Lecture Notes in Mathematics

350

Pierre Deligne
Willem Kuyk (Eds.)

Modular Functions of One Variable III

Antwerp, Belgium 1972

Springer

Lecture Notes in Mathematics

Edited by A. Dold and B. Eckmann

350

Modular Functions of One Variable III

Proceedings International Summer School
University of Antwerp, RUCA
July 17–August 3, 1972

Edited by W. Kuijk and J-P. Serre

Springer-Verlag
Berlin Heidelberg New York Tokyo

Editors

Willem Kuijk
Rijksuniversitair Centrum Antwerpen, Leerstoel Algebra
Groenenborgerlaan 171, 2020 Antwerpen, Belgium

Jean-Pierre Serre
Collège de France, 11, pl. Marcelin Berthelot
75231 Paris Cedex 05, France

1st Edition 1973
2nd Corrected Printing 1986

Mathematics Subject Classification (1970): 10D05, 10D25, 10C15, 14K22, 14K25

ISBN 3-540-06483-4 Springer-Verlag Berlin Heidelberg New York Tokyo
ISBN 0-387-06483-4 Springer-Verlag New York Heidelberg Berlin Tokyo

Printing and binding: Beltz Offsetdruck, Hemsbach/Bergstr.
2146/3140-543210

Preface

This is Volume 3 of the Proceedings of the International Summer School on

"Modular functions of one variable and arithmetical applications"

which took place at RUCA, Antwerp University, from July 17 to August 3, 1972.

It contains papers by P.Cartier-Y.Roy, B.Dwork, N.Katz, J-P.Serre and H.P.F.Swinnerton-Dyer on congruence properties of modular forms, ℓ-adic representations, p-adic modular forms and p-adic zeta functions.

W.Kuyk J-P.Serre

CONTENTS

Herrn C.L. Siegel gewidmet

ON ℓ-ADIC REPRESENTATIONS AND CONGRUENCES FOR COEFFICIENTS OF MODULAR FORMS

BY H.P.F. SWINNERTON-DYER

International Summer School on Modular Functions
Antwerp 1972

CONTENTS

ON ℓ-ADIC REPRESENTATIONS AND CONGRUENCES FOR COEFFICIENTS OF MODULAR FORMS *

1. Introduction.

The work I shall describe in these lectures has two themes, a classical one going back to Ramanujan [8] and a modern one initiated by Serre [9] and Deligne [3]. To describe the classical theme, let the unique cusp form of weight 12 for the full modular group be written

$$\Delta = q\prod_1^{\infty}(1-q^n)^{24} = \sum_1^{\infty}\tau(n)q^n \qquad (1)$$

and note that the associated Dirichlet series has an Euler product

$$\sum\tau(n)n^{-s} = \Pi(1-\tau(p)p^{-s} + p^{11-2s})^{-1}$$

so that all the $\tau(n)$ are known as soon as the $\tau(p)$ are.
Write also $\sigma_\nu(n)$ for the sum of the νth powers of the positive divisors of n; thus in particular $\sigma_\nu(p) = 1 + p^\nu$. Ramanujan was the first to observe that, modulo certain powers of certain small primes, there are congruences which connect $\tau(n)$ with some of the $\sigma_\nu(n)$. A good deal of work has gone into proving such congruences; the strongest results known to me which have been obtained by classical methods are as follows :

---

* Many of the results described in these lectures were first obtained in correspondence between Serre and me during the last five years; the disentanglement of our respective contributions is left to the reader, as an exercise in stylistic analysis. The dedication is from both of us.

$$\left.\begin{aligned}
\tau(n) &\equiv \sigma_{11}(n) \bmod 2^{11} \text{ if } n \equiv 1 \bmod 8,\\
\tau(n) &\equiv 1217\ \sigma_{11}(n) \bmod 2^{13} \text{ if } n \equiv 3 \bmod 8,\\
\tau(n) &\equiv 1537\ \sigma_{11}(n) \bmod 2^{12} \text{ if } n \equiv 5 \bmod 8,\\
\tau(n) &\equiv 705\ \sigma_{11}(n) \bmod 2^{14} \text{ if } n \equiv 7 \bmod 8,
\end{aligned}\right\} \tag{2}$$

$$\tau(n) \equiv n^{-610}\ \sigma_{1231}(n) \qquad \begin{Bmatrix} \bmod 3^6 \text{ if } n \equiv 1 \bmod 3, \\ \bmod 3^7 \text{ if } n \equiv 2 \bmod 3; \end{Bmatrix} \tag{3}$$

$$\tau(n) \equiv n^{-30}\ \sigma_{71}(n) \bmod 5^3 \text{ if } n \text{ is prime to } 5; \tag{4}$$

$$\tau(n) \equiv n\sigma_9(n) \qquad \begin{Bmatrix} \bmod 7 \text{ if } n \equiv 0,1,2 \text{ or } 4 \bmod 7, \\ \bmod 7^2 \text{ if } n \equiv 3,5 \text{ or } 6 \bmod 7; \end{Bmatrix} \tag{5}$$

$$\left.\begin{aligned}
&\tau(p) \equiv 0 \bmod 23 \text{ if } p \text{ is a quadratic non-residue}\\
&\qquad \text{of } 23,\\
&\tau(p) \equiv 2 \bmod 23 \text{ if } p = u^2 + 23v^2 \text{ for integers}\\
&\qquad u \neq 0,\ v,\\
&\qquad \tau(p) \equiv -1 \bmod 23 \text{ for other } p \neq 23;
\end{aligned}\right\} \tag{6}$$

$$\tau(n) \equiv \sigma_{11}(n) \bmod 691. \tag{7}$$

Of these, (2) is due to Kolberg [6], (3) to Ashworth [1], (4) to Lahivi (see [7]), (5) to Lehmer [7], (6) to Wilton [13] and (7) to Ramanujan [8]; the present formulations of (3) and (4) are not those of the original authors but those that appear least unnatural in the light of the multiplicativity of $\tau(n)$ and Theorem 1 below. The proofs, whether laborious as with (2) to (4) or elegant as with (6) and (7), do little to explain why such congruences occur, though they shed some light on the reasons why these particular primes occur; for example 23 = (2k - 1) where k = 12 is the weight of Δ, and 691 divides the numerator of the Bernoulli number b_{12}.

The existence of such congruences raises two obvious questions. First, are there congruences for $\tau(n)$ modulo primes other than 2,3,5,7,23 and 691; and second, are the congruences (2) to (7) best possible or could one with greater labour prove congruences modulo even higher powers of the primes cited ? These questions are the subject matter of these lectures. It will be shown that there are no congruences for $\tau(n)$ modulo any other primes. Again, it will be shown that in a well-defined sense the last three congruences (2) are best possible; but it will also be shown how they can be improved by making use of additional information about n. Similar arguments can probably be applied to the other congruences (3) to (7), some of which are certainly not best possible.

To attack these questions we need some limitation on the types of congruence that can occur; and this is provided by our second theme. In 1968 Serre [9] put forward a conjecture relating ℓ-adic representations and coefficients of modular forms; and he showed that the existence of congruences such as (2) to (7) fitted well with the conjecture. Serre's conjecture was proved by Deligne; see [3] and also the lecture of Langlands at this conference. We state here only a special case, which will be sufficient for our purpose; there is no reason to suppose that a similar study of more general modular forms will yield any essentially new phenomena.

The following notation will be used throughout these lectures. Let ℓ be a prime number; denote by K_ℓ the maximal algebraic extension of $\mathbf{Q}$ ramified only at ℓ, and by K_ℓ^{ab} the maximal subfield of K_ℓ abelian over $\mathbf{Q}$. For any prime $p \neq \ell$ denote by Frob(p) the conjugacy class of Frobenius elements of p in $\mathrm{Gal}(K_\ell/\mathbf{Q})$; by abuse of language we shall sometimes speak of Frob(p) as if it were simply an element of the Galois group. By class-field theory there is a canonical isomorphism $\mathrm{Gal}(K_\ell^{ab}/\mathbb{Q}) \sim \mathbb{Z}_\ell^*$, the group of ℓ-adic units; and this induces a canonical character

$$\chi_\ell : \mathrm{Gal}(K_\ell/\mathbb{Q}) \to \mathrm{Gal}(K_\ell^{ab}/\mathbb{Q}) \tilde{\to} \mathbb{Z}_\ell^*$$

with the property that

$$\chi_\ell(\mathrm{Frob}(p)) = p \text{ for all } p \neq \ell.$$

THEOREM 1. (Serre-Deligne). _Let_ $f = \sum a_n q^n$ _be a cusp form of weight_ k _for the full modular group, and suppose that_ $a_1 = 1$, _that every_ a_n _is in_ $\mathbb{Z}$, _and that the associated Dirichlet series has an Euler product_

$$\sum a_n n^{-s} = \Pi(1-a_p p^{-s}+p^{k-1-2s})^{-1}. \tag{8}$$

Then there is a continuous homomorphism

$$\rho_\ell : \mathrm{Gal}(K_\ell/\mathbb{Q}) \to GL_2(\mathbb{Z}_\ell),$$

depending on f, _such that_ $\rho_\ell(\mathrm{Frob}(p))$ _has characteristic polynomial_

$$X^2 - a_p X + p^{k-1}$$

for each $p \neq \ell$.

The conditions on f are certainly satisfied by the unique cusp forms of weights 12,16,18,20,22 and 26, though very possibly by no other form; of these, Δ is the most glamorous though in the end the form of weight 16 will prove even more interesting. Note that the Theorem in particular implies

$$\det \circ \rho_\ell = \chi_\ell^{k-1}. \tag{9}$$

Now if the image of ρ_ℓ is small enough, a knowledge of the determinant of an element of the image will imply some ℓ-adic information about the trace of that element; and so in particular a knowledge of p (or even an approximate ℓ-adic knowledge of p) will imply some ℓ-adic information about a_p. This is just the meaning of the congruences (2) to (7), with certain reservations in the case of (6) and with their arguments restricted to primes. Conversely the existence of such congruences implies a restriction on the image of ρ_ℓ, since the set of Frobenius elements is dense in the full Galois group and therefore any congruence relation between a_p and p^{k-1} is also a valid congruence relation between the trace and determinant of every element of the image of ρ_ℓ.

In what follows we shall use a tilde consistently to denote reduction mod ℓ; thus for example $\tilde{\rho}_\ell$ is the induced map

$$\mathrm{Gal}(K_\ell/\mathbf{Q}) \to GL_2(\mathbf{Z}_\ell) \to GL_2(\mathbf{F}_\ell).$$

By (9) the image of $\det \circ \rho_\ell$ is just the (k-1)th powers in $\mathbf{Z}_\ell^*$; so to find the image of ρ_ℓ a major step will be to find its intersection with $SL_2(\mathbf{Z}_\ell)$. In particular, if this intersection is the whole of $SL_2(\mathbf{Z}_\ell)$ then the image of ρ_ℓ will be the entire inverse image of $(\mathbf{Z}_\ell^*)^{k-1}$ in $GL_2(\mathbf{Z}_\ell)$. In view of the following lemma, it is enough to look at the image of $\tilde{\rho}_\ell$.

LEMMA 1. Suppose that $\ell > 3$ and that G is a subgroup of $GL_2(\mathbf{Z}_\ell)$ which is closed in the ℓ-adic topology. If the image of G under reduction mod ℓ contains $SL_2(\mathbf{F}_\ell)$ then G contains $SL_2(\mathbf{Z}_\ell)$.

PROOF. For each n > 0, denote by G_n the image of G in $GL_2(\mathbf{Z}/\ell^n\mathbf{Z})$. Since G is closed, to prove the lemma it is enough to prove that $G_n \supset SL_2(\mathbf{Z}/\ell^n\mathbf{Z})$ for each n > 0. This holds by hypothesis for n = 1, and it will follow by induction on n once we have proved for each n > 1 that G_n contains the kernel of

$$SL_2(\mathbf{Z}/\ell^n\mathbf{Z}) \to SL_2(\mathbf{Z}/\ell^{n-1}\mathbf{Z}).$$

Call this kernel H_n. We start with the case $n = 2$; now H_2 is generated by the three matrices $I + \ell u$, where $u = \begin{pmatrix}0 & 1\\ 0 & 0\end{pmatrix}, \begin{pmatrix}0 & 0\\ 1 & 0\end{pmatrix}$ or $\begin{pmatrix}1 & -1\\ 1 & -1\end{pmatrix}$, so it is enough to prove that G_2 contains the images of these three matrices. In each case $u^2 = 0$ and $I + u$ is in $SL_2(\mathbf{Z})$, whence there is an element σ in G such that $\sigma \equiv I + u \bmod \ell$, that is

$$\sigma = I + u + \ell v$$

for some matrix v with elements in $\mathbf{Z}_\ell$. Now

$$\sigma^\ell = I + \ell(u + \ell v) + \ldots + (u + \ell v)^\ell \equiv I + \ell u \mod \ell^2$$

since all the other terms which occur when the powers of $(u + \ell v)$ are written out in full either contain a factor ℓ^2 or a factor u^2 which vanishes. (For $\ell = 3$ the argument breaks down at this point, because of the presence of a term $3\,u\,v\,u$.) This proves that $G_2 \supset H_2$. To prove that $G_n \supset H_n$ for $n > 2$ we use induction on n, so we assume that $G_{n-1} \supset H_{n-1}$. Let $I + \ell^{n-1}v$, where v has elements in $\mathbb{Z}_\ell$, be a representative of an assigned element of H_n. The image of $I + \ell^{n-2}v \bmod \ell^{n-1}$ is in H_{n-1} and therefore in G_{n-1}; so there is an element σ of G such that

$$\sigma \equiv I + \ell^{n-2}v \mod \ell^{n-1}.$$

By an argument similar to the one above, it follows that

$$\sigma^\ell \equiv I + \ell^{n-1}v \mod \ell^n,$$

which proves that $G_n \supset H_n$. This completes the proof of the lemma.

There are analogous results for $\ell = 2$ and $\ell = 3$, in which $\mathbf{F}_\ell$ is replaced by $\mathbb{Z}/(8)$ or $\mathbb{Z}/(9)$ respectively; and the examples given by Serre ([10], p. IV - 28) show that the condition $\ell > 3$ in the lemma cannot be dropped without some modification. The proofs of these analogous results are essentially contained in the proof of the lemma.

Indeed for $\ell = 3$ we now have $G_2 \supset H_2$ by hypothesis, and the inductive proof that $G_n \supset H_n$ for each $n > 2$ works as before; for $\ell = 2$ we have $G_2 \supset H_2$ and $G_3 \supset H_3$ by hypothesis, and the induction works provided $n > 3$.

In the application of lemma 1 G will be the image of ρ_ℓ and will certainly be closed since Galois groups are compact. It will be convenient to say that ℓ is an exceptional prime for the cusp form f if the image of ρ_ℓ does not contain $SL_2(\mathbb{Z}_\ell)$; with this definition lemma 1 can be rewritten as follows.

COROLLARY. Suppose that $\ell > 3$; then ℓ is exceptional for f if and only if the image of $\tilde{\rho}_\ell$ does not contain $SL_2(\mathbb{F}_\ell)$. For $\ell = 2$ or 3 this is still a sufficient condition for ℓ to be exceptional for f.

We need not be more precise for $\ell = 2$ or 3, since for each of the six cusp forms which we shall particularly consider, the sufficient condition is then satisfied. Indeed Serre has conjectured that for $\ell < 11$ there is no continuous homomorphism $\mathrm{Gal}(K_\ell/\mathbb{Q}) \to GL_2(\mathbb{F}_\ell)$ whose determinant is an odd power of χ_ℓ and whose image contains $SL_2(\mathbb{F}_\ell)$. He further conjectures that for any ℓ such a homomorphism is always connected in an obvious sense with a modular form mod ℓ which is an eigenfunction of all T_p with $p \neq \ell$.

It is now advantageous to replace our original search for congruences for a_p by the apparently more general search for primes exceptional for f. In this search the first step will be to classify those subgroups of $GL_2(\mathbb{F}_\ell)$ which do not contain $SL_2(\mathbb{F}_\ell)$. It turns out that each such subgroup is small enough for there to be a non-trivial algebraic relation which is satisfied by the trace and determinant of any of its elements. Hence we obtain a finite list of possible types of congruence relation mod ℓ between p and a_p; and for each exceptional prime ℓ one of these congruence relations must hold. To test the validity of the possible relations, we develop a structure theorem for the ring of modular forms mod ℓ; this gives us (with one exception) a decision process for the possible relations and thence (up to finitely many undecided cases) a list of the exceptional primes for any f. All this occupies §§2-4.

For congruences modulo higher powers of ℓ the position is less satisfactory, primarily because at present we lack a structure theorem for modular forms mod ℓ^ν. We confine ourselves in §5 and the Appendix to two particular topics which illustrate again the benefits that come from combining the congruence and the representation-theory approaches. It is shown in §4 that the congruences (6) are equivalent to the fact that the image of $\tilde{\rho}_{23}$ is isomorphic to S_3, the symmetric group on three elements. In §5 we deduce from this last statement that the second congruence (6) can be improved to $\tau(p) \equiv 1 + p^{11} \bmod 23^2$. Again, the congruences (2) turn out to be sufficient to determine the image of ρ_2, a result whose proof has been put in the appendix because of the heavy algebra involved; and a number of further results flow from this.

Much of the material of these lectures can be found, more succinctly presented, in a recent Bourbaki seminar of Serre [11].

2. The possible images of $\tilde{\rho}_\ell$.

In this section we classify the subgroups of $GL_2(\mathbf{F}_\ell)$ and determine which of them are candidates to be the image of $\tilde{\rho}_\ell$; and to each such candidate which does not contain $SL_2(\mathbf{F}_\ell)$ we determine at least some of the associated congruence relations mod ℓ between p and a_p. All the group theory involved is at least fifty years old, except for the terminology; but I know of no convenient and easily accessible account of it.

We first define certain standard types of subgroup of $GL_2(\mathbf{F}_\ell)$, which for this purpose will be considered as acting on V, a vector space of dimension 2 over $\mathbf{F}_\ell$. A Borel subgroup is any subgroup conjugate to the group of non-singular upper triangular matrices; thus there is a one-one correspondence between the Borel subgroups and the one-dimensional subspaces W of V, the subgroup corresponding to W consisting of those transformations which have W as an eigenspace.

A Cartan subgroup is a maximal semi-simple commutative subgroup; there are two kinds of Cartan subgroups, the split and the non-split. (When $\ell = 2$, the group which fits the construction of a split Cartan subgroup consists only of the identity and is therefore not maximal; it turns out most convenient to say that split Cartan subgroups only happen for $\ell > 2$.) A split Cartan subgroup is any subgroup conjugate to the group of non-singular diagonal matrices; thus there is a one-one correspondence between split Cartan subgroups and unordered pairs of distinct one-dimensional subspaces W_1 and W_2 of V, the subgroup corresponding to W_1 and W_2 consisting of those transformations which have W_1 and W_2 as eigenspaces. A split Cartan subgroup is the direct product of two cyclic groups of order $(\ell - 1)$.

To define a non-split Cartan subgroup requires more notation. Let $V^{(2)}$ be the vector space obtained from V by quadratic extension of the underlying field $\mathbf{F}_\ell$; let W' be any one-dimensional subspace of $V^{(2)}$ which is not induced by a subspace of V, and let W" be the conjugate of W' over $\mathbf{F}_\ell$. The non-split Cartan subgroup corresponding to W' or W" consists of those elements of $GL_2(\mathbf{F}_\ell)$ which have W' and W" as eigenspaces. An element of the subgroup is uniquely determined by its eigenvalue with respect to W'; so a non-split Cartan subgroup is isomorphic to the multiplicative group of the field of ℓ^2 elements, and is therefore cyclic of order $(\ell^2 - 1)$.

An element of the normalizer of a Cartan subgroup (of either kind) must either fix or interchange the two eigenspaces associated with the Cartan subgroup; if it fixes them, it already lies in the Cartan subgroup. It follows that any Cartan subgroup is of index two in its own normalizer.

LEMMA 2. _Let_ G _be a subgroup of_ $GL_2(\mathbb{F}_\ell)$. _If the order of_ G _is divisible by_ ℓ, _then either_ G _is contained in a Borel subgroup of_ $GL_2(\mathbb{F}_\ell)$ _or_ G _contains_ $SL_2(\mathbb{F}_\ell)$. _If the order of_ G _is prime to_ ℓ, _let_ H _be the image of_ G _in_ $PGL_2(\mathbb{F}_\ell)$; _then_

(i) H _is cyclic and_ G _is contained in a Cartan subgroup, or_

(ii) H _is dihedral and_ G _is contained in the normalizer of a Cartan subgroup but not in the Cartan subgroup itself, or_

(iii) H _is isomorphic to_ A_4, S_4 _or_ A_5, _where_ S _denotes the symmetric and and_ A _the alternating group._

In case (ii) ℓ _must be odd; in case_ (iii) ℓ _must be prime to_ 6, 6 _or_ 30 _respectively._

PROOF. Suppose first that the order of G is divisible by ℓ, and choose σ in G of order exactly ℓ; then there is a unique one-dimensional subspace W of V which is an eigenspace of σ. If every element of G has W as an eigenspace, then G is contained in the Borel subgroup associated with W. If not, let σ_1 be an element of G which maps W to some other one-dimensional space W'; then $\sigma_1\sigma\sigma_1^{-1}$ is an element of G of order exactly ℓ with W' as its only eigenspace. Take W and W' as coordinate axes in V; then for some non-zero b,c we have

$$\sigma = \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}, \quad \sigma_1\sigma\sigma_1^{-1} = \begin{pmatrix} 1 & 0 \\ c & 1 \end{pmatrix}.$$

But it is easy to see that these two matrices generate $SL_2(\mathbb{F}_\ell)$, which must therefore be contained in G; this proves the lemma in this case.

Henceforth we can assume that the order of H is prime to ℓ. The analogous result for finite subgroups of $GL_2(\mathbb{C})$ is well known; all we have to do is choose a not too geometric proof of that result and mimic it. As is only proper, we follow Klein [5]. Since the order of H is prime to ℓ, every element of H is semi-simple and every element other than the identity has just two eigenvectors over the algebraic closure of $\mathbb{F}_\ell$. Note first that if two elements of H have one eigenvector in common they have both eigenvectors in common. For if not, suppose that σ_1 and σ_2 have just one eigenvector in common; then by a change of axes we can write them in the form

$$\sigma_1 = \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} \text{ and } \sigma_2 = \begin{pmatrix} \alpha & \beta \\ 0 & \delta \end{pmatrix}$$

where every letter is non-zero. The commutator

$$\sigma_1^{-1}\sigma_2^{-1}\sigma_1\sigma_2 = \begin{pmatrix} 1 & \alpha^{-1}\beta(1-a^{-1}d) \\ 0 & 1 \end{pmatrix}$$

is not the identity because $a \neq d$; so it is an element of H which has order ℓ, contrary to hypothesis.

The set of eigenvectors of non-trivial elements of H is finite and invariant under H; let $\xi_1, \dots, \xi_\nu$ be representatives of the orbits under H and for each ξ_i let $\mu_i > 1$ be the number of elements of H which fix ξ_i. If h is the order of H then the orbit of ξ_i contains h/μ_i elements; so by counting the number of pairs (non-trivial element of H and an eigenvector of it) in two different ways we obtain the identity

$$2h - 2 = h(\mu_1 - 1)/\mu_1 + \dots + h(\mu_\nu - 1)/\mu_\nu$$

which can be rewritten as

$$2(1 - h^{-1}) = (1 - \mu_1^{-1}) + \dots + (1 - \mu_\nu^{-1}).$$

An easy calculation shows that the solutions of this, with each μ_i dividing h, fall into the following five classes:

(i) $\nu = 2$, $\mu_1 = \mu_2 = h$.

(ii) $\nu = 3$, h even, $\mu_1 = \mu_2 = z$, $\mu_3 = \frac{1}{2}h$.

(iii) $\nu = 3$, $h = 12$, $\mu_1 = 2$, $\mu_2 = \mu_3 = 3$.

(iv) $\nu = 3$, $h = 24$, $\mu_1 = 2$, $\mu_2 = 3$, $\mu_3 = 4$.

(v) $\nu = 3$, $h = 60$, $\mu_1 = 2$, $\mu_2 = 3$, $\mu_3 = 5$.

It only remains to identify the corresponding groups.

For (i), all elements of H have the same eigenvectors, so they must form a cyclic group; and all elements of G have the same eigenvectors, so they lie in the associated Cartan subgroup. For (ii), assume for convenience $h > 4$. Then the orbit of ξ_3 consists of two elements, each fixed by half the members of H; so H has a cyclic subgroup H_o of index 2, which must be normal in H. The inverse image of H_o in G must be in a Cartan subgroup of GL_2, and the remaining elements of G interchange the two eigenspaces associated with this Cartan subgroup; so G lies in the normalizer of a Cartan subgroup but not in the Cartan subgroup itself. A similar argument works when $h = 4$.

In the remaining cases we need only identify H with A_4, S_4 or A_5 respectively. For (iii), the orbit of ξ_3 has four elements and these are permuted by H. The induced representation of H is faithful because no non-trivial element of H has more than two eigenvectors; so H is isomorphic to a subgroup of S_4 of order 12, which must be A_4. Similarly in (iv) the orbit of ξ_2 contains eight vectors; but these are the only vectors which are eigenvectors of elements of H of order 3, so they can naturally be regarded as four pairs. If there were a non-trivial element of H which fixed each of these pairs, it would be of order 2 and would therefore have to interchange the elements of each pair. This property would define it uniquely, so it would be in the centre of H and H would have elements of order 6, which it does not. So the homomorphism of H into the permutation group of these four pairs has trivial kernel and thus H is isomorphic to S_4.

In case (v) a direct representation of H as a group of permutations of five elements involves some rather artificial manoeuvres and it is better to proceed as follows. Since every μ_i is prime, every element of H has prime order; and since any two eigenvectors associated with elements of the same order are equivalent under H, any two cyclic subgroups of the same order are conjugate. So any normal subgroup of H contains all or none of the elements of any given order. But H has 15 elements of order 2, 20 elements of order 3, and 24 elements of order 5; so H can have no non-trivial normal subgroup. Since the only simple group of order 60 is A_5, H must be isomorphic to A_5. This completes the proof of the lemma.

COROLLARY 1. Let ρ_ℓ be any continuous homorphism $\mathrm{Gal}(K_\ell/\mathbb{Q}) \to GL_2(\mathbb{Z}_\ell)$ such that $\det \circ \rho_\ell = \chi_\ell^{k-1}$ for some even integer k. Let $G \subset GL_2(\mathbb{F}_\ell)$ be the image of $\tilde{\rho}_\ell$ and let H be the image of G in $PGL_2(\mathbb{F}_\ell)$. Suppose that G does not contain $SL_2(\mathbb{F}_\ell)$. Then

(i) G is contained in a Borel subgroup of $GL_2(\mathbb{F}_\ell)$; or

(ii) G is contained in the normalizer of a Cartan subgroup, but not in the Cartan subgroup itself; or

(iii) H is isomorphic to S_4.

PROOF. Any subgroup of a split Cartan subgroup is contained in a Borel subgroup - for example the one corresponding to one of the two eigenspaces of the Cartan subgroup. So we have only to show that the cases of G contained in a non-split Cartan subgroup, or of H isomorphic to A_4 or A_5, can be neglected. For the first of these, let C be a non-split Cartan subgroup, so that C is cyclic of order $(\ell^2 - 1)$; then the homomorphism

$$\tilde{\rho}_\ell : \mathrm{Gal}(K_\ell/\mathbb{Q}) \to C$$

must factor through $\mathrm{Gal}(K_\ell^{ab}/\mathbb{Q}) \sim \mathbb{Z}_\ell^*$ because C is commutative. Since the image of $\mathbb{Z}_\ell^*$ has order prime to ℓ, its order must divide $(\ell - 1)$; so the image lies in the set of matrices aI with $a \neq 0$, and thus is in a Borel subgroup. An alternative argument is to consider an element σ of

$\mathrm{Gal}(K_\ell/\mathbb{Q})$ which corresponds to complex conjugation under some complex embedding of K_ℓ. Now $\sigma^2 = 1$ and $\chi_\ell(\sigma) = -1$; so $\tilde{\rho}_\ell(\sigma)$ has eigenvalues 1 and -1, and therefore cannot be in a non-split Cartan subgroup. However this argument breaks down when $\ell = 2$.

In proving that H cannot be A_4 or A_5, we can assume that $\ell > 2$. Consider the commutative diagram :

$$\begin{tikzcd} \mathrm{Gal}(K_\ell/\mathbb{Q}) \arrow[r] & G \arrow[r, "\det"] \arrow[d] & \mathbb{F}_\ell^* \arrow[d] \\ & H \arrow[r] & \mathbb{F}_\ell^*/\mathbb{F}_\ell^{*2} \sim \{\pm 1\} \end{tikzcd}$$

By hypothesis the image of G in $\mathbb{F}_\ell^*$ consists of all $(k-1)$th powers and k is even; so the lower line is onto, which means that H must have a subgroup of index 2. Neither A_4 nor A_5 has such a subgroup.

COROLLARY 2. *Let* $f = \sum a_n q^n$ *be a cusp form of weight* k *for the full modular group, such that* $a_1 = 1$, *every* a_n *is in* $\mathbb{Z}$, *and the associated Dirichlet series has an Euler product; and let*

$$\rho_\ell : \mathrm{Gal}(K_\ell/\mathbb{Q}) \to GL_2(\mathbb{Z}_\ell)$$

be the continuous homomorphism given by Theorem 1. *Suppose that the image of* $\tilde{\rho}_\ell$ *does not contain* $SL_2(\mathbb{F}_\ell)$, *so that* ℓ *is an exceptional prime for* f. *Then the three cases listed in Corollary* 1 *imply respectively the following congruences for the coefficients of* f :

(i) *There is an integer* m *such that* $a_n \equiv n^m \sigma_{k-1-2m}(n) \bmod \ell$ *for all* n *prime to* ℓ.

(ii) $a_n \equiv 0 \bmod \ell$ *whenever* n *is a quadratic non-residue* mod ℓ.

(iii) $p^{1-k}a_p^2 \equiv 0,1,2$ *or* 4 mod ℓ *for all primes* $p \neq \ell$.

PROOF. In case (i) we may without loss of generality suppose that the Borel subgroup involved consists of the upper triangular matrices; thus for any σ in $\mathrm{Gal}(K_\ell/\mathbb{Q})$ we can write

$$\tilde{\rho}_\ell(\sigma) = \begin{pmatrix} \alpha(\sigma) & \beta(\sigma) \\ 0 & \delta(\sigma) \end{pmatrix} .$$

Now α thus defined is a continuous homomorphism $\mathrm{Gal}(K_\ell/\mathbb{Q}) \to \mathbb{F}_\ell^*$, and must therefore be equal to $\tilde{\chi}_\ell{}^m$ for some integer m. Moreover $\alpha\delta = \tilde{\chi}_\ell{}^{k-1}$ by Theorem 1, so that $\delta = \tilde{\chi}_\ell{}^{k-1-m}$. Taking $\sigma = \mathrm{Frob}(p)$ we obtain

$$a_p \equiv p^m + p^{k-1-m} \bmod \ell \tag{10}$$

for $p \nmid \ell$, and the congruence for a_n follows from this and (8).

For case (ii), note first that we can assume $\ell > 2$; for every proper subgroup of $GL_2(\mathbb{F}_2)$ is contained in either a Cartan or a Borel subgroup. Let C be the Cartan subgroup and N its normalizer, and consider the homomorphism

$$\mathrm{Gal}(K_\ell/\mathbb{Q}) \to N \to N/C \sim \{\pm 1\}.$$

By hypothesis this is onto; and since the image is commutative the homomorphism factors through $\mathrm{Gal}(K_\ell^{ab}/\mathbb{Q}) \sim \mathbb{Z}_\ell^*$. The only continuous homomorphism of this last group onto $\{\pm 1\}$ is the one whose kernel is the squares; and it follows that $\tilde{\rho}_\ell(\mathrm{Frob}(p))$ is in C if and only if p is a quadratic residue mod ℓ. Now let α be an element of N not in C; after a field extension if necessary, α interchanges two one-dimensional subspaces of the space on which it operates, and can therefore be put in the form $\left(\begin{smallmatrix} 0 & * \\ * & 0 \end{smallmatrix}\right)$. So α has zero trace. Hence $a_p \equiv 0 \bmod \ell$ whenever p is a quadratic non-residue mod ℓ, by Theorem 1; and the same conclusion follows for a_n by (8).

For (iii), note that every element of H has order 1,2,3 or 4; so every element of G has characteristic roots of the form $\lambda\mu, \lambda\mu^{-1}$ where one of μ^2, μ^4, μ^6 or μ^8 is equal to 1. Enumeration of cases now proves the Corollary.

We may distinguish (iii) from (ii) as follows. By an argument similar to that used for case (ii), the image of Frob(p) in H lies in A_4 if and only if p is a quadratic residue mod ℓ. Since Frobenius elements are dense in any Galois group, there are an infinity of p such that the image of Frob(p) in H has order 4; such p are quadratic non-residues mod ℓ and satisfy

$$p^{1-k}a_p^2 \equiv 2 \bmod \ell.$$

3. Modular forms mod ℓ.

For any integer $\nu > 0$ we write

$$G_{2\nu} = \tfrac{1}{2}\zeta(1-2\nu) + \sum_1^\infty \frac{n^{2\nu-1}q^n}{1-q^n} = -\frac{b_{2\nu}}{4\nu} + \sum_1^\infty \sigma_{2\nu-1}(n)q^n$$

where $b_{2\nu}$ is the (2ν)th Bernoulli number; and

$$E_{2\nu} = -4\nu G_{2\nu}/b_{2\nu} = 1 + \dots .$$

For $\nu > 1$ these are different normalizations of the Eisenstein series of weight 2ν. This G_2 is essentially the η_2 of the classical theory; it is not a modular form but satisfies a similar functional equation. Following Ramanujan [8] we write

$$P = E_2 = 1 - 24\sum\sigma_1(n)q^n,$$

$$Q = E_4 = 1 + 240\sum\sigma_3(n)q^n,$$

$$R = E_6 = 1 - 504\sum\sigma_5(n)q^n.$$

Any modular form of weight k can be expressed as an isobaric polynomial in Q and R (which have weights 4 and 6 respectively). More specifically,

$$1728\Delta = Q^3 - R^2; \tag{11}$$

and if f is a modular form and A the additive group generated by the coefficients of the q-series expansion of f, then f has a unique expression as an isobaric element of $A[Q,\Delta] \oplus RA[Q,\Delta]$. To find an explicit expression for f we have in general to compare q-series expansions; but for Eisenstein series we can use the recurrence relation

$$(n - 2)(n + 5)F_{n+4} = 12(F_4F_n + F_6F_{n-2} +\dots+ F_nF_4), \tag{12}$$

valid for any even n greater than 2, in which we have simplified the algebra by writing

$$F_n = G_n/(n - 2)!\ .$$

This may be proved by substituting the standard expansion

$$\wp(z;\omega_1,\omega_2) = z^{-2} + 2\sum_{m=2}^{\infty} (-1)^m \left(\frac{2\pi}{\omega_2}\right)^{2m} z^{2m-2}\ F_{2m}$$

for the Weierstrass $\wp$-function into the differential equation

$$\wp'' = 6\wp^2 - \tfrac{1}{2}\, g_2.$$

The first few cases give

$$E_8 = Q^2, E_{10} = QR,\ 691E_{12} = 441Q^3 + 250R^2, E_{14} = Q^2R; \tag{13}$$

values up to E_{32} inclusive will be found in Ramanujan [8], Table I.

