}}(m+1) \bmod p^m = pr^*_{m,m+1}(\omega_{\text{can}}(m)) \,.$$

Such choices are possible, and the set of all such is principally homogeneous under $(\mathbf{Z}_p)^\times$. There is a unique isomorphism of $\mathbf{Z}_p^\times$ with $\varprojlim_n \operatorname{Aut}(T_{m,n}/S_m)$ which is independent of m (i.e., compatible with the canonical isomorphisms

$\operatorname{Aut}(T_{m+1,n}/S_{m+1}) \simeq \operatorname{Aut}(T_{m,n}/S_m))$ and under which

$$[\alpha](\omega_{\mathrm{can}}) = \alpha^{-1}\omega_{\mathrm{can}}$$

(meaning that, $\forall\, m$, $[\alpha \bmod p^m](\omega_{\mathrm{can}}(m)) = (\alpha^{-1} \bmod p^m)\cdot\omega_{\mathrm{can}}(m))$.

(1.3.1) Notice that if we fix a cusp $\alpha_{1,0}$ of S_1, there are uniquely determined cusps $\alpha_{m,n}$ of all $T_{m,n}$ (we put $T_{m,0} = S_m$) such that $\alpha_{m,n+1}$ lies over $\alpha_{m,n}$, such that $\alpha_{m+1,n} \bmod p^m$ is $\alpha_{m,n}$, and such that $\omega_{\mathrm{can}}(m)$ has q-expansion $1 \in W_m[[q]]$ at the cusp $\alpha_{m,m}$.

Definition of the fundamental homomorphism

(1.4) For each integer $m \geqq 1$, let R_m be the graded ring of holomorphic modular forms defined over W_m, of level N and type ζ, i.e.,

$$R_m = \bigoplus_{k\geq 0} H^0(M_m, \underline{\omega}^{\otimes k}) \tag{1.4.1}$$

and let R_∞ be the graded ring of holomorphic modular forms defined over W, of level N and type ζ, i.e.,

$$R_\infty = \bigoplus_{k\geq 0} H^0(M, \underline{\omega}^{\otimes k})\ . \tag{1.4.2}$$

For $3 \leqq N \leqq 11$, we have $R_\infty/p^m R_\infty \simeq R_m$, but for $N \geqq 12$ it can happen that this map fails to be surjective on the graded part of degree *one*, though it is always injective, and is always an isomorphism on all the other graded pieces (cf. [3, 1.7]). For any fixed N, it will be true that $R_\infty/p^m R_\infty \xrightarrow{\sim} R_m$ for all but finitely many primes p.

Let $V_{m,n}$ denote the coordinate ring of $T_{m,n}$ (with the convention that $T_{m,0} = S_m$). The rings $V_{m,n}$ are smooth W_m-algebras, and every choice of cusp on $V_{m,n}$ gives us an inclusion

$$V_{m,n} \subset W_m[[q]]\ .$$

LEMMA 1.4.3. *The cokernel $W_m[[q]]/V_{m,n}$ is flat over W_m.*

Proof. Modulo p, the inclusion $V_{m,n} \to W_m[[q]]$ becomes the inclusion $V_{1,n} \hookrightarrow k[[q]]$. Q.E.D.

The rings $V_{m,n}$ sit in chains for variable n,

$$V_{m,0} \subset V_{m,1} \subset V_{m,2} \subset \cdots \tag{1.4.4}$$

and for variable m are related by canonical isomorphisms

$$V_{m+1,n}/p^m V_{m+1,n} \xrightarrow{\sim} V_{m,n}\ . \tag{1.4.5}$$

Let $V_{m,\infty} = \bigcup_{n\geq 1} V_{m,n}$; then any choice of cusp $\alpha_{1,0}$ on S_1 determines a compatible system of cusps on all $T_{m,n}$ (cf. (1.3.1)), and hence an inclusion

$$V_{m,\infty} \hookrightarrow W_m[[q]]\ . \tag{1.4.6}$$

For variable m, we have canonical isomorphisms

$$V_{m+1,\infty}/p^m V_{m+1,\infty} \xrightarrow{\sim} V_{m,\infty} . \tag{1.4.7}$$

For each integer $m \geqq 1$, we will define a homomorphism of (non-graded) rings

$$\beta_m \colon R_m \longrightarrow V_{m,m} \subset V_{m,\infty} \tag{1.4.8}$$

as follows: Let $f_i \in H^0(M_m, \underline{\omega}^{\otimes i})$ be a modular form of weight i. Then by restriction, f_i determines a section of $\underline{\omega}^{\otimes i}$ over S_m, and then by inverse image determines a section of $\underline{\omega}^{\otimes i}$ over $T_{m,m}$. But over $T_{m,m}$ we are given an invertible section $\omega_{\text{can}} = \omega_{\text{can}}(m)$ of $\underline{\omega}$, and hence the ratio $f_i/(\omega_{\text{can}}(m))^{\otimes i}$ is a well-defined section of the structural sheaf of $T_{m,m}$. Thus we define

$$\beta_m\left(\sum f_i\right) = \sum f_i/(\omega_{\text{can}}(m))^{\otimes i} . \tag{1.4.9}$$

(1.4.9.1) We define $\beta_\infty \colon R_\infty \to V_{\infty,\infty} = \varprojlim_m V_{m,\infty}$ by passage to the inverse limit.

LEMMA 1.5. *Let $\alpha_{1,0}$ be a cusp of S_1, and $\alpha_{m,m}$ the compatible system of cusps of the $T_{m,n}$ defined* (1.3.1) *by the choice of ω_{can}. For any element $f_i \in H^0(M_m, \underline{\omega}^{\otimes i})$, denote by $f_i(q)$ its q-expansion in $W_m[[q]]$ at the cusp $\alpha_{m,0}$. Then q-expansion of $\beta_m(\sum f_i)$ at the cusp $\alpha_{m,m}$ of $V_{m,m}$ is $\sum f_i(q) \in W_m[[q]]$.*

Proof. The q-expansion of $\omega_{\text{can}}(m)$ at $\alpha_{m,m}$ is the element $1 \in W_m[[q]]$.
Q.E.D.

COROLLARY 1.6. *Let $\sum f_i \in R_m$, and let $m_1 \leqq m$. If it is true at one cusp of M_m that $\sum f_i(q) \equiv 0 \bmod p^{m_1}$ in $W_m[[q]]$, then it is true at every cusp.*

Proof. By (1.5), the hypothesis implies that $\beta_m(p^{m-m_1} \sum f_i)$ has q-expansion zero at the cusp $\alpha_{m,m}$ of $T_{m,m}$ determined by $\alpha_{m,0}$. But this means that $\beta_m(p^{m-m_1} \sum f_i) = 0$, hence has q-expansion zero at every cusp of $T_{m,m}$, hence that $\beta_m(\sum f_i)$ has q-expansion $\equiv 0\ (p^{m_1})$ at every cusp of $T_{m,m}$, hence that $\sum f_i(q) \equiv 0\ (p^{m_1})$ at *every* cusp of M. Q.E.D.

COROLLARY 1.7. *If $\sum f_i \in R_m$, and if for some $m_1 \leqq m$, $\sum f_i$ has the property that $\sum f_i(q) \equiv 0\ (p^{m_1})$ at one (or equivalently at every) cusp of M_m, then for any $a \in (\mathbf{Z}/p^m\mathbf{Z})^\times$ the element $\sum a^i f_i \in R_m$ enjoys the same property.*

Proof. We must show that $\beta_m(p^{m-m_1} \cdot \sum a^i f_i) = 0$ in $V_{m,m}$. But

$$\begin{aligned}\beta_m\left(p^{m-m_1} \sum a^i f_i\right) &= p^{m-m_1} \sum a^i f_i/(\omega_{\text{can}}(m))^{\otimes i} = p^{m-m_1}[a]\left(\sum f_i/(\omega_{\text{can}}(m)^{\otimes i})\right)\\ &= [a]\beta_m\left(p^{m-m_1} \sum f_i\right) = [a](0) = 0 .\end{aligned}$$

Q.E.D.

COROLLARY 1.8. *The image of the inclusion $V_{m,n} \to W_m[[q]]$ determined by any choice of cusp on $T_{m,n}$ is independent of the choice of cusp.*

Proof. First, all cusps of M are conjugate to each other by the action of SL(2, $\mathbf{Z}/N\mathbf{Z}$) on the level-N structures, so we may assume that our cusp lies on $T_{m,n}$ over the same cusp $\alpha_{1,0}$ as the standard chosen cusp (cf. 1.3.1). Then our cusp will be the transform of the standard one by some automorphism $[a] \in (\mathbf{Z}/p^n\mathbf{Z})^\times$. Thus *all* the possible q-expansion homomorphisms $V_{m,n} \hookrightarrow W_m[[q]]$ are conjugate to each other by automorphisms of $V_{m,n}$.

(1.8.1) By passage to the limit, it follows that the image of $V_{\infty,\infty} \to W[[q]]$ is also independent of choice of cusps, *and* that the cokernel $W[[q]]/V_{\infty,\infty}$ is *flat* over W (cf. 1.4.3). Let I_{m,m_1} (resp. I_{∞,m_1}) denote the (non-graded) ideal of R_m (resp. R_∞) consisting of those elements $\sum f_i$ such that at one (or equivalently, at every) cusp of M, $\sum f_i(q) \equiv 0$ (p^{m_1}).

COROLLARY 1.9. *I_{m,m_1} is graded modulo $p-1$. (If $\sum f_i \in I_{m,m_1}$, then for each $0 \leqq i_0 < p-1$, $\sum_{i \equiv i_0 (p-1)} f_i \in I_{m,m_1}$.)*

Proof. Use the action of μ_{p-1} (which sits in $(\mathbf{Z}/p^m\mathbf{Z})^\times$ as the Teichmüller points) to decompose I_{m,m_1} into the direct sum of its $p-1$ eigenspaces for μ_{p-1}.

A generalization of the fundamental homomorphism

We wish to define a module-homomorphism

$$\text{(1.10)} \qquad \text{“}\frac{1}{p^{m_1}}\beta_m\text{”} : I_{m,m_1} \longrightarrow V_{m-m_1,m} \subset V_{m-m_1,\infty}$$

as follows: If $\sum f_i \in I_{m,m_1}$, then $p^{m-m_1}\beta_m(\sum f_i) = 0$ in $V_{m,m}$, which implies, because $V_{m,m}$ is *flat* over W_m, that $\beta_m(\sum f_i) = p^{m_1}h$ for some element $h \in V_{m,m}$. This element h is *unique* modulo $p^{m-m_1}V_{m,m}$ and thus determines a well-defined element of $V_{m-m_1,m} \subset V_{m-m_1,\infty}$ which we denote “$(1/p^{m_1})\beta_m$” $(\sum f_i)$. By passage to the inverse limit over m, we obtain a homomorphism

$$\text{(1.11)} \qquad \text{“}\frac{1}{p^{m_1}}\beta_\infty\text{”} : I_{\infty,m_1} \longrightarrow \varprojlim V_{m,\infty} \overset{\text{dfn}}{=} V_{\infty,\infty} .$$

Clearly if $\sum f_i \in R_\infty$, “$(1/p^{m_1})\beta_\infty$” $(\sum f_i)$ has q-expansions $(1/p^{m_1})\sum f_i(q)$ at corresponding (via (1.3.1)) cusps, which is to say, we have the formula

$$\text{(1.1.2)} \qquad p^{m_1}\text{“}\frac{1}{p^{m_1}}\beta_\infty\text{”} = \beta_\infty \text{ on } I_{\infty,m_1} .$$

2. The ring D of divided congruences

(2.0) Let us denote by D the W-algebra $R_\infty + (I/p)\cdot I_{\infty,1} + (1/p^2)\cdot I_{\infty,2} + \cdots$, the non-graded subring of $R_\infty[1/p]$ consisting of those elements $\sum f_i \in R_\infty[1/p]$ which at one (or equivalently at all, by 1.6) cusp(s) of M have *integral* q-expansion (i.e., $\sum f_i(q) \in W[[q]]$). (Notice that in fact $R_\infty \subset (1/p)\cdot I_{\infty,1} \subset (1/p^2)\cdot I_{\infty,2} \subset \cdots \subset (1/p^n)\cdot I_{\infty,n} \subset \cdots$, so that $D = \varinjlim p^{-n}\cdot I_{\infty,n}$ as W-module.)

We define a W-algebra homomorphism

$$\beta\colon D \longrightarrow V_{\infty,\infty} \tag{2.0.1}$$

by the requirement that on $p^{-n}\cdot I_{\infty,n}$, β is "$(1/p^n)\beta_\infty$"$\cdot p^n$. That β is a ring homomorphism follows immediately from the fact that if we choose a cusp of M, then q-expansion at the "corresponding" cusp of $V_{\infty,\infty}$ gives an inclusion $V_{\infty,\infty} \subset W[[q]]$, and the composite $D \xrightarrow{\beta} V_{\infty,\infty} \subset W[[q]]$ sits in the commutative diagram

$$\begin{array}{ccc} D \xrightarrow{\beta} V_{\infty,\infty} & \xrightarrow[q\text{-expansion}]{\subset} & W[[q]] \\ \cap & & \cap \\ R_\infty\left[\dfrac{1}{p}\right] & \xrightarrow[q\text{-expansion}]{\subset} & W[[q]]\left[\dfrac{1}{p}\right]. \end{array} \tag{2.0.2}$$

For each integer $m \geqq 1$, let $\beta(m)$ denote the reduction modulo p^m of β:

$$\beta(m)\colon D/p^mD \longrightarrow V_{m,\infty}\,. \tag{2.0.3}$$

THEOREM 2.1. *For all $m \geqq 1$, $\beta(m)$ is an isomorphism.*

Proof. By its very definition, $\beta(m)$ is *injective*, for if $\sum f_i \in p^{-n}\cdot I_{\infty,n}$ lies in its kernel, then $\sum f_i(q) \in p^m W[[q]]$, whence $\sum f_i$ lies in $p^{-n}\cdot I_{\infty,n+m} = p^m(p^{-n-m}\cdot I_{\infty,n+m}) \subset p^mD$.

