Higher Congruences Between Modular Forms

Nicholas M. Katz


Stable URL: http://links.jstor.org/sici?sici=0003-486X%28197503%292%3A101%3A2%3C332%3AHCBMF%3E2.0.CO%3B2-J


---

Your use of the JSTOR archive indicates your acceptance of JSTOR's Terms and Conditions of Use, available at http://www.jstor.org/about/terms.html. JSTOR's Terms and Conditions of Use provides, in part, that unless you have obtained prior permission, you may not download an entire issue of a journal or multiple copies of articles, and you may use content in the JSTOR archive only for your personal, non-commercial use.

Please contact the publisher regarding any further use of this work. Publisher contact information may be obtained at http://www.jstor.org/journals/annals.html.

Each copy of any part of a JSTOR transmission must contain the same copyright notice that appears on the screen or printed page of such transmission.

---

The JSTOR Archive is a trusted digital repository providing for long-term preservation and access to leading academic journals and scholarly literature from around the world. The Archive is supported by libraries, scholarly societies, publishers, and foundations. It is an initiative of JSTOR, a not-for-profit organization with a mission to help the scholarly community take advantage of advances in technology. For more information regarding JSTOR, please contact support@jstor.org.
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 $\text{SL}(2, \mathbb{Z})$ 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 $\mathbb{Q}_p$, $f_i$ of weight $i$, such that the sum of the $q$-expansions $\sum f_i(q)$ has coefficients in $\mathbb{Z}_p$. 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 $\chi$". 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 $p \geq 5$ we mean the usual Eisenstein series

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

which is a modular form of weight $p-1$ over $\mathbb{Q} \cap \mathbb{Z}_p$, whose reduction mod $p$ is the Hasse invariant. Unfortunately for $p = 2$ or $p = 3$ there are no modular forms over $\mathbb{Q} \cap \mathbb{Z}_p$ of level one and weight $p - 1$. In compensation, when $p = 2$ or 3, we will always consider modular forms of some fixed level $N \geq 3$ 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 $N \geq 3$ prime to $p$, such liftings always exist, while for $p = 2$, and $N$ odd such liftings are only known to exist for $3 \leq N \leq 11$, 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 "\mu" 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 $N \geq 3$ 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 $N^{\text{th}}$ root of unity $\zeta$. For each integer $m \geq 1$, write $W_m$ for the Witt vectors $W_m(k)$ of length $m$, and denote $W_m(k)$ simply as $W$. The unique primitive $N^{\text{th}}$ root of unity in $W$ which lifts $\zeta$, the "Teichmüller representative", will also be denoted $\zeta$.

Let $M^\circ$ be the moduli scheme over $W$ which classifies isomorphism classes of elliptic curves over $W$-algebras together with a level-$N$ structure of determinant $\zeta$, and let $M$ be its canonical compactification. Thus $M$ is a proper smooth curve over $W$ with geometrically connected fibres, and the difference $M - M^\circ$ 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 $m \geq 1$, we put $M_m^\circ = M^\circ \otimes_w W_m$, $M_m = M \otimes_w W_m$. Let $S_m$ (resp. $S_m^\circ$) denote the open subscheme of $M_m^\circ$ (resp. $M_m$) where the Hasse invariant mod $p$ (or equivalently $E_{p-1}$) is invertible. The schemes $S_m^\circ$ and $S_m$ are affine smooth curves over $W_m$, with geometrically irreducible special fibre. We have
\[ S_m = S_{m+1} \otimes W_{m+1} W_m, \quad S_m^0 = S_{m+1}^0 \otimes W_{m+1} W_m. \]

(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 \( n \geq 1 \), the kernel of multiplication by \( p^n \) on \( E \), noted \( p_n E \), is an extension
\[
0 \to p_n \hat{E} \to p_n E \to p_n E^{et} \to 0
\]
where \( p_n \hat{E} \) 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 \( \mu_{p^n} \) 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 \( \mathbb{Z}/p^n\mathbb{Z} \).

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

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

(1.2.1) The characters \( \chi_n, \chi \) on \( \pi_1(S_m^0) \) extend to characters still noted \( \chi_n, \chi \) 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 \( \chi : \pi_1(S_m) \to (\mathbb{Z}/p^n\mathbb{Z})^\times \) are surjective (for any non-empty Zariski open set \( U \subset S_m \), the composite \( \chi : \pi_1(U) \to (\mathbb{Z}/p^n\mathbb{Z})^\times \) 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 \( \chi_n : \pi_1(S_m) \to (\mathbb{Z}/p^n\mathbb{Z})^\times \). The scheme \( T_{m,n} \) is a smooth affine \( W_m \)-scheme with geometrically connected special fibre. For fixed \( n \), we have
\[
T_{m+1,n} \otimes W_m \simeq T_{m,n}
\]
and for fixed \( m \) we have
\[
T_{m,n+1} \xrightarrow{pr_{m,n+1}} T_{m,n} \to \cdots \to T_{m,1} \to S_m.
\]

The inverse image of any cusp of \( S_m \) is the disjoint unit of \( \varphi(p^n) = (p - 1)p^{n-1} = \#((\mathbb{Z}/p^n\mathbb{Z})^\times) \mathbb{W}_m \)-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 \( \chi \) 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 \( \widehat{\Gamma}_m \), hence the etale quotient of the kernel of \( p^m \) on the Tate curve isomorphic to \( \mathbb{Z}/p^m \mathbb{Z} \) over \( W_m[[q]] \); the \( \varphi(p^m) \) 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 \( \mathbb{Z}_p^\times \).)

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

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

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

\[
\begin{array}{ccc}
T_{m,n+1} & \simeq & T_{m+1,m+1} \\
\downarrow & & \downarrow \\
T_{m,n} & \rightarrow & T_{m+1,m+1} \\
\end{array}
\]

we have

\[ \omega_{\text{can}}(m + 1) \mod p^m = p r_{m,m+1}^*(\omega_{\text{can}}(m)) \]

Such choices are possible, and the set of all such is principally homogeneous under \( (\mathbb{Z}_p)^\times \). There is a unique isomorphism of \( \mathbb{Z}_p^\times \) with \( \lim_\leftarrow \text{Aut } (T_{m,n}/S_m) \) which is independent of \( m \) (i.e., compatible with the canonical isomorphisms
Aut \((T_{m+1,n}/S_{m+1}) \simeq \text{Aut} \, (T_{m,n}/S_m)\) and under which
\[ [\alpha](\omega_{\text{can}}) = \alpha^{-1}\omega_{\text{can}} \]
(meaning that, \(\forall \, m, \, [\alpha \bmod p^m](\omega_{\text{can}}(m)) = (\alpha^{-1} \bmod p^m) \cdot \omega_{\text{can}}(m))\).

(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 \(T_{0,0} = S_m \)) 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 \(\omega_{\text{can}}(m) \) has \(q\)-expansion \(1 \in W_m[[q]] \) at the cusp \(\alpha_{m,n} \).

**Definition of the fundamental homomorphism**

(1.4) For each integer \(m \geq 1\), let \(R_m \) be the graded ring of holomorphic modular forms defined over \(W_m \) of level \(N\) and type \(\zeta\), i.e.,
\[ R_m = \bigoplus_{k \geq 0} H^0(M_m, \omega^{\otimes k}) \]
and let \(R_\infty \) be the graded ring of holomorphic modular forms defined over \(W\) of level \(N\) and type \(\zeta\), i.e.,
\[ R_\infty = \bigoplus_{k \geq 0} H^0(M, \omega^{\otimes k}) \cdot \]
For \(3 \leq N \leq 11\), we have \(R_\infty /p^mR_\infty \simeq R_m\), but for \(N \geq 12\) 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 \(R_\infty /p^mR_\infty \sim R_m\) 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
\[ V_{m,n} \subset W_m[[q]] \cdot \]

**Lemma 1.4.3.** The cokernel \(W_m[[q]]/V_{m,n}\) is flat over \(W_m\).

**Proof.** Modulo \(p\), the inclusion \(V_{m,n} \rightarrow W_m[[q]]\) becomes the inclusion \(V_{1,n} \rightarrow k[[q]]\). Q.E.D.