Henceforth, following Ramanujan, we write

$$\theta = q\,\frac{d}{dq}\ ;$$

the essential property of this operator in the present context is as follows.

LEMMA 3. _Let_ f _be a modular form of weight_ k; _then_ $(12\theta f - kPf)$ _is a modular form of weight_ $(k + 2)$.

The proof of lemma 3 is by direct calculation of the effect of modular transformations on $(12\theta f - kPf)$; it can be found in Ogg's lectures at this conference. A similar calculation shows that $(12\theta P - P^2)$ is a modular form of weight 4. Examination of the constant terms in the q-series expansions now gives

$$3\theta Q - PQ = -R, \quad 2\theta R - PR = -Q^2, \qquad (14)$$
$$12\theta P - P^2 = -Q, \quad \theta\Delta - P\Delta = 0 \quad .$$

We can reformulate lemma 3 in terms of the operator ∂ defined by

$$\partial = 12\theta - kP \text{ on modular forms of weight } k. \qquad (15)$$

COROLLARY. ∂ _is the derivation on the graded algebra of modular forms such that_ $\partial Q = -4R$ _and_ $\partial R = -6Q^2$.

We can now define modular forms mod ℓ. Denote by $\mathfrak{o}$ the local ring of $\mathbb{Q}$ at ℓ - that is, the ring of rational numbers with denominator prime to ℓ. Let M_k be the $\mathfrak{o}$-module of those modular forms of weight k whose q-series expansions have all their coefficients in $\mathfrak{o}$; and let $\tilde{M}_k \subset \mathbb{F}_\ell[[q]]$ be the $\mathbb{F}_\ell$-vector space whose elements consist of the $\sum \tilde{a}_n q^n$ as $f = \sum a_n q^n$ runs through the elements of M_k. (Here, as always, the tilde denotes reduction mod ℓ.) Then the $\mathbb{F}_\ell$-algebra of modular forms mod ℓ is just the sum of the $\tilde{M}_k$. We have now to determine the structure of this algebra, which we shall write $\tilde{M}$; and since the argument involves certain Eisenstein series we shall need some standard results on the ℓ-adic nature of Bernouilli numbers.

LEMMA 4. (von Staudt-Kummer).

(i) _If_ $(\ell - 1)|2\nu$ _then_ $\ell b_{2\nu} \equiv -1 \bmod \ell$.

(ii) _If_ $(\ell - 1)\nmid 2\nu$ _then_ $b_{2\nu}/2\nu$ _is_ ℓ-_integral and its residue class_ mod ℓ _only depends on_ $2\nu \bmod(\ell - 1)$.

For a proof see [2], pp.384-6.

It is convenient to adopt the following notations, even though they involve a slight abuse of language. Let f be a function which has a q-series expansion $\sum a_n q^n$ such that every a_n is in $\mathcal{O}$; then $\tilde{f}$ will denote the formal power series $\sum \tilde{a}_n q^n$. Again, let $\phi(X,Y)$ be a polynomial in $\mathcal{O}[X,Y]$; then $\tilde{\phi}(X,Y)$ will denote the polynomial in $\mathbb{F}_\ell[X,Y]$ obtained from ϕ by reduction of the coefficients mod ℓ. However, the natural arguments for ϕ will be Q and R; and since Q and R are algebraically independent even over $\mathbb{C}$ we shall allow ourselves to regard them as independent transcendentals and therefore as acceptable formal arguments for $\tilde{\phi}$. Thus $\tilde{\phi}(Q,R)$ is a polynomial in two variables with coefficients in $\mathbb{F}_\ell$, whereas $\tilde{\phi}(\tilde{Q},\tilde{R})$ is the element of $\mathbb{F}_\ell[[q]]$ obtained from this polynomial by substitution. In particular if f is in M_k then there is a unique polynomial ϕ such that $\phi(Q,R) = f$; for $\ell > 3$ the coefficients of ϕ are in $\mathcal{O}$ and $\tilde{\phi}(\tilde{Q},\tilde{R}) = \tilde{f}$. Note that the derivation ∂ on $\mathcal{O}[Q,R]$ induces a derivation, also written ∂, on $\mathbb{F}_\ell[Q,R]$, and that Θ analogously extends to $\mathbb{F}_\ell[[q]]$.

From now until the end of the proof of lemma 5, we assume that $\ell > 3$. The cases $\ell = 2$ and $\ell = 3$ are anomalous because an element of M_k cannot necessarily be written as an isobaric polynomial of $\mathcal{O}[Q,R]$; see (11). Fortunately they are also trivial, and the analogues of Theorem 2 for them will be stated and proved as Theorem 3. For $\ell > 3$ there is a ring homomorphism

$$\mathcal{O}[Q,R] \to \mathbb{F}_\ell[Q,R] \to \tilde{M}$$

which extends $\mathcal{O} \to \mathbb{F}_\ell$ and is onto; to determine the structure of $\tilde{M}$ we have only to find the kernel of the right hand arrow. Denote by A and B the two isobaric polynomials such that

$$A(Q,R) = E_{\ell-1}, \quad B(Q,R) = E_{\ell+1}.$$

By lemma 4(i), $E_{\ell-1}$ is in $M_{\ell-1}$: and since by lemma 4(ii)

$$b_{\ell+1}/(\ell+1) \equiv \tfrac{1}{2} b_2 \equiv -1/12 \bmod \ell, \tag{16}$$

$E_{\ell+1}$ is in $M_{\ell+1}$. So A and B have coefficients in $\mathcal{O}$.

THEOREM 2. Suppose that $\ell > 3$. Then

(i) $\tilde{A}(\tilde{Q},\tilde{R}) = 1$ and $\tilde{B}(\tilde{Q},\tilde{P}) = \tilde{P}$;

(ii) $\partial\tilde{A}(Q,R) = \tilde{B}(Q,R)$ and $\partial\tilde{B}(Q,R) = -Q\tilde{A}(Q,R)$;

(iii) $\tilde{A}(Q,R)$ has no repeated factor and is prime to $\tilde{B}(Q,R)$;

(iv) $\tilde{M}$ is naturally isomorphic to $\mathbb{F}_\ell[Q,R]/(\tilde{A}-1)$ and has a natural grading with values in $\mathbb{Z}/(\ell-1)$.

PROOF. The first part of (i) follows from lemma 4(ii). Moreover

$$d \equiv d^\ell \bmod \ell$$

for any integer d, whence $\sigma_1(n) \equiv \sigma_\ell(n)$; and the second part of (i) now follows from (16). Thus $\theta\tilde{A}(\tilde{Q},\tilde{R}) = 0$ whence

$$\partial\tilde{A}(\tilde{Q},\tilde{R}) = \tilde{P}\tilde{A}(\tilde{Q},\tilde{R}) = \tilde{P} = \tilde{B}(\tilde{Q},\tilde{R}).$$

This means that $\partial A - B$ has a q-series every coefficient of which is divisible by ℓ; since it is a modular form of weight $\ell+1$, it must lie in $\ell\mathcal{O}[Q,R]$ and thus $\partial\tilde{A} = \tilde{B}$. Again

$$\partial\tilde{B}(\tilde{Q},\tilde{R}) = (12\theta - \tilde{P})\tilde{B}(\tilde{Q},\tilde{R}) = (12\theta - \tilde{P})\tilde{P} = -\tilde{Q}$$

by (14), and a similar argument shows that $\partial\tilde{B} = -Q\tilde{A}$. This proves (ii).

Now suppose that $\tilde{A}$ is exactly divisible by $(Q^3 - \tilde{c}R^2)^n$ where $n > 0$ and $\tilde{c} \neq 0$ is in the algebraic closure of $\mathbb{F}_\ell$. Since $A(\tilde{Q},\tilde{R})$ has non-zero constant term whereas $\tilde{Q}^3 - \tilde{R}^2$ has zero constant term, we cannot have $\tilde{c} = 1$; so

$$\partial(Q^3 - \tilde{c}R^2) = 12(\tilde{c} - 1)Q^2R$$

is prime to $(Q^3 - \tilde{c}R^2)$. Moreover by consideration of degree $n < \ell$. It follows from $\partial\tilde{A} = \tilde{B}$ that $\tilde{B}$ is exactly divisible by $(Q^3 - \tilde{c}R^2)^{n-1}$; and if $n > 1$ it follows from $\partial\tilde{B} = -Q\tilde{A}$ that $\tilde{A}$ is exactly divisible by $(Q^3 - \tilde{c}R^2)^{n-2}$, contrary to hypothesis. A similar argument works for powers of Q or R. Thus $\tilde{A}$ has no repeated factors and its simple factors do not divide $\tilde{B}$. This proves (iii).

Denote by $\mathfrak{a}$ the kernel of the map $\mathbb{F}_\ell[Q,R] \to \mathbb{F}_\ell[[q]]$ obtained by substituting $\tilde{Q}$ and $\tilde{R}$ for Q and R; clearly $\mathfrak{a}$ contains $\tilde{A} - 1$, and $\mathfrak{a}$ is prime because the image is an integral domain. If $\mathfrak{a}$ were maximal then $\tilde{Q}$ and $\tilde{R}$ would be algebraic over $\mathbb{F}_\ell$, which is absurd because the coefficient of q in at least one of them is non-zero. Since $\mathbb{F}_\ell[Q,R]$ has dimension 2, in order to prove that $\mathfrak{a} = (\tilde{A} - 1)$ it is now enough to prove that $\tilde{A} - 1$ is an irreducible polynomial. If not, let

$$\phi(Q,R) = \phi_n(Q,R) + \phi_{n-1}(Q,R) + \ldots + 1$$

be an irreducible proper factor of $\tilde{A} - 1$, where ϕ_ν is isobaric of weight ν, and let $\tilde{c}$ be a primitive $(\ell - 1)^{\text{th}}$ root of unity in $\mathbb{F}_\ell$; then writing $\tilde{c}^2Q$, $\tilde{c}^3R$ for Q,R does not alter $\tilde{A} - 1$, so that $\phi(\tilde{c}^2Q,\tilde{c}^3R)$ is also a factor of $\tilde{A} - 1$. But this is not equal to $\phi(Q,R)$ and hence is coprime to it; so $\phi(Q,R)\phi(\tilde{c}^2Q,\tilde{c}^3R)$ divides $\tilde{A} - 1$. By considering terms of highest weight we see that $(\phi_n(Q,R))^2$ divides $\tilde{A}$, which is absurd because $\tilde{A}$ has no repeated factors. This completes the proof of Theorem 2.

Note that ∂ is an operator of weight 2 on $\tilde{M}$; and the same is true of θ since $\tilde{P}$ is a modular form mod ℓ of weight 2. It is this last property which makes the theory of modular forms mod ℓ so much tidier than the classical theory.

It follows from Theorem 2 that $\tilde{A}(Q,R)$ is the Hasse invariant of the associated elliptic curve. This may be proved in one of two ways. On the one hand Deligne has shown that the q-series expansion of the Hasse invariant reduces to 1; and Theorem 2 shows that this property characterizes $\tilde{A}$ among polynomials of weight $\ell - 1$. On the other hand the differential equation derived from (ii) is just that which the Hasse invariant is known to satisfy - see Igusa [4]. Indeed the present proof of (iii) is essentially the same as Igusa's proof that the Hasse invariant has no repeated roots. One may also derive explicit formulae for $\tilde{A}$ and $\tilde{B}$ from (ii), as an alternative to the use of the recursion formula (12). We list the first few cases below :

<u>$\ell = 5.$</u> Now $E_4 = Q$; so $\tilde{Q} = 1$ and $\tilde{M} = \mathbb{F}_5[\tilde{R}]$

<u>$\ell = 7.$</u> Now $E_6 = R$; so $\tilde{R} = 1$ and $\tilde{M} = \mathbb{F}_7[\tilde{Q}]$.

<u>$\ell = 11.$</u> Now $E_{10} = QR$, so that $\tilde{Q}\tilde{R} = 1$; thus $\tilde{M}$ is isomorphic to

$$\mathbb{F}_{11}[Q,R]/(QR - 1) = \mathbb{F}_{11}[Q,Q^{-1}].$$

<u>$\ell = 13.$</u> Now E_{12} is given by (13) and the fundamental relation is

$$6\tilde{Q}^3 - 5\tilde{R}^2 = 1.$$

For use in the next section we introduce a filtration on $\tilde{M}$. Let $\tilde{f}$ be a graded element of $\tilde{M}$, that is to say a sum of elements of various $\tilde{M}_k$ for which all the relevant k are congruent mod(ℓ - 1). By multiplying the summands by suitable powers of $\tilde{A}$ we can make them all belong to the same $\tilde{M}_k$, so that $\tilde{f}$ itself belongs to an $\tilde{M}_k$. Define $\omega(\tilde{f})$, the filtration of $\tilde{f}$, to be the least k such that $\tilde{f}$ belongs to $\tilde{M}_k$. Thus for example only the constants have filtration 0 and there are no elements of filtration 2; there are elements of filtration 4 if and only if $\ell > 5$, and in that case they are just the non-zero multiples of $\tilde{Q}$.

LEMMA 5. (i) <u>Let</u> f <u>be a modular form of weight</u> k <u>such that</u> $f = \phi(Q,R)$ <u>for some</u> ϕ <u>in</u> $\mathfrak{O}[Q,R]$, <u>and suppose that</u> $\tilde{f} \neq 0$. <u>Then</u> $\omega(\tilde{f}) < k$ <u>if and only if</u> $\tilde{A}$ <u>divides</u> $\tilde{\phi}$.

(ii) *Let* $\tilde{f}$ *be a graded element of* $\tilde{M}$; *then* $\omega(\theta\tilde{f}) \leq \omega(\tilde{f}) + \ell + 1$, (17)
with equality if and only if $\omega(\tilde{f}) \not\equiv 0 \bmod \ell$.

PROOF. (i) is obvious from Theorem 2(iv) since we are still assuming $\ell > 3$. To prove (ii), let $k = \omega(\tilde{f})$ and let $f = \phi(Q,R)$ be a modular form of weight k whose reduction mod ℓ is $\tilde{f}$. The inequality (17) follows from

$$12\theta\tilde{f} = \tilde{A}(\tilde{Q},\tilde{R})\partial\tilde{\phi}(\tilde{Q},\tilde{R}) + k\tilde{B}(\tilde{Q},\tilde{R})\tilde{f}$$

so that $12\theta\tilde{f}$ is the image in $\tilde{M}$ of $(\tilde{A}\partial\tilde{\phi} + k\tilde{B}\tilde{\phi})$. Moreover we know by (i) that $\tilde{\phi}$ is not a multiple of $\tilde{A}$ (except in the trivial case $\tilde{f} = 0$), and by Theorem 2(iii) that $\tilde{B}$ is prime to $\tilde{A}$; so $(\tilde{A}\partial\tilde{\phi} + k\tilde{B}\tilde{\phi})$ is a multiple of $\tilde{A}$ if and only if k is a multiple of ℓ. Thus the second part of the lemma follows from the first.

In the next section we shall need a technique for deciding with as little effort as possible whether two modular forms mod ℓ are equal. It is often convenient to use

LEMMA 6. *Suppose that* $\tilde{f}_1$ *and* $\tilde{f}_2$ *are both in* $\tilde{M}_k$; *then they are equal if and only if for each* $n \leq k/12$ *the coefficients of* q^n *in* $\tilde{f}_1$ *and* $\tilde{f}_2$ *are equal.*

PROOF. The condition is obviously necessary. Suppose it holds, and let f_1 and f_2 be modular forms of weight k whose reductions mod ℓ are $\tilde{f}_1$ and $\tilde{f}_2$. The standard algorithm for expressing $(f_1 - f_2)$ as a polynomial of weight k in Q,R and Δ only makes use of the coefficients of q^n for $n \leq k/12$ in $(f_1 - f_2)$, and all these are divisible by ℓ; so $(f_1 - f_2)$ is in $\ell\mathcal{O}[Q,R,\Delta]$. This proves the lemma.

We now return to the trivial cases $\ell = 2$ and $\ell = 3$.

THEOREM 3. *If* $\ell = 2$ *or* $\ell = 3$ *then* $\tilde{P} = \tilde{Q} = \tilde{R} = 1$ *and* $\tilde{M} = \mathbf{F}_\ell[\tilde{\Delta}]$. *There is* no grading and ∂ annihilates $\tilde{M}$.

This follows trivially from the remarks at the beginning of this section, together with the facts that the coefficient of q in Δ is 1 and that $\partial\Delta = 0$.

There is as yet no satisfactory structure theory of modular forms mod ℓ^n where $n > 1$. At first sight it would seem natural to conjecture that for $\ell > 3$ the ideal of those elements of $\mathcal{O}[Q,R]$ whose q-series expansion has all its coefficients divisible by ℓ^n is $(\ell, A - 1)^n$. It is not difficult to prove this conjecture for $n \leqslant \ell$; but it is certainly false for $n > \ell$.

4. The exceptional primes.

In this section we show that for any f satisfying the conditions of Theorem 1 the set of exceptional primes is finite and can be explicitly bounded; and for the six forms $\Delta, Q\Delta, R\Delta, Q^2\Delta, QR\Delta$ and $Q^2R\Delta$ which are known to satisfy the conditions of Theorem 1 we find (with one case left undecided) the complete list of exceptional primes. This also solves our original problem of finding those ℓ for which there exist congruences for $\tau(n)$ or a_n mod ℓ. For we have seen in §2 that to each exceptional prime ℓ there correspond congruences for a_p mod ℓ; and the lemma that follows shows that there can be no congruences for a non-exceptional prime.

LEMMA 7. *Suppose that* $f = \sum a_n q^n$ *satisfies the conditions of Theorem 1; that is, it is a cusp form with* $a_1 = 1$, a_n *in* $\mathbb{Z}$ *and its Dirichlet series has an Euler product. Let* ℓ *be a prime which is not exceptional for* f, *and let* N, N^* *be non-empty open sets in* $\mathbb{Z}_\ell$ *and* $\mathbb{Z}^*_\ell$ *respectively. Then the set of primes* p *for which* p *is in* N^* *and* a_p *is in* N *has positive density.*

PROOF. The first step is to show that the image of the map

$$(\rho_\ell, \chi_\ell) : \mathrm{Gal}(K_\ell/\mathbb{Q}) \to GL_2(\mathbb{Z}_\ell) \times \mathbb{Z}_\ell^* \tag{18}$$

contains $SL_2(\mathbb{Z}_\ell) \times 1$. By hypothesis, the projection of the image onto the first factor contains $SL_2(\mathbb{Z}_\ell)$; so the image of the commutator subgroup contains $\mathrm{Comm}(SL_2(\mathbb{Z}_\ell)) \times 1$. If $\ell > 3$ this commutator subgroup is the whole of $SL_2(\mathbb{Z}_\ell)$, by lemma 1 and the simplicity of $SL_2(\mathbf{F}_\ell)$. If $\ell = 2$ or 3 and σ in $\mathrm{Gal}(K_\ell/\mathbb{Q})$ is such that $\rho_\ell(\sigma)$ is in $SL_2(\mathbb{Z}_\ell)$ then

$$\chi_\ell^{k-1}(\sigma) = 1$$

where k is the weight of f; thus $\chi_\ell(\sigma) = 1$ because $\mathbb{Z}_\ell$ contains no non-trivial roots of unity of odd order.

It follows that the image of (18) consists of all $\alpha \times \beta$ with $\det \alpha = \beta^{k-1}$; and since we can find an element of $GL_2(\mathbb{Z}_\ell)$ with any assigned trace in $\mathbb{Z}_\ell$ and determinant in $\mathbb{Z}_\ell^*$ - for example $\begin{pmatrix} \mathrm{tr} & -1 \\ \det & 0 \end{pmatrix}$ - the map

$$(\mathrm{Tr} \circ \rho_\ell, \chi_\ell) : \mathrm{Gal}(K_\ell/\mathbb{Q}) \to \mathbb{Z}_\ell \times \mathbb{Z}_\ell^*$$

is onto. The lemma now follows from the facts that this map induces $\mathrm{Frob}(p) \to a_p \times p$ and that Frobenius elements are uniformly distributed in the Galois group.

To find the exceptional primes, at least for the first two cases in the Corollaries to lemma 2, we replace the hypothetical congruences of Corollary 2 by equivalent hypothetical identities between modular forms mod ℓ; and we use the results of §3 to provide decision processes for these hypothetical identities. The first step is the following lemma, which for fixed f leaves us only finitely many possibilities to consider.

LEMMA 8. _Suppose that_ f, ℓ _and_ ρ_ℓ _are as in Corollary_ 2 _to lemma_ 2. _Then case_ (i) _of that Corollary can only happen if either_ $2m < \ell < k$ _or_ $m = 0$ _and_ ℓ _divides the numerator of_ b_k; _and case_ (ii) _can only happen if_ $\ell < 2k$.

PROOF. We may suppose that $\ell > 3$. Now case (i) is equivalent to (10), and in that congruence the exponents are only significant $\bmod(\ell - 1)$. Reducing them into the interval $[0, \ell - 2]$ and interchanging them if necessary, we can replace (10) by

$$a_p \equiv p^m + p^{m'} \bmod \ell \tag{19}$$

where $0 \leq m < m' < \ell - 1$ and $m + m' \equiv k - 1 \bmod(\ell - 1)$; here m and m' cannot be equal because their sum is odd. From this we obtain

$$a_n \equiv n^m \sigma_{m'-m}(n) \bmod \ell \text{ if } n \text{ is prime to } \ell.$$

In general this can be written in the form

$$\theta\tilde{f} = \theta^{m+1} \tilde{G}_{m' - m+1} \tag{20}$$

where the extra θ on each side has been put in to annihilate the coefficient of q^n when n is divisible by ℓ. This is illegitimate only when $m = 0$, $m' = \ell - 2$ in which case the constant term in $G_{m' - m + 1}$ is not in $\mathcal{O}$; in that case we have instead $pa_p \equiv 1 + p \bmod \ell$ whence $na_n \equiv \sigma_1(n) \bmod \ell$ for n prime to ℓ and finally

$$\theta\tilde{f} = \theta^{\ell-1} \tilde{G}_2 = \theta^{\ell-1} \tilde{G}_{\ell+1}. \tag{21}$$

By lemma 5(ii) we have $\omega(\theta\tilde{f}) \leq k + \ell + 1$. But obviously $\omega(\tilde{G}_{2\nu}) = 2\nu$ whenever $2 \leq 2\nu < \ell - 1$; and in applying lemma 5(ii) iteratively to find the filtration of the right hand side of (20) we are always in the case of equality. So provided that $m' - m > 1$ the filtration of the right hand side of (20) is exactly $(m' - m + 1) + (m + 1)(\ell + 1)$. Comparing these two results we obtain

$$m' + m\ell + 1 \leq k \text{ if } 1 < m' - m < \ell - 2. \tag{22}$$

If $\ell > k$ then $m + m' \geq k - 1$ by the condition below (19); and that is only compatible with (22) if $m = 0$, $m' = k - 1$ and $\omega(\tilde{f}) = k$. But then (20) becomes $\theta(\tilde{f} - \tilde{G}_k) = 0$; and since $(\tilde{f} - \tilde{G}_k)$ must either vanish or have filtration k, we deduce from lemma 5(ii) that it must vanish. Examination of the constant term now shows that ℓ must divide the numerator of b_k.

A similar argument works for (21) and for the case $m'-m = 1$ in (20). Now $\omega(\tilde{G}_2) = \ell + 1$ because of $\tilde{B}(\tilde{Q},\tilde{R}) = \tilde{P}$ together with the non-existence of modular forms of weight 2. Once again, in applying lemma 5(ii) repeatedly we are always in the case of equality; so the filtration of the right hand side of (20) is $(m + 2)(\ell + 1)$ and that of the right hand side of (21) is $\ell(\ell + 1)$. Comparing as before with the filtration of the left hand side we obtain

$$\left.\begin{array}{ll} (m + 1)(\ell + 1) \leq k & \text{if } m'-m = 1, \\ \ell^2 - 1 \leq k & \text{if } m = 0,\ m' = \ell - 2. \end{array}\right\} \tag{23}$$

These certainly imply $\ell < k$.

Similarly case (ii) is equivalent to

$$\theta\tilde{f} = \theta^{(\ell + 1)/2}\tilde{f} \tag{24}$$

and if $\ell > 2k$ and consequently $\omega(\tilde{f}) = k$, then the filtration of the left hand side is $k + \ell + 1$ whereas that of the right hand side is $k + \frac{1}{2}(\ell + 1)^2$. This contradiction completes the proof of the lemma; for since ℓ is odd and k is even, neither $\ell = k$ nor $\ell = 2k$ is possible.

With a little more trouble we can improve the result in case (ii). For suppose that $k < \ell < 2k$; then $\omega(\theta^{\nu}\tilde{f}) = k + \nu(\ell + 1)$ provided $\nu \leq \ell - k$, and therefore

$$\omega(\theta^{\ell-k+1}\tilde{f}) = \ell(\ell+1-k) + \ell + 1 - n(\ell - 1)$$

for some integer $n > 0$. It may be verified that in the further applications of lemma 5(ii) needed to obtain

$$\omega(\theta^{(\ell+1)/2}\tilde{f})$$

no further case of inequality occurs; and since we know that that filtration is equal to $\omega(\theta\tilde{f}) < 2(\ell + 1)$, there can be at most one more application of θ. It follows that $\ell = 2k - 1$ or $\ell = 2k - 3$. A similar idea can be applied when $\ell < k$, but this is less useful since nearly all such ℓ are already exceptional primes for case (i).

We have still to consider case (iii) of Corollary 2 to lemma 2. Here the situation is much less satisfactory, in that we no longer have a decision process; the best we can do is to generate a finite list of primes which certainly contains all exceptional primes of this kind. For choose $p \nmid 2$ such that $a_p \nmid 0$; then if ℓ is an exceptional prime of this type either $\ell = p$ or ℓ divides one of

$$a_p^2,\ a_p^2 - p^{k-1},\ a_p^2 - 2p^{k-1},\ a_p^2 - 4p^{k-1}.$$

Since all these are non-zero (k being even), this gives a finite list of possible ℓ. There are some further conditions on ℓ in this case, which reduce the calculations involved. It was shown at the end of §2 that there are primes p which are quadratic non-residues mod ℓ and for which ℓ divides $a_p^2 - 2p^{k-1}$; since k is even, it follows that 2 is a quadratic non-residue mod ℓ. Thus

$$\ell \equiv \pm 3 \bmod 8;$$

moreover taking p = 2 in the earlier condition we can now reject the second and fourth possibilities, so that

$$\ell \text{ divides } a_2 \text{ or } (a_2 \pm 2^{k/2}).$$

Again, since the image of $\tilde{\rho}_\ell$ is isomorphic to S_4 there is composite epimorphism

$$\mathrm{Gal}(K_\ell/\mathbb{Q}) \to S_4 \to S_3$$

and hence there is a field K which is normal over $\mathbb{Q}$ with Galois group S_3

and which is unramified except at ℓ. The subfield of K fixed under A_3 must be $\mathbb{Q}(\sqrt{\pm\ell})$, where the sign is plus if $\ell \equiv 5 \bmod 8$ and minus if $\ell \equiv 3 \bmod 8$; and K must be unramified over this field. Classfield theory now shows that

$$\mathbb{Q}(\sqrt{\pm\ell}) \text{ has class number divisible by } 3.$$

We can sum up our results as follows :

THEOREM 4. *Given a modular form* f *satisfying the conditions of Theorem* 1, *there are only finitely many primes exceptional for* f. *Those of types* (i) *and* (ii) *can be explicitly determined; and there is an explicitly determinable finite set which contains those of type* (iii).

We now apply these methods to the six known modular forms which satisfy the conditions of Theorem 1. For this purpose it is convenient to have a formula for the action of a power of θ on a modular form. Let f be a modular form of weight k, and write

$$f_o = f,\ f_1 = \partial f,\ f_\nu = \partial f_{\nu-1} - (k+\nu-2)(\nu-1)Qf_{\nu-2} \text{ for } \nu > 1,$$

where we have identified f with its expression as a polynomial in Q and R. Then for any $n \geqslant 0$ we have

$$(12\theta)^n f = \sum_{\nu=0}^{n} \frac{n!\ (k+n-1)!}{\nu!\ (n-\nu)!\ (k+\nu-1)!} P^{n-\nu} f_\nu . \tag{25}$$

The proof is by induction on n, using (15) and the third equation (14).

COROLLARY. (i) *For the six known modular forms which satisfy the conditions of Theorem* 1, *the exceptional primes of type* (i) *and the associated values of* m *are given by the following table.*

Form	k	2	3	5	7	11	13	17	19	23	Other ℓ
Δ	12	0	0	1	1	No					691
$Q\Delta$	16	0	0	1	1	1	No				3617
$R\Delta$	18	0	0	2	1	1	1	No			43867
$Q^2\Delta$	20	0	0	1	2	1	1	No	No		283,617
$QR\Delta$	22	0	0	2	1	No	1	1	No		131,593
$Q^2R\Delta$	26	0	0	2	2	1	No	1	1	No	657931

Here the first two columns give the form and its weight, the last column gives the exceptional $\ell > k$ *(for which necessarily* $m = 0$), *and the other columns give for each* $\ell < k$ *the value of* m *if* ℓ *is exceptional, or the word* 'No' *if* ℓ *is not exceptional.*

(ii) *For these six forms, the only exceptional primes of type* (ii) *are* $\ell = 23$ *for* Δ *and* $\ell = 31$ *for* $Q\Delta$.

(iii) *With the possible exception of* $\ell = 59$ *for* $Q\Delta$, *there are no exceptional primes of type* (iii) *for any of these six forms.*

PROOF. The results for $\ell = 2$ and $\ell = 3$ (for which the general machinery is not applicable) follow from Theorem 3 and the congruences

$$\tau(p) \equiv 0 \bmod 2, \qquad \tau(p) \equiv p + p^2 \bmod 3$$

which are weaker versions of (2) and (3) respectively. In the remaining possible cases of (i) with $\ell < k$, the only possible value of m can most easily be determined from (19) when $p = 2$ or 3, together with (22) and (23); and indeed in the case when ℓ is not exceptional this method proves that there is no possible value of m. So it is only necessary to check (20) for the positive cases in the table. This can be done either by calculations with polynomials in Q and R or by means of lemma 6.

For (ii) it is only necessary to consider $\ell = 2k-1$, $\ell = 2k-3$ and those $\ell < k$ which are not exceptional of type (i). For those cases which have to be rejected, the simplest method is to find a prime p which is a quadratic non-residue mod ℓ and to verify that a_p is not divisible by ℓ; for the cases with $\ell < k$ we can also argue as in the paragraph following equation (24). In the two remaining cases $\ell = 2k-1$ and it follows from (25) that the right hand side of (24) is in $\tilde{M}_{k+\ell+1}$. Since this is also true for the left hand side, we have only to check that the coefficients of q, q^2, q^3 and q^4 agree - this last only for $k = 16$; and this can be done without even calculating them in the case of Δ, since 2 and 3 are quadratic residues mod 23. It is however necessary to check that for $Q\Delta$ the coefficient $a_3 = -3348$ is divisible by 31.

For (iii) we have already outlined the method of calculation together with some convenient short-cuts; these enable us to reject without difficulty all values of ℓ except the one given in the Corollary. This concludes the proof of the Corollary.

For exceptional primes of type (i), nothing more needs to be done in respect of the homomorphism $\tilde{\rho}_\ell$ and the associated congruence mod ℓ; congruences modulo higher powers of ℓ, and the information about ρ_ℓ that can be derived from them, will be discussed in §5. For exceptional primes of types (ii) and (iii) however, there still remain interesting questions. For example, we have now proved the first line of (6) but we have not proved the second or third; nor have we in this case determined either the kernel or the image of $\tilde{\rho}_{23}$. It is however clear that the kernel of the homomorphism

$$\mathrm{Gal}(K_\ell/Q) \to N \to N/C \sim \{\pm 1\},$$

where C is a Cartan subgroup and N its normalizer, consists of those elements of the Galois group which are trivial on $\mathbb{Q}(\sqrt{-\ell})$; and hence for each of our two examples of case (ii) the image of $\tilde{\rho}_\ell$ is canonically isomorphic to $\mathrm{Gal}(K/\mathbb{Q})$ where K is some unramified abelian extension of $\mathbb{Q}(\sqrt{-\ell})$. In the case $k = 12$, $\ell = 23$ it is clear from (6) that K is the absolute class field of $\mathbb{Q}(\sqrt{-\ell})$; for the three lines of (6) correspond respectively to (p) remaining prime, splitting as a product of principal ideals, and splitting as a product of non-principal ideals, in $\mathbb{Q}(\sqrt{-23})$. From this point of view the natural way to prove (6) is by proving

$$2\Delta \equiv \Sigma\Sigma q^{m^2 + mn + 6n^2} - \Sigma\Sigma q^{2m^2 + mn + 3n^2} \bmod 23. \tag{26}$$

The case k = 16, ℓ = 31 is extremely similar, the analogue of (6) holding with the obvious modifications; the class number of $\mathbb{Q}(\sqrt{-31})$, like that of $\mathbb{Q}(\sqrt{-23})$, is 3. The analogue of (26) for this case is

$$2Q\Delta \equiv \Sigma\Sigma q^{m^2 + mn + 8n^2} - \Sigma\Sigma q^{2m^2 + mn + 4n^2} \bmod 31. \tag{27}$$

Wilton [13] proved (6) by means of (26); but this very simple proof of (26) depends on the product formula (1) and there seems little prospect of a similar proof of (27). However, we can argue as follows. The right hand side of (26) or (27) is a modular form of weight 1 for $\Gamma_o(\ell)$ for a certain quadratic character; so its square is a modular form of weight 2 for $\Gamma_o(\ell)$. By a theorem of Serre, proved in his lecture at this conference, any modular form of weight 2 for $\Gamma_o(\ell)$ whose q-series has integral coefficients is congruent mod ℓ to a modular form of weight (ℓ + 1) for the full modular group whose q-series has integral coefficients, and vice versa. So the square of each side of (26) or (27), reduced mod ℓ, lies in $\widetilde{M}_{\ell+1}$. By lemma 6, to prove (26) or (27) it is now enough to check it for the coefficients of q^o, q^1 and q^2; and this is easy.