It remains to show that $\beta(m)$ is *surjective*. Clearly it suffices to show that $\beta(1)$ is surjective, for if a module-homomorphism is surjective modulo a nilpotent ideal, it is *surjective*. We will establish the surjectivity of $\beta(1)$ in several steps. We begin by noting that in the tower $V_{1,0} \subset V_{1,1} \subset V_{1,2} \subset \cdots$ the lowest layer $V_{1,1}/V_{1,0}$ is cyclic of degree $p-1$, while all successive layers are cyclic of degree p.

We begin by showing that $V_{1,1}$ lies in the image of $\beta(1)$: in fact, $V_{1,1}$ is *precisely* the image under $\beta(1)$ of the subring R_∞ of D.

THEOREM 2.2. *$\beta_1\colon R_1 \to V_{1,1}$ is surjective, with kernel the principal ideal $(E_{p-1}-1)$.*

Proof. The scheme S_1 is the open sub-scheme of M_1 where E_{p-1} is invertible, thus is none other than $\operatorname{Spec}_{M_1}\big((\operatorname{Symm}(\underline{\omega}^{\otimes(p-1)}))/(E_{p-1}-1)\big)$ (because both represent the functor on Sch/M which to an M-scheme T associates those sections δ of $(\underline{\omega}^{-1})^{\otimes(p-1)}$ over T such that $\delta E_{p-1}-1=0$ in $\mathcal{O}_T$). Because $\underline{\omega}$ has positive degree, it is ample, hence S_1 is affine, hence its inclusion into M is an affine morphism; the Leray spectral sequence shows that $V_{1,0}$, the coordinate ring of S_1, is given by $H^0(M_1, \operatorname{Symm}(\underline{\omega}^{\otimes p-1}))/(E_{p-1}-1)$. Because E_{p-1} is homogeneous of positive degree, multiplication by $E_{p-1}-1$ is "formally invertible", hence injective on $\operatorname{Symm}(\underline{\omega}^{\otimes(p-1)})$ and all its cohomology groups. Thus the long exact cohomology sequence associated to the short exact sequence of sheaves on M_1

$$(2.2.1) \qquad 0 \longrightarrow \mathrm{Symm}\,(\underline{\omega}^{\otimes p-1}) \longrightarrow \mathrm{Symm}\,(\underline{\omega}^{\otimes p-1}) \longrightarrow \mathrm{Symm}\,(\underline{\omega}^{\otimes p-1})/(E_{p-1} - 1) \longrightarrow 0$$

shows that

$$(2.2.2) \qquad \begin{aligned} V_{1,0} &\simeq H^0(M_1, \mathrm{Symm}\,(\underline{\omega}^{\otimes(p-1)}))/(E_{p-1} - 1) \\ &\simeq \textstyle\bigoplus_k H^0(M_1, \underline{\omega}^{\otimes k(p-1)})/(E_{p-1} - 1) \,. \end{aligned}$$

The map is explicitly given by $\sum f_{i(p-1)} \longrightarrow \sum f_{i(p-1)}/E^i_{p-1}$ and thus coincides with the restriction to $R_1^{(p-1)}$ of β_1. Similarly, the scheme $T_{1,1}$ is the etale covering of S_1 which trivializes the etale quotient of the kernel of p on the universal elliptic curve with *invertible* Hasse invariant E_{p-1}. As is well-known from the theory of the Hasse-Witt operation, this etale covering is defined by the extraction of the $(p-1)^{\text{th}}$ root of the Hasse invariant, or equivalently of its inverse. It follows that

$$(2.2.3) \qquad T_{1,1} = \mathrm{Spec}_{M_1}\big(\mathrm{Symm}\,(\underline{\omega})/(E_{p-1} - 1)\big)$$

because both represent the functor on Sch/M whose value on a scheme T/M is the set of sections ε of $\underline{\omega}^{\otimes -1}$ over T such that $\varepsilon^{p-1}\cdot E_{p-1} - 1 = 0$ in $\mathcal{O}_T$. Because $T_{1,1}$ is finite and etale over S_1, it is affine over S_1, hence affine over M_1, so the Leray spectral sequence gives

$$(2.2.4) \qquad V_{1,1} = H^0\big(M_1, \mathrm{Symm}\,(\underline{\omega})/(E_{p-1} - 1)\big) \,.$$

The long exact cohomology sequence then gives

$$(2.2.5) \qquad V_{1,1} = H^0\big(M_1, \mathrm{Symm}\,(\underline{\omega})\big)/(E_{p-1} - 1) = R_1/(E_{p-1} - 1) \,,$$

and the map $R_1/(E_{p-1} - 1) \longrightarrow V_{1,1}$ is given explicitly by

$$(2.2.6) \qquad \textstyle\sum f_i \longrightarrow \sum \varepsilon^i f_i = \sum f_i/\omega_{\mathrm{can}}(1)^{\otimes i} = \beta_1\big(\sum f_i\big) \,.$$

Thus we have the desired commutative diagram

$$(2.2.7) \qquad \begin{tikzcd} R_1/(E_{p-1} - 1) \arrow[rr, "\sim"] & & V_{1,1} \,. \\ & R_1 \arrow[ul] \arrow[ur, "\beta_1"'] & \end{tikzcd}$$

COROLLARY 2.2.8. (*Swinnerton-Dyer*). *The ideal $I_{1,1}$ of R_1 consisting of elements $\sum f_i$ such that $\sum f_i(q) = 0$ in $k[[q]]$ is the principal ideal $(E_{p-1} - 1)$.*

Remark. For any $m \geqq 1$, we may obtain a partial generalization of Swinnerton-Dyer's result:

PROPOSITION 2.2.9. *Let $R_m^{\varphi(p^m)}$ denote the subring of R_m of all modular* *forms of weight divisible by* $\varphi(p^m) = p^{m-1}(p-1)$. *Then* $I_{m,m} \cap R_m^{\cdot\varphi(p^m)}$ *is the principal ideal of* $R_m^{\cdot\varphi(p^m)}$ *generated by* $(E_{\varphi(p^m)} - 1)$, *and* β_m *induces an isomorphism*

$$\beta_m\colon R_m^{\cdot\varphi(p^m)}/(E_{\varphi(p^m)} - 1) \xrightarrow{\sim} V_{m,0} = \Gamma(S_m, \mathcal{O}_{S_m}) . \tag{2.2.9.1}$$

Proof. As before we have $S_m = \operatorname{Spec}_M(\operatorname{Symm}(\underline{\omega}^{\otimes\varphi(p^m)})/(E_{\varphi(p^m)} - 1))$, and

$$V_{m,0} = H^0(M_m, \operatorname{Symm}(\underline{\omega}^{\otimes\varphi(p^m)}))/(E_{\varphi(p^m)} - 1) = R_m^{\cdot\varphi(p^m)}/(E_{\varphi(p^m)} - 1) .$$

Furthermore the isomorphism is given explicitly by

$$\sum f_{i\varphi(p^m)} \longrightarrow \sum f_{i\varphi(p^m)}/E^i_{\varphi(p^m)} .$$

Using the fact that $(\omega_{\mathrm{can}}(m))^{\varphi(p^m)} = E_{\varphi(p^m)}$ on $T_{m,m}$, as both have q-expansion $1 \bmod p^m$, we may write this

$$\sum f_{i\varphi(p^m)} \longrightarrow \sum f_{i\varphi(p^m)}/(\omega_{\mathrm{can}}(m))^{i\varphi(p^m)} = \beta_m(\sum f_{i\varphi(p^m)}) .$$

We now return to the problem of surjectivity. We have shown that β_1 maps R_1 onto $V_{1,1}$.

COROLLARY 2.3. *The composition* $R_\infty \to R_1 \xrightarrow{\beta_1} V_{1,1}$ *is also surjective, with kernel* $(p, E_{p-1} - 1)$.

Proof. Although $R_\infty \to R_1$ need *not* be surjective, the composite *will* be, because β_1 kills the ideal $(E_{p-1} - 1)$, hence $\beta_1(R_1) = \beta_1(E_{p-1}R_1) = \beta_1((E_{p-1})^2 R_1)$, and for $\nu \geqq 2$, $H^0(M, \omega^{\otimes\nu}) \otimes k \to H^0(M_1, \underline{\omega}^{\otimes\nu})$ is surjective. This shows that $V_{1,1}$ is precisely the image under $\beta(1)$ of the *subring* R_∞ of D.

In order to continue the proof, we will need to make use of Artin-Schreier theory, in the following explicit form:

(**2.4**) Let A be a ring of characteristic p (i.e., an $\mathbf{F}_p$-algebra), and let $B \supset A$ be a finite etale A-algebra of rank p, which is Galois with group $\mathbf{Z}/p\mathbf{Z}$ (thus $\operatorname{Aut}(B/A) \xrightarrow{\sim} \mathbf{Z}/p\mathbf{Z}$, and A is the subring of invariants). Then there exists an element $b \in B$ such that $n \in \mathbf{Z}/p\mathbf{Z}$ acts by sending $b \to b + n$. The element b is unique up to addition of an element of A, $b^p - b = a \in A$, and the choice of b defines an isomorphism $A[X]/(X^p - X - a) \xrightarrow{\sim} B$. *In particular, any element* $b \in B$ *which is sent to* $b + 1$ *by a generator of* $\mathbf{Z}/p\mathbf{Z}$ *generates* B *as an* A*-algebra.* We will successively apply this "principle" to the situation $A = V_{1,n}$, $B = V_{1,n+1}$.

Let us introduce the action of the group $\mathbf{Z}_p^\times$ on the ring D by the formula

$$[a](\sum f_i) = \sum a^i f_i , \qquad a \in \mathbf{Z}_p^\times, \ \sum f_i \in D . \tag{2.4.1}$$

(It is a priori an action of $\mathbf{Z}_p^\times$ on $R_\infty[1/p]$ but thanks to 1.7 the subring $D \subset$

$R_\infty[1/p]$ is stable under this action.) The meaning of 1.7 is simply the $\mathbf{Z}_p^\times$-*equivariance* of the homomorphisms $\beta(m): D/p^m D \to V_{m,\infty}$. In the tower $V_{m,0} \subset V_{m,1} \subset V_{m,2} \subset, \cdots$, the ring $V_{m,n} \subset V_{m,\infty}$ is, for $n \geqq 1$, precisely the subring of *invariants* of the subgroup $1 + p^n\mathbf{Z}_p$ of $\mathbf{Z}_p^\times$, and the Galois group of $V_{m,n+1}$ over $V_{m,n}$ is canonically $1 + p^n\mathbf{Z}_p/1 + p^{n+1}\mathbf{Z}_p$, a cyclic group of order p generated by the class of $1 + p^n$.

KEY LEMMA 2.5. *For each integer $n \geqq 1$, there exists an element $d_n \in D$ such that for all integers $k \geqq 0$, the action of $1 + p^{n+k} \in \mathbf{Z}_p^\times$ on d_n satisfies*:

$$[1 + p^{n+k}](d_n) \equiv d_n + p^k E_{p-1} \text{ modulo } p^{k+1}D . \tag{2.5.1}$$

Admitting this lemma for a moment, let us conclude the surjectivity of $\beta(1)$. By the lemma, $\beta(1)(d_n)$ is invariant by $1 + p^{n+1}\mathbf{Z}_p$, hence $\beta(1)(d_n) \in V_{1,n+1}$. Furthermore,

$$[1 + p^n](\beta(1)(d_n)) = \beta(1)(d_n + E_{p-1}) = \beta(1)(d_n) + 1$$

which implies by Artin-Schreier theory (2.4) that for $n \geqq 1$, we have

$$V_{1,n+1} = V_{1,n}[\beta(1)(d_n)] ,$$

and hence $V_{1,\infty}$ is generated over $V_{1,1}$ by the elements $\{\beta(1)(d_n)\}_{n\geqq 1}$. As we have already shown that $V_{1,1} = \beta(1)(R_\infty)$, this gives the desired surjectivity of $\beta(1)$, and thus of all the $\beta(m)$. In fact, the proof shows that the R_∞-submodule of $R_\infty[d_1, \cdots, d_n, \cdots]$ spanned over R_∞ by the products

$$\textstyle\prod_{i\geqq 1} (d_i)^{a_i} , \qquad a_i = 0 \text{ for all but finitely many } i,\ a_i \leqq p - 1 , \tag{2.5.2}$$

maps onto $V_{1,\infty}$, and hence onto $V_{m,\infty}$ for any $m \geqq 1$. Indeed, the proof shows that the $\beta(1)(d_i)$ form a "p-base" for $V_{1,\infty}$ over $V_{1,1}$.