The rings \(V_{m,n}\) sit in chains for variable \(n\),
\[ V_{m,0} \subset V_{m,1} \subset V_{m,2} \subset \cdots \]
and for variable \(m\) are related by canonical isomorphisms
\[ V_{m+1,n}/p^n V_{m+1,n} \sim V_{m,n} \cdot \]
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
\[ V_{m,\infty} \subset W_m[[q]] \cdot \]
HIGHER CONGRUENCES

For variable $m$, we have canonical isomorphisms

(1.4.7) \[ V_{m+1,\infty}/p^m V_{m+1,\infty} \sim V_{m,\infty}. \]

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

(1.4.8) \[ \beta_m: R_m \rightarrow V_{m,m} \subset V_{m,\infty} \]

as follows: Let $f_i \in H^0(M_m, \omega_{\eta_i})$ be a modular form of weight $i$. Then by restriction, $f_i$ determines a section of $\omega_{\eta_i}$ over $S_m$, and then by inverse image determines a section of $\omega_{\eta_i}$ over $T_{m,m}$. But over $T_{m,m}$ we are given an invertible section $\omega_{\text{can}}(m)$ of $\omega$, 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

(1.4.9) \[ \beta_m(\sum f_i) = \sum f_i/(\omega_{\text{can}}(m))^{\otimes i}. \]

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

**Lemma 1.5.** Let $\alpha_{\eta,0}$ be a cusp of $S$, and $\alpha_{m,m}$ the compatible system of cusps of the $T_{m,m}$ defined (1.3.1) by the choice of $\omega_{\text{can}}$. For any element $f_i \in H^0(M_m, \omega_{\eta_i})$, 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 $m_1 \leq m$. If it is true at one cusp of $M_m$ that $\sum f_i(q) \equiv 0 \mod p^{m_1}$ 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 $m_1 \leq m$, $\sum f_i$ 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 $a \in (\mathbb{Z}/p^m\mathbb{Z})^\times$ the element $\sum af_i \in R_m$ enjoys the same property.

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

\[
\beta_m(p^{m-m_1} \sum af_i) = p^{m-m_1} \sum af_i/(\omega_{\text{can}}(m))^{\otimes i} = p^{m-m_1}[a](\sum f_i/(\omega_{\text{can}}(m)^{\otimes i})) = [a]\beta_m(p^{m-m_1} \sum f_i) = [a](0) = 0.
\]

Q.E.D.

**Corollary 1.8.** The image of the inclusion $V_{m,n} \rightarrow W_m[[q]]$ 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 $\text{SL}(2, \mathbb{Z}/N\mathbb{Z})$ on the level-$N$ structures, so we may assume that our cusp lies on $T_{m,n}$ over the same cusp $\alpha_{i,0}$ as the standard chosen cusp (cf. 1.3.1). Then our cusp will be the transform of the standard one by some automorphism $[\alpha] \in (\mathbb{Z}/p^n\mathbb{Z})^\times$. Thus all the possible $q$-expansion homomorphisms $V_{m,n} \rightarrow W_m[[q]]$ 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 $V_{\infty,\infty} \rightarrow W[[q]]$ 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 $I_{m,1}$ (resp. $I_{\infty,1}$) denote the (non-graded) ideal of $R_m$ (resp. $R_{\infty}$) consisting of those elements $\sum f_i$ such that at one (or equivalently, at every) cusp of $M$, $\sum f_i(q) \equiv 0 \pmod{p}$.

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

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

A generalization of the fundamental homomorphism

We wish to define a module-homomorphism

(1.10) \[
\frac{1}{p^{m_1}} \beta_m : I_{m,1} \longrightarrow V_{m-m_1,1} \subset V_{m-m_1,\infty}
\]
as follows: If $\sum f_i \in I_{m,1}$, then $p^{m_1} \beta_m (\sum f_i) = 0$ 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 $p^{m_1} V_{m,m}$ and thus determines a well-defined element of $V_{m-m_1,1} \subset V_{m-m_1,\infty}$ which we denote $((1/p^{m_1}) \beta_m (\sum f_i))$. By passage to the inverse limit over $m$, we obtain a homomorphism

(1.11) \[
\frac{1}{p^{m_1}} \beta_{\infty} : I_{\infty,1} \longrightarrow \lim_{m} V_{m,\infty} \overset{df}{=} V_{\infty,\infty}.
\]

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

(1.1.2) \[
p^{m_1} \frac{1}{p^{m_1}} \beta_{\infty} = \beta_{\infty} \text{ on } I_{\infty,1}.
\]

2. The ring $D$ of divided congruences

(2.0) Let us denote by $D$ the $W$-algebra $R_{\infty} + (1/p) \cdot I_{\infty,1} + (1/p^2) \cdot I_{\infty,2} + \cdots$, 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 $R_{\infty} \subset (1/p) \cdot I_{\infty,1} \subset (1/p^2) \cdot I_{\infty,2} \subset \cdots \subset (1/p^a) \cdot I_{\infty,n} \subset \cdots$, so that $D = \lim_{\longrightarrow} p^{-a} \cdot I_{\infty,n}$ as $W$-module.)
We define a $W$-algebra homomorphism

\begin{align}
\beta : D & \longrightarrow V_{\infty, \infty} \\
\end{align}

by the requirement that on $p^{-n} \cdot I_{m,n}$, $\beta$ is \text{"}(1/p^n)\beta_{\infty, \infty}\text{"}. That $\beta$ 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{align}
D & \xrightarrow{\beta} V_{\infty, \infty} \xrightarrow{q\text{-expansion}} W[[q]] \\
\cap & \qquad \cap \\
R_{\infty} \left[ \frac{1}{p} \right] & \xrightarrow{q\text{-expansion}} W[[q]] \left[ \frac{1}{p} \right].
\end{align}

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

\begin{align}
\beta(m) : D/p^mD & \longrightarrow V_{m, \infty}.
\end{align}

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

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

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 $R_{\infty}$ of $D$.

**Theorem 2.2.** $\beta_i : R_i \rightarrow V_{1,1}$ is surjective, with kernel the principal ideal $(E_{p-1} - 1)$.

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

$0 \rightarrow \text{Symm}(\omega^{\otimes(p-1)}) \rightarrow \text{Symm}(\omega^{\otimes(p-1)}) \rightarrow \text{Symm}(\omega^{\otimes(p-1)})/(E_{p-1} - 1) \rightarrow 0$

shows that

$$V_{1,0} \simeq H^0(M, \text{Symm}(\omega^{\otimes(p-1)}))/(E_{p-1} - 1)$$

$$\simeq \bigoplus_k H^0(M, \omega^{\otimes k (p-1)})/(E_{p-1} - 1).$$

The map is explicitly given by $\sum f_{i(p-1)} \rightarrow \sum f_{i(p-1)}/E_{p-1}$ and thus coincides with the restriction to $R_i^{(p-1)}$ of $\beta_i$. Similarly, the scheme $T_{1,1}$ is the etale covering of $S$, 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 $(p-1)^{th}$ root of the Hasse invariant, or equivalently of its inverse. It follows that

$$T_{1,1} = \text{Spec}_M (\text{Symm}(\omega)/(E_{p-1} - 1))$$

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

$$V_{1,1} = H^0(M, \text{Symm}(\omega)/(E_{p-1} - 1)).$$

The long exact cohomology sequence then gives

$$V_{1,1} = H^0(M, \text{Symm}(\omega))/(E_{p-1} - 1) = R_i/(E_{p-1} - 1),$$

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

$$\sum f_i \rightarrow \sum \varepsilon f_i = \sum f_i/(\omega \text{can}(1)^{\otimes i}) = \beta_i(\sum f_i).$$

Thus we have the desired commutative diagram

$$R_i/(E_{p-1} - 1) \xrightarrow{\sim} V_{1,1}.$$

$$R_i \xrightarrow{\sim} V_{1,1} \xrightarrow{\beta_i} R_i.$$

**Corollary 2.2.8. (Swinnerton-Dyer).** The ideal $I_{1,1}$ of $R_i$ 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 $m \geq 1$, we may obtain a partial generalization of Swinnerton-Dyer's result:

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

\[
\beta_m: R_m^\varphi(p^m)/(E_{p'(p^m)} - 1) \sim V_{m,0} = \Gamma(S_m, \mathcal{O}_{S_m}).
\]

**Proof.** As before we have \( S_m = \text{Spec}_k (\text{Symm}(\omega \otimes_{p(p^m)})(E_{p(p^m)} - 1)) \), and

\[
V_{m,0} = H^q(M_m, \text{Symm}(\omega \otimes_{p(p^m)})(E_{p(p^m)} - 1)) = R_m^\varphi(p^m)/(E_{p(p^m)} - 1).
\]

Furthermore the isomorphism is given explicitly by

\[
\sum f_{i}(p^m) \longrightarrow \sum f_{i}(p^m)/E_{p'(p^m)}^i.
\]

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

\[
\sum f_{i}(p^m) \longrightarrow \sum f_{i}(p^m)/(\omega_{\text{can}}(m))^i = \beta_m(\sum f_{i}(p^m)).
\]

We now return to the problem of surjectivity. We have shown that \( \beta_i \) maps \( R_i \) onto \( V_{i,1} \).

**Corollary 2.3.** The composition \( R_\infty \rightarrow R_i \rightarrow V_{1,1} \) is also surjective, with kernel \( (p, E_{p-1} - 1) \).