There remains the case ℓ = 59 for $Q\Delta$. With the help of a computer I have verified that $p^{-15}a_p^2 \equiv 0,1,2$ or 4 mod 59 for all p < 500; so there can be no reasonable doubt that 59 is an exceptional prime of type (iii) for $Q\Delta$. There remains the problem of proving it. Let K be the fixed field of the kernel of the homomorphism

$$\mathrm{Gal}(K_{59}/\mathbb{Q}) \to PGL_2(\mathbb{F}_{59});$$

then $K/\mathbb{Q}$ is ramified only at 59 and is a normal extension with Galois group isomorphic to S_4. These specifications are enough to determine K. Indeed corresponding to the sequence of subgroups each normal in its predecessor

$$S_4 \supset A_4 \supset V \supset I$$

(where V is non-cyclic of order 4), we have the tower of fixed fields

$$\mathbb{Q} \subset \mathbb{Q}(\sqrt{-59}) \subset L \subset K.$$

Here L must be the absolute class-field of $\mathbb{Q}(\sqrt{-59})$, which is the splitting field of $x^3 + 2x - 1 = 0$. By a detailed study of the field L it can be shown that there is just one possible K and that it is the splitting field of

$$x^4 - x^3 - 7x^2 + 11x + 3 = 0.$$

Lifting the image of the Galois group back from $PGL_2(\mathbb{F}_{59})$ to $GL_2(\mathbb{F}_{59})$ is easy; but it is not very useful because the result is too large. It is better to study not ρ but $\rho\otimes\chi^7$ because $\det \circ (\rho\otimes\chi^7) = \chi^{29}$; and reduced mod 59 and applied to Frob(p) this gives the quadratic residue symbol $(\frac{p}{59})$. Thus the image of $\widetilde{\rho\otimes\chi^7}$ in $GL_2(\mathbb{F}_{59})$ is a group S_4' of order 48, and its associated field K' is a quadratic extension of K. Now lift S_4' back to characteristic zero, as a subgroup of $GL_2(\mathbb{Z}[\sqrt{-2}])$; since there is a natural isomorphism $\mathrm{Gal}(K'/\mathbb{Q}) \xrightarrow{\sim} S_4'$ this induces an Artin L-series associated with K'. According to the Artin conjecture, this series and all those obtained from it by twisting with a congruence character can be analytically continued to holomorphic functions on the whole s-plane, satisfying functional equations of standard type. Suppose this is so; then by a theorem of Weil [12] the Mellin transform of the Artin L-series will be a cusp form of weight 1 for $\Gamma_o(59^2)$, for a certain quadratic character. By construction this cusp form will have coefficients in $\mathbb{Z}[\sqrt{-2}]$ and will be congruent mod 59 (or more precisely modulo one of the prime factors of 59 in $\mathbb{Z}[\sqrt{-2}]$) to $\theta^7(Q\Delta)$.

To determine whether such a cusp form exists is a strictly finite calculation, which does not depend on the various hypotheses which I have used to render its existence plausible. Unfortunately, in the present unsatisfactory state of our knowledge about modular forms of weight 1 it is not an attractive calculation. Suppose however that such a form was shown to exist, and let its q-series expansion be $\Sigma b_n q^n$, where

$$\Sigma b_n n^{-s} = \Pi(1 - b_p p^{-s} \pm p^{-2s})^{-1}.$$

The Ramanujan-Petersson conjecture implies

$$b_p = 0, \pm 1, \pm \sqrt{-2} \text{ or } \pm 2 \tag{28}$$

for all p, and even a statistical version of the conjecture (which should be provable by classical methods without too much trouble in this case) would prove (28) for all p outside a set of density zero. It would follow that for the coefficients of $Q\Delta$

$$p^{-15} a_p^2 \equiv 0,1,2 \text{ or } 4 \bmod 59$$

either for all p or for all p outside a set of density zero. By lemma 7 this would be enough to prove that 59 is an exceptional prime of type (iii) for $Q\Delta$.

5. Congruences modulo powers of ℓ.

In this case the theory is much less complete, and to the extent that it exists it is much more dependent on heavy algebraic manipulations. We therefore confine ourselves to certain selected topics and do not treat even those completely.

If a congruence such as (2) or (3) is true, then it can be proved by brute force. We illustrate this by considering (2). For any integer μ,

$$\Delta(\tau + \mu/8) = \Delta(e^{\pi i\mu/4}q)$$

is a modular form of weight 12 for $\Gamma_o(64)$, and by combining these forms we find that for any ν so is

$$\Sigma\tau(n)q^n \text{ where the sum is over all } n \equiv \nu \bmod 8.$$

A similar argument works for $\Sigma\sigma_{11}(n)q^n$; so each of the four congruences (2) asserts the congruence of two modular forms of weight 12 for $\Gamma_o(64)$. Such modular forms are algebraic and integral over $\mathfrak{O}[Q,R,\Delta]$, so such a congruence is equivalent to a certain isobaric congruence between modular forms for the full modular group. In view of the remark following (11), to prove this last congruence one writes the difference of the two sides as a polynomial in P,Q and R which is linear in R, and verifies that each coefficient of the polynomial is individually divisible by the relevant power of 2. Of course a process as crude as this would be intolerably tedious to carry through; but it is one in which there is considerable scope for replacing hard work by ingenuity.

There is another reasonable method, though the proofs which it would provide would be even less illuminating than the existing ones. As was shown above, any one of the congruences (2) is equivalent to a congruence between two modular forms of weight 12 for $\Gamma_o(64)$; and just as in lemma 6, to prove this congruence it is enough to verify it for a limited number of coefficients - a task which is straightforward on a computer. Methods analogous to this have been used by Atkin and his pupils; see for example [1].

Similar remarks apply to (3), though here there is the additional complication that the congruence to be proved will involve θ. However, θ can be expressed in terms of ∂, which is an operator which takes modular forms to modular forms, and P which is congruent modulo any assigned prime power to a modular form, as is proved in Serre's lectures at this conference. However, it would seem that we do not yet have the right point of view for attacking these problems.

We now show that by means of Theorem 1 the middle equation (6) can be painlessly improved to

$$\tau(p) \equiv 1 + p^{11} \bmod 23^2 \text{ if } p = u^2 + 23v^2,\ p \nmid 23. \tag{29}$$

For if p is such a prime $\tilde{\rho}_{23}(\mathrm{Frob}(p))$ is the identity, and hence the image of Frob(p) in $GL_2(\mathbb{Z}/(23^2))$ has trace = 1 + det as elements of $\mathbb{Z}/(23)^2$. This is just (29). By a refinement of this argument we can determine the image of ρ_{23}, which we shall denote by G. Let G^* and $\tilde{G}$ be the images of G in $GL_2(\mathbb{Z}/(23^2))$ and $GL_2(\mathbf{F}_{23})$ respectively. We have already shown that $\tilde{G}$ is isomorphic to S_3, so without loss of generality we can assume that $\tilde{G}$ consists of the six matrices

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

Let V be the kernel of the homomorphism

$$GL_2(\mathbb{Z}/(23^2)) \to GL_2(\mathbb{F}_{23}) \tag{30}$$

and let H be the intersection of G^* and V. There is a natural action of $GL_2(\mathbf{F}_{23})$ on V given by $\sigma : v \to s\ v\ s^{-1}$ where v is in V and s is any pull-back of σ for the map (30); this induces an action of $\tilde{G}$ both on V and on H. Moreover the map

$$\begin{pmatrix} 1 + 23a & 23b \\ 23c & 1 + 23d \end{pmatrix} \mapsto (a,b,c,d)$$

identifies V with a vector space of dimension 4 over $\mathbf{F}_{23}$. The irreducible components of V under the action of $\tilde{G}$ are as follows :

V_1, the multiples of $(1,0,0,1)$;

V_2, the multiples of $(1,2,-2,-1)$;

V_3 defined by $a + d = a - b + c = 0$.

Since $\tilde{G}$ acts on H, H must be a sum of V_i. If H did not contain V_1, det would be constant on H and so $p^{11} \equiv 1 \bmod 23^2$ for all p of the form $u^2 + 23v^2$, which is absurd. Similarly if H did not contain V_2 we would have $a - d = 2(b - c)$ on H, and this would imply that (det + 2 tr) would be constant on the inverse image of

$$\begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix} \text{ and } \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$$

in G^*. Translated into terms of $\tau(p)$, this would mean that $p^{11} + 2\tau(p)$ would be congruent to some constant mod 23^2 for all p of the form

$$2u^2 + uv + 3v^2$$

- the case in the last line of (6); this can be seen to be false by considering the case $p = 2$ and $p = 3$. Finally, if H did not contain V_3 a similar argument would show that $\tau(p)$ was congruent to some constant mod 23^2 for all p which are quadratic non-residues mod 23; and this again is false. So H = V. Now an argument like those in the proof of lemma 1 or the last part of the proof of Theorem 6 shows that G is the entire inverse image of $\tilde{G}$ under the homomorphism $GL_2(\mathbb{Z}_{23}) \to GL_2(\mathbb{F}_{23})$. This result is of course independent of the particular representation of $\tilde{G}$ chosen above.

We can also make some further additions to (2), though of a rather different kind. It turns out that the congruences (2) are enough to determine the image not merely of $\tilde{\rho}_2$ but of ρ_2 essentially uniquely. The exact statement and proof of this fact are extremely tedious and are therefore relegated to the Appendix. However, certain consequences of independent interest can be easily stated. For example, the last three congruences (2) are best possible in the following sense.

THEOREM 5. *Let* N, N^* *be non-empty open subsets of* $\mathbb{Z}_2, \mathbb{Z}_2^*$ *respectively such that no element of* N^* *is congruent to* 1 mod 8 *and any* α *in* N *and* β *in* N^* *satisfy the appropriate one of*

$$\alpha \equiv 1217(1 + \beta^{11}) \bmod 2^{13} \text{ if } \beta \equiv 3 \bmod 8,$$

$$\alpha \equiv 1537(1 + \beta^{11}) \bmod 2^{12} \text{ if } \beta \equiv 5 \bmod 8,$$

$$\alpha \equiv 705(1 + \beta^{11}) \bmod 2^{14} \text{ if } \beta \equiv 7 \bmod 8.$$

Then there are an infinity of primes p *with* p *in* N^* *and* $\tau(p)$ *in* N.

PROOF. Denote by G the image of ρ_2, which is described in detail in the Appendix. By a straightforward but tedious calculation one verifies that to every α and β satisfying the congruence conditions above, there exist elements of G with trace α and determinant β^{11}. The theorem now follows because Frobenius elements are dense in $\mathrm{Gal}(K_2/\mathbb{Q})$ and therefore their images are dense in G. The corresponding statement for the first congruence (2) would be false. Indeed, for any given $\beta \equiv 1 \bmod 8$ in $\mathbb{Z}_2^*$ let $S = S(\beta)$ denote the set of α in $\mathbb{Z}_2$ such that there is an element of G with trace α and determinant β^{11}. It may be shown that $S(\beta)$ is a union of complete residue classes mod 2^{17} and that it only depends on β mod 2^{17}. By (2), $S(\beta)$ lies entirely within the residue class of $(1 + \beta^{11}) \bmod 2^{11}$; but it is never the whole of this class, and it never lies wholly within one of the two residue classes mod 2^{12} contained in this class. Thus the first congruence (2) is best possible in the sense that it cannot be improved to a congruence for $\tau(p)$ mod 2^{12}, no matter how good a 2-adic approximation to p we have; but unlike the other three congruences (2) it is not best possible in the sense of Theorem 5.

CORROLLARY. <u>The conjecture that</u> $2^n \| (p+1)$ <u>implies</u> $2^n \| \tau(p)$ <u>is false for each</u> $n > 13$.

This conjecture is of some interest since if it were true for all n it would follow that $\tau(p)$ is never zero.

Despite this theorem, one can obtain congruences modulo higher powers of 2 provided that one supplies more information about p; and the simplest way to obtain and prove such congruences is by considering G. Suppose for example that we confine ourselves to the case $p \equiv 1 \bmod 4$, so that $p = u^2 + v^2$ in essentially just one way; then we can ask for congruences which express $\tau(p)$ in terms of p, u and v. As in the Appendix, denote by G_{15} the subgroup of G consisting of those matrices whose determinant is congruent to 1 mod 4; let $K = \mathbb{Q}(i)$ and let K^{ab} be the maximal abelian extension of K inside K_2. Then K is the fixed field of $\rho_2^{-1} G_{15}$ and 2-adic knowledge of u, v and p is essentially the same as knowing the Frobenius element of $(u + iv)$ in the extension K^{ab}/K. Indeed there is a composite homomorphism

$$\phi : \mathbb{Z}_2[i]^*/\{\pm 1, \pm i\} \xrightarrow{\sim} \mathrm{Gal}(K^{ab}/K) \to G_{15}/[G_{15}, G_{15}]$$

where the square brackets on the right denote the commutator subgroup. Unfortunately, though the left hand isomorphism is canonical there is no direct method of specifying the right hand homomorphism; all we know is that $\det \circ \phi$ is induced by

$$(u + iv) \to (u^2 + v^2)^{11}.$$

Since the natural map $G_{15}/[G_{15}, G_{15}] \to G/[G,G]$ has finite kernel, this leaves only finitely many possibilities for ϕ. If ϕ is known, then for any given $p = u^2 + v^2$ we know the coset of $[G_{15}, G_{15}]$ in which the image of Frob$(u + iv)$ lies; and so we know the set of traces of elements of this coset. Since this set of traces contains $\tau(p)$, this specifies in terms of p,u and v an open subset of $\mathbb{Z}_2$ in which $\tau(p)$ lies; and since

$[G_{15}, G_{15}]$ is strictly smaller than $[G,G]$, we can reasonably hope that this open subset is smaller than that given by (2).

So to each of the finitely many possibilities for ϕ there corresponds a set of hypothetical congruences for $\tau(p)$. All but one of these hypothetical sets can be shown to be false by examining small values of p; the remaining one must correspond to the true ϕ and is thereby proved. The details of this calculation are quite unsuitable for publication; the results are four congruences of which a typical one is

$$\tau(p) \equiv 1 + p^{11} + 2^{10} + 5.2^5(p-5)^2 + 3.2^8(p-5) + 2^8(p-5)(b^2-1)$$
$$+ 5.2^9(b^2-1) \bmod 2^{16} \text{ if } p \equiv 5 \bmod 16,$$

where $p = u^2 + 4b^2$. However, to show that this extra information does not always lead to an ugly result, we conclude by stating what appears to be the analogous result for $\ell = 3$. Write for $p \equiv 1 \bmod 3$

$$4p = L^2 + 27M^2 \text{ where } M \equiv 0 \text{ or } 1 \bmod 3.$$

Then

$$\tau(p) - p^{119} - p^{-108} \equiv \begin{cases} 0 \bmod 3^8 \text{ if } M \equiv 0 \bmod 3, \\ 3^6(M+7) \bmod 3^8 \text{ if } M \equiv 1 \bmod 3. \end{cases}$$

However, this is based only on numerical evidence and has not yet been proved. The first congruence (3), when n is prime, is just the statement that the left hand side is divisible by 3^6.

APPENDIX

We shall consistently use the following notation.

An element σ of $GL_2(\mathbb{Z}_2)$ will be written as

$$\sigma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 1+2^7A & 2^4B \\ 2^5C & 1+2D \end{pmatrix};$$

here A,B,C,D are not necessarily integral, though they will be for those σ which primarily interest us. Moreover

$$S = a + d, \quad \Delta = ad - bc$$

will denote the trace and determinant of σ; in particular it follows that

$$D \equiv \tfrac{1}{2}(\Delta - 1)(1 - 2^7A) - 2^6A + 2^8BC \mod 2^{13} \tag{31}$$

and therefore that

$$S \equiv 1 + \Delta - 2^7(\Delta - 1)A + 2^9BC \mod 2^{14} \tag{32}$$

whenever A,B and C are integral. Finally θ,ϕ,ψ will be the characters of Δ mod 8 whose values are given by the following table :

Δ mod 8	1	3	5	7
θ	1	1	-1	-1
ϕ	1	-1	1	-1
ψ	1	-1	-1	1

If we have to consider several σ simultaneously, we shall distinguish them by subscripts and we shall attach the corresponding subscripts to the associated letters $a,b,c,d,A,B,C,D,S,\Delta,\theta,\phi,\psi$.

Let G_o be the set of elements σ of $GL_2(\mathbb{Z}_2)$ which satisfy the conditions

B and C are both even if $\Delta \equiv \pm 1 \bmod 8$ and both odd if

$$\Delta \equiv \pm 3 \bmod 8,$$

$$B + C\Delta \equiv \tfrac{1}{2}(\Delta^2 + 3 - 4\psi) \bmod 16, \qquad (33)$$

$$A \equiv \tfrac{1}{8}(\Delta + 2\theta - 3\phi)(3\Delta + 10\theta - 3\phi) + \tfrac{3}{2}(1 - \psi) - 2C^2 \bmod 64. \qquad (34)$$

(Here and throughout this appendix, all products will be integer-valued even when they appear to contain a power of $\tfrac{1}{2}$.) It may be verified by direct calculation, and will be implicit in the proof of the theorem that follows, that G_o is actually a group; and for a similar choice of reasons each element of G_o satisfies the appropriate one of the following congruences :

$$\left.\begin{aligned} S &\equiv (1 + \Delta) \bmod 2^{11} \text{ if } \Delta \equiv 1 \bmod 8, \\ S &\equiv 1217(1 + \Delta) \bmod 2^{13} \text{ if } \Delta \equiv 3 \bmod 8, \\ S &\equiv 1537(1 + \Delta) \bmod 2^{12} \text{ if } \Delta \equiv 5 \bmod 8, \\ S &\equiv 705(1 + \Delta) \bmod 2^{14} \text{ if } \Delta \equiv 7 \bmod 8. \end{aligned}\right\} \qquad (35)$$

These correspond to the congruences (2) of Kolberg for $\tau(p)$.

THEOREM 6. Let G be a closed subgroup of $GL_2(\mathbb{Z}_2)$ such that
(i) the homomorphism $\det : G \to \mathbb{Z}_2^*$ is onto, and
(ii) every element σ of G satisfies the appropriate congruence condition (35).

Then G can be transformed into G_o by conjugation by an element of $GL_2(\mathbb{Q}_2)$.

That we must allow conjugation by an element of $GL_2(\mathbb{Q}_2)$, and not merely by an element of $GL_2(\mathbb{Z}_2)$, corresponds to the fact that in Deligne's proof of Theorem 1 the space on which the representation acts is canonically defined, but the integral lattice in it is not canonical.

The proof will consist of a number of steps, gradually refining G until it is contained in G_o; finally we show that a closed proper subgroup of G_o cannot satisfy condition (i) of the Theorem. We begin with a partial normalization of G.

LEMMA 9. By suitable conjugation we can assume that G contains an element σ_o such that

$$b_o = c_o = 0, \quad a_o \equiv 1 \bmod 2^{13}, \quad d_o \equiv -1 \bmod 2^{13}, \qquad (36)$$
$$\Delta_o = -1.$$

Moreover with this normalization A,B,C,D are integers for every σ in G; and A is even if $\Delta \equiv \pm 1 \bmod 8$ and odd if $\Delta \equiv \pm 3 \bmod 8$.

PROOF. The congruences (35), taken mod 2^9, reduce to

$$(a - 1)(d - 1) - bc \equiv \begin{cases} 2^8 \bmod 2^9 \text{ if } \Delta \equiv 3 \bmod 8, \\ 0 \bmod 2^9 \text{ otherwise.} \end{cases} \qquad (37)$$

In particular a + d is always even, so the image of G in $GL_2(\mathbb{F}_2)$ consists of matrices of zero trace; hence this image must be the identity or one of the three conjugate subgroups of order 2. So after conjugation we may assume that a,d are odd and c even for each σ in G; and it now follows from (37) that $4|bc$ always. Let $2^\beta, 2^\gamma$ be the greatest powers of 2 which divide all b,c respectively, where σ runs through the elements of G. If σ_1, σ_2 are such that $2^\beta || b_1$ and $2^\gamma || c_2$ then for one of σ_1, σ_2 and $\sigma_1 \sigma_2$ we have both $2^\beta || b$ and $2^\gamma || c$; and now $4|bc$ gives $\beta + \gamma \geqslant 2$. By multiplying every b and dividing every c by a fixed power of 2, which is an allowed transformation of G, we can certainly ensure that $\beta \geqslant 1$ and $\gamma \geqslant 1$.

Now choose an element σ_o of G with $\Delta_o = -1$; by (35) it has $2^{14}|S_o$ and hence its characteristic roots are in $\mathbb{Z}_2$ and are congruent to $\pm$ 1 mod 2^{13}. By conjugation we can make σ_o diagonal, which proves (36); and since the conjugation is by a matrix with integer elements and determinant a unit or twice a unit, and b and c are even before the conjugation, the σ in G are still integral after the transformation. However we have temporarily lost all information about β and γ.

Applying (37) to $\sigma\sigma_o$, which mod 2^{13} only differs from σ in the signs of b and d, we have

$$(a - 1)(-d - 1) + bc \equiv \begin{cases} 2^8 \bmod 2^9 \text{ if } \Delta \equiv 5 \bmod 8, \\ 0 \bmod 2^9 \text{ otherwise.} \end{cases}$$

Adding this to (37) we obtain $2^8 | (a - 1)$ if $\Delta \equiv \pm 1 \bmod 8$ and $2^7 || (a - 1)$ if $\Delta \equiv \pm 3 \bmod 8$, which proves the assertions about A. It follows also that $2^7 | bc$, whence $ad - bc = \Delta$ shows that $d \equiv \Delta \bmod 2^7$. With this additional help, (37) now gives $2^9 | bc$. With the same definition of β,γ as above, the argument we have already used now shows that $\beta + \gamma \geq 9$; and after the allowable transfer of a power of 2 between b and c for each σ in G, we may suppose that $\beta \geq 4$ and $\gamma \geq 5$. Hence B and C are integers, and we have already seen that D is an integer. This completes the proof of the Lemma.

Using (32), the congruences (35) can be rewritten in the form

$$\left.\begin{array}{llll} BC - \tfrac{1}{4}A(\Delta-1) \equiv 0 & \bmod 4 & \text{if } \Delta \equiv 1 \bmod 8, \\ 2BC - \tfrac{1}{2}A(\Delta-1) \equiv \tfrac{1}{4}(19(1+\Delta)) & \bmod 32 & \text{if } \Delta \equiv 3 \bmod 8, \\ BC - \tfrac{1}{4}A(\Delta-1) \equiv 3(1+\Delta) & \bmod 8 & \text{if } \Delta \equiv 5 \bmod 8, \\ 2BC - \tfrac{1}{2}A(\Delta-1) \equiv \tfrac{1}{4}(11(1+\Delta)) & \bmod 64 & \text{if } \Delta \equiv 7 \bmod 8. \end{array}\right\} \quad (38)$$

Note that D and Δ are linked by the congruence

$$D \equiv \tfrac{1}{2}(\Delta - 1) \bmod 64$$

which is a weak form of (31). It is also convenient at this point to record some formulae for the product of two matrices in A,B,C,D form; if $\sigma = \sigma_1\sigma_2$ then

$$A \equiv A_1 + A_2 + 4B_1C_2,\ B \equiv B_1\Delta_2 + B_2\ ,\ C \equiv C_1 + \Delta_1 C_2 \qquad (39)$$

all mod 2^7.

LEMMA 10. <u>Each</u> σ <u>in</u> G <u>satisfies</u> $B + C\Delta \equiv 0 \bmod 8$ <u>and the congruence conditions stated in the following table</u> :

Δ mod 8	$\pm\ 1$	$\pm\ 3$
A mod 16	$\frac{1}{4}(\theta\Delta - 1) - 2C^2$	$\frac{1}{4}(3\theta\Delta + 19)$
B and C	even	odd

PROOF. As in the proof of the previous lemma we consider also $\sigma\sigma_o$ where σ_o satisfies (36). Applying (38) to $\sigma\sigma_o$ and confining ourselves to the case $\Delta \equiv \pm 3 \bmod 8$ we obtain

$$\tfrac{1}{4}A(\Delta + 1) - BC \equiv 3(1 - \Delta) \bmod 8 \text{ if } \Delta \equiv 3 \bmod 8,$$

$$\tfrac{1}{2}A(\Delta + 1) - 2BC \equiv \tfrac{1}{4}(19(1 - \Delta)) \bmod 32 \text{ if } \Delta \equiv 5 \bmod 8.$$

Combining one of these equations with the corresponding equation (38), and using the character θ to unite the two cases, we obtain first

$$A \equiv \tfrac{1}{4}(-5\theta\Delta + 43) \equiv \tfrac{1}{4}(3\theta\Delta + 19) \bmod 16 \text{ if } \Delta \equiv \pm\ 3 \bmod 8$$

and then on substituting this back,

$$BC \equiv \tfrac{1}{4}A(\Delta + \theta) + 3(\Delta - \theta) \equiv \frac{1}{16}(3\Delta\theta + 7)(\Delta + 21\theta) + 5\theta \bmod 8.$$

But the first term on the right vanishes mod 8 because each factor is divisible by 8 and one of them by 16; so this congruence reduces to $BC \equiv 5\theta \bmod 8$, which is equivalent to B and C odd, $B + C\Delta \equiv 0 \bmod 8$.

This proves the last column of the table.

Any σ in G with $\Delta \equiv 1 \bmod 8$ can be written as

$$\sigma = \sigma_1\sigma_2 \text{ with } \Delta_1 \equiv \Delta_2 \equiv 3 \bmod 8.$$

It follows immediately from the multiplication formulae (39) that B and C are even and $B + C \equiv 0 \bmod 8$; moreover mod 16 we have

$$A - \tfrac{1}{4}(\Delta - 1) + 2C^2 \equiv A_1 + A_2 - 4C_1C_2 - \tfrac{1}{4}(\Delta_1\Delta_2 - 1) + 2(C_1 + C_2)^2$$

$$\equiv 2(C_1^2 + C_2^2) - \tfrac{1}{4}(\Delta_1 - 3)(\Delta_2 - 3) + 12 \equiv 0.$$

This proves the statements in the table for $\Delta \equiv 1 \bmod 8$, and those for $\Delta \equiv -1 \bmod 8$ follow on multiplication by σ_o. This completes the proof of the lemma.

We now complete the normalization of G. Fix an element σ_3 with $\Delta_3 \equiv 3 \bmod 8$; then by lemma 10 we have

$$A_3 \equiv \tfrac{1}{8}(\Delta_3 + 5)(3\,\Delta_3 + 13) + 3 - 2C_3^2 \bmod 16,$$

for the last term is just $-2 \bmod 16$ since C_3 is odd. We can therefore find a 2-adic unit λ such that multiplying the last term on the right by λ^2 replaces the congruence by an equality. Now for every σ in G multiply c by λ and divide b by λ; this is an allowed transformation and does not affect the representation of σ_o given by (36). So henceforth we can assume that there is a σ_3 with

$$A_3 = \tfrac{1}{8}(\Delta_3 + 5)(3\Delta_3 + 13) + 3 - 2C_3^2, \; \Delta_3 \equiv 3 \bmod 8. \tag{40}$$

COROLLARY. <u>With the further normalization above</u>,

$$A \equiv \tfrac{1}{8}(\Delta - \theta)(3\Delta + 7\theta) - 2C^2 \bmod 32 \;\underline{\text{if}}\; \Delta \equiv \pm 1 \bmod 8,$$

$$A \equiv \tfrac{1}{8}(\Delta + 5\theta)(3\Delta + 13\theta) + 3 - 2C^2 \bmod 32 \;\underline{\text{if}}\; \Delta \equiv \pm 3 \bmod 8.$$

PROOF. Suppose first that $\Delta \equiv -1 \bmod 8$; then the last congruence (38) together with the facts already proved that C is even and $B \equiv C \bmod 8$ give

$$2C^2 - \tfrac{1}{2}A(\Delta - 1) \equiv \tfrac{1}{4}(11(1 + \Delta)) \bmod 32,$$

and elementary manipulation transforms this into the statement in the Corollary. Next, if $\Delta \equiv 1 \bmod 8$ apply the result just obtained to $\sigma\sigma_o$, where σ_o satisfies (36). Finally suppose that $\Delta \equiv \pm 3 \bmod 8$ and write $\sigma_1 = \sigma\sigma_3^{-1}$ where σ_3 satisfies (40); thus $\theta = \theta_1$ and σ has the property stated in the Corollary since $\Delta_1 \equiv \pm 1 \bmod 8$. Also (39) implies

$$A \equiv A_1 + A_3 - 4C_1C_3\Delta_1 \;, \; C \equiv C_1 + \Delta_1C_3 \bmod 32.$$

Hence, working mod 32,

$$A - \tfrac{1}{8}(\Delta + 5\theta)(3\Delta + 13\theta) - 3 + 2C^2$$

$$\equiv A_1 + A_3 + 2C_1^2 + 2C_3^2\Delta_1^2 - 3 - \tfrac{1}{8}(\Delta_1\Delta_3 + 5\theta_1)(3\Delta_1\Delta_3 + 13\theta_1)$$

$$\equiv \tfrac{1}{8}(\Delta_1 - \theta_1)(3\Delta_1 + 7\theta_1) + \tfrac{1}{8}(\Delta_3 + 5)(3\Delta_3 + 13) - \tfrac{1}{8}(\Delta_1\Delta_3 + 5\theta_1)$$

$$(3\Delta_1\Delta_3 + 13\theta_1)$$

by (40) and the Corollary for σ_1. This last expression vanishes mod 32, and this completes the proof of the Corollary.

LEMMA 11. G <u>is contained in</u> G_o.

PROOF. Suppose first that $\Delta \equiv 3 \bmod 8$; substituting the value for A mod 32 given by the last Corollary into the second congruence (38) we obtain

$$2BC + C^2(\Delta - 1) \equiv \Delta + 9 \bmod 32.$$

Since C is odd, for given C and Δ this congruence determines B mod 16; and as one can easily check that it is satisfied by

$B \equiv \frac{1}{2}(\Delta^2 + 7) - C\Delta \bmod 16$, this is the unique solution. Thus the condition (33) certainly holds for elements of G with $\Delta \equiv 3 \bmod 8$. It also holds when $\Delta \equiv 5 \bmod 8$, because in this case we can apply the result just proved to $\sigma\sigma_o$ where σ_o satisfies (36). Now suppose that $\Delta \equiv \pm 1 \bmod 8$, so that we can write $\sigma = \sigma_1\sigma_3$ where $\Delta_1 \equiv \pm 3 \bmod 8$. Using (39) and the result already established, we have mod 16,

$$B + C\Delta \equiv B_1\Delta_3 + B_3 + \Delta_1\Delta_3C_1 + \Delta_1^2\Delta_3C_3$$

$$\equiv \tfrac{1}{2}\Delta_3(\Delta_1^2 + 7) + \tfrac{1}{2}(\Delta_3^2 + 7) + \Delta_1^2 - 1 \equiv \tfrac{1}{2}(\Delta^2 - 1)$$

and this completes the proof of (33).

To prove (34) we suppose first that $\Delta \equiv 7 \bmod 8$ and substitute the value of B mod 16 given by (33) into the last congruence (38). This gives

$$\tfrac{1}{2}A(\Delta - 1) + 2C^2\Delta - C(\Delta^2 - 1) + \tfrac{1}{4}(11(1 + \Delta)) \equiv 0 \bmod 64$$

which for given values of C and Δ determines A mod 64; as one can easily check that it is satisfied by

$$A \equiv \tfrac{1}{8}(\Delta + 1)(3\Delta - 7) - 2C^2 \bmod 64$$

this must be the unique solution. This proves (34) for $\Delta \equiv 7 \bmod 8$, and it follows at once for $\Delta \equiv 1 \bmod 8$ by applying the result just obtained to $\sigma\sigma_o$. Now suppose that $\Delta \equiv \pm 3 \bmod 8$ and write $\sigma = \sigma_1\sigma_3$ where σ_3 satisfies (40) and therefore $\Delta_1 \equiv \pm 1 \bmod 8$. Using (39) and substituting for B_1 from (33) we have $C \equiv C_1 + \Delta_1C_3 \bmod 32$ and

$$A \equiv A_1 + A_3 - 4\Delta_1C_1C_3 + 2C_3(\Delta_1^2 - 1) \bmod 64.$$

Using (34) for A_1, a case in which it is already proved, and (40) for A_3 we obtain, all mod 64,

$$A - \tfrac{1}{8}(\Delta + 5\theta)(3\Delta + 13\theta) - 3 + 2C^2$$

$$\equiv A_1 + A_3 + 2C_1^2 + 2\Delta_1^2C_3^2 + 2C_3(\Delta_1^2 - 1) - \tfrac{1}{8}(\Delta + 5\theta)(3\Delta + 13\theta) - 3$$

$$\equiv \tfrac{1}{8}\,(\Delta_1 - \theta_1)\,(3\Delta_1 + 7\theta_1) + \tfrac{1}{8}\,(\Delta_3 + 5)\,(3\Delta_3 + 13)$$

$$- \tfrac{1}{8}\,(\Delta_1\Delta_3 + 5\theta_1)\,(3\Delta_1\Delta_3 + 13\theta_1) + 2C_3(C_3 + 1)\,(\Delta_1^2 - 1)$$

and this last expression vanishes mod 64. This completes the proof of the lemma.

To prove the Theorem it only remains to show that G cannot be strictly smaller than G_o. We show first that for any fixed Δ all eight pairs of congruence classes for B and C mod 16 allowed by (33) and the parity condition just before it, actually occur. It is enough to prove this in the special case $\Delta = 1$, since the σ in G with Δ equal to some fixed Δ_1 are obtained from one of them by multiplication by the elements of G with $\Delta = 1$. Choose σ_1 in G with $\Delta_1 = 3$; then $\sigma_2 = \sigma_o^{-1}\sigma_1\sigma_o$ will certainly have $\Delta_2 = 3$ and $B_2 \equiv -B_1 \bmod 4$. Thus $\sigma = \sigma_1\sigma_2^{-1}$ will have $\Delta = 1$ and $B \equiv B_2 - B_1 \equiv 2 \bmod 4$; and $I, \sigma, \sigma^2, \ldots, \sigma^7$ will lie one in each of the eight allowed classes.

Now for $n = 0,1,2,\ldots$ let H_n denote the set of σ with $\Delta = 1$ and

$$a \equiv d \equiv 1 \bmod 2^{n+13},\quad 2^{n+8}|b,\quad 2^{n+9}|c;$$

clearly each H_n is a group and $G_o \supset H_o \supset H_1 \supset \ldots$. The result we have just proved states that G meets every coset of H_o in G_o; so to prove $G = G_o$ it is enough to prove that $G \supset H_o$. Since G is closed and the H_n form a base for the neighbourhoods of the identity in H_o, it is enough to prove for $n = 0,1,2,\ldots$ that G meets each of the eight cosets of H_{n+1} in H_n. We begin with the case $n = 0$. For σ_1 and σ_2 in G and $\sigma = \sigma_1\sigma_2\sigma_1^{-1}\sigma_2^{-1}$, which we use in the form $\sigma_1\sigma_2 = \sigma\sigma_2\sigma_1$, it follows from (39) that

$$\left.\begin{aligned} A &\equiv 4(B_1C_2 - B_2C_1 - B(C_2 + \Delta_2C_1)) \mod 2^7, \\ B\Delta_1\Delta_2 &\equiv B_1(\Delta_2 - 1) - B_2(\Delta_1 - 1) \mod 2^7, \\ C &\equiv C_2(\Delta_1 - 1) - C_1(\Delta_2 - 1) \mod 2^7. \end{aligned}\right\} \qquad (41)$$

Moreover $\Delta = 1$. Suppose first that $\Delta_1 = -1$, $B_1 \equiv C_1 \equiv 0 \mod 16$ and that $\Delta_2 = 9$ so that $B_2 + 9C_2 \equiv 8 \mod 16$. If $B_2 \equiv 0 \mod 16$ then we obtain

$$A \equiv 0 \mod 2^7, \quad B \equiv 0 \mod 2^5, \quad C \equiv 16 \mod 2^5;$$

whereas if $B_2 \equiv 8 \mod 16$ we obtain

$$A \equiv 0 \mod 2^7, \quad B \equiv 16 \mod 2^5, \quad C \equiv 0 \mod 2^5.$$

Again take $\Delta_1 = 1$, $\Delta_2 = 9$ and $B_1 \equiv B_2 \equiv 2$, $C_1 \equiv -2$, $C_2 \equiv 6$ all mod 16; then we obtain

$$A \equiv 64 \mod 2^7, \quad B \equiv 16 \mod 2^5, \quad C \equiv 16 \mod 2^5.$$

The three elements σ thus obtained generate H_o/H_1; so G meets each coset of H_1 in H_o.