Construction-proof of the Key Lemma. We proceed by induction on n. For $n = 1$, we define

$$d_1 = \frac{1 - E_{p-1}}{p} \qquad \text{(compare Serre [6], Remark 1 after 1.3)} . \tag{2.5.3}$$

We immediately calculate

$$\begin{aligned} [1 + p^{1+k}](d_1) &= \frac{1 - (1 + p^{1+k})^{p-1}\cdot E_{p-1}}{p} \\ &= \frac{1 - E_{p-1} - (p - 1)p^{1+k}E_{p-1} + (p^{2k+2})E_{p-1}}{p} \\ &= d_1 + p^k E_{p-1} + (p^{k+2})E_{p-1} \\ &= d_1 + p^k E_{p-1} \bmod p^{k+1}D . \end{aligned} \tag{2.5.4}$$

Suppose we have already constructed $d_1, \cdots, d_n$ with the desired properties. Then Artin-Schreier theory shows that

(2.5.5) $$V_{1,n+1} = V_{1,n}[\beta(1)(d_n)]$$

and that

(2.5.6) $$(\beta(1)(d_n)) - (\beta(1)(d_n))^p \in V_{1,n} .$$

Also by Artin-Schreier theory, we have

(2.5.7) $$V_{1,n} = V_{1,1}[\beta(1)(d_1), \cdots, \beta(1)(d_{n-1})] = \beta(1)(R_\infty[d_1, \cdots, d_{n-1}]) .$$

Thus we may choose an element

(2.5.8) $$C_n \in R_\infty[d_1, \cdots, d_{n-1}] , \qquad C_n = \sum_{0 \leq i_\nu \leq p-1} \underbrace{f_{i_1,\cdots,i_{n-1}}}_{\substack{\cap \\ R_\infty}} \prod^{n-1} d_j^{i_j}$$

such that

(2.5.9) $$(\beta(1)(d_n)) - (\beta(1)(d_n))^p = \beta(1)(C_n) .$$

Consider the element

(2.5.10) $$d_n - (d_n)^p - C_n \in \operatorname{Ker} \beta(1) = pD .$$

We define

(2.5.11) $$d_{n+1} = \frac{d_n - (d_n)^p - C_n}{p} .$$

It remains to verify the transformation property. We calculate:

(2.5.12) $$\begin{aligned}&[1 + p^{n+1+k}](d_{n+1}) \\ &= \frac{[1 + p^{n+1+k}](d_n) - ([1 + p^{n+1+k}](d_n))^p - [1 + p^{n+1+k}](C_n)}{p} .\end{aligned}$$

Consider successively the three terms in the numerator. By induction,

(2.5.13) $$[1 + p^{n+1+k}](d_n) = d_n + p^{k+1}E_{p-1} + p^{k+2}D .$$

In particular,

(2.5.14) $$([1 + p^{n+1+k}](d_n))^p = (d_n + p^{k+1}D)^p = (d_n)^p + p^{k+2}D .$$

By the transformational congruences for $d_1, \cdots, d_{n-1}$, we see that

(2.5.15) $$[1 + p^{n+1+k}](C_n) = C_n + p^{k+2}D \text{ for } \textit{any } C_n \in R_\infty[d_1, \cdots, d_{n-1}] .$$

Combining all this, we find

(2.5.16) $$\begin{aligned}[1 + p^{n+1+k}](d_{n+1}) &= \frac{d_n + p^{k+1}E_{p-1} - (d_n)^p - C_n + p^{k+2}D}{p} \\ &\equiv d_{n+1} + p^k E_{p-1} \text{ modulo } p^{k+1}D .\end{aligned}$$

Q.E.D.

3. Determination of the ideals $I_{\infty,n} \subset R_\infty$

(3.0) Henceforth, let us agree to denote $I_{\infty,n}$ simply as I_n, the ideal of relations mod p^n between the q-expansions of modular forms over W. In the course of the proof of the last Lemma 2.5, we discovered a large number of "divided congruences" d_n, which give rise to "true" congruences as follows.

LEMMA 3.1. *For $n \geqq 1$, the elements $r_n = p^{(p^n-1)/(p-1)} \cdot d_n$ of D lie in R_∞, hence in $I_{(p^n-1)/(p-1)}$.*

Proof. We proceed by induction on n, the case $n = 1$ being trivial: $r_1 = 1 - E_{p-1}$. Supposing the result proven already for $r_1, \cdots, r_n$, we use the formula (2.5.1):

$$pd_{n+1} = d_n - (d_n)^p - C_n(d_1, \cdots, d_{n-1}) \tag{3.1.1}$$

where $C_n \in R_\infty[d_1, \cdots, d_{n-1}]$ has degree at most $p - 1$ in each variable d_i separately. We readily calculate:

$$\begin{aligned} r_{n+1} = p^{(p^{n+1}-1)/(p-1)} \cdot d_{n+1} &= p^{p+p^2+\cdots+p^n} p d_{n+1} \\ &= p^{p+p^2+\cdots+p^n}[d_n - (d_n)^p - C_n(d_1, \cdots, d_{n-1})] \; ; \end{aligned} \tag{3.1.2}$$

$$\begin{aligned} r_{n+1} = {} & p^{p^n-1} r_n - (r_n)^p \\ & - \sum_{0 \leqq (a_1, \cdots, a_{n-1}) \leqq p-1} f_{a_1, \cdots, a_{n-1}} p^{p+\cdots+p^n - \sum_{i=1}^{n-1} a_i((p^i-1)/(p-1))} \prod_{i=1}^{n-1} (r_i)^{a_i} \; . \end{aligned} \tag{3.1.3}$$

Q.E.D.

COROLLARY 3.2. *For each integer $n \geqq 1$,*

$$r_{n+1} + (r_n)^p \in pI_{p(p^n-1)/(p-1)-1} \; .$$

Proof. Obvious from the formula (3.1.3) above.

THEOREM 3.3. *For each integer $n \geqq 1$, the ideal $I_n = I_{\infty,n}$ of R_∞ is generated by the monomials*

$$p^{a_0} r_1^{a_1} \cdots r_j^{a_j}$$

such that

$$a_0 + \sum_{i=1}^{j} a_i \left(\frac{p^i - 1}{p - 1} \right) = n \; .$$

In particular, for $n \leqq p$, $I_n = (I_1)^n = (p, E_{p-1} - 1)^n$.

For later applications, we give a more abstract formulation of the result (a version which by virtue of (3.1), (3.2), and (2.5.2) clearly implies (3.3) above).

THEOREM 3.3 *bis*. *Let $r_1, r_2, \cdots$ be a sequence of elements of R_∞ such that*

$$r_n \in I_{(p^n-1)/(p-1)} \; , \tag{3.3.1}$$

$$r_{n+1} + (r_n)^p \in p \cdot I_{p((p^n-1)/(p-1))-1} \; . \tag{3.3.2}$$

(3.3.3) *If we let $d_n = r_n / p^{(p^n-1)/(p-1)}$, the images $\beta(1)(d_1)$, $\beta(1)(d_2)$, $\cdots$ of the d_i in $V_{1,\infty}$ form a sequence of successive Artin-Schreier generators of $V_{1,\infty}$ over $V_{1,1}$ (hence form a p-base of $V_{1,\infty}$ over $V_{1,1}$).*

(3.3.4) $r_1 = 1 - A$, *where* A *is a modular form of weight* $p-1$ *which lifts the Hasse invariant.*

Then for each integer $n \geqq 1$, *the ideal* $I_n = I_{\infty,n}$ *of* R_∞ *is generated by those monomials*

$$p^{a_0} r_1^{a_i} \cdots r_j^{a_j}$$

such that

$$a_0 + \sum_{i=1}^{j} a_i \left(\frac{p^i - 1}{p-1}\right) = n \ . \tag{3.3.5}$$

Proof. Let us denote by I'_n the ideal generated by the above monomials; clearly we have $I'_n \subset I_n$. In order to reverse this inclusion, we introduce the ideal I''_n generated by those monomials

$$p^{a_0} r_1^{a_1} \cdots r_j^{a_j}$$

which satisfy

$$\begin{cases} a_0 + \sum a_i \dfrac{(p^i - 1)}{p-1} \geqq n \\ \text{if } i \geqq 1 \ , \text{ then } 0 \leqq a_i \leqq p-1 \ . \end{cases} \tag{3.3.6}$$

LEMMA 3.4. *For every* $n \geqq 1$, *we have* $I''_n = I_n$.

Proof. We clearly have $I''_n \subset I_n$. To reverse the inclusion, we proceed by induction on n. For $n = 1$, the ideal I_1 is generated by p and r_1, hence $I_1 \subset I''_1$. Now suppose the result proven through n, and suppose we are given an element of I_{n+1}. It certainly lies in I_n, hence in I''_n by the induction hypothesis, hence may be written

$$\sum f_{a_0,\cdots,a_j} p^{a_0} r_1^{a_1} \cdots r_1^{a_j} \ , \qquad f_{a_0,\cdots,a_j} \in R_\infty \ , \tag{3.4.1}$$

the sum extended over finitely many tuples $(a_0, \cdots, a_j)$ which all satisfy

$$\begin{cases} a_0 + \sum a_i \left(\dfrac{p^i - 1}{p-1}\right) \geqq n \\ 0 \leqq a_i \leqq p-1 \text{ for } i \geqq 1 \ . \end{cases} \tag{3.4.2}$$

Any of these monomials for which $a_0 + \sum a_i((p^i - 1)/(p-1)) \geqq n+1$ already lies in I''_{n+1}. Subtracting, we may assume that only monomials satisfying

$$\begin{cases} a_0 + \sum a_i \dfrac{(p^i - 1)}{p-1} = n \\ 0 \leqq a_i \leqq p-1 \text{ if } i \geqq 1 \end{cases} \tag{3.4.3}$$

occur in the expression (3.4.1).

Now to say that the sum (3.4.1) lies in I_{n+1} is exactly to say that after we divide it by p^n, we obtain an element of D which lies in the *kernel* of $\beta(1)$.

Using the identity

$$\frac{p^{a_0}r_1^{a_1}\cdots r_j^{a_j}}{p^n} = (d_1)^{a_1}\cdots(d_j)^{a_j} \text{ if } a_0 + \sum a_i\left(\frac{p^i-1}{p-1}\right) = n \tag{3.4.4}$$

we thus conclude that

$$\sum f_{a_0,\cdots,a_j}(d_1)^{a_1}\cdots(d_j)^{a_j} \in \text{kernel of } \beta(1)\ ; \tag{3.4.5}$$

i.e.,

$$\sum \beta(1)(f_{a_0,\cdots,a_j})\prod_{i=1}^{j}\big(\beta(1)(d_i)\big)^{a_i} = 0 \text{ in } V_{1,\infty}\ . \tag{3.4.6}$$

Because the elements $\beta(1)(d_i)$ form a p-base of $V_{1,\infty}$ over $V_{1,1}$ and the exponents a_i satisfy $0 \leqq a_i \leqq p-1$, we have

$$\beta(1)(f_{a_0,\cdots,a_j}) \in \ker \beta(1)\ ; \tag{3.4.7}$$

the coefficients $f_{a_0,\cdots,a_j}$ all lie in $I_1 = (p, r_1)$. Thus we must show that if $a_0 + \sum_{i=1}^{j} a_i\big((p^i-1)/(p-1)\big) = n$, $0 \leqq a_i \leqq p-1$ for $i \geqq 1$, then

$$\begin{cases} p\, p^{a_0}\prod r_i^{a_i} \in I''_{n+1} \\ r_1 p^{a_0}\prod r_i^{a_i} \in I''_{n+1}\ . \end{cases} \tag{3.4.8}$$

The first of these inclusions is obvious. The second is obvious in case *either* $a_0 > 0$, in which case $r_1 p^{a_0}\prod r_i^{a_i} \in p\cdot I_n = pI''_n \subset I''_{n+1}$, *or* in case $a_1 \leqq p-2$, in which case $r_1p^{a_0}\prod r_i^{a_i}$ is one of the standard monomials in I''_{n+1}. Thus we must show that

$$r_1^p r_2^{a_2}\cdots r_j^{a_j} \in I''_{n+1} \text{ if } p + \sum_{i\geqq 2} a_i\left(\frac{p^i-1}{p-1}\right) = n+1\ . \tag{3.4.9}$$

In fact, let us show that if $n = \sum_{i=1}^{j} a_i\big((p^i-1)/(p-1)\big)$ and $0 \leqq a_i \leqq p-1$, then for *any* integer $1 \leqq k \leqq j$,

$$(r_k)^p r_{k+1}^{a_{k+1}}\cdots r_j^{a_j} \in I''_{n+1}\ . \tag{3.4.10}$$

We proceed by descending induction on k.