**Proof.** Although \( R_\infty \rightarrow R_i \) need not be surjective, the composite will be, because \( \beta_i \) kills the ideal \( (E_{p-1} - 1) \), hence \( \beta_i(R_i) = \beta_i(E_{p-1}R_i) = \beta_i((E_{p-1})^2R_i) \), and for \( 0 \leq 2 \), \( H^q(M, \omega^{\otimes}) \otimes k \rightarrow H^q(M, \omega^{\otimes}) \) is surjective. This shows that \( V_{1,1} \) is precisely the image under \( \beta(1) \) of the subring \( R_\infty \) 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 \( F_p \)-algebra), and let \( B \supset A \) be a finite etale \( A \)-algebra of rank \( p \), which is Galois with group \( \mathbb{Z}/p\mathbb{Z} \) (thus \( \text{Aut}(B/A) \sim \mathbb{Z}/p\mathbb{Z} \), and \( A \) is the subring of invariants). Then there exists an element \( b \in B \) such that \( n \in \mathbb{Z}/p\mathbb{Z} \) acts by sending \( b \rightarrow b + n \). 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 \( A[X]/(X^p - X - a) \sim B \). In particular, any element \( b \in B \) which is sent to \( b + 1 \) by a generator of \( \mathbb{Z}/p\mathbb{Z} \) 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 \( \mathbb{Z}_p^\times \) on the ring \( D \) by the formula

\[
[a](\sum f_i) = \sum a^if_i, \quad a \in \mathbb{Z}_p^\times, \sum f_i \in D.
\]

(It is a priori an action of \( \mathbb{Z}_p^\times \) 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 $\mathbb{Z}_p^\times$-equivariance of the homomorphisms $\beta(m): D/p^nD \to V_{m,\infty}$. 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 $n \geq 1$, precisely the subring of invariants of the subgroup $1 + p^n\mathbb{Z}_p$ of $\mathbb{Z}_p^\times$, and the Galois group of $V_{m,n+1}$ over $V_{m,n}$ is canonically $1 + p^n\mathbb{Z}_p/1 + p^{n+1}\mathbb{Z}_p$, a cyclic group of order $p$ generated by the class of $1 + p^n$.

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

$$[1 + p^{n+k}](d_n) = d_n + p^kE_{p-1} \text{ modulo } p^{k+1}D.$$  

Admitting this lemma for a moment, let us conclude the surjectivity of $\beta(1)$. By the lemma, $\beta(1)(d_n)$ is invariant by $1 + p^{n+1}\mathbb{Z}_p$, 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 $n \geq 1$, 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 $\{\beta(1)(d_n)\}_{n \geq 1}$. 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 $R_\infty$-submodule of $R_\infty[d_1, \ldots, d_n, \ldots]$ spanned over $R_\infty$ by the products

$$\prod_{i \geq 1} (d_i)^{a_i}, \quad a_i = 0 \text{ for all but finitely many } i, \quad \alpha_i \leq p - 1,$$

maps onto $V_{1,\infty}$, and hence onto $V_{m,\infty}$ for any $m \geq 1$. 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

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

We immediately calculate

$$[1 + p^{1+k}](d_1) = \frac{1 - (1 + p^{1+k})^{p-1}E_{p-1}}{p}$$

$$= \frac{1 - E_{p-1} - (p - 1)p^{1+k}E_{p-1} + (p^{2k+2})E_{p-1} - E_{p-1}}{p}$$

$$= d_1 + p^kE_{p-1} - p^{k+1}E_{p-1}$$

$$= d_1 + p^{k+1}E_{p-1} \mod p^{k+1}D.$$  

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

\[ V_{1,n} = V_{1,1}[\beta(1)(d), \ldots, \beta(1)(d_{n-1})] = \beta(1)(R_\infty[d_1, \ldots, d_{n-1}]). \]

Thus we may choose an element

\[ C_n \in R_\infty[d_1, \ldots, d_{n-1}], \quad C_n = \sum_{0 \leq i_1, \ldots, i_{n-1} \leq p-1} f_{i_1, \ldots, i_{n-1}} \prod_{j=i}^{n-1} d_j^{i_j} \]

such that

\[ (\beta(1)(d_n) - (\beta(1)(d_n))^p = \beta(1)(C_n). \]

Consider the element

\[ d_n - (d_n)^p - C_n \in Ker \beta(1) = pD. \]

We define

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

It remains to verify the transformation property. We calculate:

\[ \frac{[1 + p^{n+q+k}](d_{n+1})}{p} = \frac{[1 + p^{n+q+k}](d_n) - (1 + p^{n+q+k})(d_n)^p - [1 + p^{n+q+k}](C_n)}{p}. \]

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

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

In particular,

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

By the transformational congruences for \( d_1, \ldots, d_{n-1} \), we see that

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

Combining all this, we find

\[ [1 + p^{n+q+k}](d_{n+1}) = \frac{d_n + p^{k+1}E_{p-1} - (d_n)^p - C_n + p^{k+2}D}{p} \]

\[ \equiv d_{n+1} + p^kE_{p-1} \text{ modulo } p^{k+1}D. \text{ Q.E.D.} \]

3. Determination of the ideals \( I_{\omega,n} \subset R_\infty \)

(3.0) Henceforth, let us agree to denote \( I_{\omega,n} \), 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 $n \geq 1$, the elements $r_n = p^{(p^n-1)/(p-1)} \cdot d_n$ of $D$ lie in $R_\infty$, 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):

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

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:

$$r_{n+1} = p^{(p^{n+1}-1)/(p-1)} \cdot d_{n+1} = p^{p+p^2+p^3+\cdots+p^n}td_{n+1}$$

$$= p^{p+p^2+p^3+\cdots+p^n}[d_{n} - (d_n)^p - C_n(d_1, \cdots, d_{n-1})] = p^{p^n}r_n - (r_n)^p$$

$$- \sum_{\sigma \leq (a_1, \ldots, a_{n-1}) \leq P-1} \prod_{i=1}^{n-1} (r_i)^{a_i}.$$  

**Q.E.D.**

**Corollary 3.2.** For each integer $n \geq 1$,

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

**Proof.** Obvious from the formula (3.1.3) above.

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

$$p^{a_1}r_1^{a_1}\cdots r_n^{a_n}$$

such that

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

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

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 $R_\infty$ such that

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

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

$$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 $V_{1,i}$ form a sequence of successive Artin-Schreier generators of $V_{1,i}$ 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 \( n \geq 1 \), the ideal \( I_n = I_{\infty, n} \) of \( R_\infty \) is generated by those monomials
\[
p^{a_0} r_1^{a_1} \cdots r_j^{a_j}
\]
such that
\[
a_0 + \sum_{i=1}^{j} a_i \left( \frac{p^i - 1}{p - 1} \right) = n.
\]

**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
\[
\begin{cases}
a_0 + \sum_{i=1}^{j} a_i \left( \frac{p^i - 1}{p - 1} \right) \geq n \\
\text{if } i \geq 1, \text{ then } 0 \leq a_i \leq p - 1.
\end{cases}
\]

**Lemma 3.4.** For every \( n \geq 1 \), 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
\[
\sum f_{a_0, \ldots, a_j} p^{a_0} r_1^{a_1} \cdots r_j^{a_j}, \quad f_{a_0, \ldots, a_j} \in R_\infty,
\]
the sum extended over finitely many tuples \( (a_0, \ldots, a_j) \) which all satisfy
\[
\begin{cases}
a_0 + \sum_{i=1}^{j} a_i \left( \frac{p^i - 1}{p - 1} \right) \geq n \\
0 \leq a_i \leq p - 1 \text{ for } i \geq 1.
\end{cases}
\]
Any of these monomials for which \( a_0 + \sum a_i ((p^i - 1)/(p - 1)) \geq n + 1 \) already lies in \( I''_{n+1} \). Subtracting, we may assume that only monomials satisfying
\[
\begin{cases}
a_0 + \sum_{i=1}^{j} a_i \left( \frac{p^i - 1}{p - 1} \right) = n \\
0 \leq a_i \leq p - 1 \text{ if } i \geq 1
\end{cases}
\]
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
\[(3.4.4) \quad \frac{p^ao_{i_1} \cdots r^a_j}{p} = (d_i)^{a_1} \cdots (d_j)^{a_j} \text{ if } a_0 + \sum a_i \left( \frac{p^i - 1}{p - 1} \right) = n \]
we thus conclude that
\[(3.4.5) \quad \sum f_{a_0, \ldots, a_j}(d_i)^{a_1} \cdots (d_j)^{a_j} \in \text{kernel of } \beta(1) \; ;
\]
i.e.,
\[(3.4.6) \quad \sum \beta(1)(f_{a_0, \ldots, a_j}) \prod_{i=1}^j (\beta(1)(d_i))^{a_i} = 0 \text{ in } V_{1,\infty} .
\]
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 \( 0 \leq a_i \leq p - 1 \), we have
\[(3.4.7) \quad \beta(1)(f_{a_0, \ldots, a_j}) \in \text{ker } \beta(1) ;
\]
the coefficients \( f_{a_0, \ldots, a_j} \) all lie in \( I = (p, r) \). Thus we must show that if \( a_0 + \sum a_i((p^i - 1)/(p - 1)) = n, \; 0 \leq a_i \leq p - 1 \) for \( i \geq 1 \), then
\[(3.4.8) \quad \begin{cases} p \; p^{a_0} \prod r^a_i \in I_{n+1}'' \\ r_1 p^{a_0} \prod r^a_i \in I_{n+1}'' \end{cases}.
\]