We now proceed by induction. There is a natural isomorphism $H_{n-1}/H_n \to H_n/H_{n+1}$ obtained by doubling A,B and C; and for any σ in H_{n-1} the map that sends σ to σ^2 induces this isomorphism. So if G meets every coset of H_n in H_{n-1}, it meets every coset of H_{n+1} in H_n. This completes the proof of the Theorem.

As was explained in §5, for certain purposes it is useful to know the commutator subgroups of G and of some of its subgroups. It is easy to check from (41) and the argument following it that $[G,G] = G \cap SL_2(\mathbb{Z}_2)$. Indeed this is predicted by the general theory, for the composite map

$$\mathrm{Gal}(K_2^{ab}/\mathbb{Q}) \to G/[G,G] \to \mathbb{Z}_2^*,$$

of which the components are induced respectively by ρ_2 and det, is χ_2^{11} which is an isomorphism by class field theory; and since the left hand map is onto, the right hand one must be an isomorphism.

Now for $\nu = 3,5$ or 7 denote by $G_{1\nu}$ the subgroup of G consisting of those σ for which $\Delta \equiv 1$ or $\nu \bmod 8$, and denote by G_1 the subgroup of G for which $\Delta \equiv 1 \bmod 8$. The argument that proved $G \supset H_o$ only used the commutators of elements of G_{17}; so it certainly proves $[G_{17},G_{17}] \supset H_o$, and it now follows easily from (41) that $[G_{17},G_{17}]$ consists of those elements of $[G,G]$ for which B and C are divisible by 4.

It is convenient next to consider the commutator subgroup of G_1. It is easily verified that if σ_1 and σ_2 are in G_1 then the congruences (41) hold mod 2^8. Now $\Delta_1 = \Delta_2 = 1$, $B_1 = 16$, $C_1 = 0$, $B_2 = -2$, $C_2 = 2$ gives $2^7 || A$, $2^8 | B$, $2^8 | C$; and $\Delta_1 = 1$, $\Delta_2 = 9$, $B_1 = 16$, $B_2 = 8$, $C_1 = C_2 = 0$ gives $2^8 | A$, $2^7 || B$, $2^8 | C$; and $\Delta_1 = 9$, $\Delta_2 = 1$, $B_1 = 0$, $B_2 = -2$, $C_1 = 8$, $C_2 = 2$ gives $A \equiv 192$, $B \equiv 144$, $C \equiv 16$ all mod 2^8. It follows by an argument similar to the one used to prove $G \supset H_o$ that $[G_1,G_1]$ contains all σ with $\Delta = 1$, $16|C$, $2^7|(B-C)$ and $2^7|(A-4C)$. Conversely one shows that these conditions are implied by (41), so that they specify $[G_1,G_1]$ precisely. In particular $[G_1,G_1]$ contains all σ with $\Delta = 1$ and A,B,C all divisible by 2^7; so to find $[G_{13},G_{13}]$ and $[G_{15},G_{15}]$ we need only find which cosets are allowed by (41). On the one hand we find that $\Delta_1 \equiv \Delta_2 \equiv 5 \bmod 8$ gives all the residue classes with $8|C$, $B \equiv 5C \bmod 64$, and $\Delta_1 \equiv 1$, $\Delta_2 \equiv 5 \bmod 8$ gives nothing more; so these congruences specify $[G_{15},G_{15}]$. On the other hand $\Delta_1 \equiv \Delta_3 \equiv 3 \bmod 8$ gives all the residue classes with $4|C$, $B \equiv 3C \bmod 32$, and $\Delta_1 \equiv 1$, $\Delta_2 \equiv 3 \bmod 8$ gives nothing more; so these congruences specify $[G_{13},G_{13}]$. We sum up these results as

THEOREM 7: _The commutator subgroup of_ G _is_ $G \cap SL_2(\mathbb{Z}_2)$. _The commutator subgroups of_ G_1, G_{13}, G_{15}, _and_ G_{17} _consist of the_ σ _satisfying additional conditions as follows_.

$$G_1 \; : \; 2^4|C, \quad 2^7|(B-C), \quad 2^7|(A-4C).$$

$$G_{13} \; : \; 4|C, \quad 2^5|(B-3C).$$

$$G_{15} \; : \; 2^3|C, \quad 2^6|(B-5C).$$

$$G_{17} \; : \; 4|B \; .$$

REFERENCES

[1] M.H. ASHWORTH: Congruence and identical properties of modular forms. (D.Phil.Thesis, Oxford, 1968)

[2] Z.I. BOREVIC and I.R. SAFAREVIC: Number theory. (English translation, New York, 1966)

[3] P. DELIGNE: Formes modulaires et représentations ℓ-adiques. (Séminaire Bourbaki, 355, February 1969)

[4] J. IGUSA: Class number of a definite quaternion algebra with prime discriminant, Proc.Nat.Acad.Sci. USA 44 (1958), 312-314.

[5] F. KLEIN: Vorlesungen über das Ikosaeder und die Auflösung der Gleichungen vom fünften Grade. (Leipzig, 1884)

[6] O. KOLBERG: Congruences for Ramanujan's function $\tau(n)$, Arbok Univ. Bergen (Mat.-Naturv.Serie) 1962, No.12.

[7] D.H. LEHMER: Notes on some arithmetical properties of elliptic modular functions. (Duplicated notes, Univ. of California at Berkeley, not dated)

[8] S. RAMANUJAN: On certain arithmetical functions, Trans.Camb. Phil.Soc. 22 (1916), 159-184.

[9] J.-P. SERRE: Une interprétation des congruences relatives à la fonction τ de Ramanujan. (Séminaire Delange-Pisot-Poitou, 1967-68, exposé 14)

[10] J.-P. SERRE: Abelian ℓ-adic representations and elliptic curves. (New York, 1968)

[11] J.-P. SERRE: Congruences et formes modulaires. (Séminaire Bourbaki, 416, June 1972)

[12] A. WEIL: Über die Bestimmung Dirichletscher Reihen durch Funktionalgleichungen, Math.Ann. 168 (1967), 149-156.

[13] J.R. WILTON: Congruence properties of Ramanujan's function $\tau(n)$, Proc.Lond.Math.Soc. 31 (1930), 1-10.

The U_p operator of Atkin on modular functions of level 2 with growth conditions

B. Dwork

International Summer School on Modular Forms

ANTWERP 1972

The U_p operator of Atkin on modular functions of level 2 with growth conditions

B. Dwork

Let p be an odd prime, $p \neq 3$, and let g be the polynomial defined by

$$(1) \qquad (-1)^{(p-1)/2}\, g(\lambda) = \sum_{j=0}^{(p-1)/2} ((\tfrac{1}{2})_j/j!)^2 \lambda^j$$

so that $g(\lambda)$ is the standard formula for the Hasse invariant of the elliptic curve

$$(2) \qquad Y^2 = X(X-1)(X-\lambda) .$$

We shall follow in general the notation of our article [3]. In terms of q-expansions, Atkin [1] has defined the transformation

$$U_p : \Sigma\, a_m q^m \longrightarrow \Sigma\, a_{mp} q^m$$

but without the imposition of growth conditions one may construct eigenvectors with quite arbitrary eigenvalues; indeed formally, for any field element γ,

$$\theta_j = \sum_{s=0}^{\infty} \gamma^s q^{p^s}$$

is trivially eigenvector for eigenvalue γ. Thus to obtain an interesting theory we impose the restriction that U_p be applied to functions satisfying certain growth conditions. To explain these conditions for each pair of positive real numbers b_1, b_2, let $L(b_1,b_2)$ be the space of all functions holomorphic and bounded on the set M_{b_1,b_2} consisting of all λ such that

$$(3) \qquad \begin{aligned} &b_1 > \operatorname{ord} g(\lambda) \\ &b_2 > \operatorname{Max}\{\operatorname{ord}\lambda\ ,\ \operatorname{ord}(1-\lambda),\ \operatorname{ord}\lambda^{-1}\} . \end{aligned}$$

Let φ be the Tate-Deligne lifting of Frobenius. We give two descriptions. Let $F_p(X,Y)$ be the modular equation satisfied by $(\lambda(\tau), \lambda(p\tau))$. For ord $g(\lambda) = 0$, $\varphi(\lambda)$ is uniquely characterized by the properties

$$(4) \qquad \begin{aligned} &F_p(\lambda, \varphi(\lambda)) = 0 \\ &|\varphi(\lambda) - \lambda^p| < 1 . \end{aligned}$$

The function $\lambda \longrightarrow \varphi(\lambda)$ is extended (by p-adic analytic continuation) to an element of $L(b_1,b_2)$ for $b_1 = p/(p+1)$ and all $b_2 > 0$. A purely analytic description of φ may also be given (independent of the modular equation). Let F denote the hypergeometric functions $F(\frac{1}{2}, \frac{1}{2}, 1, \lambda)$, let F^φ denote the composition of F with φ. Let f be the function $(-1)^{(p-1)/2} F/F^\varphi$. If φ is chosen so that $\varphi-\lambda^p$ is holomorphic and bounded by p^e on the Hasse domain $\{\lambda \mid |g(\lambda)| = 1\}$, for some rational $e > 1/(p-1)$, then f has an analytic continuation to that set. The Deligne-Tate mapping is characterized by the further condition that f have analytic continuation in an annulus of at least one of the $(p-1)/2$ disjoint disks whose images in the residue class field are zeros of the Hasse invariant, g. For $\xi \in L(b_1/p, b_2/p)$, $b_1 \leq p/(p+1)$, we define $\psi \xi$, an element of $L(b_1,b_2)$, by the formula

$$(5) \qquad (\psi\xi)(\lambda) = \Sigma\ \xi(x)/\varphi'(x) ,$$

the sum being over the p solutions of the equation

$$(6) \qquad \varphi(x) = \lambda .$$

We now fix $b_1 = p/(p+1)$ and note that U_p coincides on $L(b_1,b_2)$ with $\psi \circ (\varphi'/p)$, the composition of ψ with the operation of multiplication by $p^{-1}\varphi'$. In the following we interpret U_p to mean just this mapping, it not being necessary to specify b_2. The eigenvectors are independent of the choice of b_2 since U_p maps $L(b_1,b_2)$ into $L(b_1, pb_2)$. We know that

U_p is completely continuous, that the Fredholm determinant, $\det(I-t\,U_p)$ is entire and that the constant function 1 is eigenvector with eigenvalue 1. Discarding this root as trivial, we assert:

Lemma 1. The number of non-trivial unit roots of the Fredholm determinant of U_p is at most $(p-1)/2$.

Proof. We examine the infinite matrix representing U_p relative to an orthonormal basis. For $1 \leq i \leq (p-1)/2$ let a_i be an unramified representative of each of the distinct residue classes satisfying $|g(\lambda)| < 1$. For $n > 0$ let

$$(7) \qquad t_n = \begin{cases} 1 & \\ p^{-1/(p+1)} & \text{if} \\ p^{-2/(p+1)} & \end{cases} \left.\begin{matrix} n \not\equiv 0, -1 \\ n \equiv 0 \\ n \equiv -1 \end{matrix}\right\} \bmod p+1$$

For $n > 0$, $1 \leq i \leq (p-1)/2$ let

$$(8) \qquad \begin{cases} e_{i,n} = (\lambda - a_i)^{-n} \\ \bar{e}_{i,n} = p^{nb_1} e_{i,n} \\ e_n^{(i)} = \bar{e}_{i,n} t_n \end{cases}$$

For reasons indicated above we may disregard basis elements of $L(b_1,b_2)$ corresponding to the singularities at $0, 1, \infty$. Since $\{\bar{e}_{i,n}\}$ is an orthonormal basis, a matrix suitable for our computations may be found by writing

$$(9) \qquad U_p \bar{e}_{i,n} = \sum_{j=1}^{(p-1)/2} \sum_{s=1}^{\infty} \bar{B}_{(i,n),(j,s)} \bar{e}_{j,s} .$$

Since $p\,U_p$ may be viewed as a map of norm not greater than 1 from $L(b_1/p,\, b_2/p)$ into $L(b_1,b_2)$ and since $\{e_{i,n}\, p^{nb_1/p}\}$ is an orthonormal basis of $L(b_1/p,\, b_2/p)$, we conclude, using $\bar{e}_{i,n} = p^{nb_1(1-p^{-1})} e_{i,n}\, p^{nb_1/p}$, that

(10) $$\text{ord } \overline{B}_{(i,n),(j,s)} \geq nb_1(1-p^{-1}) - 1 = n\,\frac{p-1}{p+1} - 1 .$$

However U_p is defined over Q_p and hence relative to the basis $\{e_{i,n}\}$, the matrix coefficients are unramified over Q_p and hence have ordinals which lie in $\mathbf{Z}$. It follows that

(11) $$\text{ord } \overline{B}_{(i,n),(j,s)} \equiv \frac{s-n}{p+1} \mod \mathbf{Z} .$$

We may use the basis $\{e_n^{(i)}\}$ for our computation. An easy argument gives

(12) $$U_p\, e_n^{(i)} = \sum_{j=1}^{(p-1)/2} \sum_{s=1}^{\infty} B_{(i,n),(j,s)}\, e_s^{(j)}$$

where

(13) $$B_{(i,n),(j,s)} = \overline{B}_{(i,n),(j,s)}\, t_n/t_s .$$

An elementary computation shows that this matrix has integral coefficients and that its image in the residue class field has rank of at most $(p-1)/2$. Indeed for $n \geq 3$, by equations (10), (13), (7) we have

$$\text{ord } B_{(i,n),(j,s)} \geq 3\,\frac{p-1}{p+1} - 1 + \text{ord } t_n - \text{ord } t_s$$

$$\geq 3\,\frac{p-1}{p+1} - 1 - \frac{2}{p+1} = \frac{2(p-3)}{p+1} > 0 .$$

For $n = 2$, we see that $n \not\equiv 0, -1 \mod p+1$ and hence $\text{ord } t_n = 0$. Thus

$$\text{ord } B_{(i,2),(j,s)} \geq 2\,\frac{p-1}{p+1} - 1 > 0 .$$

For $n = 1$, we have by equations (13), (11), (10),

$$\text{ord } B_{(i,1),(j,s)} = \text{ord } \overline{B}_{(i,1),(j,s)} - \text{ord } t_s$$

(15) $$\text{ord } \overline{B}_{(i,1),(j,s)} \equiv \frac{s-1}{p+1} \mod \mathbf{Z}$$

$$\text{ord } \overline{B}_{(i,1),(j,s)} \geq -\frac{2}{p+1} .$$

It follows that ord $\bar{B}_{(i,1),(j,s)}$ is non-negative unless $s \equiv 0, -1 \bmod p+1$. It follows that the matrix B has integral coefficients and units can occur only in the $(p-1)/2$ rows indexed by $(i,1)$, $1 \leq i \leq (p-1)/2$. This completes the proof of the lemma.

It may be of interest to estimate the Newton polygon of the Fredholm determinant of U_p by this method.

We now compute the number of unit eigenvalues by means of the trace formulae of Reich and Monsky (cf.[3, equation 16]). Thus

$$\text{(16)} \qquad \operatorname{Tr} U_p = \Sigma \frac{\varphi'/p}{\varphi'-1} ,$$

the sum being over all $\lambda \neq 0, 1, \infty$, $|g(\lambda)| = 1$, such that $\varphi(\lambda) = \lambda$. Since $\varphi'/p = (w/w^{\varphi})/(f(\lambda))^2$, where w is the wronskian $1/\lambda(1-\lambda)$ and since we are summing over fixed points of φ, we see that

$$\text{(17)} \qquad \operatorname{Tr} U_p = \Sigma \, (p^2-f)^{-1} .$$

More generally for $s \geq 1$,

$$\text{(18)} \qquad \operatorname{Tr} U_p^s = \Sigma \, (p^s - f^{2(1+\varphi+\dots+\varphi^{s-1})})^{-1} ,$$

the sum being over all fixed points of φ^s and excluding points lying near $0, 1, \infty$ and excluding representatives of supersingular moduli.

Thus modulo p, we have, since $f \equiv g \bmod p$,

$$\text{(19)} \qquad \operatorname{Tr} U_p^s \equiv -\Sigma \, 1/(g(\lambda)g(\lambda^p)\dots g(\lambda^{p^{s-1}}))^2 ,$$

the sum being over all $\lambda \in \mathbb{F}_{p^s}$ such that

$$\lambda(\lambda-1)g(\lambda) \neq 0 .$$

We now use an observation of N. Katz; for $\lambda \in \mathbb{F}_{p^s}$, $g(\lambda) \neq 0$, we see that $g(\lambda)g(\lambda^p)\dots g(\lambda^{p^{s-1}})$ lies in $\mathbb{F}_p^*$ and hence the reciprocal of its square coincides with its $(p-3)$ power. Thus

(20) $$\operatorname{Tr} U_p^s \equiv -\Sigma \left(g(\lambda)g(\lambda^p)\ldots g(\lambda^{p^{s-1}})\right)^{p-3} ,$$

the sum now being over all elements of $\mathbb{F}_{p^s}$ other than $0, 1$ since the supersingular moduli now contribute nothing to the sum. Since $g(1) = 1$, we have

(21) $$\operatorname{Tr} U_p^s = 1 - \Sigma \left(g(\lambda)g(\lambda^p)\ldots g(\lambda^{p^{s-1}})\right)^{p-3} ,$$

the sum being over all $\lambda \in \mathbb{F}^*_{p^s}$. We now use the symbol ψ to denote the endomorphism

(22) $$\Sigma\, a_m\lambda^m \longrightarrow \Sigma\, a_{mp}\lambda^m$$

of elements of say $\mathbb{F}_p[\lambda]$. We know [2, §3]

(23) $$\xi \longrightarrow \psi(g^{p-3}\xi)$$

is an endomorphism of $\mathbb{F}_p[\lambda]$ with trace given by the formula

(24) $$(p-1)\operatorname{Tr} \psi\circ g^{p-3} = \Sigma\, g(\lambda)^{p-3} ,$$

the sum being over $\mathbb{F}_p^*$. More generally

(25) $$(p^s-1)\operatorname{Tr}(\psi\circ g^{p-3})^s = \Sigma \left(g(\lambda)\ldots g(\lambda^{p^{s-1}})\right)^{p-3} ,$$

the sum now being over $\mathbb{F}^*_{p^s}$. Thus

(26) $$\operatorname{Tr} U_p^s \equiv 1 + \operatorname{Tr}(\psi\circ g^{p-3})^s .$$

We now compute the Fredholm determinant of U_p but since we need the exponential of terms with denominators, we obtain results only modulo p and t^p, i.e. using $\det(I-t\,U_p)$ to denote the reduction mod p of the Fredholm determinant of U_p,

(27) $$\det(I-t\,U_p) \equiv (1-t)\det(I-t\,\psi\circ g^{p-3}) \bmod (p,t^p) .$$

By Lemma 1, the left side is a polynomial of degree not greater than $1 + \frac{p-1}{2}$.

It is well known [2, §3] that in computing the characteristic polynomial of $\psi\circ g^{p-3}$ we may restrict the operator to polynomials of degree not greater than $(p-1)^{-1} \deg g^{p-3} = (p-3)/2$. Thus $\psi\circ g^{p-3}$ operates on a space of dimension $(p-1)/2$ and hence both sides of equation (27) have degree bounded by $(p+1)/2$ and so

$$(\det(I-t\ U_p))/(1-t) \equiv \det(I-t\ \psi\circ g^{p-3}) \bmod p\ . \tag{28}$$

__Theorem.__ The degree of each side of equation (28) is $(p-1)/2$.

__Proof.__ It is enough to show that $\psi\circ g^{p-3}$ is invertible as endomorphism of the space of polynomials of degree not greater than $(p-3)/2$ in $\mathbb{F}_p[\lambda]$. Thus let ξ be an element $\mathbb{F}_p[\lambda]$ of degree not greater than $(p-3)/2$ such that

$$\psi(\xi g^{p-3}) = 0\ . \tag{29}$$

We assert that $\xi = 0$. If ξ were of degree $(p-3)/2$ then the degree of ξg^{p-3} would be $\frac{p-3}{2} + (p-3)\frac{p-1}{2} = \frac{p-3}{2}$ and hence the left hand side of equation (29) would have degree $(p-3)/2$ contrary to hypothesis. Thus we have shown that

$$\deg \xi \leq (p-5)/2\ . \tag{30}$$

We may extend ψ from $\mathbb{F}_p[\lambda]$ to $\mathbb{F}_p(\lambda)$ and conclude from (29) since $g(\lambda)^p \equiv g(\lambda^p) \bmod p$ that

$$\psi(\xi/g^3) = 0\ . \tag{31}$$

Let a be a zero of g, since the zeros of g are simple, we see that the principal part of ξ/g^3 at a is of the form

$$v_a = \frac{\alpha_1}{\lambda-a} + \frac{\alpha_2}{(\lambda-a)^2} + \frac{\alpha_3}{(\lambda-a)^3} \tag{32}$$

and since the degree of ξ is strictly bounded by that of g^3, we conclude that ξ/g^3 is indeed equal to the sum of $(p-1)/2$ such partial fractions.

By an elementary computation for $p \geq c$, we have if $a \neq 0$

$$(33) \qquad \psi \frac{1}{(\lambda-a)^c} = -\frac{a^p}{(-a)^c\ (\lambda-a^p)}$$

and thus

$$(34) \qquad \psi(v_a) = -\frac{a^p}{\lambda-a^p}\left(\frac{\alpha_1}{-a} + \frac{\alpha_2}{(-a)^2} + \frac{\alpha_3}{(-a)^3}\right).$$

From this computation we deduce the partial fraction decomposition of $\psi(\xi/g^3)$ and thus by (31),

$$(35) \qquad a^2\alpha_1 - a\alpha_2 + \alpha_3 = 0 .$$

We now compute $\alpha_1, \alpha_2, \alpha_3$ explicitly. Let $t = \lambda-a$, put

$$(36) \qquad g(\lambda) = tg'(a)(1+tX + t^2Y) + (t^4)$$

where

$$(37) \qquad \begin{aligned} X &= \tfrac{1}{2}\left(\tfrac{g''}{g'}\right)(a) \\ Y &= \tfrac{1}{6}\left(\tfrac{g'''}{g'}\right)(a) \end{aligned}$$

Putting

$$(38) \qquad \xi(\lambda) = \xi + t\xi + \frac{1}{2}t^2\xi'' + (t^3) ,$$

where ξ, ξ', ξ'' refer to the value at a, we obtain (as relation between triples)

$$(39) \qquad (g'(a))^3(\alpha_3,\alpha_2,\alpha_1) = (\xi, \xi' - 3X\xi, \xi''\tfrac{1}{2} - 3X\xi' + \xi(6X^2 - 3Y)) .$$

Equation (35) now assumes the form,

$$(40) \qquad 0 = \xi - a(\xi' - 3X\xi) + a^2(\tfrac{\xi''}{2} - 3X\xi' + \xi(6X^2 - 3Y)) .$$

We now compute X, Y by means of the 2nd order linear differential operator

$$(41) \qquad \ell = D^2 + \rho D + \sigma$$

which annihilates g. (Here $\sigma = -1/4\lambda(1-\lambda)$, $\rho = (1-2\lambda)/\lambda(1-\lambda)$). We obtain

$$(42) \qquad X = -\frac{1}{2}\rho \qquad Y = \frac{\rho^2 - \rho' - \sigma}{6}$$

both to be evaluated at a, the zero of g under consideration. We may now deduce from (40) that if H denotes the linear differential operator

$$(43) \qquad H_\ell = \frac{\lambda^2}{2} D^2 - \lambda(1 - \frac{3\lambda\rho}{2})D + (1 - \frac{3\lambda\rho}{2} + (\rho^2 + \frac{\rho'+\sigma}{2})\lambda^2)$$

then

$$(H_\ell \xi)(a) = 0$$

for each zero, a, of g. This means that

$$(44) \qquad H_\ell \xi \equiv 0 \bmod g .$$

For σ and ρ as indicated, H_ℓ assumes the form λH where

$$(45) \qquad H = 4\lambda(\lambda-1)^2 D'' + 4(\lambda-1)(4\lambda-1)D + (9\lambda-5) .$$

Using equation (30),

$$\deg H(\xi) \leq \deg \xi + 1 \leq (p-3)/2$$

and hence equation (44) implies (since λ does not divide g)

$$(46) \qquad H(\xi) = 0 .$$

The indicial polynomial at infinity of H shows that

$$\deg \xi \equiv -3/2 \bmod p$$

but degree $\xi < p$, hence

$$\text{degree } \xi = (p-3)/2 ,$$

contradicting equation (30). This completes the proof of the theorem.

Note. 1. The relations between ℓ and H_ℓ as given by equation (43) may be restated. Let W_ℓ/λ be the wronskian of ℓ , then

$$H_\ell = \frac{\lambda^2}{2} W_\ell \circ \ell \circ W_\ell^{-1} .$$

Thus aside from the factor λ^2 , H is simply a twisted form of ℓ .

2. The computation of the number of unit roots of U_p in the case of level 1 is sometimes referred to as "the" Atkin's conjecture.

We apologize to the reader for forgetting to correct an error in exposition pointed out some time ago by J.-P. Serre. Equations (9) and (10) are correct as stated but $\{\bar{e}_{i,n}\}$ is not an ortho-normal basis of $L(b_1, b_2)$ which is of type $b(I)$ in the notation of Serre, IHES No. 12, §2. However U_p is a completely continuous endomorphism and its Fredholm determinant may be calculated by means of the matrix $(\bar{B}_{(i,n), (j,s)})$ which indeed may be identified with the matrix of the endomorphism, U, of the corresponding $c(I)$ space chosen such that U_p is the dual of U .

Alternately we may avoid dual spaces, replace the strict inequalities of equation (3) by non-strict inequalities so that $L(b_1, b_2)$ becomes a $c(I)$ type space. But with this choice we must take b_1 strictly less than $p/(p+1)$ and make corresponding changes in the definition of t_n (equation (7)) for $n \equiv 0, -1$ and let b_1 be sufficiently close to $p/(p+1)$.

References

1. Atkin, A. O. Congruence Hecke operators, Proc. Symp. Pure Math. 12, pp.33-40.
2. Dwork, B. Amer. J. Math. 82(1960), pp.631-648.
3. Dwork, B. Inv. Math. 12(1971), pp.249-256.

Institut des Hautes Etudes Scientifiques
Princeton University

P-ADIC PROPERTIES OF MODULAR SCHEMES AND MODULAR FORMS

Nicholas M. Katz

International Summer School on Modular Functions
ANTWERP 1972

TABLE OF CONTENTS

List of Notations

1.0	$\underline{\omega}_{E/S}$
1.1	Tate(q), ω_{can}, $S(R_0,1,k)$
1.2	$_nE, \alpha_n$; $S(R_0,n,k)$
1.3	$\Gamma_0(p)$
1.4	$M_n, \overline{M}_n$
1.9	$S(K,n,k)$
1.11	T_ℓ
2.0	A
2.1	E_{p-1}, E_k
2.2	$M(R_0r,n,k)$, $S(R_0,r,n,k)$
2.6	$B(n,k,j)$, $B(R_0,n,k,j)$, $B^{rigid}(R_0,r,n,k)$
2.8	P, P_1 (projectors)
2.9	$M_n(R_0,r)$, $\overline{M}_n(R_0,r)$
3.1	H,Y
3.3	φ
3.4	F,V
3.11	tr φ, U
4.1	$W_n(k)$, φ, S_n
4.2	S_m^ζ , $\overline{S}_m^\zeta$
4.4	G_χ^*, Ramanujan's series P
A1.1	
A1.2	H^1_{DR} ; ω, η
A1.3	∇ , Weierstrass's ζ
A1.4	θ, ∂
A2.1	$F(\varphi)$
A2.2	ω_{can} , η_{can}

(In 1)

Introduction

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

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

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

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

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

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

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

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

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

In the first appendix, which is a sort of "chapter zero", we explain the relation between the classical approach to elliptic curves via their period lattices and the "modern" one, the relation of DeRham cohomology of elliptic curves to modular forms, and the relation between the Gauss-Manin connection, Ramanujan's function P(q), and Serre's ∂-operator on modular forms. The results are due to Weierstrass and Deligne. It is concluded by a "table" of formulas.

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

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

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

Chapter 1: Moduli schemes and the q-expansion principle

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

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

$$\begin{tikzcd} E \arrow[d, "p"'] \\ S \arrow[u, bend right, "e"'] \end{tikzcd}$$

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

1.1 Modular forms of level 1

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

1. $f(E/S)$ depends only on the S-isomorphism class of the elliptic curve E/S.

2. The formation of $f(E/S)$ commutes with arbitrary change of base $g: S' \longrightarrow S$ (meaning that $f(E_{S'}/S') = g^*f(E/S)$).

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

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

1. $f(E/R,\omega)$ depends only on the R-isomorphism class of the pair $(E/R,\omega)$.

2. f is homogeneous of degree $-k$ in the "second variable"; for any $\lambda \in R^{\times}$ (the multiplicative group of R), $f(E,\lambda\omega) = \lambda^{-k}f(E,\omega)$.

3. The formation of $f(E/R,\omega)$ commutes with arbitrary extension of scalars $g\colon R \longrightarrow R'$ (meaning $f(E_{R'}/R',\omega_{R'}) = g(f(E/R,\omega))$).

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

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

valid whenever $S = \mathrm{Spec}(R)$ and $\underline{\omega}_{E/R}$ is a <u>free</u> R-module, with basis ω .)

If, in the preceding definitions we consider <u>only</u> schemes S (or rings R) lying over a <u>fixed</u> ground-ring R_0 , and only changes of base by R_0-morphisms, we obtain the notion of a modular form of weight k and level one defined over R_0 , the R_0-module of which is noted $M(R_0,1,k)$.

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

The <u>q-expansion</u> of a modular form f is by definition the finite-tailed Laurent series

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

The modular form f is called <u>holomorphic</u> at ∞ if its q-expansion lies in the subring $\mathbf{Z}[[q]]\otimes_{\mathbf{Z}} R_0$; the module of all such is noted $S(R_0;1,k)$. Notice that the q-expansion lies in $\mathbf{Z}((q))\otimes_{\mathbf{Z}} R_0 \subset R_0((q))$, i.e., it is <u>finite</u> R_0-linear combination of elements of $\mathbf{Z}((q))$. This implies, for example, that if R_0 is the field of fractions of a discrete valuation ring, then the q-expansion coefficients of any modular form of weight k and level one over R_0

have <u>bounded</u> denominators.

1.2. Modular forms of level n

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

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

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

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

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

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

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

1.2.1 $$f((\mathrm{Tate}(q^n), \omega_{can}, \alpha_n)_{R_o}) \in \mathbf{Z}((q)) \otimes_{\mathbf{Z}} R_o$$

obtained by varying α_n over all the level n structures.

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

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

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

1.3. Modular forms on $\Gamma_o(p)$

Analogously, for an integer $n \geq 1$ and a prime number $p \nmid n$, a modular form of weight k and level n on $\Gamma_o(p)$ is a rule f which assigns to each triple $(E/S, \alpha_n, H)$ consisting of an elliptic curve, a level n structure, and a finite flat subgroup-scheme $H \subset E$ of rank p , a section $f(E/S, \alpha_n, H)$ of $(\underline{\omega}_{E/S})^{\otimes k}$ over S , which depends only on the isomorphism class of $(E/S, \alpha_n, H)$, and whose formation commutes with arbitrary change of base $S' \longrightarrow S$. Equivalently, it is a rule which assigns to each quadruple $(E/R, \omega, \alpha_n, H)$ an element $f(E/R, \omega, \alpha_n, H) \in R$, which depends only on the isomorphism class of the quadruple, whose formation commutes with arbitrary change of base, and which is homogeneous of degree $-k$ in the second variable. As before, we define the notion of a modular form of weight k and level n on $\Gamma_0(p)$ being defined over a ring R_0.

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

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

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

For each integer $n \geq 3$, the functor "isomorphism classes of elliptic curves with level n structure" is representable, by a scheme M_n which is an affine smooth curve over $\mathbf{Z}[\frac{1}{n}]$, finite and flat of degree $= \#(GL_2(\mathbf{Z}/n\mathbf{Z})/\pm 1)$ over the affine j-line $\mathbf{Z}[\frac{1}{n}, j]$, and étale over the open set of the affine j-line where j and j-1728 are invertible. The normalization of the projective j-line $\mathbb{P}^1_{\mathbf{Z}[1/n]}$ in M_n is a proper and smooth curve $\overline{M}_n$ over $\mathbf{Z}[1/n]$, the global sections of whose structural sheaf are $\mathbf{Z}[1/n,\zeta_n]$. The curve $M_n \otimes_{\mathbf{Z}[1/n]} \mathbf{Z}[1/n,\zeta_n]$ (resp. $\overline{M}_n \otimes_{\mathbf{Z}[1/n]} \mathbf{Z}[1/n,\zeta_n]$) is a disjoint union of $\varphi(n)$ affine (resp. proper) smooth geometrically connected curves over $\mathbf{Z}[1/n,\zeta_n]$, the partitioning into components given by the $\varphi(n)$ primitive n'th roots of one occurring as values of the e.m. pairing on the basis of ${}_nE$ specified by the level n structure. The scheme $\overline{M}_n - M_n$ over $\mathbf{Z}[1/n]$ is finite and étale, and over $\mathbf{Z}[1/n,\zeta_n]$, it is a disjoint union of sections, called the <u>cusps</u> of $\overline{M}_n$, which in a natural way <u>are</u> the set of isomorphism classes of level n structures on the Tate curve $\mathrm{Tate}(q^n)$ viewed over $\mathbf{Z}((q)) \otimes_{\mathbf{Z}} \mathbf{Z}[1/n,\zeta_n]$. The completion of $\overline{M}_n \otimes \mathbf{Z}[1/n,\zeta_n]$ along any of the cusps is isomorphic to $\mathbf{Z}[1/n,\zeta_n][[q]]$. The completion of the projective j-line $\mathbb{P}^1_{\mathbf{Z}[1/n,\zeta_n]}$ along ∞ is itself isomorphic to $\mathbf{Z}[1/n,\zeta_n][[q]]$, via the formula $j(\mathrm{Tate}(q)) = 1/q + 744 + \ldots$, and the endomorphism of $\mathbf{Z}[1/n,\zeta_n][[q]]$ arising from the projection $\overline{M}_n \longrightarrow \mathbb{P}^1$ is just given by $q \longmapsto q^n$. In fact, for each cusp, the inverse image of the <u>universal</u> elliptic curve with level n structure $(E/M_n, \alpha_n)$ over (the spectrum of) $\mathbf{Z}[1/n,\zeta_n]((q))$ (viewed as a punctured disc around the cusp) is isomorphic to the inverse image over $\mathbf{Z}[1/n,\zeta_n]((q))$ of the Tate curve $\mathrm{Tate}(q^n)$ with the level n structure corresponding to that cusp.

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

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

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

extends to an isomorphism

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

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

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

1.6. The q-expansion principle

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

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

Before proving it, we give the main corollary.

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

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

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

hence a cohomology exact sequence

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

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

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

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

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

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

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

is an isomorphism.