For $k = j$, we notice that $r_{j+1} \in I''_{n+1}$, and that by (3.3.2)

$$(r_j)^p + r_{j+1} \in p\cdot I_{p(p^j-1)/(p-1)} \subset p\cdot I_n = pI''_n \subset I''_{n+1} \tag{3.4.11}$$

(the inclusion $I_{p((p^j-1)/(p-1))-1} \subset I_n$ because

$$n = \sum_{i=1}^{j} a_i\left(\frac{p^i-1}{p-1}\right) \leqq \sum_{i=1}^{j}(p^i-1) = -j + p\left(\frac{p^j-1}{p-1}\right)$$
$$\leqq -1 + p\left(\frac{p^j-1}{p-1}\right)\bigg)\ .$$

For $k < j$, we have, again by (3.3.2),

(3.4.12) $$r_{k+1} + (r_k)^p \in p \cdot I_{p((p^k-1)/(p-1))-1} \subset pI_{n-\sum_{i=k+1}^{j} a_i((p^i-1)/(p-1))} \,.$$

Hence,

(3.4.13) $$r_{k+1}(r_{k+1})^{a_{k+1}} \cdots r_j^{a_j} + (r_k)^p r_{k+1}^{a_{k+1}} \cdots r_j^{a_j} \in pI_n = pI''_n \subset I''_{n+1} \,.$$

If $a_{k+1} \leqq p-2$, then the first term in the sum (3.4.13) is a standard monomial of I''_{n+1}, and if $a_{k+1} = p-1$, then by the descending induction hypothesis for $k+1$ we know that the first term in the sum (3.4.13) lies in I''_{n+1}. This concludes the proof of (3.4.8), and hence of (3.4). To conclude the proof of the theorem, it remains to prove:

LEMMA 3.5. *For every* $n \geqq 1$, $I'_n = I''_n$.

Proof. Because $I'_n \subset I_n = I''_n$, it suffices to prove that $I''_n \subset I'_n$. Consider one of the standard monomial generators of I''_n, say $p^{a_0} r_1^{a_j} \cdots r_j^{a_j}$. If $\sum_{i \geq 0} a_i \geqq 2$, we may write this monomial non-trivially as a product of monomials, as an element of $I_a \cdot I_b$ for some integers $a, b \geqq 1$, $a+b=n$. By induction on n, we may suppose $I_a = I'_a$, $I_b = I'_b$, and clearly $I'_a \cdot I'_b \subset I'_{a+b} = I'_n$. Thus it remains to treat the case of the element p if $n=1$ (i.e., to show that $I'_1 = I_1$, which is obvious) and the case of r_j if $(p^j-1)/(p-1) \geqq n$. If $(p^j-1)/(p-1) = n$, then $r_j \in I'_n$. If $(p^j-1)/(p-1) > n$, then by (3.3.2) we have

$$r_j + (r_{j-1})^p \in pI_{p(p^{j-1}-1)/(p-1)-1} \subset pI_{n-1} = pI'_{n-1} \subset I'_n$$

and by the first case treated above, $(r_{j-1})^p \in I'_n$. This concludes the proof of the lemma, and hence of Theorem 3.3 as well.

4. Application to congruences between modular forms of levels 1 and 2: $p \geqq 5$

(4.0) Suppose first $p \geqq 5$, and choose $N = p-1$, $k = \mathbf{F}_p W = \mathbf{Z}_p$. Let us write

$$\begin{cases} G = \mathrm{SL}_2(\mathbf{Z}/(p-1)\mathbf{Z}) \\ G_1 = \text{the subgroup of } G \text{ of elements} \equiv 1 \text{ modulo } 2. \end{cases}$$

The group G acts on all of our objects: R_∞, D, $V_{n,m}$, $\cdots$ and commutes with the action of $\mathbf{Z}_p^\times$. The ring R_∞^G (resp. $R_\infty^{G_1}$) of G-invariants (resp. of G_1-invariants) in R_∞ is none other than the ring of holomorphic modular forms over $\mathbf{Z}_p$ of level *one* (resp. 2), and the ideal $I_n^G = I_n \cap R_\infty^G$ (resp. $I_n^{G_1} = I_n \cap R_\infty^{G_1}$) is the ideal of relations mod p^n between the q-expansions of such modular forms.

LEMMA 4.1. *If* $p \geqq 5$, *then the order of the group* G *is prime to* p.

Proof.

$$\# G = (p-1)^3 \prod_{l \mid p-1} \frac{(l-1)(l+1)}{l^2}$$

is clearly a p-adic unit because $p - 1 < p$, $l - 1 < p$, $l < p$, and $l + 1 < p$ if $p \neq 3$.

LEMMA 4.2. *Hypotheses as above* ($p \geqq 5$, $N = p - 1$), *the elements* d_1, $d_2, \cdots$ *may be chosen to be G-invariant.*

Proof. Clearly $d_1 = (1/p)(1 - E_{p-1})$ is G-invariant, because E_{p-1} *is* a modular form of level one, defined over $\mathbf{Z}_p$. Suppose that $d_1, \cdots, d_n$ have been chosen to be G-invariant. Then $(d_n)^p - d_n$ is G-invariant, and its image under $\beta(1)$ in $V_{1,n}$ is thus a G-invariant. Let $G_n(d_1, \cdots, d_{n-1})$ be a polynomial in $d_1, \cdots, d_{n-1}$ with coefficients in R_∞, and degree $\leqq p - 1$ in each d_i, such that $\beta(1)(C_n) = \beta(1)\big((d_n)^p - d_n\big)$. Writing $C_n = \sum f_{a_1,\cdots,a_{n-1}} d_1^{a_1} \cdots d_{n-1}^{a_{n-1}}$ with coefficients $f \in R_\infty$, we see that if we *replace* each $f = f_{a_1,\cdots,a_{n-1}}$ by its *integral over* G $\big(= (1/\#G) \sum_{\sigma \in G} \sigma(f)\big)$ then we replace C_n by *its* integral over G. But because $\beta(1)(C_n)$ is G-invariant, we have $\beta(1)(C_n) = \beta(1)\Big(\int_G C_n\Big)$. Thus we may suppose that C_n is G-invariant; then the definition of d_{n+1} as

$$d_{n+1} = \frac{(d_n)^p - d_n - C_n}{p}$$

shows that d_{n+1} is also G-invariant.

COROLLARY 4.3. *The relations $r_1, r_2, \cdots$ may be chosen G-invariant.*

THEOREM 4.4. *The ideal I_n^G of R_∞^G, and the ideal $I_n^{G_1}$ of $R_\infty^{G_1}$, are generated by those monomials*

$$p^{a_0} r_1^{a_1} \cdots r_j^{a_j}$$

which satisfy

$$a_0 + \sum_{i \geqq 1} a_i \left(\frac{p^i - 1}{p - 1}\right) = n\ .$$

Proof. By (3.3), any element of I_n^G (resp. $I_n^{G_1}$) may be written as an R_∞-linear combination of the above monomials:

$$\sum f_{a_0,\cdots,a_j} \cdot p^{a_0} r_1^{a_1} \cdots r_j^{a_j}\ .$$

As this expression is G (resp. G_1) invariant, it is equal to its integral over G (resp. G_1), hence (as the r_i are G-invariant), it is equal to

$$\sum \left(\int_G f_{a_0,\cdots,a_j}\right) p^{a_0} r_1^{a_1} \cdots r_j^{a_j}\ . \qquad \text{Q.E.D.}$$

3-adic congruences in level 2

(4.5) The problem of 3-adic congruences between modular forms of level-two defined over $\mathbf{Z}_3$ may be handled by a similar integration argument, as follows. Choose $N=4$, $k=\mathbf{F}_q=\mathbf{F}_3[i]$, $W=\mathbf{Z}_3[i]$, and view the corresponding modular scheme M as a scheme over $\mathbf{Z}_3$. So viewed, the subgroup G_1 of $\mathrm{GL}_2(\mathbf{Z})$ of matrices congruent to the identity modulo 2 acts on M (the subgroup $G_1 \cap \mathrm{SL}_2$ acting "geometrically", the quotient ± 1 acting as $\mathrm{Gal}\,(\mathbf{Z}_3[i]/\mathbf{Z}_3)$), and the quotient is the projective λ-line over $\mathbf{Z}_3$, denoted simply $\mathbf{P}^1$. The invertible sheaf $\underline{\omega}$ does *not* descend to $\mathbf{P}^1$, but its *square* $\underline{\omega}^{\otimes 2}$ descends *canonically* to the sheaf $\mathcal{O}(1) = \Omega^1_{\mathbf{P}}1\,(\log\,\{0, 1\})$ of differentials with first-order poles at 0, 1, thanks to the Kodaira-Spencer isomorphism (cf. [3], A. 3.17). (Under this isomorphism, the square of the differential dx/y on the almost-universal level-2 curve $y^2 = x(x-1)(x-\lambda)$ corresponds to the differential $2d\lambda/\lambda(1-\lambda)$.) The ring of modular forms of level-2 defined over $\mathbf{Z}_3$ is just the subring $(R_\infty)^{G_1} \simeq \bigoplus_{k\geqq 0} H^0(\mathbf{P}^1, \mathcal{O}(k)) = \mathrm{Symm}\,(H^0(\mathbf{P}^1, \Omega^1_{\mathbf{P}^1}(\log\,\{0, 1, \infty\})))$.

Because the Hasse invariant *lifts* to a level-2 modular form over $\mathbf{Z}_3$ (for instance the section $(-1-\lambda)d\lambda/2\lambda(1-\lambda)$ of $\Omega^1_{\mathbf{P}^1}(\log\,\{0, 1, \infty\})$, we may choose the relation r_1 to be G_1-invariant. Because the group G_1 has order 16 (prime to 3), the integration technique used above (cf. 4.4) allows us to select the successive relations $r_2, r_3, \cdots$, in a G_1-invariant way. We obtain, for any such selection, the following

THEOREM 4.6. *The ideal $I_n^{G_1}$ of $R_\infty^{G_1}$ is generated by those monomials*

$$p^{a_0} r_1^{a_1} \cdots r_j^{a_j}$$

which satisfy

$$a_0 + \sum_{i=1}^{j} a_i\left(\frac{3^i - 1}{2}\right) = n\ .$$

5. Explicit generators for the ideals I_n via Weierstrass ($p \geqq 5$)

(5.0) *The Weierstrass curve and its differential* ([3], A.1, [9] and [38]). We begin by recalling the "Weierstrass normal form" of an elliptic curve. Let B be any ring in which $6 = 2\cdot 3$ is invertible, and let (E, ω) be a pair consisting of an elliptic curve E over B and a nowhere-vanishing differential ω or E. Let us denote by $\mathcal{O}_E(-\infty)$ the invertible sheaf on E which is the inverse of the ideal sheaf of the identity section of E/B, and by $\mathcal{O}_E(-n\infty)$ its n^{th} tensor power. Then there exist *unique* meromorphic functions on E

$$\text{(5.0.1)} \qquad \begin{cases} X = X(E, \omega) \in H^0(E, \mathcal{O}_E(-2\infty)) \\ Y = Y(E, \omega) \in H^0(E, \mathcal{O}_E(-3\infty)) \end{cases}$$

and unique "constants" $g_2, g_3 \in B$

$$\begin{cases} g_2 = g_2(E,\ \omega) \\ g_3 = g_3(E,\ \omega) \end{cases} \tag{5.0.2}$$

such that the pair (E, ω) is the pair

$$\begin{cases} Y^2 = 4X^3 - g_2X - g_3 \\ \omega = dX/Y\ . \end{cases} \tag{5.0.3}$$

We denote by $T = T(E, \omega)$ the uniformizing parameter X/Y, by means of which the formal completion of E along the identity section is identified with (the formal spectrum of) $B[[T]]$. By *uniqueness*, we have the following transformation formulas, for any unit $\lambda \in B^\times$.

$$X(E,\ \lambda\omega) = \lambda^{-2}X(E,\ \omega)\ , \tag{5.0.4}$$

$$Y(E,\ \lambda\omega) = \lambda^{-3}Y(E,\ \omega)\ , \tag{5.0.5}$$

$$g_2(E,\ \lambda\omega) = \lambda^{-4}g_2(E,\ \omega)\ , \tag{5.0.6}$$

$$g_3(E,\ \lambda\omega) = \lambda^{-6}g_3(E,\ \omega)\ , \tag{5.0.7}$$

$$T(E,\ \lambda\omega) = \lambda T(E,\ \omega)\ . \tag{5.0.8}$$

(Formulas (5.0.6) and (5.0.7) express the fact that g_2 and g_3 are modular forms of weights 4 and 6 respectively.) Consider now the expansion along the identity section of the differential ω:

$$\omega = \textstyle\sum_{n\geq 1} a_n T^{n-1}dT \tag{5.0.9}$$

where the coefficients $a_n = a_n(E, \omega)$ lie in B, and are expressed by universal polynomials with $\mathbf{Z}$-coefficients in terms of g_2 and g_3. Let us compare the developments of ω and $\lambda\omega$, for a unit $\lambda \in B^\times$:

$$\omega = \textstyle\sum a_n(E,\ \omega)\cdot\big(T(E,\ \omega)\big)^{n-1}dT(E,\ \omega)\ , \tag{5.0.10}$$

$$\lambda\omega = \textstyle\sum a_n(E,\ \lambda\omega)\big(T(E,\ \lambda\omega)\big)^{n-1}dT(E,\ \lambda\omega) \tag{5.0.11}$$

by (5.0.8)
$$= \textstyle\sum a_n(E,\ \lambda\omega)\cdot\lambda^n\cdot\big(T(E,\ \omega)\big)^{n-1}dT(E,\ \omega)\ .$$