The first of these inclusions is obvious. The second is obvious in case either \( a_0 > 0 \), in which case \( r_1 p^{a_0} \prod r^a_i \in p \cdot I_n = pI_{n'} \subset I_{n''} \), or in case \( a_1 \leq p - 2 \), in which case \( r_1 p^{a_0} \prod r^a_i \) is one of the standard monomials in \( I_{n+1}'' \). Thus we must show that
\[(3.4.9) \quad r^a_i \prod r^a_j \in I_{n+1}'' \text{ if } p + \sum a_i \left( \frac{p^i - 1}{p - 1} \right) = n + 1 .
\]
In fact, let us show that if \( n = \sum a_i((p^i - 1)/(p - 1)) \) and \( 0 \leq a_i \leq p - 1 \), then for any integer \( 1 \leq k \leq j \),
\[(3.4.10) \quad (r_1)^p r^{a_1+1}_k \cdots r^a_j \in I_{n+1}'' .
\]
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)
\[(3.4.11) \quad (r_j)^p + r_{j+1} \in p \cdot I_{p((p^j-1)/(p-1))} = p \cdot I_n = pI_n'' \subset I_{n+1}
\]
the inclusion \( I_{p((p^j-1)/(p-1))} \subset I_n \) because
\[
n = \sum a_i \left( \frac{p^i - 1}{p - 1} \right) \leq \sum a_i (p^i - 1) = -j + p \left( \frac{p^j - 1}{p - 1} \right)
\]
\[
\leq -1 + p \left( \frac{p^j - 1}{p - 1} \right) .
\]
For \( k < j \), we have, again by (3.3.2),
HIGHER CONGRUENCES

(3.4.12) \( r_{k+1} + (r_k)^p \in p \cdot I_{p((p^{k-1})/(p-1)) - 1} \subseteq pI_n - \sum_{i=k+1}^n a_i(({p^i-1})/(p-1)) \cdot \)

Hence,

(3.4.13) \( r_{k+1}(r_{k+1})^{p^{k+1}} \cdots r_{ij}^{p^{k+1}} + (r_k)^p r_{k+1}^{p^{k+1}} \cdots r_{ij}^{p^{k+1}} \in pI_n = pI_n'' \subseteq I_n''' \).

If \( a_{k+1} \leq p - 2 \), then the first term in the sum (3.4.13) is a standard monomial of \( I_n''' \), 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 \( I_n''' \). 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 \( n \geq 1 \), \( I_n' = I_n'' \).

**Proof.** Because \( I_n' \subseteq I_n = I_n'' \), it suffices to prove that \( I_n'' \subseteq I_n' \). Consider one of the standard monomial generators of \( I_n'' \), say \( p^{a_0}r_{ij}^{a_1} \cdots r_{ij}^{a_n} \). If \( \sum_{i \geq 0} a_i \geq 2 \), we may write this monomial non-trivially as a product of monomials, as an element of \( I_a \cdot I_b \) for some integers \( a, b \geq 1 \), \( a + b = n \). By induction on \( n \), we may suppose \( I_n = I_n' \), \( I_n = I_n'' \), and clearly \( I_n' \cdot I_n'' \subseteq I_n' = I_n'' \). 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 \( (p^j-1)/(p-1) \geq n \). 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

\[ r_j + (r_{j-1})^p \in pI_{p((p^{j-1})/(p-1)) - 1} \subseteq pI_{n-1} = pI_{n-1}'' \subseteq I_n' \]

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: \( p \geq 5 \)

(4.0) Suppose first \( p \geq 5 \), and choose \( N = p - 1 \), \( k = F_p W = Z_p \). Let us write

\[ G = SL_2(Z/(p-1)Z) \]

\[ G_1 = \text{the subgroup of } G \text{ of elements } \equiv 1 \text{ modulo 2.} \]

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

**Lemma 4.1.** If \( p \geq 5 \), 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 ($p \geq 5$, $N = p - 1$), the elements $d_1$, $d_2$, ... may be chosen to be $G$-invariant.

**Proof.** Clearly $d_1 = (1/p)(1 - E_p)$ is $G$-invariant, because $E_p$ is a modular form of level one, defined over $\mathbb{Z}$. Suppose that $d_1$, $d_2$, ..., $d_n$ 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 $G_n(d_1, ..., d_{n-1})$ be a polynomial in $d_1$, $d_2$, ..., $d_{n-1}$ with coefficients in $R_{\infty}$, and degree $\leq p - 1$ in each $d_i$, such that $\beta(1)(C_n) = \beta(1)((d_n)^p - d_n)$. Writing $C_n = \sum f_{a_1, ..., a_{n-1}} d_{i_1}^a \cdots d_{i_{n-1}}^a$ with coefficients $f \in R_{\infty}$, we see that if we replace each $f = f_{a_1, ..., a_{n-1}}$ by its integral over $G$ (i.e., $\frac{1}{\# G} \sum_{g \in G} f(g)$) then we replace $C_n$ by its integral over $G$. But because $\beta(1)(C_n)$ is $G$-invariant, we have $\beta(1)(C_n) = \beta(1)(\sum G C_n)$. 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 $r_1$, $r_2$, ... may be chosen $G$-invariant.

**Theorem 4.4.** The ideal $I_n^0$ of $R_{\infty}$, and the ideal $I_n^G$ of $R_{\infty}$, are generated by those monomials

\[ p^{a_0} r_1^{a_1} \cdots r_j^{a_j} \]

which satisfy

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

**Proof.** By (3.3), any element of $I_n^0$ (resp. $I_n^G$) may be written as an $R_{\infty}$-linear combination of the above monomials:

\[ \sum f_{a_0, ..., a_j} p^{a_0} r_1^{a_1} \cdots r_j^{a_j} . \]

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

\[ \sum \left( \int_G f_{a_0, ..., a_j} p^{a_0} r_1^{a_1} \cdots r_j^{a_j} . \right) \quad Q.E.D. \]

**3-adic congruences in level 2**

(4.5) The problem of 3-adic congruences between modular forms of level-
two defined over $\mathbb{Z}_p$ may be handled by a similar integration argument, as follows. Choose $N = 4$, $k = F_q = F_q[i]$, $W = \mathbb{Z}_p[i]$, and view the corresponding modular scheme $M$ as a scheme over $\mathbb{Z}_p$. So viewed, the subgroup $G_i$ of $\text{GL}_2(\mathbb{Z})$ acts on $M$, the quotient $\pm 1$ acting as $\text{Gal}(\mathbb{Z}_p[i]/\mathbb{Z}_p)$, and the quotient is the projective $\lambda$-line over $\mathbb{Z}_p$, denoted simply $\mathbb{P}^1$. The invertible sheaf $\omega$ does not descend to $\mathbb{P}^1$, but its square $\omega^{\otimes 2}$ descends canonically to the sheaf $\mathcal{O}(1) = \Omega_1(\log (0, 1))$ 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 $dx/\gamma$ 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 $\mathbb{Z}_p$ is just the subring $(R_{\infty})^{G_1} \simeq \bigotimes_{k \geq 0} H^0(\mathbb{P}^1, \mathcal{O}(k))$.