Proof. By standard base-changing theorems, it suffices to show that $H^1(\overline{M}_n, \underline{\omega}^{\otimes k}) = 0$. The isomorphism $(\underline{\omega})^{\otimes 2} \xrightarrow{\sim} \Omega^1_{\overline{M}_n/\mathbf{Z}[1/n]}(\log(\overline{M}_n - M_n))$, together with the fact that each connected component of $\overline{M}_n \otimes \mathbf{Z}[1/n, \zeta_n]$ contains at least one cusp, shows that for $k \geq 2$, the restriction of $(\underline{\omega})^{\otimes k}$ to each connected component of $\overline{M}_n \otimes \mathbf{Z}[1/n, \zeta_n]$ has <u>degree</u> strictly greater than $2g-2$, g the (common) genus of any of these components, and hence $H^1(\overline{M}_n, (\underline{\omega})^{\otimes k}) = 0$ by Rieman-Roch. For $3 \leq n \leq 11$, explicit calculation shows that $\underline{\omega}$ restricted to each connected component of $\overline{M}_n \otimes \mathbf{Z}[1/n, \zeta_n]$ has degree strictly greater than $2g-2$, and we conclude as before. QED

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

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

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

Proof. First we should remark that there are no non-zero modular forms of level two and odd weight k over R_o , because the automorphism "-1" of an elliptic curve transforms (E,ω,α_2) into $(E,-\omega,-\alpha_2)$, hence $f(E,\omega,\alpha_2) = f(E,-\omega,-\alpha_2)$, but $\alpha_2 = -\alpha_2$, hence $f(E,-\omega,-\alpha_2) = f(E,-\omega,\alpha_2) = (-1)^{-k} f(E,\omega,\alpha_2)$, hence $2f(E,\omega,\alpha_2) = 0$ for k odd .

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

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

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

is an isomorphism.

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

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

is an isomorphism. Thus it remains only to handle the passage from $\mathbf{Z}[1/6]$. But for any ring R , $S(R,1,k)$ is the fibre product of the diagram:

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

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

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

<u>1.9. Modular forms of level 1 and 2: q-expansion principle</u>

For $n = 1, 2$, and any $\mathbf{Z}[1/n]$-module K, we <u>define</u> a modular form of level n and weight k, holomorphic at ∞, with coefficients in K to be

for $n = 1$: an element of the fibre-product of the diagram

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

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

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

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

As a corollary of (1.6.1), we have

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

1.10. Modular schemes of level 1 and 2

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

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

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

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

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

Analogously for $n=2$, we define

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

$$\overline{M}_2 = \overline{M}_4/\text{the subgroup of } GL_2(\mathbf{Z}/4\,\mathbf{Z}) \text{ of matrices } \equiv I \bmod 2\,.$$

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

1.11. Hecke operators

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

If ω is a nowhere vanishing differential on E/R, then $\check{\pi}^*(\omega_{R'}) = \operatorname{trace}_\pi(\omega_{R'})$ is a nowhere vanishing differential on $E_{R'}/H$. If $\alpha_n\colon {}_nE \simeq (\mathbf{Z}/n\,\mathbf{Z})^2_R$ is a level n structure on E/R, there is unique level n structure $\pi(\alpha_n)$ on $E_{R'}/H$ such that the diagram

(1.11.0.0)
$$\begin{tikzcd} & (\mathbb{Z}/n\,\mathbb{Z})_{R'} & \\ {}_nE_{R'} \arrow[ur, "\alpha_n"] \arrow[rr, "\pi"] & & {}_n(E_{R'}/H) \arrow[ul, "\pi(\alpha_n)"'] \end{tikzcd}$$

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

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

(1.11.0.1)
$$\sum_H f(E_{R'}/H, \check{\pi}^*(\omega), \pi(\alpha_n))$$

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

(1.11.0.2)
$$(T_\ell f)(E/R, \omega, \alpha_n) = \ell^{k-1} \sum f(E_{R'}/H, \check{\pi}^*(\omega), \pi(\alpha_n)) ,$$

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

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

μ_ℓ, generated by ζ_ℓ

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

For the subgroup μ_ℓ, the quotient $\mathrm{Tate}(q^n)/\mu_\ell$ is $\mathrm{Tate}(q^{n\ell})$ (the projection induced by the ℓ'th power map on $\mathbb{G}_m$) and the <u>dual</u> isogeny consists of dividing

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

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

The quotient $\mathrm{Tate}(q^n)/\mu_\ell \simeq \mathrm{Tate}(q^{n\ell})$ may be viewed as obtained from $\mathrm{Tate}(q^n)$ by the extension of scalars $\varphi_\ell\colon \mathbf{Z}((q)) \longrightarrow \mathbf{Z}((q))$ sending $q \longmapsto q^\ell$. We denote by α'_n the unique level n structure on $\mathrm{Tate}(q^n)$ such that $\varphi_\ell^*(\alpha'_n) = \pi_\ell(\alpha_n)$, $\pi_\ell(\alpha_n)$ denoting the image of α_n by the _projection_ of $\mathrm{Tate}(q^n)$ onto $\mathrm{Tate}(q^n)/\mu_\ell \simeq \mathrm{Tate}(q^{n\ell})$.

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

Thus we have

$$
\begin{aligned}
f(\mathrm{Tate}(q^n)/\mu_\ell, \check{\pi}_\ell^*(\omega_{can}), \pi_\ell(\alpha_n)) &= f(\mathrm{Tate}(q^{n\ell}), \omega_{can}, \varphi_\ell^*(\alpha'_n)) \\
&= \varphi_\ell(f(\mathrm{Tate}(q^n), \omega_{can}, \alpha'_n)) .
\end{aligned} \tag{1.11.0.3}
$$

$$f(\mathrm{Tate}(q^n)/H_i, \check{\pi}_i^*(\omega_{can}), \pi_i(\alpha_n)) = f(\mathrm{Tate}((\zeta^i q^{1/\ell})^n), \ell\cdot\omega_{can}, \varphi_i^*(\pi_o(\alpha_n)))$$

$$(1.11.0.4) \qquad = \varphi_i(f(\mathrm{Tate}(q^{n/\ell}), \ell\cdot\omega_{can}, \pi_o(\alpha_n))$$

$$= \varphi_i\circ(i_\ell)^{-1}(f(\mathrm{Tate}(q^n), \ell\cdot\omega_{can}, \alpha_n''))$$

$$= \ell^{-1}\cdot\varphi_i\circ(i_\ell)^{-1}(f(\mathrm{Tate}(q^n), \omega_{can}, \alpha_n'')) .$$

Combining these, we have the following formula for T_ℓ .

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

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

Then

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

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

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

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

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

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

Proposition 1.11.3. Let $n \geq 2$ and $k \geq 2$, or $3 \leq n \leq 11$ and $k \geq 1$. For any prime ℓ not dividing n , and any $\mathbb{Z}[1/n]$-module K , there is a necessarily unique endomorphism of the space of modular forms of weight k and level n, holomorphic at ∞ , with coefficients in K , whose effect on q-expansions is that given by the formulas (1.11.1.0-2).

Proof. By the base-changing theorem, we are reduced to the case $K = \mathbf{Z}[1/n]$. For a modular form f over $\mathbf{Z}[1/n]$, T_ℓ exists à priori over $\mathbf{Z}[1/n\ell]$, but its q-expansions all have coefficients in $\mathbf{Z}[1/n,\zeta_n]$, so by (1.6.2) and (1.9.1), $T_\ell(f)$ is in fact a modular form over $\mathbf{Z}[1/n]$. QED

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

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

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

The desired T_ℓ is the fibre product of the T_ℓ constructed above on this diagram. QED

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

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

Result 1.12.0. Let $n \geq 1$ be an integer, K a field of characteristic $p \nmid n$, and f a modular form over K of level n and weight $k \geq 1$, holomorphic at infinity. Suppose $p-1 \nmid k$. Then if all the q-expansions of f at the cusps of $\overline{M}_n \otimes K(\zeta_n)$ are <u>constants</u>, $f = 0$.

Using this result, we will now prove

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

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

Consider the finite-dimensional K-space V of such modular forms, and choose a basis $f_1,\ldots,f_r$ of V. Let N be the maximum of the degrees of the q-expansions of the f_i at any of the cusps. At each cusp, record the q-expansion of $F = \begin{pmatrix} f_1 \\ \vdots \\ f_r \end{pmatrix}$:

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

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

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

Passing to q-expansions gives the equation

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

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

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

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

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

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

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

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

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

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

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

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

Chapter 2: p-adic modular forms

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

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

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

An alternative method of establishing holomorphy is to use the fact that for any elliptic curve E/R over any base ring R, $H^1(E, \mathcal{O}_E)$ is the tangent space of E/R at the origin, which is to say the R-module of all translation-invariant derivations of E/R, and that when R is an $\mathbb{F}_p$-algebra, the action of F^*_{abs} on $H^1(E, \mathcal{O}_E)$ consists of taking the p'th iterate of an invariant derivation. Now we use the fact that there is a local parameter t on the completion of the Tate curve along its identity section in terms of which $\omega_{can} = dt/1+t$. Let D be the invariant derivation dual to ω_{can}. Then $D(t) = 1+t$, hence $D(1+t) = 1+t$, hence $D^n(1+t) = 1+t$ for all $n \geq 1$. Over $\mathbb{F}_p$, D^p is an invariant derivation, and it agrees with D on ω_{can}, hence $D^p = D$, hence $F^*_{abs}(\eta_{can}) = \eta_{can}$, and $A(\text{Tate }(q), \omega_{can}) = 1$.

2.1 <u>Deligne's congruence $A \equiv E_{p-1} \bmod p$</u>

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

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

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

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

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

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

2.2 p-adic modular forms with growth conditions

2.2.0 Let R_0 be a p-adically complete ring (i.e. $R_0 \simeq \varprojlim R_0/p^N R_0$), and choose an element $r \in R_0$. For any integer $n \geq 1$, prime to p, (resp. $3 \leq n \leq 11$ for $p=2$, and $n \geq 2$ for $p=2$) we define the module $M(R_0,r,n,k)$ of p-adic modular forms over R_0 of growth r, level n and weight k: An element $f \in M(R_0,r,n,k)$ is a rule which assigns to any triple $(E/S, \alpha_n, Y)$ consisting of:

(2.2.1) an elliptic curve E/S, where S is a R_0-scheme on which p is nilpotent (i.e. $p^N=0$ for $N \gg 0$);

(2.2.2) a level n structure α_n;

(2.2.3) a section Y of $\underline{\omega}^{\otimes(1-p)}$ satisfying $Y\cdot E_{p-1}=r$;

a section $f(E/S, \alpha_n, Y)$ of $(\underline{\omega}_{E/S})^{\otimes k}$ over S, which depends only on the isomorphism class of the triple, and whose formation commutes with arbitrary change of base of R_0-schemes $S' \longrightarrow S$.

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

(2.2.4) an elliptic curve E/R, R an R_0-algebra in which p is nilpotent;

(2.2.5) a base ω of $\underline{\omega}_{E/R}$;

(2.2.6) a level n-structure;

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

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

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

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

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

As formal consequence of the definitions, we have

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

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

2.3 <u>Determination of $M(R_o,r,n,k)$ when p is nilpotent in R_o</u>

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

$\mathcal{F}_{R_o,r,n}: S \longmapsto$ S-isomorphism classes of triples $(E/S, \alpha_n, Y)$ <u>is</u> the functor

$$\mathcal{F}_{R_o,r,n}: S \longmapsto \begin{cases} R_o\text{-morphisms } g: S \longrightarrow M_n \otimes R_o \text{ , together with a section} \\ Y \text{ of } g^*(\mathcal{L}) \text{ verifying } Y \cdot g^*(E_{p-1}) = r \end{cases}$$

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

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

This last functor is <u>representable</u>, by the $M_n \otimes R_o$-scheme

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

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

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

These $\tilde{g}_i$ piece together to define a morphism from S to $\underline{\mathrm{Spec}}\ (\underline{\mathrm{Symm}}(\check{\mathcal{L}}))$.

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

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

$$\begin{aligned} M(R_o,r,n,k) &= H^o(\underline{\mathrm{Spec}}_{M_n \otimes R_o}\ (\underline{\mathrm{Symm}}(\check{\mathcal{L}})(E_{p-1} - r),\ \underline{\omega}^{\otimes k}) \\ &= H^o(M_n \otimes R_o,\ \bigoplus_{j \geq o}\ (\underline{\omega})^{\otimes(k+j(p-1))}\Big/(E_{p-1} - r)) \\ \text{(because } M_n \text{ is affine)} &= H^o(M_n \otimes R_o,\ \bigoplus_{j \geq o}\ (\underline{\omega})^{\otimes(k+j(p-r))})\Big/(E_{p-1} - r) \\ &= \bigoplus_{j \geq o} M(R_o,\ n,\ k+j(p-1))\Big/(E_{p-1} - r)\ . \end{aligned}$$

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

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

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

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

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

Remark 2.4.1.1. Analogously to (2.3.1), we have

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

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

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

$$\varprojlim H^0(\overline{M}_n, \bigoplus_{j \geq 0} \underline{\omega}^{k+j(p-1)}) \underset{\mathbf{Z}[1/n]}{\otimes} (R_0/p^N R_0)/(E_{p-1} - r)$$

2.5.1.0

$$\downarrow$$

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

is an isomorphism.

Proof. Let $\mathcal{S}$ denote the quasicoherent sheaf $\bigoplus_{j \geq 0} \underline{\omega}^{k+j(p-1)}$ on $\overline{M}_n$, and put $\mathcal{S}_N = \mathcal{S} \otimes R_0/p^N R_0$. The inverse system of exact sequences

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

gives an inverse system of six-term cohomology sequences

2.5.1.2 $$\begin{aligned} 0 \longrightarrow H^0(\overline{M}_n, \mathcal{S}_N) \xrightarrow{E_{p-1} - r} H^0(\overline{M}_n, \mathcal{S}_N) \longrightarrow H^0(\overline{M}_n, \mathcal{S}_N/(E_{p-1} - r) \longrightarrow H^1(\overline{M}_n, \mathcal{S}_N) \longrightarrow \\ \xrightarrow{E_{p-1} - r} H^1(\overline{M}_n, \mathcal{S}_N) \longrightarrow H^1(\overline{M}_n, \mathcal{S}_N/(E_{p-1} - r)) \longrightarrow 0 . \end{aligned}$$

Suppose first that $k > 0$. Under our hypotheses, the base-changing theorem (1.7.1) applies, according to which $H^0(\overline{M}_n, \mathcal{S}_N) = H^0(\overline{M}_n, \mathcal{S}) \otimes (R_0/p^N R_0)$, and $H^1(\overline{M}_n, \mathcal{S}_N) = 0$. Thus the H^0 terms in (2.5.1.2) form a short exact sequence of inverse systems, the first of which has surjective transition morphisms. Hence the inverse limits of these inverse systems form the desired short exact sequence.

In case $k = 0$ and $p \neq 2$ or $k = 0$, $p = 2$ and $n \leq 11$, we have $H^1(\overline{M}_n, \underline{\omega}^{\otimes k}) = 0$ for $k \geq 1$, hence $H^1(\overline{M}_n, \mathcal{S}) = H^1(\overline{M}_n, \mathcal{O})$, and by (1.7.1)), $H^0(\overline{M}_n, \mathcal{S}_N) = H^0(\overline{M}_n, \mathcal{S}) \otimes R_0/p^N R_0$. The exact sequence (2.5.1.2) becomes

$$0 \longrightarrow H^0(\overline{M}_n, \mathcal{S}) \otimes R_0/p^N R_0 \longrightarrow H^0(\overline{M}_n, \mathcal{S}) \otimes R_0/p^N R_0 \longrightarrow H^0(\overline{M}_n, \mathcal{S}_N/(E_{p-1} - r)) \longrightarrow$$

$$\rightarrow H^1(\overline{M}_n, \mathcal{O}) \otimes R_0/p^N R_0 \xrightarrow{-r} H^1(\overline{M}_n, \mathcal{O}) \otimes R_0/p^N R_0 \longrightarrow H^0(\overline{M}_n, \mathcal{O}) \otimes R_0/(p^N, r) \longrightarrow 0 .$$

For variable N, these form a six-term exact sequence of inverse systems. If the sequence of their inverse limits were exact, the theorem would follow, because the map $\varprojlim H^0(\overline{M}_n, \mathcal{O}) \otimes R_0/p^N R_0 \xrightarrow{-r} \varprojlim H^0(\overline{M}_n, \mathcal{O}) \otimes R^0/p^N R_0$ is injective (this because $H^0(\overline{M}_n, \mathcal{O})$ is a finite free $\mathbb{Z}[1/n]$-module, and r is not a zero divisor in $R_0 \xrightarrow{\sim} \varprojlim R_0/p^N R_0$). To prove the exactness we apply a general lemma.

<u>Lemma 2.5.2.</u> Let $0 \longrightarrow K^0 \longrightarrow K^1 \longrightarrow K^2 \longrightarrow \ldots$ be a (long) exact sequence in the category of projective systems of abelian groups indexed by the positive integers. Suppose that for all $i \neq i_0$, the projective system K^i has surjective transition morphisms, and that the sequence

$\varprojlim K^{i_0+1} \longrightarrow \varprojlim K^{i_0+2} \longrightarrow \varprojlim K^{i_0+3}$ is exact. Then the sequence

$$0 \longrightarrow \varprojlim K^0 \longrightarrow \varprojlim K^1 \longrightarrow \varprojlim K^2 \longrightarrow \ldots$$

is exact.

<u>Proof.</u> Consider the 2 spectral sequences of hypercohomology for the functor $\varprojlim$.

$$_{I}E_2^{p,q} = H^p(R^q(\varprojlim)(K^\cdot)) \Longrightarrow \mathbb{R}^{p+q}(\varprojlim)(K^\cdot)$$

$$_{II}E_2^{p,q} = R^p(\varprojlim)(H^q(K^\cdot)) \Longrightarrow \mathbb{R}^{p+q}(\varprojlim)(K^\cdot)$$

By hypothesis, we have $_{II}E_2^{p,q} = 0$ for all values of q, hence $\mathbb{R}^n(\varprojlim)(K^\cdot) = 0$ for all n. According to ([48]), we have $R^i(\varprojlim) = 0$ for $i \geq 2$, hence $_{I}E_2^{p,q} = 0$ for $q \geq 2$. By ([48]), we have $R^1(\varprojlim)(K^i) = 0$ for $i \neq i_0$, hence

$$_{I}E_2^{p,q} = 0 \text{ unless } q = 0 \ \underline{\text{or}} \ q = 1 \text{ and } p = i_0 .$$

As we have also supposed that $_{I}E_2^{i_0+2,0} = 0$, we have degeneration: $E_2^{p,q} = E_\infty^{p,q}$ for all p,q. As $E_\infty^{p,q} = 0$ for all p,q, we get in particular $_{I}E_2^{p,0} = 0$ for all p, which is the desired conclusion. QED

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

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

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

admits a section.

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

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

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

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

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

$$2.6.1.2 \qquad H^o(\overline{M}_n, \underline{\omega}^{\otimes k+(j+1)(p-1)}) \simeq E_{p-1} \cdot H^o(\overline{M}_n, \underline{\omega}^{k+j(p-1)}) \oplus B(n,k,j+1)$$

and

$$2.6.1.3 \qquad H^o(\overline{M}_n, \underline{\omega}^{\otimes k}) \stackrel{\text{dfn}}{=\!=} B(n,k,o) .$$

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

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

2.6.1.3

$$\Sigma\, E_{p-1}^{j-a} b_a \longleftarrow \Sigma\, b_a \ .$$

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

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

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

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

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

2.6.2.1

$$\Sigma\, b_a \longrightarrow \text{"}\sum_{a \geq o} \frac{r^a \cdot b_a}{(E_{p-1})^a}\text{"}$$

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

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

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

Then $\sum_a s_a = \sum_a \sum_{i+j=a} (E_{p-1})^i b_j(a) = \sum_a \sum_{i+j=a} r^i b_j(a) +$

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

Corollary 2.6.3. Hypotheses as in (2.5.1), the canonical mapping $S(R_o,r,n,k) \longrightarrow S(R_o,1,n,k)$ defined modularly by composition with the transformation of functors: $(E/S, \alpha_n, Y) \longrightarrow (E/S, \alpha_n, rY)$, is injective; the corresponding map

$$B^{rigid}(R_o,r,n,k) \longrightarrow B^{rigid}(R_o,1,n,k)$$

is given by

$$\Sigma\, b_a \longrightarrow \Sigma\, r^a b_a .$$

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

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

(1) $f \in x \cdot S(R_o,1,n,k)$,

(2) the q-expansions of f all lie in $x \cdot R_o[\zeta_n][[q]]$,

(3) on each of the $\varphi(n)$ connected components of $\overline{M}_n \underset{\mathbb{Z}[1/n]}{\otimes} \mathbb{Z}[1/n,\zeta_n]$, there is at least one cusp where the q-expansion of f lies in $x \cdot R_o[\zeta_n][[q]]$.

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

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

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

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

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

1. The f_α are the q-expansions of an (necessarily unique) element $f \in S(R_o,1,n,k)$.

2. For every power p^N of p, there exists a positive integer $M \equiv 0 \bmod p^{N-1}$, and a "true" modular form $g_N \in S(R_o,n,k+M(p-1))$ whose q-expansions are congruent mod p^N to the given f_α.

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

(2) ===> (1). Multiplying necessary g_N by a power of $(E_{p-1})^{p^{N-1}}$, we may assume that the <u>weights</u> $k+M_N(p-1)$ of the g_N are <u>increasing</u> with N. Let $\Delta_N = M_{N+1} - M_N$. Then $(g_{N+1} - g_N \cdot (E_{p-1})^{\Delta_N})$ lies in $p^N \cdot S(R_0,n,k+M_{N+1}(p-1))$ by the q-expansion principle (1.6.2), hence $\sum_N (g_{N+1} - g_N \cdot (E_{p-1})^{\Delta_N})$ "converges" to an element of $S(R_0,1,n,k)$, whose q-expansions are congruent modulo p^N to those of g_N. QED

2.8. Bases for levels one and two

Suppose $p \neq 2,3$. Then E_{p-1} <u>is</u> a modular form of level <u>one</u> which lifts the Hasse invariant, and hence for any p-adically complete ring $R_0 \ni r$ and integer $n \geq 3$ prime to p, the group $GL_2(\mathbf{Z}/n\mathbf{Z})$ acts on the functor $\mathcal{F}_{R_0,r,n}$ [by $g(E/S, \alpha_n, Y) = (E/S, g\circ\alpha_n, Y)$ on the set $\mathcal{F}_{R_0,r,n}(S)$], hence on $M(R_0,r,n,k)$ and on $S(R_0,r,n,k)$. Clearly $M(R_0,r,1,k)$ is just the submodule $M(R_0,r,n,k)^{GL_2(\mathbf{Z}/n\mathbf{Z})}$ of <u>invariants</u> under this action, and $S(R_0,r,1,k)$ is the submodule $S(R_0,r,n,k)^{GL_2(\mathbf{Z}/n\mathbf{Z})}$ of $S(R_0,r,n,k)$. Now suppose $n=3$ <u>or</u> $n=4$. This choice has the advantage that $GL_2(\mathbf{Z}/n\mathbf{Z})$ then has order prime to p (because $p \neq 2,3$), and $P = \frac{1}{\#GL_2(\mathbf{Z}/n\mathbf{Z})} \Sigma g$ is then a <u>projection</u> onto the invariants. Using P we may also make the chosen section of (2.6.1.1) invariant by $GL_2(\mathbf{Z}/3\mathbf{Z})$, and define

$B(1,k,j) = B(n,k,j)^{GL_2(\mathbf{Z}/n\mathbf{Z})} = P(B(n,k,j))$,

$B(R_0,1,k,j) = B(1,k,j) \underset{\mathbf{Z}[1/n]}{\otimes} R_0 = B(R_0,n,k,j)^{GL_2(\mathbf{Z}/n\mathbf{Z})}$. Similarly, we define

$B^{\text{rigid}}(R_0,r,1,k) = P(B^{\text{rigid}}(R_0,r,n,k)) = (B^{\text{rigid}}(R_0,r,n,k))^{GL_2(\mathbf{Z}/n\mathbf{Z})}$; it is the subspace of $B^{\text{rigid}}(R_0,r,n,k)$ consisting of the elements $\Sigma\, b_a$ <u>each</u> of whose terms b_a is invariant by $GL_2(\mathbf{Z}/n\mathbf{Z})$.

Applying the projector P to (2.6.2) gives:

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

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

is an isomorphism.

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

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

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

is an isomorphism.

Applying the projectors P or P_1 to (2.7.1) gives

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

(1) $f \in x \cdot S(R_o,1,n,k)$,

(2) the q-expansions of f all lie on $xR_o[[q]]$.

2.9. Interpretation via formal schemes

Let $n \geq 3$, $p \nmid n$, R_o a p-adically complete ring, and $r \in R_o$. We denote by $M_n(R_o,r)$ (resp. $\overline{M}_n(R_o,r)$) the formal scheme over R_o given the compatible family of $R_o/p^N R_o$-schemes $\underline{\mathrm{Spec}}_{M_n \otimes R_o/p^N R_o}(\mathrm{Symm}(\check{\mathcal{L}})/(E_{p-1} - r))$ (resp. $\underline{\mathrm{Spec}}_{\overline{M}_n \otimes R_o/p^N R_o}(\mathrm{Symm}(\check{\mathcal{L}})/(E_{p-1} - r))$). We have

$$M(R_o,r,n,k) = H^0(M_n(R_o,r),\underline{\omega}^{\otimes k})$$

$$S(R_o,r,n,k) = H^0(\overline{M}_n(R_o,r),\underline{\omega}^{\otimes k}) .$$

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

Chapter 3. Existence of the Canonical Subgroup: Applications

In this chapter we study the "canonical subgroup" of an elliptic curve whose Hasse invariant is "not too near zero." For simplicity, we assume throughout this chapter that the groundring R_0 is a complete discrete valuation ring of residue characteristic p and generic characteristic zero. We normalize the ordinal function by requiring that $\mathrm{ord}(p) = 1$.

Theorem 3.1. (Lubin) I. Let $r \in R_0$ have $\mathrm{ord}(r) < p/p+1$. There is one and only one way to attach to every r-situation $(E/R, \alpha_n, Y)$ (R a p-adically complete R_0-algebra, $p \nmid n$, $n \geq 1$ if $p \neq 2,3$, $n \geq 3$ if $p = 2,3$, $Y \cdot E_{p-1} = r$) a finite flat rank p subgroup scheme $H \subset E$, called the canonical subgroup of E/R, such that:

> H depends only on the isomorphism class of $(E/R, \alpha_n, Y)$, and only on that of $(E/R, Y)$ if $p \neq 2,3$.
>
> The formation of H commutes with arbitrary change of base $R \longrightarrow R'$ of p-adically complete R_0-algebras.
>
> If $p/r = 0$ in R, H is the kernel of Frobenius: $E \longrightarrow E^{(p)}$.
>
> If E/R is the Tate curve $\mathrm{Tate}(q^n)$ over $R_0/p^N R_0((q))$, then H is the subgroup μ_p of $\mathrm{Tate}(q^n)$.

II. Suppose $r \in R_0$ has $\mathrm{ord}(r) < 1/p+1$. Then there is one and only one way to attach to every r-situation $(E/R, \alpha_n, Y)$ (R a p-adically complete R_0-algebra, $p \nmid n$, $n \geq 1$ if $p \neq 2,3$, $n \geq 3$ if $p = 2,3$, $Y\, E_{p-1} = r$) an r^p-situation $(E'/R, \alpha'_n, Y')$, where

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

such that

> Y' depends only on the isomorphism class of $(E/R, \alpha_n, Y)$, and only on that of $(E/R, Y)$ if $p \neq 2,3$.
>
> The formation of Y' commutes with arbitrary change of base $R \longrightarrow R'$ of p-adically complete R_0-algebras.
>
> If $p/r = 0$ in R , Y' is the inverse image $Y^{(p)}$ of Y on $E^{(p)} = E'$.

Before giving the proof, we give some applications.

<u>Theorem 3.2.</u> Suppose $n \geq 3$, $p \nmid n$. Let f be a modular form of level n and weight k on $\Gamma_0(p)$, defined over R_0 , and which is holomorphic at the unramified cusps of $\overline{M}_{n,p}$. There exists a (necessarily unique) element $\tilde{f} \in S(R_0,1,n,k)$ whose q-expansions at each cusp of $\overline{M}_n$ is that of $\tilde{f}$ at the overlying unramified cusp of $\overline{M}_{n,p}$. Furthermore, if $r \in R_0$ has $\mathrm{ord}(r) < p/p+1$, then in fact $\tilde{f} \in S(R_0,r,n,k)$.

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

<u>Theorem 3.3.</u> Suppose $n \geq 3$, $p \nmid n$, and that either $k \geq 2$ or $k=1$ and $n \leq 11$, or that $k=0$, $p \neq 2$, or that $k=0$, $p=2$ and $n \leq 11$. Let $r \in R_0$ have $\mathrm{ord}(r) < 1/p+1$. For any $f \in S(R_0,r^p,n,k)$, there is a unique element $\varphi(f) \in S(R_0,1,n,k)$ whose q-expansions are given by

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

[where π: $\mathrm{Tate}(q^n) \longrightarrow \mathrm{Tate}(q^{np})$ is the map "dividing by $\boldsymbol{\mu}_p$ ", and $\pi(\alpha_n)$ is the induced level n-structure]. Furthermore, $\varphi(f)\cdot(E_{p-1})^k \in S(R_0,r,n,pk)$.

<u>Proof.</u> Define $\varphi(f)(E/R,\omega,\alpha_n,Y) = f(E'/R, \check{\pi}^*(\omega),\alpha_n',Y')$, $[E'=E/H$, π: $E \longrightarrow E'$ is the projection]. This makes sense if $Y\cdot E_{p-1}=1$, for then $\check{\pi}$ is <u>étale</u> and so $\check{\pi}^*(\omega)$ is a nowhere vanishing differential on $E' = E/H$. To see that $E^k_{p-1}\cdot\varphi(f)$ actually lies in $S(R_0,r,n,kp)$, notice that its value on

$(E/R,\omega,\alpha_n,Y)$, $Y\cdot E_{p-1} = r^p$, is given formally by $(E_{p-1}(E/R,\omega,\alpha_n))^k\cdot f(E'/R,\check{\pi}^*(\omega),\alpha_n',Y')$. [In fact this expression has no meaning, because $\check{\pi}^*(\omega)$ may well <u>fail</u> to be nowhere-vanishing on E' .] However, if we write $\check{\pi}^*(\omega) = \lambda\cdot\omega'$ with $\lambda \in R$ and ω' nowhere-vanishing on E' , then

$$((E_{p-1})^k\cdot\varphi(f))(E/R,\omega,\alpha_n,Y) = \left(\frac{E_{p-1}(E/R,\omega,\alpha_n)}{\lambda}\right)^k\cdot f(E'/R,\omega',\alpha_n',Y') .$$

But a simple tangent calculation (cf. 3.6.5) shows that λ and E_{p-1} are essentially <u>equal</u>; they differ multiplicatively by a unit of R . By "reduction to the universal case", in which R is flat over $\mathbb{Z}_p$, we can make sense of the ratio E_{p-1}/λ , and interpret it as a <u>unit</u> in any R ; this permits us to define

$$(E_{p-1})^k\cdot\varphi(f)(E/R,\omega,\alpha_n,Y)) = \left(\frac{E_{p-1}(E/R,\omega,\alpha_n)}{\lambda}\right)^k f(E',\omega',\alpha_n',Y') . \qquad \text{QED}$$

<u>3.4 Construction of the canonical subgroup in case $r=1$</u>

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

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

3.6 Lemmas on the formal group

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

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

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

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

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

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

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

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

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

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

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

(2) Given any parameter X_o, there exists a (non-unique!) parameter $X = X_o$ + higher terms such that for any p-1'st root of unity $\zeta \in \mathbb{Z}_p$, we have $[\zeta](X) = \zeta X$.

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

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

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

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

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

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

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

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

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

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

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

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

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

We may summarize our findings in a proposition.

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

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

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

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

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

Suppose we are given $(E/R, \alpha_n, Y)$ with R a p-adically complete R_0-algebra, $n \geq 1$ if $p \neq 2,3$, $n \geq 3$ for $p = 2,3$, $Y \cdot E_{p-1} = r$, $\mathrm{ord}(r) < p/p+1$. Because it suffices to treat the case when p is nilpotent in R, we may, by ordinary localization on R, suppose that the formal group of E/R is given by a one-parameter formal group law over R, with formal paramter X; we denote by ω the "dual" differential. By reduction to the universal case, we may now reduce to the case when R is a flat $\mathbf{Z}_p$-algebra. By (3.6.2), we may suppose that $[\zeta](X) = \zeta X$ for all p-1'st roots of unity $\zeta \in \mathbf{Z}_p$. By (3.6.6), the endomorphism $[p]$ on the formal group looks like

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

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

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

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

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

suggests that in fact the equation for the orbits is

$$g(T) \overset{\mathrm{dfn}}{=\!=} p + aT + \sum_{m \geq 2} c_r T^m = 0 , \tag{3.7.2}$$

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

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

$$t_o = \frac{r_1 Y}{1+r_1 bY} \tag{3.7.4}$$

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

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

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

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

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

$$g_2(T) = 1 - T + \sum_{m\geq 2} d_m T^m , \tag{3.7.6.1}$$

with $d_m \in r_3 R$, and $d_m \to 0$ as $m \to \infty$.

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

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

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

Proof. Making the substitution $T = 1-S$, we introduce $h_1(S) = h(1-S) = e_0 + (1+e_1)S + \sum_{m \geq 2} e_m S^m$, with coefficients $e_i \in I$. For $s \in I$, $h_1(s) = h(1-s)$, so our problem is to show that h_1 has a unique zero s_∞ in I. For any $s \in I$, $h_1'(s) \in 1+I$, hence is invertible in R, while $h_1(s) \in I$. The Newton process of successive approximations: $s_0 = 0, \ldots, s_{n+1} = s_n - h_1(s_n)/h_1'(s_n)$ is easily seen to converge to a zero of h_1. If s and $s+\Delta$ are two zeros of h_1 in I, we have $0 = h_1(s+\Delta) = h_1(s) + h_1'(s)\cdot\Delta + (\Delta^2) = h_1'(s)\cdot\Delta + (\Delta^2)$, hence as $h_1'(s)$ is invertible, we have $\Delta \in (\Delta^2)$. Because $\Delta \in I$ and R is I-adically separated, this implies $\Delta = 0$. QED

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

3.8 The canonical subscheme is a subgroup

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

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

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

Because t_{can} lies in r_1R , it is topologically nilpotent in R , hence the R-algebra $\mathbf{A} = R[[X,Y]]/(X^p - t_{can}X, Y^p - t_{can}Y)$ is finite and free of rank p^2 with basis X^iY^j , $0 \leq i, j \leq p-1$. The condition that $G(X,Y)^p - t_\infty G(X,Y)$ vanish in $\mathbf{A}$ is simply that the p^2 "coefficients" $g_{ij} \in R$ defined by the equation

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

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

(3.9) We now turn to proving part II of 3.1, by constructing Y' . As before we may suppose R flat over $\mathbb{Z}_p$. Let $r \in R_o$ have $\mathrm{ord}(r) < 1/p+1$. Then $r_1 = p/r$ has $\mathrm{ord}(r_1) > p/p+1$, and hence r_1 is <u>divisible</u> by r^p , and $r_4 = r_1/r^p$ has $\mathrm{ord}(r_4) > 0$. Since $t_{can} \in r_1R$, modulo r_1R the canonical subgroup is just the kernel of $F: E \longrightarrow E^{(p)}$. Hence E' mod r_1R is $E^{(p)}$. Let ω' be any nowhere vanishing one-form on E' which reduces modulo r_1R to $\omega^{(p)}$ on $E^{(p)}$. Hence we have the congruence

(3.9.1) $$E_{p-1}(E'/R,\omega',\alpha_n') \equiv (E_{p-1}(E,\omega,\alpha_n))^p \text{ modulo } r_1R .$$

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

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

Using the equation

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

one immediately checks that if we define

$$(3.9.4) \qquad Y'(E'/R,\omega',\alpha_n') = (Y(E/R,\omega,\alpha_n))^p/1 + r_4 j\cdot(Y(E/R,\omega,\alpha_n))^p \ ,$$

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

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

Throughout the rest of this chapter, we denote by R_0 a complete discrete valuation ring of mixed characteristic with perfect residue field R_0/m . The Frobenius endomorphism φ of $S(R_0,1,n,k)$ is defined by $\varphi(f)(E,\omega,\alpha_n,Y = (E_{p-1})^{-1}) = f(E/H,\check{\pi}^*(\omega),\pi(\alpha_n),Y' = 1/E_{p-1})$, where H denotes the canonical subgroup of E , $\pi\colon E \longrightarrow E/H$ denotes the projection. As we have seen above, for $r \in R_0$ having $\operatorname{ord}(r) < 1/p+1$, the composite $(E_{p-1})^k\cdot\varphi$ "extends" to give a commutative diagram

$$\text{3.10.0} \qquad \begin{array}{ccccc} S(R_0,1,n,k) & \xrightarrow{\varphi} & S(R_0,1,n,k) & \xrightarrow{(E_{p-1})^k} & S(R_0,1,n,pk) \\ \uparrow & & & & \uparrow \\ S(R_0,r^p,n,k) & & \dashrightarrow & & S(R_0,r,n,pk) \end{array}$$

For k=0, we find simply that the endomorphism φ maps $S(R_0,r^p,n,0)$ to $S(R_0,r,n,0)$ for any $r \in R_0$ having $\operatorname{ord}(r) < 1/p+1$.