Thus we have the transformation formulas, for $n \geqq 1$:

$$a_n(E,\ \lambda\omega) = \lambda^{1-n}a_n(E,\ \omega) \tag{5.0.12}$$

which say precisely that a_n is a modular form (over $\mathbf{Z}[1/6]$) of weight $n - 1$. It follows by reduction to the universal case that the universal expression of a_{n-1} as a $\mathbf{Z}$-polynomial in g_2, g_3 is isobaric of weight $n - 1$, when we attribute to the g_2 and g_3 their weights 4 and 6 respectively. The a_{2i} are all zero, and the first few a_{2i+1} are given by

$$\begin{cases} a_1 = -2 \\ a_3 = 0 \\ a_5 = 16g_2 \\ a_7 = 96g_3 \\ a_9 = -192(g_2)^2 \\ a_{11} = -512g_2g_3 . \end{cases}$$

q-expansions; the Weierstrass differential on the Tate curve

(5.1) Recall that the q-expansions of g_2 and g_3 are given by

$$\left.\begin{aligned} &(5.1.1) \qquad g_2(q) = \frac{1}{12}E_4(q) = \frac{1}{12}\left(1 + 240\sum_{n\geq 1}\sigma_3(n)q^n\right) \\ &(5.1.2) \qquad g_3(q) = \frac{-1}{216}E_6(q) = \frac{-1}{216}\left(1 - 504\sum_{n\geq 1}\sigma_5(n)q^n\right) \end{aligned}\right\} \in \mathbf{Z}[1/6][[q]]$$

which is an oblique way of recalling that the Tate curve with its canonical differential $(\mathrm{Tate}\,(q), \omega_{\mathrm{can}})$ is given over $\mathbf{Z}[1/6]((q))$ by

$$(5.1.3) \qquad \begin{cases} Y^2 = 4X^3 - \dfrac{E_4X}{12} + \dfrac{E_6}{216} \\ \omega_{\mathrm{can}} = dX/Y . \end{cases}$$

We must also recall the existence of a uniformizing parameter Z along the identity section

$$(5.1.4) \qquad Z \equiv -2T \bmod T^2\mathbf{Z}[1/6][[q]][[T]]$$

in terms of which the expansions of X and Y along the identity section are given by

$$(5.1.5) \qquad X = \sum_{n\in\mathbf{Z}}\frac{q^n(1+Z)}{\left(1-q^n(1+Z)\right)^2} + \frac{1}{12} - 2\sum_{n=1}^{\infty}\frac{q^n}{1-q^n} ,$$

$$(5.1.6) \qquad Y = (1+Z)\frac{d}{dZ}(X)$$

so that, *on the Tate curve*, we have the expansion identity

$$(5.1.7) \qquad \omega_{\mathrm{can}} = dX/Y = dZ/(1+Z) = d\log(1+Z) .$$

Let us denote by $a_n(q) \in \mathbf{Z}[1/6][[q]]$ the q-expansions of the modular forms a_n; comparing the expansions (5.0.9) and (5.1.6), we obtain the formal identity

$$1 + Z = \exp\left(\sum_{n\geq 1} a_n(q)\frac{T^n}{n}\right).$$

The key point here is that, thanks to (5.1.4), we know that

FACT (5.2). *The series* $\exp\left(\sum a_n(q)(T^n/n)\right)$ *actually lies in* $\mathbf{Z}[1/6][[q]][[T]]$.

Definition of the divided congruences b_n, c_n, d_n

(5.3) We return to the universal Weierstrass curve and its differential, expanded in terms of T:

(5.3.1) $$\omega = \sum_{n\geq 1} a_n T^{n-1} dT\,, \qquad a_n \in \mathbf{Z}[g_2, g_3]\,.$$

We define the sequences $b_0 = 1, b_1, b_2, \cdots$ and $c_1, c_2, \cdots$ of elements of $\mathbf{Q}[g_2, g_3]$ by the formulas

(5.3.2) $$\prod_{n\geq 1} (1 - c_n T^n)^{-1} = \sum_{n\geq 0} b_n T^n = \exp\Big(\sum_{n\geq 1} a_n \frac{T^n}{n}\Big)\,.$$

Thanks to FACT (5.2), we have the remarkable

PROPOSITION 5.3.3. *The elements $b_0 = 1, b_1, b_2, \cdots$ and $c_1, c_2, \cdots$, of $\mathbf{Q}[g_2, g_3]$ all have q-expansions which lie in* $\mathbf{Z}[1/6][[q]]$.

Applications to congruences

(5.4) Fix a prime number $p \geqq 5$. We define a sequence $d_0, d_1, d_2, \cdots$ of divided congruences by setting

(5.4.1) $$d_n \overset{\text{dfn}}{=\!=} c_{p^n}\,.$$

Taking the logarithmic derivative of both sides of (5.3.2), we obtain the following formulas expressing the d_i in terms of the a_{p^i}:

(5.4.2) $$p^n d_n + p^{n-1}(d_{n-1})^p + p^{n-2}(d_{n-2})^{p^2} + \cdots + (d_0)^{p^n} = a_{p^n}\,;$$

(5.4.3) $$\begin{cases} d_0 = c_1 = 1 \\ d_1 = \dfrac{a_p - 1}{p} \\ d_2 = \dfrac{a_{p^2} - 1}{p^2} - \dfrac{1}{p}\Big(\dfrac{a_p - 1}{p}\Big)^p \\ d_3 = \dfrac{a_{p^3} - 1}{p^3} - \dfrac{1}{p^2}\cdot\Big(\dfrac{a_p - 1}{p}\Big)^{p^2} - \dfrac{1}{p}\Big[\dfrac{a_{p^2} - 1}{p^2} - \dfrac{1}{p}\Big(\dfrac{a_p - 1}{p}\Big)^p\Big]\,. \end{cases}$$

LEMMA 5.4.4. *For each $n \geqq 1$, the element*

$$r_n \overset{\text{dfn}}{=\!=} p^{(p^n-1)/(p-1)}\cdot d_n \text{ lies in } \mathbf{Z}[g_2, g_3]\,.$$

Proof. This follows immediately from the formula (5.4.2) above by induction on n.

THEOREM 5.5. *For any integer $N \geqq 1$ prime to p, and any perfect field k of characteristic p containing a primitive N^{th} root of unity ζ, denote by R_∞ the ring of holomorphic modular forms of level N and type ζ over $W = W_\infty(k)$. The ideal $I_n \subset R_\infty$ of all q-expansion congruences modulo p^n is generated by those monomials in the r_i* (cf. 5.4.4)

$$p^{a_0} r_1^{a_1} \cdots r_\nu^{a_\nu}$$

which satisfy

$$a_0 + \sum a_i\left(\frac{p^i - 1}{p - 1}\right) = n \ .$$

Proof. The cases $N = 1, 2$ follow from the case $N = p - 1$ over $\mathbf{Z}_p$ by the "integration" argument of (4.4), which is valid because the r_i are of level-one and defined over $\mathbf{Z}_p$. To do the case $N \geqq 3$, it suffices to check that these r_i satisfy the four conditions of Theorem 3.3 bis.

The first condition, that $r_n \in I_{(p^n-1)/(p-1)}$, is satisfied in virtue of (5.4.4). The second condition, that

$$r_{n+1} + (r_n)^p \in pI_{p((p^n-1)/(p-1))-1} \tag{5.5.1}$$

is easily deduced from the fundamental formula (5.4.2):

$$p^{n+1}d_{n+1} + p^n(d_n)^p + p^{n-1}(d_{n-1})^{p^2} + \cdots (d_0)^{p^{n+1}} = a_{p^{n+1}} \ . \tag{5.5.2}$$

Multiplying by $p^{(p^{n+1}-1)/(p-1)-n-1}$, we have the formula

$$0 = r_{n+1} + (r_n)^p + \sum\nolimits_{j=1}^{n} p^{\sum_{i=1}^{j}(p^i-1)}(r_{n-j})^{p^{j+1}} - p^{\sum_{i=1}^{n}(p^i-1)}a_{p^{n+1}} \ . \tag{5.5.3}$$

Let us denote by $r_{n-1,2}$ the element of $\mathbf{Z}[g_2, g_3]$ given by

$$r_{n-1,2} \overset{\mathrm{dfn}}{=\!=} (r_{n-1})^{p^2} + \sum\nolimits_{j=2}^{n} p^{\sum_{i=2}^{j}(p^i-1)}(r_{n-j})^{p^{j+1}} - p^{\sum_{i=2}^{n}(p^i-1)}a_{p^{n+1}} \ . \tag{5.5.4}$$

Then (5.5.3) says that

$$r_{n+1} + (r_n)^p + p^{p-1}r_{n-2,2} = 0 \ . \tag{5.5.5}$$

By (5.4.4), we know that

$$r_{n+1} \in I_{(p^{n+1}-1)/(p-1)} \ , \qquad (r_n)^p \in I_{p(p^n-1)/(p-1)} \ . \tag{5.5.6}$$

Hence

$$p^{p-1}r_{n-1,2} \in I_{p(p^n-1)/(p-1)} \ , \tag{5.5.7}$$

which is to say

$$r_{n-1,2} \in I_{p(p^n-1)/(p-1)-(p-1)} \ . \tag{5.5.8}$$

Thus the second condition of (3.3 bis) is verified:

$$r_{n+1} + (r_n)^p = p^{p-1}r_{n-1,2} \in p \cdot I_{p(p^n-1)/(p-1)-1} \ . \tag{5.5.9}$$

Let us delay verification of the third condition for a moment. The fourth condition is satisfied, because $r_1 = 1 - a_p$, and it is well-known that a_p reduces mod p to the Hasse invariant.

To verify the third condition, we will compute the action of $\mathbf{Z}_p^\times$ on the elements b_i, c_i, and $d_i \in D$ (cf. 2.4).

LEMMA 5.6. *Let*

$$f(T) = \exp\left(\sum_{n\geq 1} a_n \frac{T^n}{n}\right) = \sum_{n\geq 0} b_n T^n = \prod_{n=1}^{\infty} (1 - c_n T^n)^{-1} . \tag{5.6.1}$$

For any $\alpha \in \mathbf{Z}_p^\times$, let $[\alpha]$ denote the canonical galois action of α on the ring D, and define

$$[\alpha](f(T)) \overset{\text{dfn}}{=\!=} \sum_{n\geq 0} [\alpha](b_n) T^n = \prod_{n\geq 1} (1 - [\alpha](c_n) T^n)^{-1} . \tag{5.6.2}$$

Then we have the formula

$$[\alpha](f(T)) = (f(\alpha T))^{\alpha^{-1}} . \tag{5.6.3}$$

Proof. Recall that the action of $\mathbf{Z}_p^\times$ on $D \subset R_\infty[1/p]$ is simply given by $[\alpha]f_k = \alpha^k f_k$ whenever f_k is a modular form of weight k. Recalling that a_n is modular of weight $n - 1$, we readily compute

$$\begin{aligned}[\alpha](f(T)) &= [\alpha]\left(\exp\left(\sum a_n \frac{T^n}{n}\right)\right) \\ &= \exp\left(\sum [\alpha](a_n)\frac{T^n}{n}\right) \\ &= \exp\left(\sum \alpha^{n-1} a_n \frac{T^n}{n}\right) \\ &= \exp\left(\alpha^{-1}\sum a_n \frac{(\alpha T)^n}{n}\right) \\ &= \left(\exp\left(\sum a_n \frac{(\alpha T)^n}{n}\right)\right)^{\alpha^{-1}} \\ &= (f(\alpha T))^{\alpha^{-1}} .\end{aligned} \tag{5.6.4}$$

Q.E.D.

COROLLARY 5.7. *For each integer $k \geqq 1$, we have the following congruences modulo pD.*

$$[1 + p^k](b_n) \equiv \begin{cases} b_n & \text{if } n < p^k \\ b_n - 1 & \text{if } n = p^k \end{cases} \quad \text{modulo } pD , \tag{5.7.1}$$

$$[1 + p^k](c_n) \equiv \begin{cases} c_n & \text{if } n < p^k \\ c_n - 1 & \text{if } n = p^k \end{cases} \quad \text{modulo } pD , \tag{5.7.2}$$

$$[1 + p^k](d_n) \equiv \begin{cases} d_n & \text{if } n < k \\ d_n - 1 & \text{if } n = k \end{cases} \quad \text{modulo } pD . \tag{5.7.3}$$

Proof. It suffices to demonstrate the first batch (on the b_n), in view of the identities

$$\begin{aligned} c_n &= b_n + \mathbf{Z}\text{-polynomial in } b_0, b_1, \cdots, b_{n-1} , \\ d_n &= c_{p^n} . \end{aligned} \tag{5.7.4}$$

Now by (5.6), we have the formula

$$(5.7.5)\qquad ([1+p^k](f(T)))^{1+p^k} = f((1+p^k)T) \equiv f(T) \quad \text{modulo } pD[[T]]\,.$$

Recalling that $f(T) = 1 + T + (T^2)$, we have the congruence

$$(5.7.6)\qquad ([1+p^k]f(T))^{p^k} \equiv 1 + T^{p^k} \bmod (p,\ T^{2p^k})\cdot D[[T]]\,,$$

which together with (5.7.5) gives the congruence

$$(5.7.7)\qquad [1+p^k](f(T))\cdot(1+Tp^k) \equiv f(T) \bmod (p,\ T^{2p^k})D[[T]]\,.$$

Comparing coefficients of T^n for $n = 0, 1, \cdots, p^k$ gives the desired result. It now follows directly from (2.4) that the elements $\beta(1)(d_n)$ are successive Artin-Schreier generators of $V_{1,\infty}$ over $V_{1,1}$, hence that the third condition of (3.3) is satisfied by the r_i. This concludes the proof of (5.5).