Because the Hasse invariant lifts to a level-2 modular form over $\mathbb{Z}_p$ (for instance the section $(-1 - \lambda)dx/2\lambda(1 - \lambda)$ of $\Omega_1(\log (0, 1, \infty))$, we may choose the relation $r_1$ to be $G_i$-invariant. Because the group $G_i$, has order 16 (prime to 3), the integration technique used above (cf. 4.4) allows us to select the successive relations $r_2, r_3, \ldots$, in a $G_i$-invariant way. We obtain, for any such selection, the following

**Theorem 4.6.** The ideal $I_{\infty}^{G_1}$ 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 ($p \geq 5$)**

(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 $(E, \omega)$ be a pair consisting of an elliptic curve $E$ over $B$ and a nowhere-vanishing differential $\omega$ 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 $E$ and unique "constants" $g_2, g_3 \in B$

\[
\begin{align*}
X &= X(E, \omega) \in H^0(E, \mathcal{O}_E(-2\infty)) \\
Y &= Y(E, \omega) \in H^0(E, \mathcal{O}_E(-3\infty))
\end{align*}
\]
350 NICHOLAS M. KATZ

\begin{align}
\begin{cases}
g_2 &= g_2(E, \omega) \\
g_3 &= g_3(E, \omega)
\end{cases}
\end{align}

such that the pair \((E, \omega)\) is the pair

\begin{align}
\begin{cases}
Y^2 &= 4X^3 - g_2X - g_3 \\
\omega &= dX/Y
\end{cases}
\end{align}

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 \(\lambda \in B^\times\).

\begin{align}
X(E, \lambda \omega) &= \lambda^{-2}X(E, \omega) , \\
Y(E, \lambda \omega) &= \lambda^{-3}Y(E, \omega) , \\
g_4(E, \lambda \omega) &= \lambda^{-4}g_4(E, \omega) , \\
g_5(E, \lambda \omega) &= \lambda^{-6}g_5(E, \omega) , \\
T(E, \lambda \omega) &= \lambda T(E, \omega) .
\end{align}

(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 \(\omega\):

\begin{align}
\omega &= \sum_{n \geq 1} a_n \lambda^n dT \\
\omega &= \sum a_n(E, \omega) \cdot (T(E, \omega))^{-1} dT(E, \omega) , \\
\lambda \omega &= \sum a_n(E, \lambda \omega) (T(E, \lambda \omega))^{-1} dT(E, \lambda \omega)
\end{align}

by (5.0.8)

\begin{align}
= \sum a_n(E, \lambda \omega) \cdot \lambda^n \cdot (T(E, \omega))^{-1} dT(E, \omega) .
\end{align}

Thus we have the transformation formulas, for \(n \geq 1\):

\begin{align}
a_n(E, \lambda \omega) &= \lambda^{1-n}a_n(E, \omega)
\end{align}

which say precisely that \(a_n\) is a modular form (over \(\mathbb{Z}[1/6]\)) of weight \(n - 1\). It follows by reduction to the universal case that the universal expression of \(a_{n-1}\) as a \(\mathbb{Z}\)-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 \(a_{2t}\) are all zero, and the first few \(a_{2t+1}\) are given by
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

\[
\begin{align*}
g_2(q) &= \frac{1}{12} E_4(q) = \frac{1}{12} \left(1 + 240 \sum_{n \geq 1} \sigma_3(n) q^n \right) \\
g_3(q) &= \frac{-1}{216} E_6(q) = \frac{-1}{216} \left(1 - 504 \sum_{n \geq 1} \sigma_5(n) q^n \right)
\end{align*}
\]

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

\[
\begin{cases}
Y^2 = 4X^3 - \frac{E_4}{12}X + \frac{E_6}{216} \\
\omega_{\text{can}} = dX/Y.
\end{cases}
\]

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

\[
Z = -2T \mod T^n\mathbb{Z}[1/6][[q]][[T]]
\]

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

\[
\begin{align*}
X &= \sum_{n \geq 1} \frac{q^n (1 + Z)}{(1 - q^n(1 + Z))^2} + \frac{1}{12} - 2 \sum_{n=1}^\infty \frac{q^n}{1 - q^n}, \\
Y &= (1 + Z) \frac{d}{dZ}(X)
\end{align*}
\]

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

\[
\omega_{\text{can}} = dX/Y = dZ/(1 + Z) = d \log (1 + Z)
\]

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

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

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

**Fact (5.2).** The series \(\exp(\sum a_n(q)(T^n/n))\) actually lies in \(\mathbb{Z}[1/6][[q]][[T]]\).
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 $T$:

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

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

\[(5.3.2) \quad \prod_{n \geq 1} (1 - c_n T^n)^{-1} = \sum_{n \geq 0} b_n T^n = \exp \left( \sum_{n \geq 1} a_n \frac{T^n}{n} \right).\]

Thanks to FACT (5.2), we have the remarkable

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

**Applications to congruences**

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

\[(5.4.1) \quad d_n \overset{\text{dfn}}{=} c_{p^n}.\]

Taking the logarithmic derivative of both sides of (5.3.2), we obtain the following formulas expressing the $d_i$ in terms of the $a_p$:

\[(5.4.2) \quad p^n d_n + p^{n-1}(d_{n-1})^p + p^{n-2}(d_{n-2})^{p^2} + \cdots + (d_0)^{p^n} = a_p^n; \]

\[
\begin{align*}
    d_0 &= c_1 = 1 \\
    d_1 &= \frac{a_p - 1}{p} \\
    d_2 &= \frac{a_{p^2} - 1}{p^2} - \frac{1}{p} \left( \frac{a_p - 1}{p} \right)^p \\
    d_3 &= \frac{a_{p^3} - 1}{p^3} - \frac{1}{p} \left( \frac{a_p - 1}{p} \right)^{p^2} - \frac{1}{p} \left[ \frac{a_{p^2} - 1}{p^2} - \frac{1}{p} \left( \frac{a_p - 1}{p} \right)^p \right].
\end{align*}
\]

**Lemma 5.4.4.** For each $n \geq 1$, the element

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

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

**Theorem 5.5.** For any integer $N \geq 1$ prime to $p$, and any perfect field $k$ of characteristic $p$ containing a primitive $N^{\text{th}}$ root of unity $\zeta$, denote by $R_\infty$ the ring of holomorphic modular forms of level $N$ and type $\zeta$ 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)
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 \( \mathbb{Z} \), by the "integration" argument of (4.4), which is valid because the \( r_i \) are of level-one and defined over \( \mathbb{Z} \). To do the case \( N \geq 3 \), 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

\[ \text{(5.5.1)} \quad r_{n+1} + (r_n)^p \in pI_{p((p^{n-1})/(p-1))-1} \]

is easily deduced from the fundamental formula (5.4.2):

\[ \text{(5.5.2)} \quad p^{n+1}d_{n+1} + p^n(d_n)^p + p^{n-1}(d_{n-1})^p + \cdots + (d_0)^{p^{n+1}} = a_{p^{n+1}}. \]

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

\[ \text{(5.5.3)} \quad 0 = r_{n+1} + (r_n)^p + \sum_{j=1}^n p^{\gamma_j} (p^{i-1})(r_{n-j})^{p^{j+1}} - p^{\gamma_i} (p^{i-1}) a_{p^{n+1}}. \]

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

\[ \text{(5.5.4)} \quad r_{n-1,2} \overset{\text{dfn}}{=} (r_{n-1})^{p^2} + \sum_{j=2}^n p^{\gamma_j} (p^{i-1})(r_{n-j})^{p^{j+1}} - p^{\gamma_i} (p^{i-1}) a_{p^{n+1}}. \]

Then (5.5.3) says that

\[ \text{(5.5.5)} \quad r_{n+1} + (r_n)^p + p^{p-1}r_{n-2,3} = 0. \]

By (5.4.4), we know that

\[ \text{(5.5.6)} \quad r_{n+1} \in I_{(p^{n+1}-1)/(p-1)}, \quad (r_n)^p \in I_{p(p^{n-1})/(p-1)}. \]

Hence

\[ \text{(5.5.7)} \quad p^{p-1}r_{n-1,2} \in I_{p(p^{n-1})/(p-1)}, \]

which is to say

\[ \text{(5.5.8)} \quad r_{n-1,2} \in I_{p(p^{n-1})/(p-1)-(p-1)}. \]

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

\[ \text{(5.5.9)} \quad r_{n+1} + (r_n)^p = p^{p-1}r_{n-1,2} \in p \cdot I_{p(p^{n-1})/(p-1)-1}. \]

Let us delay verification of the third condition for a moment. The fourth condition is satisfied, because \( r_i = 1 - a_p \), 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 \( Z^*_p \) on the elements \( b_i, c_i, \) and \( d_i \in D \) (cf. 2.4).
Lemma 5.6. Let

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

For any \( \alpha \in \mathbb{Z}_p^* \), let \([\alpha]\) denote the canonical galois action of \( \alpha \) on the ring \( D \), and define

\[(5.6.2) \quad [\alpha](f(T)) \overset{def}{=} \sum_{n \geq 0} [\alpha](b_n) T^n = \prod_{n=1}^{\infty} (1 - [\alpha](c_n) T^n)^{-1}. \]

Then we have the formula

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

Proof. Recall that the action of \( \mathbb{Z}_p^* \) 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

\[(5.6.4) \quad [\alpha](f(T)) = [\alpha] \left( \exp \left( \sum a_n \frac{T^n}{n} \right) \right) \]

\[= \exp \left( \sum \frac{[\alpha](a_n) T^n}{n} \right) \]

\[= \exp \left( \sum \frac{\alpha^{-1} a_n T^n}{n} \right) \]

\[= \exp \left( \alpha^{-1} \sum \frac{a_n (\alpha T)^n}{n} \right) \]

\[= \left( \exp \left( \sum \frac{a_n (\alpha T)^n}{n} \right) \right)^{a^{-1}} \]

\[= (f(\alpha T))^{a^{-1}}. \]

Q.E.D.