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

I. For $r \in R_o$ with $\mathrm{ord}(r) < 1/p+1$, the Frobenius morphism $\varphi\colon S(R_o, r^p, n, 0) \longrightarrow S(R_o, r, n, 0)$ is a finite morphism (but not in general flat).

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

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

$$\varphi \otimes K\colon S(R_o, r^p, n, 0) \otimes K \longrightarrow S(R_o, r, n, 0) \otimes K$$

is finite and etale of rank p.

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

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

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

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

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

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

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

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

to irreducible components) or <u>maximal</u> (corresponding to conjugacy classes of points with values in finite extensions of K). Indeed, the closed points of $S(R_0,r,n,0)\otimes K$ are conjugacy classes of homomorphisms $\pi\colon S(R_0,r,n,0) \longrightarrow K'$, K' a finite extension of K , or equivalently they are homomorphisms $\pi\colon D_n\otimes K \longrightarrow K'$ which satisfy the continuity conditions $|\pi(D_n)| \leq 1$, $1 \geq |\pi(E_{p-1})| \geq |r|$ (i.e., that the images of E_{p-1} <u>and</u> of $Y = r/E_{p-1}$ be "power bounded"). Further, the completions of the local rings at corresponding closed points are isomorphic, hence are regular local rings of dimension one, hence $S(R_0,r,n,0)\otimes K$ is <u>a regular ring of dimension one</u>. Thus the map

3.10.4 $$S(R_0,r^p,n,0)\otimes K \xrightarrow{\varphi\otimes K} S(R_0,r,n,0)\otimes K$$

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

Let $E^{(i)} = E/H_i$. The points lying over E are <u>among</u> the $p+1$ curves $E^{(i)}$, ($E^{(i)}$ carrying the induced level n structure); indeed, $E^{(i)}$ lies over if and only if $E^{(i)}$ <u>is</u> a point of $S(R_0,r,n,0)\otimes\Omega$ whose canonical subgroup is ${}_pE/H_i$.

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

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

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

$$(3.10.6) \qquad [p](X) = pX + aX^p + \sum_{m=2}^{p} C_m X^{m(p-1)+1} + C_{p+1}X^{p^2} + \sum_{m \geq p+2} C_m X^{m(p-1)+1}$$

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

<u>Theorem 3.10.7.</u> (Lubin)

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

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

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

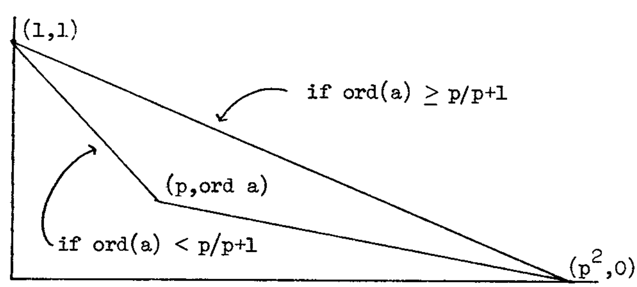
with $\mathrm{ord}(a') = p\,\mathrm{ord}(a)$.

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

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

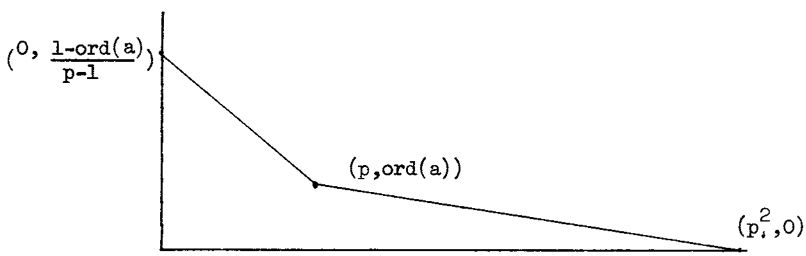
5. If $0 < \mathrm{ord}(a) < p/p+1$, there exist precisely p curves $E^{(i)}$ having $\mathrm{ord}(a_i) < 1/p+1$ such that $E = E^{(i)}/H_0(E^{(i)})$, namely the curves $E^{(i)} = E/H_i$, $i = 1,\ldots,p$ (cf. 3.10.4ff), and $\mathrm{ord}(a_i) = \frac{1}{p}\mathrm{ord}(a)$.

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



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

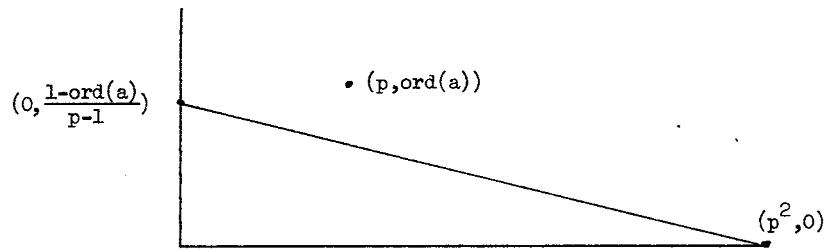
2. By Lubin ([32]), we know that if H is any finite subgroup of a one-parameter formal group over R_0, then $X \longrightarrow \prod_{x \in H} G(X,x)$ <u>is</u> the projection onto the quotient. Thus the non-zero points of order p on E/H_0 are of two sorts, the points $\prod_{x \in H_0} G(y,x)$ with $[p](y) = 0$, $\operatorname{ord}(y) = \frac{\operatorname{ord}(a)}{p^2-p}$, and the points $\prod_{x \in H_0} G(z,x)$ where $[p](z) \in H_0$, $[p](z) \neq 0$. The first sort of point has ordinal given by $\sum_{x \in H_0} \operatorname{ord}(G(y,x))$, and as $\operatorname{ord}(y) < \operatorname{ord}(x)$ for any $x \in H_0$, this sum is just $p(\operatorname{ord} y) = \frac{\operatorname{ord}(a)}{p-1}$. The second sort of point has ordinal $\sum_{x \in H_0} \operatorname{ord}(G(z,x))$. From the equation $[p](z) \in H_0 - \{0\}$, we see that $\operatorname{ord}([p](z)) = \frac{1-\operatorname{ord}(a)}{p-1}$. The Newton polygon of $[p](z) = x \in H_0 - \{0\}$ is thus



and hence z has <u>either</u> ordinal $\operatorname{ord}(a)/p^2-p$ <u>or</u> $\frac{1-p \operatorname{ord}(a)}{p^2-p}$. In <u>either</u> case, $\operatorname{ord}(z) < \operatorname{ord}(x)$ for any $x \in H_0$. Hence the second sort of point has ordinal either $\operatorname{ord}(a)/p-1$ <u>or</u> $(1-p \operatorname{ord}(a))/p-1$. Thus among the non-zero points of order p on E/H_0, there are two distinct ordinals which occur, namely $\operatorname{ord}(a)/p-1$ and $(1-p \operatorname{ord}(a))/p-1$, of which the <u>greater</u> is $(1-p \operatorname{ord}(a))/p-1$.

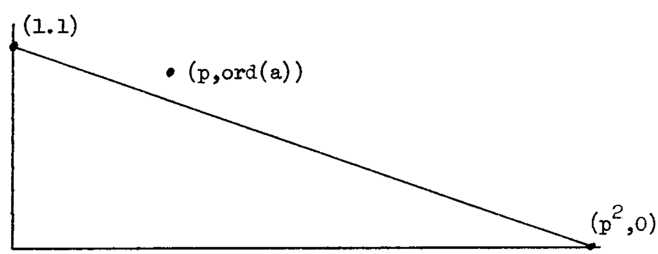
Thus by 1, E/H_0 has $\operatorname{ord}(a') < p/p+1$, and $\frac{1-\operatorname{ord}(a')}{p-1} = \frac{1-p \operatorname{ord}(a)}{p-1}$, which proves 2. We note that the image of ${}_pE$ is <u>not</u> the canonical subgroup.

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

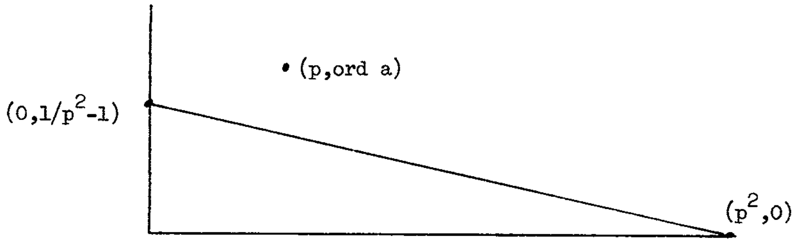


hence $\mathrm{ord}(z) = \frac{1-\mathrm{ord}(a)}{p^2(p-1)} < \mathrm{ord}(x)$ for any $x \in H_o$, hence the second sort of point has ordinal $1-(\mathrm{ord}(a)/p(p-1))$. Thus E/H_o has a canonical subgroup, namely its points of order p of largest ordinal $= \mathrm{ord}(a)/p-1$. Hence $\frac{1-\mathrm{ord}(a')}{p-1}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

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



Hence all non-zero points of order p have the same ordinal $1/p^2-1$. The points z such that $[p](z) = x$, $[p](x) = 0$, $x \neq 0$, have ordinal $1/p^2(p^2-1)$, because the Newton polygon of $[p](Z) = x$, $\mathrm{ord}(x) = 1/p^2-1$, is



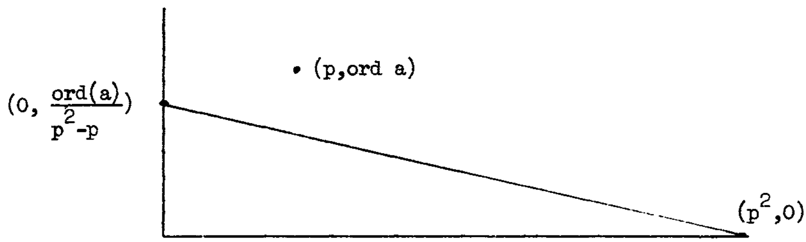
Thus for any subgroup H_i of order p of E , the first sort of point of order p has $\mathrm{ord} = \sum_{x \in H_i} \mathrm{ord}(G(y,x)) \geq p\,\mathrm{ord}(y) = p/p^2-1$ (since $\mathrm{ord}(y) = \mathrm{ord}(x)$ if $x \neq 0$). The second sort of point has ordinal $p\cdot\mathrm{ord}(z) = 1/p(p^2-1)$,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

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

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

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

What about the image of a point z such that $[p](z) \in H_i - \{0\}$? The Newton polygon of $[p](Z) = x$, $x \in H_i - \{0\}$, is



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

3.11 Applications to the congruences of Atkin - the U operator

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

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

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

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

In terms of q-expansion, we have

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

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

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

then we have the formula (in which α''_n is the level n structure on $\mathrm{Tate}(q^n)$ obtained as the inverse image of $\pi_0(\alpha_n)$ on $\mathrm{Tate}(q^{n/p})$ by the extension of scalars $q^{1/p} \longrightarrow q$, compare pp.32-33)

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

Notice that we have the relation, for any $f \in S(R_0,r,n,0)\otimes K$,

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

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

Integrality Lemma 3.11.4. For any $r \in R_0$ with $\mathrm{ord}(r) < 1/p+1$, we have $\mathrm{tr}_\varphi(S(R_0,r,n,0)) \subset S(R_0,r^p,n,0)$ (although $\varphi\colon S(r_0,r^p,n,0) \longrightarrow S(R_0,r,n,0)$ is finite but not flat if $\mathrm{ord}(r) > 0$!).

Proof. We may suppose $\mathrm{ord}(r) > 0$, the case $r=1$ being trivial. It follows (from Tate [45]) that for any finite flat morphism $\varphi\colon A \longrightarrow B$ of rigid algebras over K, we have tr_φ (power-bounded elements of B) $\subset$ power-bounded elements of A. Thus we must show that the power-bounded elements of $S(R_0,r,n,0)\otimes K$ are precisely $S(R_0,r,n,0)$. For this, we introduce the finitely generated R_0-algebra $B = H^0(\overline{M}_n\otimes R_0, \underline{\mathrm{Symm}}(\underline{\omega}^{\otimes p-1}))/(E_{p-1}-r)$. Its p-adic completion $\hat{B} \overset{dfn}{=\!=} \varprojlim B/p^N B$ is $S(R_0,r,n,0)$, and indeed via the isomorphism (2.6.2.1), B corresponds to the R_o-submodule of $B^{\text{rigid}}(R_o,r,n,0)$ consisting of all <u>finite</u> sums, which shows incidentally that B is a (free and hence) flat R_o-module, and that $B/\underline{m}B \simeq \hat{B}/\underline{m}\hat{B}$. The fact that E_{p-1} modulo $\underline{m}$ has <u>simple</u> zeros implies that $B/\underline{m}B$ is <u>reduced</u>. (Indeed, $B/\underline{m}B$ is $H^o(M_n \otimes R_o/\underline{m}, \text{Symm}(\underline{\omega}^{\otimes p-1}))/(E_{p-1})$, and if $\sum_o^N f_i$ represents a nilpotent element, with minimal N , then a power of f_N is divisible by E_{p-1} , hence f_N is divisible by E_{p-1} , which contradicts the minimality of N .) We may thus conclude by the following lemma.

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

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

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

$$S(R_o,r^p,n,0)\otimes K \hookrightarrow S(R_o,r,n,0)\otimes K \xrightarrow{\frac{1}{p}\,\text{tr}_\varphi} S(R_o,r^p,n,0)\otimes K .$$

Thus if $f \in S(R_o,r^p,n,0)$ has q-expansions

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

then $U\,f \in S(R_o,r^p,n,0)\otimes K$ has q-expansions

3.11.6.2. $$(U\,f)(\text{Tate}(q^n),\omega_{\text{can}},\alpha_n) = \sum A_{pi}(\tfrac{1}{p}\,\alpha_n'')\cdot q^i .$$

[This formula shows that $U(S(R_o,1,n,0)) \subset S(R_o,1,n,0)$] . It is <u>not</u> true in general that $U(S(R_o,r^p,n,0)) \subset S(R_o,r^p,n,0)$, but the situation is as good as if it were true, as Dwork was the first to realize.

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

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

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

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

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

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

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

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

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

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

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

3.11.12. $$\operatorname{tr}_\varphi\left(\frac{rb_1}{E_{p-1}}\right) = \sum_{a \geq 1} \frac{r^{pa}\, b'_a}{(E_{p-1})^a} \; .$$

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

3.11.13 $$U\left(\frac{r^p\, b_1}{E_{p-1}}\right) = \frac{r^{p-1}}{p} \operatorname{tr}_\varphi\left(\frac{rb_1}{E_{p-1}}\right) = \frac{r^{p-1}}{p}\left(b'_0 + \frac{r^p b'_1}{E_{p-1}}\right) +$$

$$+ \, p \text{ (an element of } \frac{r^{3(p-1)}}{p^2} \, S(R_0,r,n,0) \, .$$

Notice that $U(\frac{r^p b_1}{E_{p-1}})$ has q-expansions divisible by r^p , as does $p \cdot$(any element of $S(R_0,r^p,n,0)$) , and hence so does

$$(r^{p-1}/p)\left(b'_0 + \frac{r^p b'_1}{E_{p-1}}\right) = \frac{r^{p-1}}{p}\left(\frac{b'_0 E_{p-1} + r^p b'_1}{E_{p-1}}\right) \, ,$$

and hence so does $\frac{r^{p-1}}{p}(b'_0\, E_{p-1} + r^p b'_1)$. By the q-expansion principle, there exists an element $b''_1 \in H^0(\overline{M}_n \otimes R_0, \underline{\omega}^{\otimes p-1})$ such that

$\frac{r^{p-1}}{p}(b_0\, E_{p-1} + r^p b'_1) = r^p b''_1$, hence $\frac{r^{p-1}}{p}\left(b_0 + \frac{r^p b'_1}{E_{p-1}}\right) = \frac{r^p b''_1}{E_{p-1}}$, hence

$$U\left(\frac{r^p b_1}{E_{p-1}}\right) = \frac{r^p b''}{E_{p-1}} + p \cdot \text{(an element of } \frac{r^{3(p-1)}}{p^2} \, S(R_0,r,n,0)) \, .$$

Again using the fact that $pU = \operatorname{tr}_\varphi$ maps $S(R_0,r,n,0)$ to $S(R_0,r^p,n,0)$, we find

$$U^2\left(\frac{r^p b_1}{E_{p-1}}\right) = U\left(\frac{r^p b''_1}{E_{p-1}}\right) + \text{an element of } S(R_0,r^p,n,0) \, ,$$

which proves (3.11.11) and the lemma. QED

3.12 p-adic Hecke operators

For any prime number ℓ which is prime to both p and to the level n, we may define T_ℓ on $S(R_0,r,n,k)$ by the usual formula

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

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

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

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

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

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

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

$$(S(R_0,r^p,n,0) + U(S(R_0,r^p,n,0))\otimes_{R_0} R_0/\underline{m}\ .$$

But for $f \in S(R_0, r^p, n, 0)$, $f = \sum_{a \geq 0} \frac{r^{pa} b_a}{(E_{p-1})^a}$, we have

$U(f) \equiv b_0 + U(\frac{r^p b_1}{E_{p-1}})$ modulo $\underline{m} \cdot S(R_0, r^p, n, 0)$ and

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

3.13 Interpretation of Atkin's congruences on j

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

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

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

Thus $U(j)$ lies in $S(\mathbf{Z}_p, 1, n, 0)$, and $p \cdot U(j)$ lies in $S(R_0, r, n, 0)$ for any $r \in R_0$ having $\operatorname{ord}(r) < p/p+1$. Combining this observation with the remark (3.11.8), we see that for <u>every</u> $m \geq 1$, we have $U^m(j) \in S(\mathbf{Z}_p,1,n,0) \cap p^{-2}\cdot S(R_o,r,n,0)$.

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

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

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

3.13.3.1 $$U(j) \equiv \sum_{a=0}^{p^n} \frac{b_a}{(E_{p-1})^a} \ \text{modulo} \ p^{n+1}S(\mathbf{Z}_p,1,1,0)$$

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

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

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

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

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

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

Let $c_\infty(i) = \lim_m a^{-m} c(p^m i)$. Then for $r \in R_0$ having $\mathrm{ord}(r) < p/p+1$, there is a unique element " lim " $a^{-m} U^m(j-744) \in S(\mathbf{Z}_p,1,n,0) \cap p^{-2} S(R_0,r,n,0)$ which is of level one (i.e., invariant under $GL_2(\mathbf{Z}/n\,\mathbf{Z})$), whose q-expansion is $\sum_{m \geq 1} c_\infty(i) q^i$, and which is <u>fixed</u> by $a^{-1}U$.

<u>Proof.</u> By (2.7), the hypothesis is in fact equivalent to the congruences

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

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

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

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

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

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

(3.13.6) Using the fact that the twelfth power $\underline{\omega}^{\otimes 12}$ of $\underline{\omega}$ descends to the invertible sheaf $\mathcal{O}(1)$ on the projective j-line over $\mathbb{Z}$, one can copy the construction of a basis of $S(R_0,r,n,0)$, $n \geq 3$, to get a basis of $S(R_0,r,1,0) \overset{\text{dfn}}{=\!=} S(R_0,r,n,0)^{GL_2(\mathbb{Z}/n\mathbb{Z})}$ for primes $p \equiv 1 \bmod 12$. Then one can copy the proof given in ([14]) to show that the dimension of the unit root subspace of $S(R_0,r,1,0)\otimes K$ is at most $\dim H^0(\mathbb{P}^1,\underline{\omega}^{\otimes p-1}) = \dim H^0(\mathbb{P}^1,\mathcal{O}(\frac{p-1}{12})) = 1 + \frac{p-1}{12}$, for $p \equiv 1 \bmod 12$. In particular, for $p = 13$, the unit root space has a base consisting of the constant function and the function "lim"$(a^{-1}U)^n(j-744)$, and this latter function is necessarily the unique "unit root cusp form" in $S(R_0,r,1,0)$. This unicity, together with the stability of the space of unit root cusp forms under the Hecke operators T_ℓ, $\ell \neq 13$, gives a startling result of Atkin.

Theorem 3.13.7. (Atkin) The 13-adic modular function "lim"$(a^{-1}U)^m(j-744) = \sum_{i \geq 1} c_\infty(i)q^i$ is a simultaneous eigenfunction of all the Hecke operators T_ℓ, $\ell \neq 13$.

(3.13.8) Using the fact that $\underline{\omega}^{\otimes 2}$ descends to the invertible sheaf $\mathcal{O}(1)$ on the projective λ-line $\overline{M}_2$ over $\mathbb{Z}[1/2]$, one may construct as above a base of $S(R_0,r,2,0)$, and prove as above that the unit root subspace of $S(R_0,r,2,0)\otimes K$ has dimension at most $\dim H^0(\overline{M}_2,\underline{\omega}^{\otimes p-1}) = \dim H^0(\mathbb{P}^1,\mathcal{O}(\frac{p-1}{2})) = 1 + \frac{p-1}{2}$, for p odd. In fact, Dwork has proven that in this case the dimension is exactly $1 + \frac{p-1}{2}$, (cf. his exposé in this volume).

(3.13.9) Dwork's result implies that for $p \equiv 1 \bmod 12$, the dimension of the unit root subspace of $S(R_0,r,1,0)$ is precisely $1 + \frac{p-1}{12}$, and hence that there are precisely $\frac{p-1}{12}$ independent unit root cusp forms in $S(R_0,r,1,0)$.

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

Chapter 4. p-adic representations and congruences for modular forms

4.1 p-adic representations and locally free sheaves

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

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

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

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

$$\begin{cases} X(T) = \text{global sections of } H_T \\ Y(T) = \text{bases of } H_T \ \ (\mathcal{O}_T\text{-isomorphisms } (\mathcal{O}_T)^r \longrightarrow H_T \text{, where} \\ \qquad\qquad\qquad r = \operatorname{rank}(H)) \\ Z(T) = \text{bases of } H_T \text{ consisting of fixed points of } F_T \end{cases}$$

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

Consider the functor on S-schemes

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

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

$$X_j = \sum_i a_{ji}(X_i)^q , \qquad j = 1,\ldots,r .$$

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

$$(X_i)^q = \sum_j b_{ij} X_j \qquad i = 1,\ldots,r \ ,$$

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

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

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

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

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

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

$$\varphi(E) + \Delta \equiv E \qquad \text{mod } (p) ,$$

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

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

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

(4.1.2.3) Because S_1 is normal, reduced and irreducible, a representation of $\pi_1(S_m) = \pi_1(S_1)$ is just a suitably unramified representation of the Galois group of the function field of S_1. Thus for any non-void open set $U \subset S_n$, the functor "restriction" from the category of representations of $\pi_1(S_n)$ to the category of representations of $\pi_1(U)$ is <u>fully faithful.</u> Hence the functor "restriction" from the category of (H,F)'s over S_n to the category of those over U is <u>fully faithful.</u>

4.2. Application to modular schemes

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

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

We wish to determine <u>which</u> representation of $\pi_1(\bar{S}^{\zeta}_m)$ in a free $\mathbb{Z}/p^m\mathbb{Z} = W_m(\mathbb{F}_p)$-module of rank one corresponds via (4.11) to $(\underline{\omega}^{\otimes k},\varphi)$ on $\bar{S}^{\zeta}_m$. Of course it suffices to do this for $k=1$, by (4.1.2.1). There is an obvious candidate, namely the representation of $\pi_1(S^{\zeta}_m)$ on the <u>étale quotient</u> of the kernel of p^m on the <u>universal</u> curve E. [Noting by $\pi\colon E \longrightarrow E^{(\varphi)} = E/H$ the projection onto the quotient by the canonical subgroup, the composite $\pi_m\colon E \longrightarrow E^{(\varphi^m)}$ induces an isomorphism of the étale quotient ${}_{p^m}E/{}_{p^m}\hat{E} = {}_{p^m}E/\mathrm{Ker}(\pi^m) \xrightarrow[\sim]{\pi^m} \mathrm{Ker}(\check{\pi})^m$ in $E^{(\varphi^m)}$.] If this candidate is to "work", we must have:

<u>Lemma 4.2.1.</u> The representation of $\pi_1(S^{\zeta}_m)$ on $\mathrm{Ker}(\check{\pi})^m$ extends to a representation of $\pi_1(\bar{S}^{\zeta}_m)$, i.e., it is "unramified at ∞".

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

<u>Theorem 4.2.2.</u> The representation of $\pi_1(\bar{S}^{\zeta}_m)$ on $\mathrm{Ker}(\check{\pi})^m$ ($\simeq$ to the étale quotient of $\mathrm{Ker}\ p^m$ on the universal curve) corresponds, via the equivalence (4.1.1), to $(\underline{\omega},\varphi)$.

<u>Proof.</u> By the "full-faithfulness" of restriction to open sets, it suffices to prove this over S^{ζ}_m. Let's take a finite étale covering T of S_m which

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

It remains to see that this isomorphism is compatible with the φ-linear endomorphisms. Tensoring one with the inverse of the other, we obtain a φ-linear endomorphism on $\mathcal{O}_{S_m}$; we must show that it carries "1" to "1". To check this, it suffices to do so in a "punctured disc at ∞", over $W_m(\mathbb{F}_q)((q))$ when we look at the Tate curve $\mathrm{Tate}(q^n)$. The morphism $\check{\pi}$: $\mathrm{Tate}(q^{n\cdot p^m}) \longrightarrow \mathrm{Tate}(q^n)$ has kernel the subgroup generated by q^n. The point q^n is a rational point of $\mathrm{Ker}(\check{\pi})^m$, and the corresponding differential is precisely the Tate differential $\omega_{can} = dt/t$. As q^n is a rational point, the section $[q^n]\otimes 1$ of $\mathrm{Ker}(\check{\pi})^m \underset{\mathbf{Z}/p^n\mathbf{Z}}{\otimes} \mathcal{O}$ is fixed by the canonical F , and the corresponding section ω_{can} of $\underline{\omega}$ is fixed by φ (because ω_{can} has q-expansion identically "1"). Hence our isomorphism respects the φ-linear endomorphisms in a punctured disc around ∞ , and hence respects it everywhere.

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

Theorem 4.3. (Igusa [21]) The homomorphism $\pi_1(\bar{S}_m^\zeta) \longrightarrow \mathrm{Aut}(\mathrm{Ker}(\check{\pi})_T^m) \xrightarrow{\sim} (\mathbf{Z}/p^m\mathbf{Z})^\times$ is surjective, and for every non-void open set $U \subset \bar{S}_m^\zeta$, the composite $\pi_1(U) \longrightarrow \pi_1(\bar{S}_m^\zeta) \longrightarrow (\mathbf{Z}/p^m\mathbf{Z})^\times$ remains surjective.

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

Theorem 4.3 bis(Igusa). Let E,ω be an elliptic curve over $k[[A]]$ with Hasse invariant A , k being an algebraically closed field of characteristic p. Then the extension of $k((A))$ obtained by adjoining the points of $\mathrm{Ker}\ V^m\colon E^{(p^m)} \longrightarrow E$ is fully ramified of degree $p^{m-1}(p-1)$, with Galois group canonically isomorphic to $\mathrm{Aut}(\mathbb{Z}/p^m\mathbb{Z})$.

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

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

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

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

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

$$\begin{cases} 0 = V(y_0) = Ay_0 + \alpha(y_0)^p + \ldots \\ y_0 = V^{(p)}(y_1) = A^p y_1 + \alpha^p (y_1)^p + \ldots \\ y_{m-2} = V^{(p^{m-1})}(y_{m-1}) = A^{p^{m-1}} y_{m-1} + \alpha^{p^{m-1}} (y_{m-1})^p + \ldots . \end{cases}$$

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

$$\begin{cases} \mathrm{ord}(y_0) = 1/p-1 \\ \mathrm{ord}(y_1) = 1/p(p-1) \\ \vdots \\ \mathrm{ord}(y_{m-1}) = 1/p^{m-1}(p-1) . \end{cases}$$

QED

4.4. Applications to congruences between modular forms à la Serre

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

1) $k \equiv 0 \bmod (p-1)\cdot p^{m-1}$ if $p \neq 2$, and $k \equiv 0 \bmod 2^{\alpha(m)}$ if $p = 2$, where $\alpha(1) = 0$, $\alpha(2) = 1$, and $\alpha(m) = m-2$ if $m \geq 3$.

2) The k'th (tensor) power of the representation of $\pi_1(\overline{S}^{\zeta}_m)$ on the étale quotient of ${}_{p^m}E$ is trivial.

3) The sheaf $\underline{\omega}^{\otimes k}$ on $\overline{S}^{\zeta}_m$ admits a nowhere vanishing section fixed by φ .

4) Over a non-void open set $U \subset \overline{S}^{\zeta}_m$, $\underline{\omega}^{\otimes k}$ admits a nowhere vanishing section fixed by φ .

5) Over $\overline{S}^{\zeta}_m$, $\underline{\omega}^{\otimes k}$ admits a section whose q-expansion at one of the cusps of $\overline{S}^{\zeta}_m$ is identically 1.

6) Over a non-void open set $U \subset \overline{S}^{\zeta}_m$ which contains a cusp, $\underline{\omega}^{\otimes k}$ admits a section whose q-expansion at that cusp is identically 1.

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

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

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

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

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

Proof. For $N \gg 0$, $p^N f$ is a true modular form of level n and weight k on $\Gamma_0(p)$, defined over $W(\mathbb{F}_q)$. By (3.2), there is a unique element g of $S(W(\mathbb{F}_q),1,n,k)$ whose q-expansions are those of $p^N f$ at the corresponding unramified cusps. If $-m_0$ denotes the minimum of the ordinals of the constant terms of these q-expansions, then g is divisible by p^{N-m_0} in $S(W(\mathbb{F}_q),1,n,k)$, by (2.7). Thus we may write $g = p^{N-m_0}h$, with $h \in S(W(\mathbb{F}_q),1,n,k)$ having the same q-expansions as does $p^{m_o}f$ at the corresponding unramified cusps. Then h has integral q-expansions, and at least one of them is congruent modulo p^{m_o} to a <u>constant</u> which is a <u>unit</u> on $W(\mathbb{F}_q)$. Multiplying f by the reciprocal of this unit, we get a q-expansion which is congruent mod p^N to "1". As the constant function "1" is modular of weight zero, we must have $k \equiv 0 \bmod p^{m_o-1}(p-1)$ if $p \neq 2$, $k \equiv 0 \bmod 2^{\alpha(m_o)}$ for $p=2$. QED

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

<u>4.5. Applications to Serre's "modular forms of weight χ"</u>

4.5.0. Let $\chi \in \mathrm{End}(\mathbf{Z}_p^\times)$. For each power p^m of p, χ induces an endomorphism of $(\mathbf{Z}/p^m\mathbf{Z})^\times$. For any primitive n'th root of unity ζ, and for any representation ρ of $\pi_1(\overline{S}_m^\zeta)$ in a free $\mathbf{Z}/p^m\mathbf{Z}$ module of rank one, we may define the representation $\rho^\chi \overset{\mathrm{dfn}}{=\!=} \chi\circ\rho$. Taking for ρ the representation given by the étale quotient of ${}_{p^m}E$, we denote by $(\underline{\omega}^\chi,\varphi)$ the invertible sheaf with φ-linear endomorphism which corresponds to ρ^χ. For variable m, the sheaves $\underline{\omega}^\chi$ on S_m^ζ are compatible, and we define a compatible family of global sections to be a p-adic modular form of weight χ and level n, holomorphic at ∞, defined over $W(\mathbb{F}_q)$. If $\chi = k \in \mathbf{Z} \subset \mathrm{End}(\mathbf{Z}_p^\times)$, we just recover the elements of $S(W(\mathbb{F}_q),1,n,k)$. For $p \neq 2$, $\mathbf{Z}$ is dense in $\mathrm{End}(\mathbf{Z}_p^\times)$, and indeed $\mathrm{End}(\mathbf{Z}_p^\times) \xleftarrow{\sim} \varprojlim \mathbf{Z}/\varphi(p^m)\mathbf{Z}$; for $p=2$, $\mathbf{Z}_2$ has <u>index four</u> in the (non-commutative) ring $\mathrm{End}(\mathbf{Z}_2^\times)$. If $p \neq 2$, then for any χ (resp. if $p=2$, for any $\chi \in \mathbf{Z}_2$), the pair $(\underline{\omega}^\chi,\varphi)$ on $\overline{S}_m^\zeta$ is isomorphic to $(\underline{\omega}^{\otimes k_m},\varphi)$ for any $k_m \in \mathbf{Z}$ such that $k_m \equiv \chi$ modulo $\varphi(p^m)$ (resp. if $p=2$, modulo 2^0 if $m=1$, 2^1 if $m=2$, and 2^{m-2} if $m \geq 3$). The isomorphism between $(\underline{\omega}^{\otimes k_m},\varphi)$ and $(\underline{\omega}^{\otimes k'_m},\varphi)$ for different choices $k_m, k'_m \in \mathbf{Z}$ approximating χ is given by multiplication by $(E_{p-1})^{(k'_m-k_m)/(p-1)}$. As this isomorphism leaves <u>invariant</u> the q-expansion modulo p^m (resp. modulo 2^{m-1} for $p=2$), it follows that a p-adic modular form of weight χ and level n, holomorphic at ∞, defined over $(W(\mathbb{F}_q)$, has a well defined q-expansion in $W[[q]]$ at each cusp, and that for given χ, f is uniquely determined by its q-expansions.