APPENDIX I

Modular interpretation, and relation to Serre's "p-adic modular forms of weight χ"

(A1) *Modular interpretation of the ring* $V_{m,n}$. The ring $V_{m,\infty}$ is the W_m-algebra of all "rules" f which assign to any situation

$$(\text{A1.1})\qquad \begin{array}{c}(E,\ \alpha_N,\ \varphi)\\ \downarrow\\ \operatorname{Spec} B\end{array}$$

consisting of an elliptic curve E over a W_m-algebra B together with a level-N structure of type ζ and an isomorphism $\varphi\colon \hat{E} \xrightarrow{\sim} (\hat{G}_m)_B$, an element

$$(\text{A1.2})\qquad f(E/B,\ \alpha_N,\ \varphi) \in B$$

which depends only on the isomorphism class of $(E/B,\ \alpha_N,\ \varphi)$ and whose formation commutes with arbitrary extension of scalars of W_m-algebras, and which satisfies the following "holomorphy at ∞" condition:

$$(\text{A1.3})\qquad f(\text{Tate}\,(q^N)/W_m((q)),\ \alpha_N,\ \varphi) \in W_m[[q]]$$

for every choice of level-N structure α_N of type ζ and for *every* choice of φ.

The ring $V_{\infty,\infty} = \varprojlim_m V_{m,\infty}$ may similarly be described as the rule of all such rules, where we allow B to be an arbitrary W-algebra in which p is nilpotent, and where in the holomorphy condition we check all W_m. Still equivalently, we may allow B to vary over all p-adically complete W-algebras, and check holomorphy on the Tate curves over the p-adic completion of $W((q))$.

In this optic, the homomorphism $\beta\colon R_\infty \to V_{\infty,\infty}$ may be described modularly as follows: For a modular form f of weight k, $\beta(f) \in V_{\infty,\infty}$ is the rule

$$\beta(f)(E/B, \alpha_N, \varphi) = f\Big(E/B, \alpha_N, \varphi^*\Big(\frac{dT}{1+T}\Big)\Big) \tag{A1.4}$$

where by abuse of notation we denote $\varphi^*(dT/(1+T))$ the unique invariant differential on E/B whose restriction to $\hat{E}$ is $\varphi^*(dT/(1+T))$.

The action of $\alpha \in \mathbf{Z}_p^\times$ on $V_{\infty,\infty}$ is deduced from its action on Isom $(\hat{E}, \hat{G}_m)$ by the formula

$$([\alpha]f)(E/B, \alpha_N, \varphi) = f(E/B, \alpha_N, \alpha^{-1}\varphi) . \tag{A1.5}$$

Application to modular forms of weight χ

Let $\chi \in \mathrm{Hom}_{\mathrm{contin}}(\mathbf{Z}_p^\times, \mathbf{Z}_p^\times)$ be a rational p-adic character of $\mathbf{Z}_p^\times$, and let $V_{\infty,\infty}^\chi$ denote the submodule of $V_{\infty,\infty}$ consisting of elements $f \in V_{\infty,\infty}$ such that $[\alpha](f) = \chi(\alpha)f$ for all $\alpha \in \mathbf{Z}_p^\times$.

PROPOSITION A1.6. *Let χ be as above, and if $p = 2$ suppose in addition that χ lies in the closure of $\mathbf{Z}$ in* End $(\mathbf{Z}_2^\times)$ *(this is automatically satisfied for $p \neq 2$). Then a p-adic modular form of weight χ and level-N, type ζ is precisely an element of $V_{\infty,\infty}^\chi$.*

Proof. We will give a direct, "computational" proof. Suppose first that f is a p-adic modular form of weight χ. This means that there is a sequence of true modular forms f_i, each *homogeneous* of some weight k_i, defined over W, whose q-expansions have a uniform p-adic limit q-expansion at each cusp of M, and this collection of limit q-expansions "is" f.

But the condition on the q-expansions of the f_i means precisely that, in the ring D, the elements f_i are p-adically convergent, and their *limit* in $\hat{D} = \varprojlim D/p^m D$ *is* f. In particular the sequence of elements $\beta(f_i) \in V_{\infty,\infty}$ is p-adically convergent, with limit $\beta(f)$. We must show that

$$\beta(f)(E, \alpha_N, \alpha^{-1}\varphi) = \chi(\alpha)\cdot\beta(f)(E, \alpha_N, \varphi) \tag{A1.7}$$

whenever $(E/B, \alpha_N, \varphi)$ is as in (A1.1), and $\alpha \in \mathbf{Z}_p^\times$. But $\beta(f) = \lim \beta(f_i)$ in $V_{\infty,\infty}$, hence for any fixed $(E/B, \alpha_N, \varphi)$, we have

$$\begin{aligned}\beta(f)(E/B, \alpha_N, \alpha^{-1}\varphi) &= \lim \beta(f_i)(E/B, \alpha_N, \alpha^{-1}\varphi)\\ &= \lim f_i\Big(E/B, \alpha_N, \alpha^{-1}\varphi^*\Big(\frac{dT}{1+T}\Big)\Big)\\ &= \lim \alpha^{k_i} f_i\Big(E/B, \alpha_N, \varphi^*\Big(\frac{dT}{1+T}\Big)\Big)\\ &= \chi(\alpha)\lim f_i\Big(E/B, \alpha_N, \varphi^*\Big(\frac{dT}{1+T}\Big)\Big)\\ &= \chi(\alpha)\lim \beta(f_i)(E/B, \alpha_N, \varphi)\\ &= \chi(\alpha)\cdot f(E/B, \alpha_N, \varphi) .\end{aligned} \tag{A1.8}$$

Suppose now that $g \in V^{\chi}_{\infty,\infty}$. Let $\{k_n\}$ be a sequence of integers such that

$$\chi(\alpha) \equiv \alpha^{k_n} \bmod p^n \quad \forall\, \alpha \in \mathbf{Z}_p^\times \,. \tag{A1.9}$$

We will use g to define a sequence f_n of "p-adic modular forms modulo p^n" of weight k_n, whose q-expansions tend p-adically to those of g. For each f_n there exists a *true* modular form g_n over W_n of weight k'_n such that

$$\begin{aligned} k_n &\equiv k'_n \text{ modulo } p^{n-1}(p-1)\,, \\ g_n(q) &\equiv f_n(q) \bmod p^n \text{ at each cusp} \end{aligned} \tag{A.10}$$

and we may choose $k'_n \gg 0$, in particular $k'_n \geqq 2$. Then the g_n may be lifted to true modular forms $\tilde{g}_n$ over W of weight k'_n, whose q-expansions tend to those of g. So it remains only to define the f_n.

Let B be a W_n-algebra, and $(E/B, \alpha_N, \omega)$ an elliptic curve over B with level-N structure and nowhere-vanishing invariant differential ω, such that $E \otimes B/pB$ has *invertible* Hasse invariant. We must define an element

$$f_n(E/B, \alpha_N, \omega) \in B \tag{A1.11}$$

which is homogeneous of degree k_n in the choice of ω, which depends only on the isomorphism class of $(E/B, \alpha_N, \omega)$, which commutes with extension of scalars of W_n-algebras, and which is holomorphic at infinity.

Over the ring $B_\infty = B \otimes_{V_{n,0}} V_{n,\infty}$ (B is a $V_{n,0}$-algebra by the homomorphism $V_{n,0} \to B$ which "classifies" (E, α_N)), there exists an isomorphism φ: $\hat{E} \xrightarrow{\sim} \hat{G}_m$. Let us write $\omega = \lambda\varphi^*(dT/(1+T))$, with $\lambda \in (B_\infty)^\times$; we "define"

$$f_n(E/B, \alpha_N, \omega) = \lambda^{-k_n}\cdot g(E/B, \alpha_N, \varphi) \tag{A1.12}$$

which is a priori an element of B_∞. It does not depend on the *choice* of isomorphism φ; if φ_1 is another, then $\varphi_1 = \alpha\varphi$ for some $\alpha \in \mathbf{Z}_p^\times$,

$$\omega = (\alpha^{-1}\cdot\lambda)(\varphi_1)^*\Big(\frac{dT}{1+T}\Big)\,,$$

and we could also "define"

$$f_n(E/B, \alpha_N, \omega) = (\alpha^{-1}\lambda)^{-k_n} g(E/B, \alpha_N, \varphi_1)\,. \tag{A1.13}$$

But indeed we readily calculate

$$\begin{aligned} (\alpha^{-1}\lambda)^{-k_n} g(E/B, \alpha_N, \varphi_1) &= \alpha^{k_n}\lambda^{-k_n} g(E/B, \alpha_N, \alpha\varphi) \\ &= \chi^{-1}(\alpha)\cdot\alpha^{k_n}\lambda^{-k_n} g(E/B, \alpha_N, \varphi) \\ &= \lambda^{-k_n} g(E/B, \alpha_N, \varphi) \end{aligned} \tag{A1.14}$$

because by choice of k_n we have

$$\chi(\alpha) \equiv \alpha^{k_n} \bmod p^n\,. \tag{A1.15}$$

Further, this very independence of $f_n(E/B, \alpha_N, \omega)$ of the auxiliary choice of

φ implies immediately that the value $f_n(E/B, \alpha_N, \omega)$ lies in B, because B is the subring of invariants of $\alpha \in \mathbf{Z}_p^\times$ acting as $\mathrm{id} \otimes [\alpha]$ on $B \otimes_{V_{n,0}} V_{n,\infty} = B_\infty$. It is clear that the remaining conditions for f_n to be a p-adic modular form modulo p^n are verified. Finally, the q-expansions of f_n are precisely the reductions mod p^n of those of g, because for the Tate curve the differential ω_{can} used for q-expansions is itself $\varphi^*(dT/(1+T))$, i.e., $\lambda = 1$.

A remark for the specialist. Let $\mathcal{O}$ be the ring of integers in any complete algebraically closed over-field of $W \otimes \mathbf{Q}_p$, and let

(A1.16) $$\chi\colon \mathbf{Z}_p^\times \longrightarrow \mathcal{O}^\times$$

be *any* continuous character. Then we may define a p-adic modular form of weight χ to be an element of $(V_{\infty,\infty} \hat{\otimes}_W \mathcal{O})^\chi$, where

$$V_{\infty,\infty} \hat{\otimes}_W \mathcal{O} \overset{\mathrm{dfn}}{=} \varprojlim_m V_{m,\infty} \otimes_{W_m} \mathcal{O} = \varprojlim_m \varinjlim_n V_{m,n} \otimes_{W_m} \mathcal{O}$$

is the ring of all rules ... as in (A1.1) but where we now restrict B to vary only over $\mathcal{O}$-algebras which are killed by some power of p (or, if we prefer, which are p-adically complete).

In down to earth terms, a p-adic modular form f of weight $\chi \in \mathrm{Hom}(\mathbf{Z}_p^\times, \mathcal{O}^\times)$ is thus a rule which assigns to each situation

(A1.17) $$\begin{array}{c} (E, \alpha_N, \varphi) \\ \downarrow \\ \mathrm{Spec}(B) \end{array}$$

where

(A1.18) $$\begin{cases} B \text{ is an } \mathcal{O}\text{-algebra in which } p \text{ is nilpotent} \\ (E, \alpha_N) \text{ is an elliptic curve with level-}N\text{ structure over } B \\ \varphi \text{ is an isomorphism } \varphi\colon \hat{E} \xrightarrow{\sim} \hat{G}_m \end{cases}$$

an element

(A1.19) $$f(E/B, \alpha_N, \varphi) \in B$$

such that

(A1.20) for any $\alpha \in \mathbf{Z}_p^\times$, $f(E/B, \alpha_N, \alpha^{-1}\varphi) = \chi(\alpha) f(E/B, \alpha_N, \varphi)$;

(A1.21) $f(E/B, \alpha_N, \varphi)$ depends only on the isomorphism class of $(E/B, \alpha_N, \varphi)$, and its formation commutes with arbitrary extension of $\mathcal{O}$-algebras $B \to B'$.

(A1.22) $f(\mathrm{Tate}(q^N), \alpha_N, \varphi) \in \mathcal{O}[[q]]$ for every level-N structure α_N and every φ on the Tate curve. (More precisely, the condition is that whenever we consider $\mathrm{Tate}(q^N)$ over $\mathcal{O}/p^n\mathcal{O}((q))$, any n, with any choice of α_N and φ, the value of f lies in $\mathcal{O}/p^n\mathcal{O}[[q]]$.)

By "pure thought", it may be checked that this definition of a p-adic modular form of weight χ is equivalent to that of a compatible system of sections of the invertible sheaf $\underline{\omega}^{\otimes\chi}$ on the various schemes $S_m \otimes_{W_m} \mathcal{O}$, where we denote by $\underline{\omega}^{\otimes\chi}$ the invertible *coherent* sheaf on $S_m \otimes \mathcal{O}$ associated to the p-adic etale sheaf T_p^χ over $S_m \otimes \mathcal{O}$ deduced from the p-adic etale sheaf T_p by "extension of the structural group" from $\mathbf{Z}_p^\times$ to $\mathcal{O}^\times$ via the character $\chi\colon \mathbf{Z}_p^\times \to \mathcal{O}^\times$. This description shows that there is a *plethora* of p-adic modular forms of weight χ, for

$$(V_{\infty,\infty} \otimes \hat{\mathcal{O}})^\chi = \varprojlim_m (V_{m,\infty} \otimes \mathcal{O})^\chi = \varprojlim_m H^0(S_m \otimes \mathcal{O}, \omega^{\otimes\chi}) .$$

Because the S_m are all affine we know that each individual $H^0(S_m \otimes \mathcal{O}, \underline{\omega}^{\otimes\chi})$ is an invertible module of rank one over the coordinate ring $V_{m,0} \otimes \mathcal{O}$ of $S_m \otimes \mathcal{O}$, and that the transition maps $H^0(S_{m+1} \otimes \mathcal{O}, \underline{\omega}^{\otimes\chi}) \to H^0(S_m \otimes \mathcal{O}, \underline{\omega}^{\otimes\chi})$ are all *surjective*. Thus there are "just as many" p-adic modular forms of weight χ as there are p-adic modular functions defined over $\mathcal{O}$.