Corollary 5.7. For each integer \( k \geq 1 \), we have the following congruences modulo \( pD \).

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

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

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

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

\[(5.7.4) \quad c_n = b_n + \text{\(Z\)-polynomial in } b_n, b_1, \ldots, b_{n-1}, \quad d_n = c_{p^n}. \]
Now by (5.6), we have the formula
\[(5.7.5) \quad ([1 + p^k](f(T)))^{1 + p^k} = f((1 + p^k)T) \equiv f(T) \mod pD[[T]].\]
Recalling that \(f(T) = 1 + T + (T^2)\), we have the congruence
\[(5.7.6) \quad ([1 + p^k](f(T))^{p^k} = 1 + T^{p^k} \mod (p, T^{p^k})D[[T]],\]
which together with (5.7.5) gives the congruence
\[(5.7.7) \quad [1 + p^k](f(T)) \cdot (1 + T^{p^k}) = f(T) \mod (p, T^{p^k})D[[T]].\]
Comparing coefficients of \(T^n\) for \(n = 0, 1, \ldots, p^k\) gives the desired result.

It now follows directly from (2.4) that the elements \(\beta(1)(d_n)\) are successive Artin-Schreier generators of \(V_{i,\infty}\) over \(V_{i,1}\), 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 \(V_{\mathfrak{m},\infty}\).** The ring \(V_{\mathfrak{m},\infty}\) is the \(W_\mathfrak{m}\)-algebra of all “rules” \(f\) which assign to any situation
\[(E, \alpha_N, \varphi)\]

consisting of an elliptic curve \(E\) over a \(W_\mathfrak{m}\)-algebra \(B\) together with a level-
\(N\) structure of type \(\zeta\) and an isomorphism \(\varphi: \hat{E} \xrightarrow{\sim} (\hat{G}_\mathfrak{m})_B\), an element
\[(A1.2) \quad f(E/B, \alpha_N, \varphi) \in B\]

which depends only on the isomorphism class of \((E/B, \alpha_N, \varphi)\) and whose formation commutes with arbitrary extension of scalars of \(W_\mathfrak{m}\)-algebras, and which satisfies the following “holomorphy at \(\infty\)” condition:

(A1.3) \(f(\text{Tate}(q^\infty)/W_\mathfrak{m}((q)), \alpha_N, \varphi) \in W_\infty[[q]]\)

for every choice of level-
\(N\) structure \(\alpha_N\) of type \(\zeta\) and for every choice of \(\varphi\).

The ring \(V_{\infty,\infty} = \lim_{\leftarrow} V_{\mathfrak{m},\infty}\) 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 \(W_\mathfrak{m}\). 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 \(\beta: R_\infty \rightarrow V_{\infty,\infty}\) may be described modularly as follows: For a modular form \(f\) of weight \(k\), \(\beta(f) \in V_{\infty,\infty}\) is the rule
(A1.4) \[
\beta(f)(E/B, \alpha_N, \varphi) = f\left(\frac{dT}{1 + T}\right)
\]

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

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

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

**Application to modular forms of weight \(\chi\)**

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

**Proposition A1.6.** Let \(\chi\) be as above, and if \(p = 2\) suppose in addition that \(\chi\) lies in the closure of \(\mathbb{Z}\) in \(\text{End}(\mathbb{Z}_p^\times)\) (this is automatically satisfied for \(p \neq 2\)). Then a \(p\)-adic modular form of weight \(\chi\) and level-N, type \(\zeta\) 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 \(\chi\). This means that there is a sequence of true modular forms \(f_i\), each homogeneous of some weight \(k_i\), defined over \(\mathbb{W}\), 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 \(\tilde{D} = \lim D/p^mD\) 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

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

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

\[
\beta(f)(E/B, \alpha_N, \alpha^{-1}\varphi) = \lim \beta(f_i)(E/B, \alpha_N, \alpha^{-1}\varphi)
= \lim f_i(E/B, \alpha_N, \alpha^{-1}\varphi^*\left(\frac{dT}{1 + T}\right))
= \lim \alpha^{k_i}f_i(E/B, \alpha_N, \varphi^*\left(\frac{dT}{1 + T}\right))
= \chi(\alpha) \lim f_i(E/B, \alpha_N, \varphi^*\left(\frac{dT}{1 + T}\right))
= \chi(\alpha) \lim \beta(f_i)(E/B, \alpha_N, \varphi)
= \chi(\alpha) \cdot f(E/B, \alpha_N, \varphi).
\]
Suppose now that \( g \in V_{\omega, \infty} \). Let \( \{ k_n \} \) be a sequence of integers such that
\[
\chi(\alpha) = \alpha^{k_n} \mod p^n \ \forall \alpha \in \mathbb{Z}_p^*.
\]
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 \( W \) of weight \( k_n \) such that
\[
k_n \equiv k'_n \mod p^{n-1}(p - 1),
\]
and we may choose \( k'_n \geq 2 \). 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 \( W_\infty \)-algebra, and \( (E/B, \alpha_N, \omega) \) an elliptic curve over \( B \) with level-\( N \) structure and nowhere-vanishing invariant differential \( \omega \), such that \( E \otimes B/pB \) has invertible Hasse invariant. We must define an element
\[
f_n(E/B, \alpha_N, \omega) \in B
\]
which is homogeneous of degree \( k_n \) in the choice of \( \omega \), which depends only on the isomorphism class of \( (E/B, \alpha_N, \omega) \), which commutes with extension of scalars of \( W_\infty \)-algebras, and which is holomorphic at infinity.

Over the ring \( B_\infty = B \otimes_{\mathbb{Z}_p, 0} V_{\omega, \infty} \) \( (B \) is a \( V_{\omega, \infty} \)-algebra by the homomorphism \( V_{\omega, \infty} \to B \) which "classifies" \( (E, \alpha_N) \)), there exists an isomorphism \( \varphi: \tilde{E} \sim \tilde{G}_m \). Let us write \( \omega = \lambda \varphi^* (dT/(1 + T)) \), with \( \lambda \in (B_\infty)^* \); we "define"
\[
f_n(E/B, \alpha_N, \omega) = \lambda^{-k_n} g(E/B, \alpha_N, \varphi)
\]
which is a priori an element of \( B_\infty \). It does not depend on the choice of isomorphism \( \varphi \); if \( \varphi_1 \) is another, then \( \varphi_1 = \alpha \varphi \) for some \( \alpha \in \mathbb{Z}_p^* \),
\[
\omega = (\alpha^{-1} \lambda)(\varphi_1)^* \left( \frac{dT}{1 + T} \right),
\]
and we could also "define"
\[
f_n(E/B, \alpha_N, \omega) = (\alpha^{-1} \lambda)^{-k_n} g(E/B, \alpha_N, \varphi_1).
\]
But indeed we readily calculate
\[
(\alpha^{-1} \lambda)^{-k_n} g(E/B, \alpha_N, \varphi_1) = \alpha^{k_n} \lambda^{-k_n} g(E/B, \alpha_N, \alpha \varphi)
\]
\[
= \chi^{-1}(\alpha) \cdot \alpha^{k_n} \lambda^{-k_n} g(E/B, \alpha_N, \varphi)
\]
\[
= \lambda^{-k_n} g(E/B, \alpha_N, \varphi)
\]
because by choice of \( k_n \) we have
\[
\chi(\alpha) = \alpha^{k_n} \mod p^n.
\]
Further, this very independence of \( f_n(E/B, \alpha_N, \omega) \) of the auxiliary choice of
\( \varphi \) implies immediately that the value \( f_n(E/B, \alpha_N, \omega) \) lies in \( B \), because \( B \) is the subring of invariants of \( \alpha \in \mathbb{Z}_p^\times \) acting as \( \text{id} \otimes [\alpha] \) on \( B \otimes_{\mathbb{Z}_p} V_{n,0} = B_{\infty \omega} \).

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 \( \omega_{\text{can}} \) used for \( q \)-expansions is itself \( \varphi^*(dT/(1+T)) \), i.e., \( \lambda = 1 \).