<u>Theorem 4.5.1.</u> Let $\chi \in \mathrm{End}(\mathbf{Z}_p^\times)$, and suppose $\chi \in \mathbf{Z}_2$ if $p=2$. Let f be a modular form of weight χ and level n, holomorphic at ∞, defined over $W(\mathbb{F}_q)$. Then there exists a sequence of integers $0 \leq k_1 \leq k_2 \leq k_3 \leq \cdots$, satisfying

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

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

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

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

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

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

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

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

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

QED

<u>Corollary 4.5.3.</u> (Serre) Let $\chi \in \mathrm{End}(\mathbf{Z}_p^\times)$, and suppose $\chi \in \mathbf{Z}_2$ if $p=2$. Let $0 \leq k_1 \leq k_2 \leq \ldots$ be a sequence of integers such that $k_m \equiv \chi$ modulo $\varphi(p^m)$ if $p \neq 2$, and modulo 2^{m-2} if $p=2$ and $m \geq 3$. Let $\{f_m\}$ be a sequence of <u>true</u> modular forms of weight k_m and level n on $\Gamma_0(p)$, holomorphic at

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

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

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

Proof. The integrality of the q-expansions of the $p^{m_o} f_m$ follows from (4.4.3). Let $g_m = p^{m_o} f_m$, which has integral q-expansions. Then g_m and $h_m \overset{\text{dfn}}{=\!=} g_m \cdot (E_{p-1})^{(k_{m+1}-k_m)/(p-1)}$ have q-expansions which are congruent modulo p^m if $p \neq 2$, (resp. modulo 2^{m-1} if $p = 2$) and $g_m(0) = h_m(0)$. Thus $g_{m+1} - h_m$ has q-expansions congruent to the constants $g_{m+1}(0) - h_m(0)$ modulo p^m if $p \neq 2$, (resp. modulo 2^{m-1} if $p = 2$). Applying (4.4.3) to the function $(g_{m+1} - h_m)/p^m$ for $p \neq 2$, (resp. to $g_{m+1} - h_m/2^{m-1}$ for $p = 2$) we find that its constant term has denominator at most p^{m_o}. Thus $g_{m+1}(0) \equiv h_m(0)$ modulo p^{m-m_o} if $p \neq 2$, and 2^{m-1-m_o} if $p = 2$. QED

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

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

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

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

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

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

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

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

Taking $k=1$, we obtain a p-adic modular form G^*_2 of weight 2, and we may define G_2 as a p-adic modular form by setting

$$G_2 \stackrel{\text{dfn}}{=} \sum_{n \geq 0} p^n\varphi^n(G^*_2) .$$

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

$$G_2(q) = \frac{-1}{24} + \sum_{n \geq 1} q^n \sum_{d|n} d = \frac{-1}{24} P(q)$$

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

Appendix 1: Motivations

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

A1.1 Lattices and elliptic curves

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

A1.1.1 $$y^2 = 4x^3 - g_2x - g_3 ,$$

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

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

where

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

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

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

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

A1.1.2.4 $$L(E,\omega) = \left\{ \int_\gamma \omega \;\middle|\; \gamma \in H_1(E;\mathbf{Z}) \right\} \subset \mathbf{C} .$$

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

A1.1.2.5 $$L(E,\lambda\omega) = \lambda\cdot L(E,\omega) .$$

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

A1.1.3 $$f\left(\frac{a\tau+b}{c\tau+d}\right) = f(\tau)\cdot(c\tau+d)^k \qquad \forall \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbf{Z}) .$$

As explained in [$42\frac{1}{2}$], there is associated to f a unique function of <u>lattices</u> $F(L)$ such that $f(\tau) = F(\mathbf{Z}\tau + \mathbf{Z})$, and which is homogeneous of degree $-k$ in L: $F(\lambda L) = \lambda^{-k}F(L)$ for $\lambda \in \mathbf{C}^*$. (Explicitly, $F(L) = \omega_2^{-k}f(\omega_1/\omega_2)$ if $L = \mathbf{Z}\omega_1 + \mathbf{Z}\omega_2$ and $\mathrm{Im}(\omega_1/\omega_2) > 0$.)

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

<u>A1.2 Homomorphy at ∞ and the Tate curve</u>

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

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

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

A1.2.1
$$Y^2 = 4X^3 - \frac{E_4}{12}X + \frac{E_6}{216}\ , \text{ with differential } dX/Y$$
$$(X = \wp(2\pi i z, L), \qquad Y = \wp'(2\pi i z, L))$$

with coefficients the Eisenstein series

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

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

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

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

then we may rewrite the equation in the form

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

with coefficients

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

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

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

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

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

A1.2.6 $$(\zeta_n)^i q^j \, , \qquad 0 \leq i,\, j \leq n-1 \, .$$

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

A1.2.7 $$\begin{cases} x(t) = \displaystyle\sum_{k \in \mathbf{Z}} \frac{q^{nk}t}{(1-q^{nk}t)^2} - 2 \sum_{k=1}^{\infty} \frac{q^{nk}}{1-q^{nk}} \\[2ex] y(t) = \displaystyle\sum_{k \in \mathbf{Z}} \frac{(q^{nk}t)^2}{(1-q^{nk}t)^3} + \sum_{k=1}^{\infty} \frac{q^{nk}}{1-q^{nk}} \, , \end{cases}$$

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

A1.2 Modular forms and de Rham cohomology

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

$$\begin{array}{c} E \; ; \; \omega \\ \pi \big\downarrow \quad \\ R \quad \end{array}$$

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

0) $f(E,\lambda\omega) = \lambda^{-k} f(E,\omega)$ for all $\lambda \in R^\times$;

1) $f(E,\omega)$ depends only on the isomorphism class of (E,ω) over R;

2) if $\varphi: R \longrightarrow R'$ is a ring homomorphism, then, denoting by $(E_\varphi, \omega_\varphi)$ the curve with differential over R' deduced by extension of scalars, we have $f(E_\varphi, \omega_\varphi) = \varphi(f(E,\omega))$.

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

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

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

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

1) if $\alpha: E \longrightarrow E'$ is an isomorphism of elliptic curves over R, then $\alpha^*(f(E')) = f(E)$;

2) if $\varphi: R \longrightarrow R'$ is a ring homomorphism, then $f(E_\varphi) = \varphi^*(f(E))$.

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

A1.2.1

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \underline{\omega}_{E/R} & \longrightarrow & H^1_{DR}(E/R) & \longrightarrow & \underline{\mathrm{Lie}}(E/R) & \longrightarrow & 0 \\ & & & & & & \| & & \\ & & & & & & H^1(E,\mathcal{O}_E) & & \\ & & & & & & \| & & \\ & & & & & & (\underline{\omega}_{E/R})^{\otimes -1} & & \end{array}$$

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

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

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

$$Y^2 = 4X^3 - g_2X - g_3\ , \qquad g_2,\ g_3 \in R$$

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

A1.2.2
$$\begin{cases} X(E,\lambda\omega) = \lambda^{-2}\cdot Y(E,\omega) \\ Y(E,\lambda\omega) = \lambda^{-3}\cdot Y(E,\omega) \\ g_2(E,\lambda\omega) = \lambda^{-4} g_2(E,\omega) \\ g_3(E,\lambda\omega) = \lambda^{-6} g_3(E,\omega) \end{cases}$$

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

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

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

$$\begin{aligned} \mathbb{H}^1(E,\mathcal{O}_E(\infty) \longrightarrow \Omega^1_{E/R}(2\infty)) &= \mathrm{Coker}(H^0(E,\mathcal{O}_E(\infty)) \longrightarrow H^0(E,\Omega^1_{E/R}(2\infty)) \\ &= \mathrm{Coker}(R \xrightarrow{0} H^0(E,\Omega^1_{E/R}(2\infty))) \\ &= H^0(E,\Omega^1_{E/R}(2\infty)) \ . \end{aligned} \tag{A1.2.3}$$

If we suppose 6 to be invertible in R , then as soon as we choose a nowhere vanishing differential ω on E , we may canonically specify a basis of $H^1(E,\Omega^1_{E/R}(2\infty))$, namely

$$\omega = \frac{dX(E,\omega)}{Y(E,\omega)} \quad \text{and} \quad \eta = X(E,\omega)\cdot\omega = \frac{X(E,\omega)\cdot dX(E,\omega)}{Y(E,\omega)} \ . \tag{A1.2.4}$$

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

$$\lambda\omega = \frac{dX(E,\lambda\omega)}{Y(E,\lambda\omega)} \quad \text{and} \quad \lambda^{-1}\eta = \frac{X(E,\lambda\omega)\,dX(E,\lambda\omega)}{Y(E,\lambda\omega)} \ , \tag{A1.2.5}$$

which is to say that we have defined an isomorphism

$$H^1_{DR}(E/R) \xleftarrow{\sim} \underline{\omega}_{E/R} \oplus \underline{\omega}^{-1}_{E/R} \tag{A1.2.6}$$

given locally on R in terms of the choice of a nowhere vanishing ω by

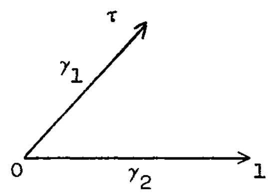
$$a\omega + b\eta \longleftrightarrow a\omega \oplus b\omega^{-1} \ .$$

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

$$\mathrm{Symm}^k(H^1_{DR}(E/R)) \simeq (\underline{\omega}_{E/R})^{\otimes k} \oplus (\underline{\omega}_{E/R})^{\otimes k-2} \oplus \cdots \oplus (\underline{\omega}_{E/R})^{\otimes -k} \ . \tag{A1.2.7}$$

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

We begin by computing the Gauss-Manin connection on $H^1_{DR}(E/R)$ in the case where R is the ring of holomorphic functions of τ, and E is the relative elliptic curve defined by the lattice $\mathbb{Z} + \mathbb{Z}\tau$. The dual $H_1(E/R)$ of $H^1_{DR}(E/R)$ is R-free on the two families of paths γ_1 and γ_2 :

(A1.3.1) 

on $E_\tau = \mathbb{C}/\mathbb{Z}+\mathbb{Z}\tau$

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

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

(i.e., it is the dual of the connection on $H_1(E/R)$ for which γ_1 and γ_2 are the horizontal sections).

To actually compute, let's note by ω (resp. η) the cohomology classes of $\frac{dx}{y}$ and $\frac{xdx}{y}$ respectively, and denote by ω_i, $i=1,2$ and η_i, $i=1,2$ the periods $\int_{\gamma_i}\omega$ and $\int_{\gamma_i}\eta$, which we view simply as elements of R. We will also denote by γ_1 and γ_2 the elements of $H^1_{DR}(E/R)$ defined by Poincaré duality and the requirement that for any $\xi \in H^1_{DR}(E/R)$, $\int_{\gamma_i}\xi = \langle\xi,\gamma_i\rangle$. Thus $\langle\gamma_2,\gamma_1\rangle = 1 = -\langle\gamma_1,\gamma_2\rangle$, and $\langle\gamma_1,\gamma_1\rangle = \langle\gamma_2,\gamma_2\rangle = 0$. We have $\omega_i = \langle\omega,\gamma_i\rangle$ and $\eta_i = \langle\eta,\gamma_i\rangle$ for $i=1,2$. Hence we necessarily have

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

(because both sides have the same periods over both γ_1 and γ_2).

But the classical "period relation" of Legendre

A1.3.4 $$\eta_1\omega_2 - \eta_1\omega_2 = 2\pi i$$

[which expresses that the topological cup-product $\langle\omega,\eta\rangle$ is $2\pi i$, or equivalently that the DR-cup-product $\langle\omega,\eta\rangle_{DR} = 1$]. This allows us to express ω and η in terms of γ_1 and γ_2:

A1.3.5 $$2\pi i\begin{pmatrix}\gamma_2\\ \gamma_1\end{pmatrix} = \begin{pmatrix}-\eta_2 & \omega_2\\ -\eta_1 & \omega_1\end{pmatrix}\begin{pmatrix}\omega\\ \eta\end{pmatrix}.$$

Applying ∇_τ, we annihilate γ_1 and γ_2, hence, noting $\frac{d}{d\tau}$ by a prime ',

A1.3.6 $$0 = \begin{pmatrix}-\eta_2' & \omega_2'\\ -\eta_1' & \omega_1'\end{pmatrix}\begin{pmatrix}\omega\\ \eta\end{pmatrix} + \begin{pmatrix}-\eta_2 & \omega_2\\ -\eta_1 & \omega_1\end{pmatrix}\begin{pmatrix}\nabla_\tau(\omega)\\ \nabla_\tau(\eta)\end{pmatrix}$$

an equation we may solve using Legendre's relation:

A1.3.7 $$\begin{pmatrix}\nabla_\tau(\omega)\\ \nabla_\tau(\eta)\end{pmatrix} = \frac{-1}{2\pi i}\begin{pmatrix}\omega_1 & -\omega_2\\ \eta_1 & -\eta_2\end{pmatrix}\begin{pmatrix}-\eta_2' & \omega_2'\\ -\eta_1' & \omega_1'\end{pmatrix}\begin{pmatrix}\omega\\ \eta\end{pmatrix}$$
$$= \frac{-1}{2\pi i}\begin{pmatrix}\eta_1'\omega_2-\eta_2'\omega_1 & \omega_1\omega_2'-\omega_2\omega_1'\\ \eta_2\eta_1'-\eta_1\eta_2' & \eta_1\omega_2'-\eta_2\omega_1'\end{pmatrix}\begin{pmatrix}\omega\\ \eta\end{pmatrix}.$$

At this point we must recall that $\omega_1 = \tau$, $\omega_2 = 1$ and Legendre's relation becomes: $\eta_1 - \tau\eta_2 = 2\pi i$. Fed back into (A1.3.7), this information gives

A1.3.8 $$\begin{pmatrix}\nabla_\tau(\omega)\\ \nabla_\tau(\eta)\end{pmatrix} = \frac{-1}{2\pi i}\begin{pmatrix}\eta_2 & -1\\ (\eta_2)^2-2\pi i\eta_2' & -\eta_2\end{pmatrix}\begin{pmatrix}\omega\\ \eta\end{pmatrix}.$$

Lemma A1.3.9. $\eta_2 = -\sum_m \sum_n{}' \frac{1}{(m\tau+n)^2} = \frac{-\pi^2}{3}P$, where Σ' means that the term $(m=0, n=0)$ is omitted, and P is the function of $q = e^{2\pi i\tau}$ given by $P(q) = 1 - 24\sum_{n\geq 1}\sigma_1(n)q^n$, where $\sigma_1(n) = \sum_{d\geq 1, d|n} d$.

Proof. The first follows from the definition of η_2 as a period of $\eta = XdX/Y = \wp(z)dz$, and the fact that $\eta = -d\zeta$, where ζ is the Weierstrauss ζ-function

$$\zeta(z) = \frac{1}{z} + \sum_m \sum_n{}' \left\{ \frac{1}{z-m\tau-n} + \frac{1}{m\tau+n} + \frac{z}{(m\tau+n)^2} \right\}. \tag{A1.3.10}$$

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

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

$$= \frac{1}{z} - \frac{1}{z+1} + \sum_{m \neq 0} \sum_n \frac{-1}{(m\tau+n)^2} + \sum_{n \neq 0} \left\{ \frac{-1}{n^2} + \frac{1}{z-n} - \frac{1}{z+1-n} \right\} \tag{A1.3.11}$$

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

The second equality is ubiquitous (cf.[$42\frac{1}{2}$], pp.154-155).

Remark A1.3.12. A similar calculation, based on the fact that the ζ is an absolutely convergent double sum, hence also given by function

$$\zeta(z) = \frac{1}{z} + \sum_n \sum_m{}' \left\{ \frac{1}{z-m\tau-n} + \frac{1}{m\tau+n} + \frac{z}{(m\tau+n)^2} \right\} \tag{A1.3.12.1}$$

shows that $\eta_1 = \zeta(z) - \zeta(z+\tau) = -\sum_n \sum_m{}' \frac{\tau}{(m\tau+n)^2}$. Comparing these two formulas, we see that $\eta_2(-1/\tau) = \tau\eta_1(\tau)$, and hence Legendre's formula $\eta_1(\tau) - \tau\eta_2(\tau) = 2\pi i$ is equivalent to the transformation formula

$$\frac{\eta_2(-1/\tau)}{\tau} - \tau\eta_2(\tau) = 2\pi i, \tag{A1.3.12.2}$$

i.e.

$$\eta_2(-1/\tau) = \tau^2\eta_2(\tau) + 2\pi i\tau$$

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

Remark (A1.3.13). Viewing Legendre's relation as saying that $\langle\omega,\eta\rangle_{DR} = 1$, one can prove it easily using Serre's cup-product formula, valid on any complete nonsingular curve over $\mathbf{C}$: for any dfk ω and any dsk η, the cup-product $\langle\eta,\omega\rangle_{DR}$ is given by the sum $\sum_{\mathfrak{p}} \mathrm{res}_{\mathfrak{p}}(f_{\mathfrak{p}}\cdot\omega)$, where at each point $\mathfrak{p}$, $f_{\mathfrak{p}}$ is an element of the $\mathfrak{p}$-adic completion of the function field such that $\eta = df_{\mathfrak{p}}$. If one bears in mind that, analytically, we have $\eta = -d\zeta$, then the usual proof of Legendre's relation on an elliptic curve (cf. [46], 20.4.11) just becomes an analytic proof of Serre's cup-product formula in that particular case.

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

$$\begin{pmatrix}\nabla_\tau(\omega)\\ \nabla_\tau(\eta)\end{pmatrix} = \frac{1}{2\pi i}\begin{pmatrix}\frac{\pi^2 P}{3} & 1\\ \frac{\pi^4}{9}\left(P^2 - \frac{12}{2\pi i}P'\right) & -\frac{\pi^2}{3}P\end{pmatrix}\begin{pmatrix}\omega\\ \eta\end{pmatrix} \tag{A1.3.14}$$

Consider now the differentials $\omega_{can} = 2\pi i\omega$, $\eta_{can} = \frac{1}{2\pi i}\eta$, and let $\theta = \frac{1}{2\pi i}\frac{d}{d\tau} = q\frac{d}{dq}$. Then ω_{can} is the canonical differential dt/t on the Tate curve Tate(q) over $\mathbf{C}((q))$, η_{can} is the d.s.k. "dual" to ω_{can} in the sense of the splitting (A1.2.6), and the Gauss-Manin connection on $\mathbf{H}^1_{DR}(\mathrm{Tate}(q)/\mathbf{C}((q)))$ is given in terms of $\omega = \frac{1}{2\pi i}\omega_{can}$ and $\eta = 2\pi i\,\eta_{can}$ by

$$\begin{aligned}\nabla(\theta)\begin{pmatrix}\omega\\ \eta\end{pmatrix} &= \frac{1}{2\pi i}\begin{pmatrix}\nabla_\tau(\omega)\\ \nabla_\tau(\eta)\end{pmatrix} = \frac{-1}{4\pi^2}\begin{pmatrix}\frac{\pi^2 P}{3} & 1\\ \frac{\pi^4}{9}(P^2-12\theta P) & -\frac{\pi^2 P}{3}\end{pmatrix}\begin{pmatrix}\omega\\ \eta\end{pmatrix}\\ &= \begin{pmatrix}\frac{-P}{12} & \frac{-1}{4\pi^2}\\ \frac{\pi^2}{36}(P^2-12\theta P) & \frac{P}{12}\end{pmatrix}\begin{pmatrix}\omega\\ \eta\end{pmatrix}\end{aligned} \tag{A1.3.15}$$

and hence is given in terms of ω_{can}, η_{can} by

$$\nabla(\theta)\begin{pmatrix}\omega_{can}\\ \eta_{can}\end{pmatrix} = \begin{pmatrix}\frac{-P}{12} & 1\\ \frac{P^2-12\theta P}{144} & \frac{P}{12}\end{pmatrix}\begin{pmatrix}\omega_{can}\\ \eta_{can}\end{pmatrix}. \tag{A1.3.16}$$

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

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

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

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

<u>A1.4 The Gauss-Manin connection and Serre's ∂ operator ([41]): d'après Deligne</u>

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

We now view the Gauss-Manin connection on $H^1_{DR}(E/S)$, where S is a smooth T-scheme, as an arrow $\nabla\colon H^1_{DR}(E/S) \longrightarrow H^1_{DR}(E/S)\otimes\Omega^1_{S/T}$. Its k'th symmetric power is a connection on $\mathrm{Symm}^k(H^1)$, so an arrow

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

A1.4.1 $$\sum_{j=0}^{k} \underline{\omega}^{\otimes k-2j} \longrightarrow \sum_{j=0}^{k} \underline{\omega}^{\otimes k-2j}\otimes\underline{\omega}^{\otimes 2} = \sum_{j=0}^{k} \underline{\omega}^{\otimes k+2-2j} .$$

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

$$\theta(f)\cdot(\omega_{can})^{\otimes 2}\cdot(\omega_{can})^{\otimes a}\cdot(\eta_{can})^{\otimes b}\cdot$$
$$+ f\cdot a\cdot(\omega_{can})^{\otimes a-1}\left(\frac{-P}{12}\,\omega_{can} + \eta_{can}\right)\otimes(\omega_{can})^{\otimes 2}\otimes(\eta_{can})^{b}$$
$$+ f\cdot(\omega_{can})^{\otimes a}\cdot b\cdot(\eta_{can})^{\otimes b-1}\left(\frac{P^2-12\theta P}{144}\,\omega_{can} + \frac{P}{12}\,\eta_{can}\right)\cdot(\omega_{can})^{\otimes 2}$$

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

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

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

(A1.4.2) $$\begin{cases} \theta(f) - kf\cdot\frac{P}{12} & \text{is modular of weight } k+2 = a+2-b \\ af & \text{is modular of weight } k = a-b \\ b\cdot f\cdot\left[\frac{P^2-12\,\theta P}{144}\right] & \text{is modular of weight } k+4 = a+3-(b-1) . \end{cases}$$

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

Corollary A1.4.3. $P^2 - 12\,\theta P$ is modular of weight 4, hence $P^2 - 12\,\theta P = E_4 \overset{\text{dfn}}{=\!=} Q$.

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

Corollary A1.4.4. (Deligne) $P = \frac{\theta\Delta}{\Delta}$, where Δ denotes the unique normalized cusp form of weight 12, the discriminant $(E_4^3 - E_3^4)/1728$.

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

Corollary A1.4.5. The Gauss-Manin connection on H^1_{DR} of Tate(q) over $\mathbf{Z}[1/6]((q))$ is given by

$$\begin{pmatrix} \nabla(\theta)(\omega_{can}) \\ \nabla(\theta)(\eta_{can}) \end{pmatrix} = \begin{pmatrix} \frac{-P}{12} & 1 \\ \frac{Q}{144} & \frac{P}{12} \end{pmatrix} \begin{pmatrix} \omega_{can} \\ \eta_{can} \end{pmatrix}. \tag{A1.4.6}$$

Proof. ω_{can}, η_{can} give a base of H^1_{DR} over $\mathbf{Z}(\frac{1}{6})((q)) \subset \mathbf{C}((q))$, and we have the desired assertion by transcendental means over $\mathbf{C}((q))$.

Remarks.

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

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

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

(A1.5) Formulas

(A1.5.0) For $n \geq 3$, $\bar{M}_n$ is proper and smooth over $\mathbf{Z}[1/n]$, and its inverse image over $\mathbf{Z}[1/n, \zeta_n]$ is the disjoint union of $\varphi(n)$ proper smooth schemes with geometrically connected fibres $\bar{M}_n^{\zeta}$, one for each primitive n'th root of unity ζ (corresponding to the value of the e.m. pairing on the given basis of points of order n). The $\mathbf{Z}[1/n, \zeta_n]$ schemes $\bar{M}_n^{\zeta}$ are non-canonically isomorphic to each other. We give below the formulas for their (common) genus, the (common) number of their cusps, and the degree of the invertible sheaf $\underline{\omega}$. The method of deducing such relations is very simple: one notes that by flatness, the fact that $\bar{M}_n^{\zeta} - M_n^{\zeta}$ is a disjoint union of sections, and the isomorphism $\underline{\omega}^{\otimes 2} \simeq \Omega^1_{\bar{M}_n^{\zeta}/\mathbf{Z}[1/n, \zeta_n]}$ (log "cusps"), it suffices to calculate these invariants for any geometric fibre $\bar{M}_n^{\zeta} \otimes k$ [k any algebraically closed field containing $1/n$]. One then applies the standard Hurwitz formula to the morphism $\bar{M}_n^{\zeta} \otimes k \longrightarrow \mathbb{P}^1_k$ provided by the j-invariant. A closed point of $\mathbb{P}^1_k$ other than ∞ "is" an elliptic curve E over k, up to isomorphism. The points of $\bar{M}_n^{\zeta} \otimes k$ lying over it are the set of all level n structures on E such that the value of the e.m. pairing on the given basis of ${}_nE$ is ζ, modulo the natural action of $\mathrm{Aut}(E)$ of ${}_nE$. The cardinality of the fibre over the point "E" is thus $\#SL_2(\mathbf{Z}/n\,\mathbf{Z})/\#\,\mathrm{Aut}(E)$. For $j(E) \neq 0$, 1728, $\mathrm{Aut}(E) = \pm 1$, and hence over $\mathbb{P}^1_k - \{0, 1728, \infty\}$, the projection is étale of degree $\#SL_2(\mathbf{Z}/n\mathbf{Z})/2$. The fibre over 0 has $\#SL_2(\mathbf{Z}/n\mathbf{Z})/6$ points, and that over 1728 has $\#SL_2(\mathbf{Z}/n\mathbf{Z})/4$ points. The points over ∞ are the cusps, each of which is ramified of degree n, hence the number of cusps is $\#SL_2(\mathbf{Z}/n\mathbf{Z})/2n$. Letting χ denote the topological Euler characteristic, we thus have the formula:

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

i.e., $\chi(\bar{M}_n^{\zeta} \otimes k) = \#SL_2(\mathbf{Z}/n\,\mathbf{Z})\,[\tfrac{1}{6} + \tfrac{1}{4} + \tfrac{1}{2n} - \tfrac{1}{2}] = \#SL_2(\mathbf{Z}/n\,\mathbf{Z}) \cdot [\tfrac{6-n}{12n}]$. Now

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

(A1.5.1) Formulas

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

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

(A1.5.4) degree($\underline{\omega}$) on $\overline{M}_n^{\zeta} = \frac{1}{2}\deg(\Omega^1(\log \text{cusps})) = \frac{1}{2}(2g-2 + \#\text{ cusps})$

$$= (\frac{n-6}{24n} + \frac{1}{4n}) \#SL_2(\mathbb{Z}/n\mathbb{Z})$$

$$= \frac{1}{24} \#SL_2(\mathbb{Z}/n\mathbb{Z}) .$$

(A1.5.5) Sample consequences

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

Appendix 2 - Frobenius

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

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

<u>Lemma (A2.1).</u> On $\underline{\omega}$, $F(\varphi) = p\varphi$; on $\underline{\omega}^{-1}$, $F(\varphi) = \varphi$.

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

$F(\varphi)(f(E,\omega) \overset{\text{dfn}}{=\!=} \pi^*((f(E,\omega)\cdot\omega)^{(\varphi)}) = \varphi(f(E,\omega))\cdot\pi^*(\omega^{(\varphi)}) = \varphi(f(E,\omega))\cdot \frac{p\omega}{\lambda}$, [the last equality because $p\omega = [p]^*(\omega) = \pi^*(\check{\pi}^*(\omega)) = \pi^*(\lambda\cdot\omega^{(\varphi)}) = \lambda\cdot\pi^*(\omega^{(\varphi)})]$. Thus $F(\varphi) = p\varphi$ as φ-linear endomorphism.

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

<u>A2.2 Calculation at ∞</u>

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

A2.2.1
$$\begin{cases} \displaystyle\int_{\gamma_1(\tau)} \pi^*(\omega_{can}(q^p)) = \int_{\pi\gamma_1} \omega_{can}(q^p) = \int_{\gamma_1(p\tau)} \omega_{can}(q^p) = p\tau \\[2ex] \displaystyle\int_{\gamma_2(\tau)} \pi^*(\omega_{can}(q^p)) = \int_{\pi\gamma_2} \omega_{can}(q^p) = \int_{p\cdot\gamma_2(p\tau)} \omega_{can}(q^p) = p\ . \end{cases}$$

By functionality, $F(\varphi)$ respects the Gauss-Manin connection, and $\nabla(\theta)(\omega_{can}) = \frac{-p}{12}\,\omega_{can} + \eta_{can}$ is the <u>unique</u> (up to scalars) element of $H^1_{DR}(\mathrm{Tate}(q)/\mathbf{Z}((q)))$ killed by $\nabla(\theta)$ (as a direct calculation shows - indeed by (A1.4.6), this rank two differential equation over $\mathbb{C}$ has non-trivial (unipotent) monodromy around $q = 0$, hence has at most <u>one</u> solution which is single-valued at $q = 0$). It follows that

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

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

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

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

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

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

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

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

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

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

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

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

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

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

so we want $f \in R$ to satisfy

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

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

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

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

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

Looking at ∞ , we see that in terms of the base $\omega_{can}, \nabla(\theta)(\omega_{can})$ of $H^1_{DR}(\mathrm{Tate}(q)/\mathbf{Z}((q)))$, we have simply "<u>constructed</u>" the vector $\nabla(\theta)(\omega_{can})$, which is indeed fixed by $F(\varphi)$. Hence we have proven

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

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

$0 \longrightarrow \underline{\omega} \longrightarrow H^1_{DR}(E/\overline{M}_n(W(\mathbb{F}_q),1)) \longrightarrow \underline{\omega}^{-1} \longrightarrow 0$, (the <u>image</u> of which we denote $U \subset H^1_{DR}(E/\overline{M}_n(W(\mathbb{F}_q),1))$; it is a horizontal (by unicity!) $F(\varphi)$-stable rank one submodule).

<u>A2.4 P as a p-adic modular form of weight 2</u>

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

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

Clearly the right-hand expression is independent of the choice of base u of U, and the effect of replacing ω by $\lambda\omega$, $\lambda \in R^\times$ is to replace η by $\lambda^{-1}\eta$, hence $\tilde{P}(E/R,\lambda\omega) = \lambda^{-2}\tilde{P}(E/R,\omega)$. Hence $\tilde{P}$ is a p-adic modular form of weight two and level one. Its q-expansion is

$$\text{A2.4.2} \qquad \tilde{P}(\text{Tate}(q),\omega_{\text{can}}) = 12\,\frac{\langle\eta_{\text{can}},u\rangle}{\langle\omega_{\text{can}},u\rangle} = 12\,\frac{\langle\eta_{\text{can}},\nabla(\theta)(\omega_{\text{can}})\rangle}{\langle\omega_{\text{can}},\nabla(\theta)(\omega_{\text{can}})\rangle}$$

because, formally at ∞ , U is spanned by $\nabla(\theta)(\omega_{\text{can}})$. If we denote by $P(q)$ the series $1 - 24\Sigma\ \sigma_1(n)q^n$, then by (A1.3.16) we have $\nabla(\theta)(\omega_{\text{can}}) = \frac{-P(q)}{12}\,\omega_{\text{can}} + \eta_{\text{can}}$. Substituting into (A2.4.2) gives

$$\text{(A2.4.3)} \qquad \tilde{P}(\text{Tate}(q),\omega_{\text{can}}) = 12\,\frac{\langle\eta_{\text{can}},\frac{-P(q)}{12}\,\omega_{\text{can}}+\eta_{\text{can}}\rangle}{\langle\omega_{\text{can}},\frac{-P(q)}{12}\,\omega_{\text{can}}+\eta_{\text{can}}\rangle} = \frac{12\cdot P(q)}{12}\,\frac{\langle\eta_{\text{can}},-\omega_{\text{can}}\rangle}{\langle\omega_{\text{can}},\eta_{\text{can}}\rangle}$$

$$= P(q)\ .$$

This provides a modular proof that P is p-adically modular.

Appendix 3: Hecke polynomials, coherent cohomology, and U

In this final appendix, we explain the relation between Hecke polynomials mod p, coherent cohomology, and the endomorphism U of $S(R,r,n,0)\otimes K$ (notations as in (3.11)).

(A3.1.0) Let us begin by computing the trace of U^n, using the Dwork-Monsky fixed point formula. For simplicity, we take R to have residue field $\mathbb{F}_p$. Let R_m be its unramified extension of degree m, and K_m the fraction field of R_m. The endomorphism φ acts on the points of $\overline{M}_n(\mathbb{F}_p,1)$ with values in the algebraic closure $\overline{\mathbb{F}}_p$ of $\mathbb{F}_p$ as the relative Frobenius. For each integer $m \geq 1$ we denote by T_m^o the set of $\overline{\mathbb{F}}_p$-valued points of $\overline{M}_n(\mathbb{F}_p,1)$ which are fixed by the m'th iterate φ^m, i.e., T_m^o is the set of $\mathbb{F}_{p^m}$-valued points of $\overline{M}_n(\mathbb{F}_p,1)$. It is known (cf.[36]) that each element of T_m^o lifts to a unique R_m-valued point of the formal scheme $\overline{M}_n(R,1)$ which is fixed by φ. We denote by T_m the set of such φ-fixed R_m-valued points of $\overline{M}_n(R,1)$ (so $T_m \xrightarrow{\sim} T_m^o$ by reduction mod $\mathfrak{P}$). The tangent space to $\overline{M}_n(R,1)$ at a point $t \in T_m$ is a free R_m-module of rank one, on which φ^m acts as an R_m-linear endomorphism. We denote by $d\varphi^m(t) \in R_m$ its "matrix". The Dwork-Monsky trace formula [36] is as follows:

$$\text{(A3.1.1)} \qquad \operatorname{trace}(U^m) = \sum_{t \in T_m} \frac{-1}{p^m} \, \frac{d\varphi^m(t)}{1-d\varphi^m(t)} .$$

It remains to determine the "local terms" in this formula. We begin with the cusps, i.e., the points $t \in T_m$ whose image $t_o \in T_m^o$ is a cusp of $\overline{M}_n(\mathbb{F}_q,1)$. Then, as we have seen, the overlying point $t \in T_m$ is itself a cusp of $\overline{M}_n(R_m,1)$, the completion of its local ring is $R_m[[q]]$, and the action of φ^m is given by $q \longmapsto q^{p^m}$, whose linear term is zero. Hence $d\varphi^m(t) = 0$ at the cusps.

Now suppose $t \in T_m$ is not a cusp. Then the corresponding elliptic curve E_t is the so-called canonical lifting of its reduction E_{t_o} (because the m'th iterate of the Frobenius endomorphism of E_{t_o} lifts to an endomorphism of E_t, namely m-fold division by the canonical subgroup -(cf.Messing [34]). In this case it is known that the completion of the local ring at t is isomorphic to $R_m[[X]]$, where $1+X$ is the Serre-Tate parameter (cf. ft note, p.186). Let $\alpha \in \mathbf{Z}_p^x = \alpha(m,t_o)$ be the "matrix" of the action of the automorphism "p^m-th power" acting on the Tate module $T_p(E_{t_o}(\overline{\mathbb{F}}_p))$ of the reduced curve. Then (cf.Messing [34]), the action of φ^m on $R_m[[X]]$ is the one sending $1+X \longrightarrow (1+X)^{p^m/\alpha^2}$, hence $d\varphi^m(t) = p^m/\alpha(m,t_o)^2$. Combining all this, we find the formula

(A3.1.2) $$\operatorname{trace}(U^m) = \sum_{\substack{t \in T_m \\ t \text{ not a cusp}}} \frac{1}{p^m - \alpha(m,t_o)^2} .$$

Denoting by T_m^{oo} the set of $\mathbb{F}_{p^m}$-valued points of $M_n(\mathbb{F}_p,1)$, i.e. the set of ordinary elliptic curves over $\mathbb{F}_{p^m}$ with level n structure, we have

(A3.1.3) $$\operatorname{trace}(U^m) = \sum_{t_o \in T_m^{oo}} \frac{1}{p^m - \alpha(m,t_o)^2} .$$

The next step is to assemble this data into an expression for the Fredholm determinant $\det(1-tU)$ as a product of L-series on $M_n(\mathbb{F}_p,1)$. For any closed point x of $M_n(\mathbb{F}_p,1)$ (i.e., an orbit of $\mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$ acting on the $\overline{\mathbb{F}}_p$- valued ppints of $M_n(\mathbb{F}_p,1)$), we define $\alpha(x) = \alpha(\deg(x),\tilde{x})$, where $\tilde{x}$ is any $\mathbb{F}_{p^{\deg(x)}}$-valued point of $M_n(\mathbb{F}_p,1)$ lying over x. For each integer r, the L-series $L(M_n(\mathbb{F}_p,1);\alpha^r;t)$ is the element of $\mathbf{Z}_p[[t]]$ given by the infinite product over all closed points x of $M_n(\mathbb{F}_p,1)$

(A3.1.4) $$\prod_x (1-\alpha^r(x)\cdot t^{\deg(x)})^{-1} .$$

An elementary calculation now yields the following identity.