This shows in particular that it is hopeless to try to decompose the ring $V_{\infty,\infty}$ as a $\mathbf{Z}_p^\times$ module according to the p-adic characters of $\mathbf{Z}_p^\times$, because every time we make an extension of scalars to an $\mathcal{O}$ as above, *new* characters of $\mathbf{Z}_p^\times$ occur in $V_{\infty,\infty} \hat{\otimes} \mathcal{O}$. (Indeed for $p \neq 2$, we have canonical isomorphisms

$$\operatorname{Hom}(\mathbf{Z}_p^\times, \mathcal{O}^\times) = \operatorname{Hom}\bigl(\mathbf{Z}/(p-1)\mathbf{Z}, \mu_{p-1}(\mathcal{O})\bigr) \times \operatorname{Hom}(1 + p\mathbf{Z}_p, \mathcal{O}^\times)$$

and via "evaluation at $1 + p$" we have an isomorphism

$$\operatorname{Hom}(1 + p\mathbf{Z}_p, \mathcal{O}^\times) \xrightarrow{\sim} 1 + \operatorname{Max}(\mathcal{O})$$

where $\operatorname{Max}(\mathcal{O})$ denotes the maximal ideal of $\mathcal{O}$.)

APPENDIX II

Congruences at a (finite) ordinary point on the moduli scheme (cf. [2])

Suppose k algebraically closed. Let E_0 be an *ordinary* elliptic curve (with level-N structure of type ζ) over k, viewed as a closed point of the moduli scheme M/W. Let us denote by $\mathcal{O}$ the completion of the local ring of M at this point. (Thus $\mathcal{O}$ is non-canonically isomorphic to $W[[X]]$, where $1 + X$ is some choice of Serre-Tate parameter "q".) Let

$$\text{(A2.1)} \qquad \begin{array}{c} E \\ \downarrow \\ \operatorname{Spec}(\mathcal{O}) \end{array}$$

be the inverse image of the universal curve over $\operatorname{Spec}(\mathcal{O}) \to M$. Then the formal group $\hat{E}$ over $\mathcal{O}$ is non-canonically isomorphic to $\hat{\mathbf{G}}_m$, the formal multiplicative group, and the set of isomorphisms between them is principal homogeneous under $\mathrm{Aut}_{\mathcal{O}}(\hat{\mathbf{G}}_m) = \mathbf{Z}_p^\times$. Each isomorphism $\varphi\colon \hat{E} \xrightarrow{\sim} \hat{\mathbf{G}}_m$ determines an invariant differential $\omega_\varphi \overset{\mathrm{dfn}}{=} \varphi^*(dT/(1+T))$ on $\hat{E}$ (where T is the usual parameter on the formal multiplicative group: $\Delta(T) = T \otimes 1 + 1 \otimes T + T \otimes T$), hence a nowhere-vanishing differential ω_φ on E itself.

Each such choice of φ allows us to define a sort of "q-expansion homomorphism"

(A2.2)
$$\begin{aligned} \beta_\varphi\colon R_\infty &\longrightarrow \mathcal{O}\ , \\ \sum f_i &\longrightarrow \sum f_i(E, \omega_\varphi) = \sum f_i/(\omega_\varphi)^{\otimes i}\ , \end{aligned}$$

and, by reduction modulo p^n, homomorphisms

(A2.3)
$$\begin{aligned} \beta_\varphi(n)\colon R_\infty &\longrightarrow \mathcal{O}/p^n\mathcal{O} \\ \beta_\varphi(n) &= \beta_\varphi \bmod p^n\ . \end{aligned}$$

PROPOSITION (A2.4). *For any choice of isomorphism $\varphi\colon \hat{E} \xrightarrow{\sim} \hat{\mathbf{G}}_m$, and for any $n \geqq 1$, we have*

$$I_n = \textit{kernel of } \beta_\varphi(n)\colon R_\infty \longrightarrow \mathcal{O}/p^n\mathcal{O}\ .$$

Proof. The isomorphism $\varphi\colon \hat{E} \xrightarrow{\sim} \hat{\mathbf{G}}_m$ induces an isomorphism ${}_{p^n}\hat{E} \xrightarrow{\sim} \mu_{p^n}$, and by reduction modulo p^n gives an isomorphism ${}_{p^n}\hat{E} \otimes \mathcal{O}/p^n\mathcal{O} \xrightarrow{\sim} \mu_{p^n}$ over $\mathcal{O}/p^n\mathcal{O}$. But the scheme $T_{m,n}$ over M_n is *the* etale covering of $S_n \subset M_n$ defined by "adjoining" all isomorphisms of ${}_{p^n}\hat{E} \mid S^n$ with μ_{p^n}, and the differentials ω_{can} are the (unique invariant differentials on $\hat{E}_{T_{m,n}}$ whose restrictions to $({}_{p^n}\hat{E})_{T_{n,n}}$ are the) inverse images by these isomorphisms of the standard differential $dT/(1+T)$ on μ_{p^n}. If we recall that $\mathcal{O}/p^n\mathcal{O}$ is "simply connected", it follows that in the diagram

(A2.5)
$$\begin{tikzcd} & T_{n,n} \arrow[d] \\ \mathrm{Spec}\,(\mathcal{O}/p^n\mathcal{O}) \arrow[r, hook] \arrow[ur, dashed] & S_n \end{tikzcd}$$

there are precisely $p^{n-1}(p-1)$ sections over Spec $(\mathcal{O}/p^n\mathcal{O})$, and that the inverse images by these sections of any ω_{can} on $T_{n,n}$ are precisely the $p^{n-1}(p-1)$ distinct (mod p^n) differentials ω_φ. Thus the homomorphism $\beta_\varphi(n)$ is obtained by composing the homomorphism

$$\beta(n)\colon R_\infty \longrightarrow V_{n,n}$$

with the inclusion $V_{n,n} \subset \mathcal{O}/p^n\mathcal{O}$ defined by one of the sections of (A2.5).

Q.E.D.

APPENDIX III

Deligne's Generalization of Theorem 2.1 to "false" Modular Forms

This appendix is devoted to formulating and proving a generalization of Theorem 2.1, without recourse to Artin-Schreier theory. Both the formulation and the proof are Deligne's. I have let my original proof stand in the text because its construction of successive Artin-Schreier generators is still needed for the actual determination of the higher congruences between modular forms.

A. The affine case

Let W be a mixed characteristic complete discrete valuation ring of residue characteristic p. Let π be a uniformizing parameter, and for each integer $m \geqq 1$, let $W_m = W/\pi^m W$. Let S_m be a sequence of flat affine W_m-schemes, given with isomorphisms $S_{m+1} \otimes_{W_{m+1}} W_m \xrightarrow{\sim} S_m$. Let P be a rank one p-adic etale sheaf on the S_m (i.e., P on S_{m+1} is the unique p-adic etale sheaf on S_{m+1} which induces P on S_1). Thus P "is" an inverse system $P_n = P/p^n P$ of etale sheaves which are twisted forms of the *constant* etale sheaves $\mathbf{Z}/p^n\mathbf{Z}$. Let $\underline{\omega}_n$ be the invertible (coherent) sheaf $P \otimes_{\mathbf{Z}_p} \mathcal{O}_{S_m}$ on S_m, which for variable m are compatible via the isomorphisms $S_m \simeq S_{m+1} \otimes W_m$.

We define graded rings

$$R'_m = \bigoplus_{k \geqq 0} H^0(S_m, \underline{\omega}^{\otimes k}) ,$$
$$R'_\infty = \bigoplus_{k \geqq 0} \varprojlim_m H^0(S_m, \underline{\omega}^{\otimes k}) .$$

Notice that because each S_m is *affine*, and $S_m = S_{m+1} \bmod \pi^m$, we have

$$R'_\infty/\pi^m R'_\infty \xrightarrow{\sim} R'_m .$$

Let us define

$$T_{m,n} = \mathrm{Isom}_{S_m}(\mathbf{Z}/p^n\mathbf{Z}, P_n) \qquad (= \mathrm{Spec}\,(V_{m,n}))$$

a finite etale S_m-scheme which represents the functor on Sch/S_m,

$$\begin{array}{c} X \\ \big\downarrow \pi \\ S_m \end{array} \longmapsto \text{isomorphisms } \psi_n\colon (\mathbf{Z}/p^n\mathbf{Z})_X \xrightarrow{\sim} \pi^*(P_n) .$$

The group $(\mathbf{Z}/p^n\mathbf{Z})^\times$ acts freely on $T_{m,n}([\alpha]\psi_n = \alpha^{-1}\psi_n)$ with quotient S_m.

For variable n, the schemes $T_{m,n}$ form a projective system $(T_{m,n+1} \twoheadrightarrow T_{m,n})$ whose inverse limit $T_{m,\infty} = \mathrm{Spec}\,(V_{m,\infty} = \varinjlim_n V_{m,n})$ represents the functor

$$\begin{array}{c} X \\ \Big\downarrow \pi \\ S_m \end{array} \longmapsto \text{isomorphisms } \psi\colon \mathbf{Z}_p \xrightarrow{\sim} \pi^*(P) .$$

The group $\mathbf{Z}_p^\times$ acts freely on $T_{m,\infty}$ ($[\alpha]\psi = \alpha^{-1}\psi$), with quotient S_m.

The homomorphism $\beta(m)$

$$\beta(m)\colon R'_m \longrightarrow V_{m,m} = \Gamma(T_{m,m}, \mathcal{O}) \hookrightarrow V_{m,\infty}$$

may be defined as follows. Over $T_{m,m}$, we have the *universal* isomorphism from $\mathbf{Z}/p^m\mathbf{Z}$ to P_m, under which the element $1 \in \mathbf{Z}/p^m\mathbf{Z}$ gives rise to a section of P_m and then to an invertible section of $\underline{\omega} = P_m \otimes \mathcal{O}_{T_{m,m}}$ over $T_{m,m}$, denoted $\omega_{\mathrm{can}}(m)$. So we define

$$\beta(m)(\textstyle\sum f_i) = \sum f_i/(\omega_{\mathrm{can}}(m))^{\otimes i} .$$

In the spirit of Appendix I, we may view $V_{m,m}$ as the ring of all "functions"

$$f\left(\begin{array}{c} X \\ \Big\downarrow \\ S_m \end{array} \pi,\ \psi_m\colon \mathbf{Z}/p^m\mathbf{Z} \xrightarrow{\sim} P_m\right)$$

with values in $\Gamma(X, \mathcal{O}_X)$, for variable X and variable ψ_m whose formation is compatible with arbitrary change of base $X' \to X$. Then $\beta(m)$ identifies $H^0(S_m, \underline{\omega}^{\otimes k})$ with those functions which transform under $(\mathbf{Z}/p^m\mathbf{Z})^\times$ (the indeterminacy in the choice of ψ_m) by $\alpha \mapsto \alpha^k$. This shows that $H^0(S_m, \underline{\omega}^{\otimes k})$ and $H^0(S_m, \underline{\omega}^{\otimes k+(p-1)p^{m-1}})$ have identical images in $V_{m,m}$, and shows how far $\beta(m)$ is from being injective on all of R'_m. Passing to the inverse limit in each degree, we obtain a homomorphism

$$\beta(\infty)\colon R'_\infty \longrightarrow V \overset{\mathrm{dfn}}{=\!=} \varprojlim_m V_{m,\infty} .$$

Exactly as in Appendix I, we can view V as the ring of all "functions"

$$f\left(\begin{array}{c} X \\ \Big\downarrow \\ S_m \end{array} \pi,\ \psi\colon \mathbf{Z}_p \xrightarrow{\sim} \pi^*(P)\right)$$

with values in $\Gamma(X, \mathcal{O}_X)$ for variable X and variable m whose formation is compatible with all changes of base $X' \to X$. This ring V is p-adically complete, flat over W (because $V/\pi^m V = V_{m,\infty} = \varinjlim_n V_{m,n}$ is etale over S_m, hence flat over W_m), and $\mathbf{Z}_p^x$ acts on it, by the rule

$$([\alpha]f)(X, \psi) = f(X, \alpha^{-1}\psi) .$$

The reasoning of Appendix I shows that $\beta(\infty)$ *identifies* the homogeneous components $\varprojlim_m H^0(S_m, \underline{\omega}^{\otimes k})$ of R'_∞ with the subspaces $V^{(k)} \subset V$ consisting of the functions $f \in V$ which satisfy $[\alpha]f = \alpha^k f$ for all $\alpha \in \mathbf{Z}_p^\times$. Because V is *flat* over W, the usual "independence of characters" argument shows that the map $\beta(\infty)$ is *injective:*

$$R'_\infty \subset V .$$

Since V and (hence) R'_∞ are *flat* over W, we may tensor this inclusion with the fraction field of W, and obtain a diagram of inclusions

$$\begin{tikzcd} R'_\infty \arrow[r, hook] \arrow[d, hook] & V \arrow[d, hook] \\ R'_\infty\left[\frac{1}{p}\right] \arrow[r, hook] & V\left[\frac{1}{p}\right] . \end{tikzcd}$$

We define D' to be the intersection

$$D' = V \cap R'_\infty\left[\frac{1}{p}\right] .$$

THEOREM. *The inclusion* $D' \xhookrightarrow{\beta(\infty)} V$ *induces isomorphisms*

$$D'/\pi^m D' \xrightarrow{\sim} V/\pi^m V ;$$

equivalently, V *is the p-adic completion of* D'.