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

\[
\chi: \mathbb{Z}_p^\times \longrightarrow \mathfrak{O}^\times
\]

be any continuous character. Then we may define a \( p \)-adic modular form of weight \( \chi \) to be an element of \( (V_{\alpha,\omega} \otimes_{W} \mathfrak{O})^\chi \), where

\[
V_{\alpha,\omega} \otimes_{W} \mathfrak{O} = \lim_{\leftarrow} V_{m,\infty} \otimes_{W} \mathfrak{O} \subset \lim_{\leftarrow} \lim_{\leftarrow} V_{m,n} \otimes_{W} \mathfrak{O}
\]

is the ring of all rules... as in (A1.1) but where we now restrict \( B \) to vary only over \( \mathfrak{O} \)-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 \( \chi \in \text{Hom}(\mathbb{Z}_p^\times, \mathfrak{O}^\times) \) is thus a rule which assigns to each situation

\[
\begin{align*}
(E, \alpha_N, \varphi) & \quad \xrightarrow{\text{Spec } (B)} \\
\end{align*}
\]

where

\[
\begin{align*}
\text{B is an } \mathfrak{O} \text{-algebra in which } p \text{ is nilpotent} \\
\text{(E, } \alpha_N) \text{ is an elliptic curve with level-N structure over } B \\
\varphi \text{ is an isomorphism } \varphi: \hat{E} \sim \hat{G}_m
\end{align*}
\]

an element

\[
\begin{align*}
f(E/B, \alpha_N, \varphi) & \in B
\end{align*}
\]

such that

\[
\begin{align*}
\text{for any } \alpha \in \mathbb{Z}_p^\times, f(E/B, \alpha_N, \alpha^{-1}\varphi) = \chi(\alpha)f(E/B, \alpha_N, \varphi); \\
f(E/B, \alpha_N, \varphi) \text{ depends only on the isomorphism class of } (E/B, \alpha_N, \varphi) \text{, and its formation commutes with arbitrary extension of } \mathfrak{O} \text{-algebras } B \rightarrow B'.
\end{align*}
\]

\[
\begin{align*}
f(\text{Tate } (q^N), \alpha_N, \varphi) & \in \mathfrak{O}[[q]] \text{ for every level-N structure } \alpha_N \text{ and every } \varphi \text{ on the Tate curve. (More precisely, the condition is that whenever we consider } \\
\text{Tate } (q^N) \text{ over } \mathfrak{O}/p^n\mathfrak{O}((q)), \text{ any } n, \text{ with any choice of } \alpha_N \text{ and } \varphi, \text{ the value of } f \text{ lies in } \mathfrak{O}/p^n\mathfrak{O}[[q]].)
\end{align*}
\]
By “pure thought”, it may be checked that this definition of a \( p \)-adic modular form of weight \( \chi \) is equivalent to that of a compatible system of sections of the invertible sheaf \( \omega^{\otimes \chi} \) on the various schemes \( S_m \otimes_w \mathcal{O} \), where we denote by \( \omega^{\otimes \chi} \) the invertible coherent sheaf on \( S_m \otimes \mathcal{O} \) associated to the \( p \)-adic etale sheaf \( T^\chi \) over \( S_m \otimes \mathcal{O} \) deduced from the \( p \)-adic etale sheaf \( T_p \) by “extension of the structural group” from \( \mathbb{Z}^\chi \) to \( \mathcal{O}^\chi \) via the character \( \chi : \mathbb{Z}^\chi \to \mathcal{O}^\chi \). This description shows that there is a plethora of \( p \)-adic modular forms of weight \( \chi \), for

\[
(V_{m,\infty} \otimes \mathcal{O})^\chi = \lim_m (V_{m,\infty} \otimes \mathcal{O})^\chi = \lim_m H^\chi(S_m \otimes \mathcal{O}, \omega^{\otimes \chi}).
\]

Because the \( S_m \) are all affine we know that each individual \( H^\chi(S_m \otimes \mathcal{O}, \omega^{\otimes \chi}) \) is an invertible module of rank one over the coordinate ring \( V_{m,\infty} \otimes \mathcal{O} \) of \( S_m \otimes \mathcal{O} \), and that the transition maps \( H^\chi(S_{m+1} \otimes \mathcal{O}, \omega^{\otimes \chi}) \to H^\chi(S_m \otimes \mathcal{O}, \omega^{\otimes \chi}) \) are all surjective. Thus there are “just as many” \( p \)-adic modular forms of weight \( \chi \) 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 \( \mathbb{Z}^\chi \) module according to the \( p \)-adic characters of \( \mathbb{Z}^\chi \), because every time we make an extension of scalars to an \( \mathcal{O} \) as above, new characters of \( \mathbb{Z}^\chi \) occur in \( V_{\infty,\infty} \otimes \mathcal{O} \). (Indeed for \( p \neq 2 \), we have canonical isomorphisms

\[
\text{Hom}(\mathbb{Z}^\chi, \mathcal{O}^\chi) = \text{Hom}(\mathbb{Z}/(p-1)\mathbb{Z}, \mu_{p-1}(\mathcal{O})) \times \text{Hom}(1+p\mathbb{Z}_p, \mathcal{O}^\chi)
\]

and via “evaluation at \( 1+p \)” we have an isomorphism

\[
\text{Hom}(1+p\mathbb{Z}_p, \mathcal{O}^\chi) \xrightarrow{\sim} 1 + \text{Max}(\mathcal{O})
\]

where \( \text{Max}(\mathcal{O}) \) 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 \( \xi \)) 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

\[
E \quad (A2.1)
\]

\[
\text{Spec}(\mathcal{O}) \quad \text{Spec}(\mathcal{O}) \to M.
\]

be the inverse image of the universal curve over \( \text{Spec}(\mathcal{O}) \to M \). Then the
formal group $\hat{E}$ over $\mathcal{O}$ is non-canonically isomorphic to $\hat{\mathbb{G}}_m$, the formal multiplicative group, and the set of isomorphisms between them is principal homogeneous under $\text{Aut}_c(\hat{\mathbb{G}}_m) = \mathbb{Z}_p$. Each isomorphism $\varphi: \hat{E} \rightarrow \hat{\mathbb{G}}_m$ determines an invariant differential $\omega_{\varphi} \in \mathcal{O}^{\times} \varphi^*(dT/(1 + T))$ 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 $\omega_{\varphi}$ on $E$ itself.

Each such choice of $\varphi$ allows us to define a sort of "$q$-expansion homomorphism"

$$(A2.2) \quad \beta_\varphi: R_\infty \rightarrow \mathcal{O}, \quad \sum f_i \mapsto \sum f_i(E, \omega_{\varphi}) = \sum f_i(\omega_{\varphi})^e,$$

and, by reduction modulo $p^n$, homomorphisms

$$(A2.3) \quad \beta_\varphi(n): R_\infty \rightarrow \mathcal{O}/p^n \mathcal{O}, \quad \beta_\varphi(n) = \beta_\varphi \mod p^n.$$

**PROPOSITION (A2.4).** For any choice of isomorphism $\varphi: \hat{E} \rightarrow \hat{\mathbb{G}}_m$, and for any $n \geq 1$, we have

$$I_n = \text{kernel of } \beta_\varphi(n): R_\infty \rightarrow \mathcal{O}/p^n \mathcal{O}.$$

**Proof.** The isomorphism $\varphi: \hat{E} \rightarrow \hat{\mathbb{G}}_m$ induces an isomorphism $p^n\hat{E} \rightarrow \mu_{p^n}$, and by reduction modulo $p^n$ gives an isomorphism $p^n\hat{E} \otimes \mathcal{O}/p^n \mathcal{O} \rightarrow \mu_{p^n}$ over $\mathcal{O}/p^n \mathcal{O}$. But the scheme $T_{n, n}$ over $M_n$ is the etale covering of $S_n \subset M_n$ defined by “adjoining” all isomorphisms of $p^n\hat{E} | S^n$ with $\mu_{p^n}$, and the differentials $\omega_{\text{can}}$ are the (unique invariant differentials on $\hat{E}_{T_{n, n}}$, 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 $\mu_{p^n}$. If we recall that $\mathcal{O}/p^n \mathcal{O}$ is “simply connected”, it follows that in the diagram

$$(A2.5) \quad \text{Spec } (\mathcal{O}/p^n \mathcal{O}) \longleftarrow S_n$$

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

$$\beta(n): R_\infty \rightarrow V_{n, n}$$

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 \( \pi \) be a uniformizing parameter, and for each integer \( m \geq 1 \), let \( W_m = W/\pi^m W \). Let \( S_\bullet \) be a sequence of flat affine \( W_\bullet \)-schemes, given with isomorphisms \( S_{m+1} \otimes_{W_{m+1}} W_m \rightarrow S_m \). 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 \( P_n = P/p^n \mathcal{P} \) of etale sheaves which are twisted forms of the \( \text{constant} \) etale sheaves \( \mathbb{Z}/p^n \mathbb{Z} \). Let \( \omega_n \) be the invertible (coherent) sheaf \( P \otimes_{\mathbb{Z}/p^n} \mathcal{O}_{S_m} \) 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

\[
R'_m = \bigoplus_{k \geq 0} H^0(S_m, \omega^{\otimes k}),
R_m = \bigoplus_{k \geq 0} \lim_{\leftarrow} H^0(S_m, \omega^{\otimes k}).
\]

Notice that because each \( S_m \) is affine, and \( S_m = S_{m+1} \mod \pi^m \), we have

\[
R'_m/\pi^m R'_{m+1} \rightarrow R_m.
\]

Let us define

\[
T_{m,n} = \text{Isom}_{S_m} (\mathbb{Z}/p^n \mathbb{Z}, P_n) \quad (= \text{Spec} (V_{m,n}))
\]

a finite etale \( S_m \)-scheme which represents the functor on \( \text{Sch}/S_m \),

\[
X \quad \xrightarrow{\pi} \quad \text{isomorphisms } \psi_n : (\mathbb{Z}/p^n \mathbb{Z})_X \rightarrow \pi^{*}(P_n).
\]

The group \((\mathbb{Z}/p^n \mathbb{Z})^*\) 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 \( (T_{m,n+1} \rightarrow T_{m,n}) \) whose inverse limit \( T_{m,\infty} = \text{Spec} (V_{m,\infty} = \lim_{\rightarrow} V_{m,n}) \) represents the functor
The group $\mathbb{Z}_p^*$ acts freely on $T_{m,\infty} ([\alpha]_p = \alpha^{-1}\psi)$, with quotient $S_m$.

The homomorphism $\beta(m)$

$$\beta(m): R_m' \longrightarrow V_{m,m} = \Gamma(T_{m,m}, \emptyset) \leftarrow V_{m,\infty}$$

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

$$\beta(m)(\sum f_i) = \sum f_i/((\omega_{\text{can}}(m))^\otimes t).$$

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

$$f(X, \psi_m: \mathbb{Z}/p^m\mathbb{Z} \rightarrow P_m)$$

with values in $\Gamma(X, \mathcal{O}_X)$, for variable $X$ and variable $\psi_m$ whose formation is compatible with arbitrary change of base $X' \rightarrow X$. Then $\beta(m)$ identifies $H^q(S_m, \omega_{\otimes k})$ with those functions which transform under $(\mathbb{Z}/p^m\mathbb{Z})^\times$ (the indeterminacy in the choice of $\psi_m$) by $\alpha \mapsto \alpha^k$. This shows that $H^q(S_m, \omega_{\otimes k})$ and $H^q(S_m, \omega_{\otimes k+(p-1)p^{m-1}})$ 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

$$\beta(\infty): R_m' \longrightarrow \mathcal{V}_{\text{f.d.}} \leftarrow \lim_{m} V_{m,\infty}.$$

Exactly as in Appendix I, we can view $V$ as the ring of all “functions”

$$f(X, \psi: \mathbb{Z}_p \sim \pi^*(P))$$

with values in $\Gamma(X, \mathcal{O}_X)$ for variable $X$ and variable $m$ whose formation is compatible with all changes of base $X' \rightarrow X$. This ring $V$ is $p$-adically complete, flat over $W$ (because $V/\pi^m V = V_{m,\infty} = \lim_{m} V_{m,n}$ is etale over $S_m$, hence flat over $W_m$), and $\mathbb{Z}_p^*$ 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 \( \lim_m H^0(S_m, \omega^\otimes k) \) of \( R_m' \) with the subspaces \( V^{(k)} \subset V \) consisting of the functions \( f \in V \) which satisfy \( [\alpha]f = \alpha^tf \) for all \( \alpha \in \mathbb{Z}_p^\times \). Because \( V \) is flat over \( W \), the usual "independence of characters" argument shows that the map \( \beta(\infty) \) is injective:

\[
R_m' \subset V.
\]

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

\[
\begin{array}{c}
R_m' \hookrightarrow V \\
\downarrow \downarrow \\
R_m' \left[ \frac{1}{p} \right] \hookrightarrow V \left[ \frac{1}{p} \right].
\end{array}
\]

We define \( D' \) to be the intersection

\[
D' = V \cap R_m' \left[ \frac{1}{p} \right].
\]

**Theorem.** The inclusion \( D' \xrightarrow{\beta(\infty)} V \) 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 \( 0 \rightarrow D' \rightarrow V \rightarrow V/D' \rightarrow 0 \) remains exact when reduced modulo \( \pi^m ; D'/\pi^m D' \hookrightarrow V/\pi^m V \). It remains to check that the map is onto, and for this it suffices to show that \( D'/\pi D' \rightarrow V/\pi V = V_{1,\infty} \). So take \( f \in V_{1,\infty} \), say \( f \in V_{1,n} \). To make clear the idea of the proof, suppose first that \( P_m = P/p^mP \) is trivial, where \( m \) is so large that

\[
\pi^{m-i}f \in W \text{ if } 0 < i < p^m.
\]

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

\[
\pi^{m-i}F_m \in \beta(m)R_m'.
\]

As we supposed that \( P_m \) is trivial, we have

\[
T_m = \text{Aut}_{S_m}(\mathbb{Z}/p^m\mathbb{Z}) = S_m \times (\mathbb{Z}/p^m\mathbb{Z})^\times
\]
so that \( V_{m,0} = H^0(S_m, \emptyset) \)-valued functions on the group
(Z/p^nZ)^\times. The sheaf \( \omega \) on \( S_m \) becomes the structure sheaf \( \mathcal{O}_{S_m} \), because

\[
\omega = P \otimes \mathbb{Z}_p \mathcal{O}_{S_m} = P_m \otimes \mathbb{Z}/p^n\mathbb{Z} \mathcal{O}_{S_m} \simeq \mathcal{O}_{S_m},
\]

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

\[
\beta(m) : R'_m \longrightarrow V_{m,m}
\]

becomes the map

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

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

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

\[
\sum_{i=0}^{p^{n-1}} a_i \binom{X}{i}, \quad a_i \in \pi^{m-1}H^0(S_m, \mathcal{O}_{S_m}).
\]

But \( m \) was so chosen that

\[
\pi^{m-1}\binom{X}{i} \in W[X], \quad \text{for } 0 \leq i \leq p^n - 1
\]

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 \( W \)-scheme \( S_m \), a "twisted" form \( P_m \) of \( \mathbb{Z}/p^n\mathbb{Z} \) on \( S_m \), and an integer \( n \ll m \) such that \( \pi^{m-1} \in (p^n - 1)! \). \( W \).

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

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

is the \emph{zero} map. For this, it suffices that the map
be zero, or, what is the same, that our problem have an affirmative solution over $A$, which we know is the case if $P_n$ 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 étale sheaf $P$ on the $S_m$, and we give ourselves further an invertible sheaf $\omega$ on $M$ which induces $P \otimes_{Z_p} \mathcal{O}_{S_m}$ on $S_m$.

Notice that $\omega^{zp-1}$ is trivial on $S_1$, because

$$P \otimes_{Z_p} \mathcal{O}_{S_1} = (P \otimes \mathbb{Z}/p\mathbb{Z})^{zp-1} \otimes \mathbb{Z}/p\mathbb{Z}$$

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

**THEOREM.** Suppose that $A \in H^0(S_1, \omega)$ extends to a (necessarily unique) section $A \in H^0(M_1, \omega)$ which vanishes at each point of $H$. Then if we define $R_\infty = \bigoplus_{k \geq 0} H^0(M, \omega^{\otimes k})$, 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 $\pi$:

$$D/\pi^n D \simeq D'/\pi^n D' \simeq V/\pi^n V.$$  

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

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

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

For this, we argue as follows. The sheaf $\omega$ 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 $\omega^{\otimes \nu(p-1)}$ has degree $\geq 2g - 2$, $g =$ genus of $M_1$. Then the section $A^\nu \in H^0(M_1, \omega^{\otimes \nu(p-1)})$ lifts to a section $E \in H^0(M, \omega^{\otimes \nu(p-1)})$. Notice that
The image of $E^n$ 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 $V_{1,i}$, viewed as a "function" of situations (an $S_i$-scheme $X$, an isomorphism $\psi_i : \mathbb{Z}/p\mathbb{Z} \rightarrow P_i$ on $X$) with values in $\Gamma(X, \mathcal{O}_X)$ which is homogeneous of degree $p-1$ in the choice of $\psi_i$ (indeterminacy: $(\mathbb{Z}/p\mathbb{Z})^s$) is tautologically the constant function "1":

$$A \left( \begin{array}{c} X \\ S_i \end{array} \right), \psi_i : \mathbb{Z}/p\mathbb{Z} \rightarrow P_i \text{ on } X = 1 \in \Gamma(X, \mathcal{O}_X).$$

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

$$H^0(S_m, \omega^{\otimes k}) = \lim_{n \to \infty} \frac{H^0(M_n, \omega^{\otimes k+m_{n+1} \nu(p-1)})}{E^n}.$$ 

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

$$f_i = \frac{g_{i+N\nu P^m(p-1)}}{E^{N\nu P^m}} \mod \pi^{m+1} R_{\infty}$$

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

$$f_i = g_{i+N\nu P^m(p-1)} \in \pi^{m+1} V.$$ 

Q.E.D.

Institut des Hautes Études Scientifiques, France
Princeton University

References


HIGHER CONGRUENCES


(Received October 4, 1973)