Proof. It follows from the *definition* of D' that the cokernel V/D' is W-flat, so the exact sequence $0 \to D' \to V \to V/D' \to 0$ remains exact when reduced modulo π^m; $D'/\pi^m D' \hookrightarrow V/\pi^m V$. It remains to check that the map is *onto*, and for this it suffices to show that $D'/\pi D' \twoheadrightarrow V/\pi V = V_{1,\infty}$. So take $f \in V_{1,\infty}$, say $f \in V_{1,n}$. To make clear the idea of the proof, suppose first that $P_m = P/p^m P$ is *trivial*, where m is so large that

$$\pi^{m-1}/i! \in W \quad \text{if } 0 < i < p^n .$$

Now let $F \in \varprojlim_m V_{m,n} \subset V$ lift $f \in V_{1,n}$. It suffices to show that $\pi^{m-1}F \in \beta(\infty)R'_\infty + \pi^m V$, for then $F \in \beta(\infty)D' + \pi V$ as required. Notice that, as $R'_\infty/\pi^m R'_\infty \simeq R'_m$, this statement is *equivalent* to the statement (where $F_m =$ the image of F in $V_{m,n}$)

$$\pi^{m-1}F_m \in \beta(m)R'_m .$$

As we supposed that P_m is *trivial*, we have

$$T_{m,m} = \mathrm{Aut}_{S_m}(\mathbf{Z}/p^m\mathbf{Z}) = S_m \times (\mathbf{Z}/p^m\mathbf{Z})^\times$$

so that $V_{m,m}$ is the ring of all $V_{m,0} = H^0(S_m, \mathcal{O})$-valued functions on the group

$(\mathbf{Z}/p^m\mathbf{Z})^\times$. The sheaf $\underline{\omega}$ on S_m becomes the structure sheaf $\mathcal{O}_{S_m}$, because

$$\underline{\omega} = P \otimes_{\mathbf{Z}_p} \mathcal{O}_{S_m} = P_m \otimes_{\mathbf{Z}/p^m\mathbf{Z}} \mathcal{O}_{S_m} \simeq \mathcal{O}_{S_m} ,$$

and R'_m becomes the polynomial ring $H^0(S_m, \mathcal{O}_{S_m})[X]$. The mapping

$$\beta(m)\colon R'_m \longrightarrow V_{m,m}$$

becomes the map

$$H^0(S_m, \mathcal{O}_{S_m})[X] \longrightarrow H^0(S_m, \mathcal{O}_{S_m})\text{-valued functions on } (\mathbf{Z}/p^m\mathbf{Z})^\times$$

obtained by viewing polynomials as *functions* (well-defined because $p^m = 0$ in $H^0(S_m, \mathcal{O}_{S_m})$).

The function $\pi^{m-1}F_m \in \pi^{m-1} V_{m,n} \subset V_{m,m}$ becomes a $\pi^{m-1}H^0(S_m, \mathcal{O})$-valued function on $(\mathbf{Z}/p^m\mathbf{Z})^x$ which factors through $(\mathbf{Z}/p^n\mathbf{Z})^x$. If we recall that $\pi^{m-1}H^0(S_m, \mathcal{O}_{S_m})$ is an $\mathbf{F}_p$-vector space, then the fact ("Mahler's theorem") that the $\mathbf{F}_p$-vector space Maps $(\mathbf{Z}/p^n\mathbf{Z}, \mathbf{F}_p)$ has as basis the "binomial coefficient functions" $x \longrightarrow \binom{x}{i}$, $0 \leqq i \leqq p^n - 1$ shows that any $\pi^{m-1} V_{m,0}$-valued function on $(\mathbf{Z}/p^n\mathbf{Z})^\times \subset \mathbf{Z}/p^n\mathbf{Z}$ may be written as a sum

$$\sum_{i=0}^{p^n-1} a_i \binom{x}{i} , \qquad\qquad a_i \in \pi^{m-1}H^0(S_m, \mathcal{O}_{S_m}) .$$

But m was so chosen that

$$\pi^{m-1}\binom{x}{i} \in W[X] , \qquad \text{for } 0 \leqq i \leqq p^n - 1$$

and therefore the function $\pi^{m-1}F_m$ indeed lies in the image of R'_m.

Now let us turn to the general case where we no longer suppose P_m trivial. Arguing as above, we must show that, in the above notations,

$$V_{m,m} \supset \beta(m)R'_m \supset \pi^{m-1} V_{m,n} ,$$

a statement which "involves" only a flat affine W_m-scheme S_m, a "twisted" form P_m of $\mathbf{Z}/p^m\mathbf{Z}$ on S_m, and an integer $n \ll m$ such that $\pi^{m-1} \in (p^n - 1)! \cdot W$.

Now suppose that A is any faithfully flat over-ring of $H^0(S_m, \mathcal{O}_{S_m})$. If we consider the inverse image of our problem over A, its statement remains the same, save that $V_{m,m}$, R'_m, and $V_{m,n}$ have become $V_{m,m} \otimes A$, $R'_m \otimes A$, $V_{m,n} \otimes A$. The original problem was to show that, in $V_{m,m}$, we have

$$\pi^{m-1} V_{m,n} \subset \beta(m)R'_m ,$$

or equivalently that the composite map

$$V_{m,n} \xrightarrow{\pi^{m-1}} V_{m,m}/\beta(m)R'_m$$

is the *zero* map. For this, it suffices that the map

$$V_{m,n} \otimes A \xrightarrow{\pi^{m-1}} V_{m,m} \otimes A/\beta(m)R'_m \otimes A$$

be zero, or, what is the same, that our problem have an affirmative solution over A, which we know *is* the case if P_m becomes trivial on A. So we simply take $V_{m,m}$ itself for A. Q.E.D.

B. The proper case

We retain the preceding notations, but now begin with a proper and smooth W-scheme M, whose fibres are geometrically connected curves. We put $M_m = M \otimes_W M_m$. Let $H \subset M_1$ be a finite set of closed points, and let $S_m \subset M_m$ be the affine open set $M_m - H$. We are given a rank one p-adic etale sheaf P on the S_m, and we give ourselves further an invertible sheaf $\underline{\omega}$ on M which induces $P \otimes_{\mathbf{Z}_p} \mathcal{O}_{S_m}$ on S_m.

Notice that $\underline{\omega}^{\otimes p-1}$ is *trivial* on S_1, because

$$P^{\otimes p-1} \otimes_{\mathbf{Z}_p} \mathcal{O}_{S_1} = (P \otimes \mathbf{Z}/p\mathbf{Z})^{\otimes p-1} \otimes_{\mathbf{Z}/p\mathbf{Z}} \mathcal{O}_{S_1} \quad \text{and} \quad (P \otimes \mathbf{Z}/p\mathbf{Z})^{\otimes p-1} \simeq \mathbf{Z}/p\mathbf{Z}$$

canonically. This trivialization determines a section $A \in H^0(S_1, \underline{\omega})$, corresponding to $1 \in \mathbf{Z}/p\mathbf{Z}$.

THEOREM. *Suppose that $A \in H^0(S_1, \underline{\omega})$ extends to a (necessarily unique) section $A \in H^0(M_1, \underline{\omega})$ which vanishes at each point of H. Then if we define $R_\infty = \bigoplus_{k \geq 0} H^0(M, \underline{\omega}^{\otimes k})$, we have $R_\infty \subset R'_\infty \subset V$, and if we put $D = R_\infty[1/p] \cap V$, then the inclusions*

$$D \subset D' \subset V$$

induce isomorphisms modulo any power of π:

$$D/\pi^m D \simeq D'/\pi^m D' \simeq V/\pi^m V\,.$$

Proof. Because M_m is smooth over W_m and is *irreducible*, the restriction map $H^0(M_m, \underline{\omega}^{\otimes k}) \to H^0(S_m, \underline{\omega}^{\otimes k})$ is injective. As

$$H^0(M, \underline{\omega}^{\otimes k}) \xrightarrow{\sim} \varprojlim_m H^0(M_m, \underline{\omega}^{\otimes k})\,,$$

we certainly have $R_\infty \subset R'_\infty$, and then $D \subset D'$. By definition of D, D', the maps $D/\pi^m D \to V/\pi^m V$ and $D'/\pi^m D' \to V/\pi^m V$ are both injective, therefore the map $D/\pi^m D \to D'/\pi^m D'$ is injective. To show surjectivity, it suffices to show $D/\pi D \to D'/\pi D'$ is surjective.

For this, we argue as follows. The sheaf $\underline{\omega}$ on M has positive degree, because a power of it on M_1 has a non-zero section which has zeros (namely A). Pick any integer $\nu > 0$ such that $\underline{\omega}^{\otimes \nu(p-1)}$ has degree $> 2g-2$, g = genus of M_1. Then the section $A^\nu \in H^0(M_1, \underline{\omega}^{\otimes \nu(p-1)})$ lifts to a section $E \in H^0(M, \underline{\omega}^{\otimes \nu(p-1)})$. Notice that

(1) The image of E^{p^n} in V lies in $1+\pi^{n+1}V$. This follows by induction on n once we know that the image of E lies in $1+\pi V$. This in turn follows from the fact that the image of A in $V_{1,1}$, viewed as a "function" of situations (an S_1-scheme X, an isomorphism $\psi_1\colon \mathbf{Z}/p\mathbf{Z} \xrightarrow{\sim} P_1$ on X) with values in $\Gamma(X, \mathcal{O}_X)$ which is homogeneous of degree $p-1$ in the choice of ψ_1 (indeterminacy: $(\mathbf{Z}/p\mathbf{Z})^\times$) is tautologically the *constant* function "1";

$$A\left(\begin{matrix} X \\ \downarrow \\ S_1 \end{matrix}, \ \psi_1\colon \mathbf{Z}/p\mathbf{Z} \xrightarrow{\sim} P_1 \text{ on } X\right) = 1 \in \Gamma(X, \mathcal{O}_X)\ .$$

(2) Because the open-subscheme $S_m \subset M_m$ is the open set where E is an *invertible* section of $\underline{\omega}^{\otimes\nu(p-1)}$, we have

$$H^0(S_m, \underline{\omega}^{\otimes k}) = \varinjlim_n \frac{H^0(M_m, \underline{\omega}^{\otimes k+n\nu(p-1)})}{E^n}\ .$$

Now let $\sum f_i \in R'_\infty$ lie in $\pi^m V$. We must approximate it modulo $\pi^{m+1}V$ by an element of R_∞. For this, it suffices to approximate each homogeneous $f_i \in \varprojlim H^0(S_m, \underline{\omega}^{\otimes i})$ modulo $\pi^{m+1}V$ by an element of R_∞. Now

$$f_i \equiv \frac{g_{i+N\nu p^m(p-1)}}{E^{Np^m}} \bmod \pi^{m+1}R'_\infty$$

for some $g_{i+Np^m\nu(p-1)} \in H^0(M, \underline{\omega}^{\otimes i+Np^m\nu(p-1)})$ where $N \gg 0$ depends upon f_i, by (2) above. By (1) above, f_i and $g_{i+Np^m\nu(p-1)}$ differ multiplicatively in V by an element of $1+\pi^{m+1}V$, so that

$$f_i - g_{i+Np^m\nu(p-1)} \in \pi^{m+1}V\ . \qquad \text{Q.E.D.}$$

INSTITUT DES HAUTES ÉTUDES SCIENTIFIQUES, FRANCE
PRINCETON UNIVERSITY

REFERENCES

[1] P. DELIGNE and M. RAPOPORT, Les schémas de modules de courbes elliptiques, Proc. of the 1972 Antwerp International Summer School on Modular Functions, Springer Lecture Notes in Mathematics **349** (1973), 143-317.
[2] B. DWORK, *P*-adic cycles, Pub. Math. I.H.E.S. **37** (1969), 327-415.
[3] N. Katz, *P*-adic properties of modular schemes and modular forms, Proceedings of the 1972 Antwerp International Summer School on Modular Functions, Springer Lecture Notes in Mathematics **350** (1973), 70-189.
[4] T. KUBOTA and W. LEOPOLDT, Eine *p*-adische Theorie der Zetawerte, I, Jour. Reine und Angew. Math. **214/215** (1964), 328-339.
[5] B. MAZUR, Analyse *p*-adique; secret Bourbaki rédaction, 1973.
[6] J. P. SERRE, Congruences et formes modularies, Exposé 416, Séminaire N. Bourbaki 1971/72, Springer Lecture Notes in Mathematics **317** (1973), 319-338.
[7] ———, Formes modularies et fonctions zeta *p*-adiques, Proceedings of the 1972 Antwerp International Summer School on Modular Functions, Springer Lecture Notes

in Mathematics **350** (1973).

[8] H. P. F. SWINNERTON-DYER, On l-adic representations and congruences for coefficients of modular forms, Proceedings of the 1972 Antwerp International Summer School on Modular Functions, Springer Lecture Notes in Mathematics **350** (1973), 1-55.

(Received October 4, 1973)