Identity A3.1.5

$$\det(1-tU) = \prod_{r \geq 0} L(M_n(\mathbb{F}_p,1),\alpha^{-2(r+1)},p^r t)$$ (which is the key point

of [12]). It shows <u>independently</u> of (3.11.7) that $\det(1-tU)$ lies in $\mathbf{Z}_p[[t]]$, and gives as a corollary the following congruence formula.

<u>Corollary A3.1.6.</u> $\det(1-tU) \equiv L(M_n(\mathbb{F}_p,1), \alpha^{p-3},t)$ modulo $p\cdot\mathbf{Z}_p[[t]]$.

<u>Proof.</u> the term with $r=0$ remains modulo p, and modulo p the characters α^{-2} and α^{p-3} are equal, hence give L-series which coincide mod p.

But the character $\alpha_0 = \alpha$ mod p is the one associated to the locally constant rank-one $\mathbb{F}_p$-etalé sheaf $R^1f_*\mathbb{F}_p$, and the L-series $L(M_n(\mathbb{F}_p,1), \alpha_0^{p-3},t)$ is just the L-series $L(M_n(\mathbb{F}_p,1), (R^1f_*\mathbb{F}_p)^{\otimes p-3},t)$ associated to $(R^1f_*\mathbb{F}_p)^{\otimes p-3}$ in (4.1.1).

[NB the apparent inversion is due to the fact that α describes the action of the arithmetic Frobenius on the etalé quotient of Ker p, and hence by duality it is the action of the <u>geometric</u> Frobenius on its dual $R^1f_*\mathbb{F}_p$.]

Furthermore, the sheaf $R^1f_*\mathbb{F}_p$ <u>extends</u> to a locally constant rank-one $\mathbb{F}_p$-etalé sheaf on $\overline{M}_n(\mathbb{F}_p,1)$, and the value of the <u>extended</u> character (still denoted α_0) is 1 at each cusp (cf. (4.2.1)). Thus we have

$$\text{(A3.1.7)} \quad L(M_n(\mathbb{F}_p,1),\alpha_0^{p-3},t) = \Big[\prod_{\substack{x \text{ closed} \\ \text{point among} \\ \text{the cusps}}} (1-t^{\deg x})\Big]\cdot L(\overline{M}_n(\mathbb{F}_p,1),(R^1f_*\mathbb{F}_p)^{\otimes p-3},t).$$

<u>(A3.2.)</u> Let H^i_{comp} denote the etalé cohomology groups with compact supports $H^i_{\text{comp}}(\overline{M}_n(\overline{\mathbb{F}}_p,1),(R^1f_*\mathbb{F}_p)^{\otimes p-3})$, which are $\mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$-modules over $\mathbb{F}_p$. Only H^1_{comp} is $\neq 0$. Let $F_{\text{geom}} \in \mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$ denote the <u>inverse</u> of the automorphism $x \longrightarrow x^p$. According to ([47]), we have the formula

$$\text{(A3.2.1)} \qquad L(\overline{M}_n(\mathbb{F}_p,1),(R^1f_*\mathbb{F}_p)^{\otimes p-3},t) = \det(1-t\,F_{\text{geom}}|H^1_{\text{comp}}).$$

By (4.2.2), the invertible sheaf with p-linear "automorphism" corresponding to $(R^1f_*\mathbb{F}_p)^{\otimes p-3}$ is $(\underline{\omega}^{3-p},\varphi)$ over $M_n(\mathbb{F}_p,1)$. But the pair $(\underline{\omega}^{\otimes 3-p},\varphi)$ extends to an invertible sheaf with p-linear endomorphism <u>on all</u> of $\overline{M}_n\otimes\mathbb{F}_p$, namely to the invertible sheaf $\underline{\omega}^{\otimes 3-p}$ on $\overline{M}_n\otimes\mathbb{F}_p$, with p-linear <u>endomorphism</u>

$$\bar{\varphi}: \underline{\omega}^{\otimes 3-p} \longrightarrow \underline{\omega}^{\otimes 3-p}$$

given by

$$\bar{\varphi}: g \longrightarrow A^{p-3}.g^p$$

where $A = E_{p-1} \bmod p$ denotes the <u>Hasse invariant</u> $\in \Gamma(\bar{M}_n \otimes \mathbb{F}_p, \underline{\omega}^{\otimes p-1})$, (compare q-expansions!)

Because this <u>extended</u> endomorphism <u>vanishes</u> at the fibres <u>outside</u> $\bar{M}_n(\mathbb{F}_p, 1)$, we have an isomorphism

(A3.2.2) $\quad H^i_{\mathrm{comp}} \simeq$ the <u>fixed</u> points of $\bar{\varphi}$ acting p-linearly on

$$H^i(\bar{M}_n \otimes \bar{\mathbb{F}}_p, \underline{\omega}^{\otimes 3-p})$$

under which the action of the <u>arithmetic</u> Frobenius on H^i_{comp} is its obvious action on the fixed points of $\bar{\varphi}$. It follows formally that we have the identity

(A3.2.3) $$\det(1 - t\, F_{\mathrm{geom}} | H^i_{\mathrm{comp}}) = \det(1 - t\bar{\varphi} | H^i(\bar{M}_n \otimes \bar{\mathbb{F}}_p, \underline{\omega}^{\otimes 3-p})) .$$

Putting this all together, we have the following congruence relation modulo $p\, \mathbb{Z}_p[[t]]$.

(A3.2.4) $$\det(1 - tU) \equiv \Big[\prod_{\substack{x \text{ closed} \\ \text{point lying} \\ \text{among the cusps}}} (1 - t^{\deg x})\Big] \cdot \det(1 - t\bar{\varphi} | H^1(\bar{M}_n \otimes \bar{\mathbb{F}}_p, \underline{\omega}^{\otimes 3-p})) .$$

<u>(A3.3)</u> We now wish to calculate the determinant of $\bar{\varphi}$ on $H^1(\bar{M}_n \otimes \bar{\mathbb{F}}_p, \underline{\omega}^{\otimes 3-p})$ by using Serre duality and the <u>Cartier operator</u>. For this it is convenient to abstract the situation slightly in the following lemma - in which X is $\bar{M}_n \otimes \mathbb{F}_p$, $\mathcal{L}$ is $\underline{\omega}^{\otimes p-3}$, and B is A^{p-3}.

<u>Lemma A3.3.1.</u> Let X be a projective smooth curve over $\mathbb{F}_p$, $\mathcal{L}$ an invertible sheaf, and B a section of $\mathcal{L}^{\otimes p-1}$. The composition

(A3.3.2) $$\mathcal{L} \otimes \Omega^1_X \xrightarrow{B} \mathcal{L}^{\otimes p} \otimes \Omega^1_X \xrightarrow{C} \mathcal{L} \otimes \Omega^1_X$$

(where C is the Cartier operation, defined locally by $C(\ell^p \otimes \omega) = \ell \otimes C(\omega)$) induces an endomorphism of $H^0(X, \mathcal{L} \otimes \Omega^1)$ which is dual to the endomorphism of $H^1(X, \mathcal{L}^{-1})$ induced by the endomorphism $\check{\ell} \longrightarrow B(\check{\ell})^p$ of $\mathcal{L}^{-1}$.

Proof. We begin by remarking that although $X \hookrightarrow \mathbb{P}^n$ need not be geometrically connected, Serre duality on $\mathbb{P}^n$ gives a perfect pairing between $H^i(X, \mathcal{F})$ and $\mathrm{Ext}^{1-i}_{\mathcal{O}_X}(\mathcal{F}, \Omega^1_X)$ with values in $H^n(\mathbb{P}^n, \Omega^m_{\mathbb{P}^n}) \simeq \mathbb{F}_p$ for any coherent $\mathcal{F}$ on X, which just as in the usual case may be computed via repartitions and residues. The desired duality now follows from the fact that if $x \in X$ is a closed point, and $\check{\ell}$ and ξ are meromorphic sections of $\mathcal{L}^{-1}$ and $\mathcal{L} \otimes \Omega^1$, then $\mathrm{residue}_x(B\cdot(\check{\ell})^p \cdot \xi) = (\mathrm{residue}_x(\check{\ell}\cdot C(B\xi)))^p$, (the usual Cartier formula applied to the one-form $B(\check{\ell})^p\xi$). QED

Lemma A3.3.3. Take $X = \bar{M}_n \otimes \mathbb{F}_p$, $\mathcal{L} = \underline{\omega}^{\otimes 2k}$, $k \geq 0$, and $B = A^{2k}$ in the previous lemma. Under the isomorphism $H^0(\bar{M}_n \otimes \mathbb{F}_p, \underline{\omega}^{\otimes 2k} \otimes \Omega^1) \simeq H^0(\bar{M}_n \otimes \mathbb{F}_p, \underline{\omega}^{\otimes 2k+2} \otimes I(\text{cusps})) \simeq$ the space of cusp forms of level n and weight $2k+2$ over $\mathbb{F}_p$, the endomorphism $\xi \longrightarrow C(A^{2k}\xi)$ is the Hecke operator T_p.

Proof. It suffices to check the q-expansions. But in terms of q-expansions and the isomorphism $\Omega^1_X(\log \text{cusps}) \simeq \underline{\omega}^{\otimes 2}$, if ξ in q-expansion is $f(q)(\frac{dq}{q})^{k+1}$ then $C(A^k\xi)$ in q-expansion is $C(f(q)\cdot(\frac{dq}{q})^{\otimes(2kp+2)/2}) = C(f(q)\frac{dq}{q})\cdot(\frac{dq}{q})^{\otimes k}$ But if $f(q) = \Sigma\, a_n q^n$, $C(f(q)\frac{dq}{q}) = \Sigma\, (a_{np})^{1/p}\cdot q^n \frac{dq}{q}$. Comparing this with the explicit formula (1.11.1.2) for T_p gives the desired result (because $p^{2k-1} \equiv 0\ (p)!$). QED

Putting this all together, we obtain the congruence relation mod $p\, \mathbb{Z}_p[[t]]$:

$$(A3.3.3)\quad\begin{cases}\det(1-tU) \equiv \left[\prod_{\substack{x \text{ closed}\\ \text{point lying}\\ \text{among the cusps}}} (1-t^{\deg x})\right]\cdot\det\left(1-tT_p \,\middle|\, \begin{matrix}\text{cusp forms of weight } p-1\\ \text{and level } n\end{matrix}\right)\\[2ex] \det\left(1-tT_p \,\middle|\, \begin{matrix}\text{cusp forms of weight } p-1\\ \text{and level } n\end{matrix}\right) \equiv \det\left(1-t\cdot C\circ A^{p-3} \,\middle|\, H^0(\overline{M}_n \otimes \mathbb{F}_p, \underline{\omega}^{\otimes p-3} \otimes \Omega^1)\right)\end{cases}$$

This formula is the starting point for recent work of Adolphson [0].

FOOTNOTE : the first new sentence on page 182 is incorrect, though the tangent calculation we deduce from it is correct. The difficulty is that the Serre-Tate parameter is not "rational" over R_m, but only over R_∞, the completion of the maximal unramified extension of R. However, if we view t as defining, by extension of scalars, a rational point of $\overline{M}_n(R_\infty,1)$, then the completion of its local ring is indeed isomorphic to $R_\infty[[X]]$, where $1+X$ is the Serre-Tate parameter (cf. Messing [34]). Further, the R_∞-linear endomorphism of $R_\infty[[X]]$ deduced from ϕ^m by extension of scalars is given by $1+X \mapsto (1+X)^{p^m/\alpha^2}$, in the notation of page 182, and the formula (A3.1.2) remains true.

References

0. Adolphson, A.: Thesis, Princeton University 1973.

1. Atkin, A. O. L.: Congruence Hecke operators, Proc. Symp. Pure Math., vol. 12,

2. ----- : Congruences for modular forms. Proceedings of the IBM Conference on Computers in Mathematical Research, Blaricium, 1966. North-Holland (1967).

3. ----- , and J. N. O'Brien: Some properties of p(n) and c(n) modulo powers of 13. TAMS 126, (1967), 442-459.

4. Cartier, P.: Une nouvelle opération sur les formes différentielles, C. R. Acad. Sci. Paris 244, (1957), 426-428.

5. ----- : Modules associés à un groupe formel commutatif.Courbes typiques. C. R. Acad. Sci. Paris 256, (1967), 129-131.

6. ----- : Groupes formels, course at I.H.E.S., Spring, 1972. (Notes by J. F. Boutot available (?) from I.H.E.S., 91-Bures-sur-Yvette, France.)

7. Deligne, P.: Formes modulaires et représentations ℓ-adiques. Exposé 355. Séminaire N. Bourbaki 1968/1969. Lecture Notes in Mathematics 179, Berlin-Heidelberg-New York: Springer 1969.

8. ----- : Equations Différentielles à Points Singuliers Réguliers. Lecture Notes in Mathematics 163. Berlin-Heidelberg-New York: Springer 1970.

9. ----- : Courbes Elliptiques: Formulaire (d'après J. Tate). Multigraph available from I.H.E.S., 91-Bures-sur-Yvette, France, 1968.

10. ----- , and M. Rapoport: Article in preparation on moduli of elliptic curves.

11. Dwork, B.: P-adic cycles, Pub. Math. I.H.E.S. 37, (1969), 27-115.

12. ----- : On Hecke Polynomials, Inventiones Math. 12(1971), 249-256.

13. ----- : Normalized Period Matrices I, II. Annals of Math. 94, 2nd series, (1971), 337-388, and to appear in Annals of Math.

14. ----- : Article in this volume.

15. Grothendieck, A.: Fondements de la Géométrie Algébrique, Secrétariat Mathématique, 11 rue Pierre Curie, Paris 5^e, France, 1962.

15 bis -----: Formule de Lefschetz et rationalité des fonctions L, Exposé 279, Séminaire Bourbaki 1964/1965.

16. Hasse, H. : Existenz separabler zyklischer unverzweigter Erweiterungskörper vom Primzahlgrade über elliptischen Funktionenkörpern der Charakteristik p . J. Reine angew. Math. 172, (1934), 77-85.

17. Igusa, J. : Class number of a definite quaternion with prime discriminant, Proc. Natl. Acad. Sci. 44, (1958), 312-314.

18. -----: Kroneckerian model of fields of elliptic modular functions, Amer. J. Math. 81, (1959), 561-577.

19. -----: Fibre systems of Jacobian varieties III, Amer. J. Math. 81, (1959), 453-476.

20. -----: On the transformation theory of elliptic functions, Amer. J. Math. 81, (1959), 436-452.

21. -----: On the algebraic theory of elliptic modular functions, J. Math. Soc. Japan 20, (1968), 96-106.

22. Ihara, Y.: An invariant multiple differential attached to the field of elliptic modular functions of characteristic p. Amer. J. Math. 78, (1971), 137-147.

23. Katz, N.: Une formule de congruence pour la fonction zeta. Exposé 22, SGA 7, 1969, to appear in Springer Lecture Notes in Mathematics. (Preprint available from I.H.E.S., 91-Bures-sur-Yvette, France.)

24. -----: Nilpotent connections and the monodromy theorem - applications of a result of Turrittin, Pub. Math. I.H.E.S. 39, (1971), 355-412.

25. -----: Travaux de Dwork. Exposé 409, Séminaire N. Bourbaki 1971/72, Springer Lecture Notes in Mathematics, 317, (1973), 167-200.

26. -----: Algebraic solutions of differential equations (p-curvature and the Hodge filtration). Invent. Math. 18, (1972), 1-118.

27. -----, and T. Oda: On the differentiation of de Rham cohomology classes with respect to parameters, J. Math. Kyoto Univ. 8, (1968), 199-213.

28. Koike, M.: Congruences between modular forms and functions and applications to a conjecture of Atkin, to appear.

29. Lehner, J.: Lectures on modular forms. National Bureau of Standards, Applied Mathematics Series 61, Washington, D.C., 1969.

30. Lubin, J., J.-P. Serre and J. Tate: Elliptic curves and formal groups, Woods Hole Summer Institute 1964 (mimeographed notes).

31. Lubin, J.: One-parameter formal Lie groups over p-adic integer rings, Ann. of Math. 80, 2nd series (1964), 464-484.

32. -----: Finite subgroups and isogenies of one-parameter formal groups, Ann. of Math. 85, 2nd series (1967), 296-302.

33. -----: Newton factorizations of polynomials, to appear.

33.bis ----: Canonical subgroups of formal groups, secret notes.

34. Messing, W.: The crystals associated to Barsotti-Tate groups: with applications to abelian schemes. Lecture Notes in Mathematics 264, Berlin-Heidelberg-New York: Springer 1972.

35. -----: Two functoriality, to appear.

36. Monsky, P.: Formal cohomology III - Trace Formulas. Ann. of Math. 93, 2nd series (1971), 315-343.

37. Newman, M.: Congruences for the coefficients of modular forms and for the coefficients of $j(\tau)$. Proc. A.M.S. 9, (1958), 609-612.

38. Roquette, P.: Analytic theory of elliptic functions over local fields. Göttigen: Vanderhoeck und Ruprecht, 1970.

39. Serre, J.-P.: Endomorphismes complètement continus des espaces de Banach p-adiques. Pub. Math. I.H.E.S. 12, (1962).

40. -----: Course at Collège de France, spring 1972.

41. -----: Congruences et formes modulaires. Exposé 416, Séminaire N. Bourbaki, 1971/72, Lecture Notes in Math. 317, (1973), Springer, 319-338.

42. -----: Formes modulaires et fonctions zêta p-adiques, these Proceedings.

$42\frac{1}{2}$. -----: Cours d'arithmétique. Paris: Presses Univ. de France 1970.

43. Swinnerton-Dyer, H. P. F.: On ℓ-adic representations and congruences for coefficients of modular forms, these Proceedings.

44. Tate, J.: Elliptic curves with bad reduction. Lecture at the 1967 Advanced Science Summer Seminar, Bowdoin College, 1967.

45. -----: Rigid analytic spaces. Inventiones Math. 12, (1971), 257-289.

46. Whittaker, E. T. and G. N. Watson: A course of modern analysis, Cambridge, Cambridge University Press, 1962.

47. Deligne, P., Cohomologie à Supports Propres, Exposé 17, SGA 4, to appear in Springer Lecture Notes in Mathematics.

48. Roos, J. E., Sur les foncteurs dérivés de $\varprojlim$. Applications, C. R. Acad. Sci. Paris, tome 252, 1961, pp. 3702-04.

Summer School on Modular Functions
ANTWERP 1972

Formes modulaires et fonctions zêta p-adiques

par Jean-Pierre SERRE

à Carl Ludwig Siegel
à l'occasion de son 76-ième anniversaire

Table des Matières

Introduction

Soient K un corps de nombres algébriques totalement réel, et ζ_K sa fonction zêta. D'après un théorème de Siegel [24], $\zeta_K(1-k)$ est un nombre rationnel si k est entier ≥ 1; il est $\neq 0$ si k est pair. Lorsque K est abélien sur **Q**, on peut écrire ce nombre comme produit de "nombres de Bernoulli généralisés" :

$$\zeta_K(1-k) = \prod_\chi L(\chi, 1-k) = \prod_\chi (-b_k(\chi)/k), \qquad \text{cf. [18]},$$

où χ parcourt l'ensemble des caractères de **Q** attachés à K. Cela permet de démontrer des propriétés de congruence reliant les $\zeta_K(1-k)$ pour diverses valeurs de k, et d'en déduire par interpolation une fonction zêta p-adique pour le corps K, au sens de Kubota-Leopoldt (cf. [7], [10], [11], [16]).

Dans ce qui suit, je me propose d'étendre une partie de ces résultats au cas d'un corps totalement réel quelconque (non nécessairement abélien sur **Q**). La méthode suivie est celle de Klingen [13] et Siegel [25], [26]. Elle consiste à utiliser le fait que $\zeta_K(1-k)$ est le terme constant d'une certaine forme modulaire sur $SL_2(\mathbf{Z})$ dont les autres termes se calculent par des formules simples (ce sont des combinaisons linéaires d'exponentielles en k). Tout revient donc à transférer les propriétés de ces termes au terme constant lui-même. On est amené, pour ce faire, à définir les "formes modulaires p-adiques", limites de formes modulaires au sens usuel (sur le groupe $SL_2(\mathbf{Z})$); de telles formes intervenaient déjà, au moins implicitement, dans les travaux d'Atkin sur les coefficients c(n) de l'invariant modulaire j, cf. [2]. L'étude de ces formes fait l'objet des §§ 1, 2 et 3; elle repose de façon essentielle sur le théorème récent de Swinnerton-Dyer [27] donnant la structure de l'algèbre des formes modulaires (mod.p). Les principaux résultats sont les suivants :

a) Une forme modulaire p-adique a un poids qui est, non plus un entier, mais un élément d'un certain groupe p-adique $X = \mathbf{Z}_p \times \mathbf{Z}/(p-1)\mathbf{Z}$, cf. n°1.4.

b) Si

$$f = \sum_{n=0}^{\infty} a_n(f)\, q^n$$

est une forme modulaire p-adique de poids $\neq 0$, il existe des formules donnant $a_o(f)$ en termes des $a_n(f)$, $n \geq 1$, cf. n°2.3.

c) Toute forme modulaire (au sens usuel) sur le groupe $\Gamma_o(p)$ est une forme modulaire p-adique, cf. §3.

Dans l'application aux fonctions zêta, on rencontre des familles (f_s) de formes modulaires p-adiques dépendant (ainsi que leur poids) d'un paramètre p-adique s. L'étude de ces familles fait l'objet du §4. Le cas le plus important est celui où les fonctions $s \mapsto a_n(f_s)$, $n \geq 1$, appartiennent à l'algèbre d'Iwasawa Λ du n°4.1; on en déduit alors des propriétés analogues pour la fonction $s \mapsto a_o(f_s)$, cf. n^{os} 4.6 et 4.7.

Une fois ces résultats établis, leur application à l'interpolation p-adique de ζ_K ne présente pas de difficultés; c'est l'objet du §5. La fonction zêta p-adique de K est définie au n° 5.3; ses principales propriétés sont données par les ths. 20, 21, et 22. De nombreuses questions restent ouvertes; on en trouvera une brève discussion au n°5.6.

§1. Formes modulaires p-adiques

1.1. Notations

a) Congruences

La lettre p désigne un nombre premier; on note v_p la valuation du corps p-adique $\mathbf{Q}_p$, normée de telle sorte que $v_p(p) = 1$; un élément x de $\mathbf{Q}_p$ est dit p-entier s'il appartient à $\mathbf{Z}_p$, i.e. si $v_p(x) \geqslant 0$.

Si $f = \sum a_n q^n \in \mathbf{Q}_p[[q]]$ est une série formelle en une indéterminée q, on pose

$$v_p(f) = \inf . v_p(a_n).$$

Ainsi, $v_p(f) \geqslant 0$ signifie que $f \in \mathbf{Z}_p[[q]]$. Lorsque $v_p(f) \geqslant m$, on écrit aussi $f \equiv 0 \pmod{p^m}$.

Soit (f_i) une suite d'éléments de $\mathbf{Q}_p[[q]]$. On dit que f_i tend vers f si les coefficients de f_i tendent uniformément vers ceux de f, i.e. si $v_p(f - f_i) \to +\infty$.

b) Séries d'Eisenstein

Si k est un entier pair $\geqslant 2$, nous poserons

$$G_k = -b_k/2k + \sum_{n=1}^{\infty} \sigma_{k-1}(n)\, q^n \qquad (q = e^{2\pi i z}),$$

$$E_k = -\frac{2k}{b_k} G_k = 1 - \frac{2k}{b_k} \sum_{n=1}^{\infty} \sigma_{k-1}(n)\, q^n,$$

où b_k désigne le k-ième nombre de Bernoulli et $\sigma_{k-1}(n) = \sum_{d|n} d^{k-1}$. Si $k \geqslant 4$, G_k et E_k sont des formes modulaires de poids k (relativement au groupe $SL_2(\mathbf{Z})$).

c) Les séries P,Q,R

On pose, avec Ramanujan,

$$P = E_2 = 1 - 24 \sum \sigma_1(n)\, q^n$$

$$Q = E_4 = 1 + 240 \sum \sigma_3(n)\, q^n$$

$$R = E_6 = 1 - 504 \sum \sigma_5(n)\, q^n.$$

Les séries Q et R engendrent l'algèbre graduée des formes modulaires : toute forme modulaire de poids k s'écrit de façon unique comme polynôme isobare de poids k en Q et R. Par exemple :

$$E_8 = Q^2, \quad E_{10} = QR, \quad E_{12} = \frac{441\, Q^3 + 250\, R^2}{691}, \quad E_{14} = Q^2R,$$

$$\Delta = 2^{-6}3^{-3}(Q^3 - R^2) = q \prod_{n=1}^{\infty} (1 - q^n)^{24} = \sum_{n=1}^{\infty} \tau(n) q^n.$$

La série P n'est pas une forme modulaire au sens habituel. Toutefois nous démontrerons plus loin (cf. n° 2.1) que c'est une "forme modulaire p-adique" de poids 2.

d) Exemples de congruences

D'après Kummer, $b_k/2k$ est p-entier si et seulement si k n'est pas divisible par p - 1; on a alors $v_p(G_k) = 0$. De plus, si $k' \equiv k \pmod{(p-1)}$, on a $b_k/2k \equiv b_{k'}/2k' \pmod{p}$; comme la congruence analogue pour $\sigma_{k-1}(n)$ est évidente, on en conclut que :

$$G_k \equiv G_{k'} \pmod{p} \quad \text{si } k' \equiv k \not\equiv 0 \pmod{(p-1)}.$$

(Plus généralement, il semble que toute congruence sur les nombres de Bernoulli puisse être étendue en une congruence sur les G_k.)

Lorsque k, par contre, est divisible par p - 1, le théorème de Clausen-von Staudt montre que $v_p(b_k/k) = -1 - v_p(k)$. On a donc $v_p(k/b_k) \geqslant 1$, d'où :

$$E_k \equiv 1 \pmod{p} \qquad \text{si } k \equiv 0 \pmod{(p-1)}.$$

Plus précisément :

$$E_k \equiv 1 \pmod{p^m} \Longleftrightarrow k \equiv 0 \pmod{(p-1)p^{m-1}} \quad \text{si } p \neq 2$$

$$E_k \equiv 1 \pmod{2^m} \Longleftrightarrow k \equiv 0 \pmod{2^{m-2}}.$$

1.2. <u>L'algèbre des formes modulaires</u> (<u>mod</u>.p)

Si $k \in Z$, notons M_k l'ensemble des formes modulaires

$$f = \sum_{n=0}^{\infty} a_n q^n,$$

de poids k, dont les coefficients a_n sont rationnels et p-entiers. Si $f \in M_k$, la réduction $\tilde{f}$ de f modulo p appartient à l'algèbre $\mathbf{F}_p[[q]]$ des séries formelles à coefficients dans $\mathbf{F}_p = \mathbf{Z}/p\mathbf{Z}$. L'ensemble des séries ainsi obtenues sera noté $\widetilde{M}_k$. On pose

$$\widetilde{M} = \sum_{k \in \mathbf{Z}} \widetilde{M}_k;$$

c'est une sous-algèbre de $\mathbf{F}_p[[q]]$, appelée <u>algèbre des formes modulaires</u> (<u>mod</u>.p). La structure de $\widetilde{M}$ a été déterminée par Swinnerton-Dyer [27]. Rappelons brièvement le résultat (pour plus de détails, voir [20] ou [27]) :

(i) <u>Le cas</u> $p \geq 5$

On a vu (n° 1.1) que $E_{p-1} \equiv 1 \pmod{p}$, autrement dit $\widetilde{E}_{p-1} = 1$. La multiplication par E_{p-1} applique M_k dans M_{k+p-1}, et l'on en déduit des inclusions :

$$\widetilde{M}_k \subset \widetilde{M}_{k+p-1} \subset \dots \subset \widetilde{M}_{k+n(p-1)} \subset \dots$$

Si $\alpha \in \mathbf{Z}/(p-1)\mathbf{Z}$, notons $\widetilde{M}^{\alpha}$ la réunion des $\widetilde{M}_k$, pour k parcourant α. L'un des résultats de Swinnerton-Dyer est que $\widetilde{M}$ <u>est somme directe des</u> $\widetilde{M}^{\alpha}$, pour $\alpha \in \mathbf{Z}/(p-1)\mathbf{Z}$; en d'autres termes, $\widetilde{M}$ est une algèbre graduée, de groupe des degrés $\mathbf{Z}/(p-1)\mathbf{Z}$; on a $\widetilde{M}^{\alpha} = 0$ si α est impair, i.e. non divisible par 2 dans $\mathbf{Z}/(p-1)\mathbf{Z}$. De plus, $\widetilde{M}$ s'identifie au quotient de l'algèbre de polynômes $\mathbf{F}_p[Q,R]$ par l'idéal principal engendré par $\widetilde{A} - 1$, où $\widetilde{A}(Q,R)$ est le polynôme isobare de poids $p - 1$ obtenu par réduction (mod.p) à partir du polynôme A tel que $E_{p-1} = A(Q,R)$. (En termes imagés, la relation $\widetilde{E}_{p-1} = 1$ est "la seule relation" entre formes modulaires (mod.p).)

Cette description de $\widetilde{M}$ montre que $\widetilde{M}$ (resp. sa sous-algèbre $\widetilde{M}^{\circ}$) est l'algèbre affine d'une courbe algébrique Y (resp. Y°) qui est lisse sur $\mathbf{F}_p$; on trouvera une interprétation "géométrique" de Y et de Y° dans [20], p.416-05; notons seulement ici que $\widetilde{M}$ et $\widetilde{M}^{\circ}$ sont des anneaux de Dedekind, puisque Y et Y° sont lisses.

Exemples

- Pour $p = 11$, on a $E_{p-1} = QR$, d'où :

$$\widetilde{M} = \mathbf{F}_{11}[Q,R]/(QR - 1) \quad \text{et} \quad \widetilde{M}^{\circ} = \mathbf{F}_{11}[Q^5,R^5]/(Q^5R^5 - 1).$$

Les courbes $Y = \mathrm{Spec}(\widetilde{M})$ et $Y^{\circ} = \mathrm{Spec}(\widetilde{M}^{\circ})$ sont des courbes de genre 0, ayant chacune deux points à l'infini, rationnels sur $\mathbf{F}_{11}$.

- Pour $p = 13$, on a $E_{p-1} = \dfrac{441\ Q^3 + 250\ R^2}{691}$, d'où :

$$\widetilde{M} = \mathbf{F}_{13}[Q,R]/(Q^3 + 10R^2 - 11) \quad \text{et} \quad \widetilde{M}^{\circ} = \mathbf{F}_{13}[Q^3].$$

La courbe Y (resp. Y°) est une courbe de genre 1 (resp. de genre 0), ayant un seul point à l'infini, rationnel sur $\mathbf{F}_{13}$.

(ii) Le cas $p = 2,3$

On a alors $\widetilde{Q} = \widetilde{R} = 1$. On en déduit facilement que $\widetilde{M}$ s'identifie à l'algèbre de polynômes $\mathbf{F}_p[\widetilde{\Delta}]$, engendrée par la réduction (mod.p) de Δ. On a $\widetilde{M}_{k-2} \subset \widetilde{M}_k$ et même $\widetilde{M}_{k-2} = \widetilde{M}_k$ si k n'est pas divisible par 12. On convient que $\widetilde{M}^{\circ} = \widetilde{M}$.

1.3. <u>Congruences (mod p^m) entre formes modulaires</u>

THÉORÈME 1. *Soit* m *un entier* $\geqslant 1$. *Soient* f *et* f' *deux formes modulaires à coefficients rationnels, de poids* k *et* k' *respectivement. On suppose que* $f \neq 0$ *et que*

$$v_p(f - f') \geqslant v_p(f) + m.$$

On a alors :

$$k' \equiv k \quad (\mathrm{mod.}(p-1)p^{m-1}) \qquad \textit{si} \quad p \geqslant 3$$

$$k' \equiv k \quad (\mathrm{mod.} 2^{m-2}) \qquad \textit{si} \quad p = 2.$$

Quitte à multiplier f par un scalaire, on peut supposer que $v_p(f) = 0$, auquel cas l'hypothèse équivaut à :

$$f' \equiv f \quad (\mathrm{mod.} p^m).$$

En particulier, les coefficients de f et de f' sont p-entiers, et l'on a $\tilde{f} = \tilde{f}' \neq 0$. Si $p \geqslant 5$, on voit que $\tilde{f}$ et $\tilde{f}'$ appartiennent à la même composante $\tilde{M}^{\alpha}$ de l'algèbre $\tilde{M}$ (cf. n° 1.2), autrement dit, on a $k' \equiv k$ (mod.(p-1)); la même congruence subsiste si p = 2 ou 3, puisque k' et k sont pairs. Le th.1 est donc démontré pour m = 1.

Supposons maintenant $m \geqslant 2$. Soit $h = k' - k$. Quitte à remplacer f' par

$$f'E_{(p-1)p^n}$$

avec n assez grand, on peut supposer que $h \geqslant 4$. La série d'Eisenstein E_h est alors une forme modulaire de poids h; comme h est divisible par p-1, on a $E_h \equiv 1$ (mod.p). Posons $r = v_p(h) + 1$ si $p \geqslant 3$ et $r = v_p(h) + 2$ si p = 2. Il nous faut montrer que $r \geqslant m$. Supposons que $r < m$. On a $f.E_h - f' = f - f' + f(E_h - 1)$.

Or $f - f' \equiv 0 \pmod{p^m}$ et $E_h - 1 \equiv 0 \pmod{p^r}$, cf. n° 1.1. On en conclut que $f.E_h - f' \equiv 0 \pmod{p^r}$ et que

$$p^{-r}(f.E_h - f') \equiv p^{-r}f(E_h - 1) \pmod{p}.$$

Or, d'après le théorème de Clausen-von Staudt, on a

$$p^{-r}(E_h - 1) = \lambda\phi, \quad \text{où} \quad \phi = \sum_{n=1}^{\infty} \sigma_{h-1}(n)q^n, \quad \text{et} \quad v_p(\lambda) = 0.$$

La congruence ci-dessus équivaut donc à

$$f\phi \equiv g \pmod{p},$$

où g est la forme modulaire $\lambda^{-1}p^{-r}(f.E_h - f')$, qui est de poids k'. Comme $\tilde{f} \neq 0$, ceci peut s'écrire $\tilde{\phi} = \tilde{g}/\tilde{f}$ et montre que $\tilde{\phi}$ appartient au corps des fractions de $\tilde{M}$; de plus, $\tilde{g}$ et $\tilde{f}$ ont même poids (mod.(p-1)); on en déduit que $\tilde{\phi}$ appartient au corps des fractions de $\tilde{M}^\circ$. Or, on a

$$\tilde{\phi} - \tilde{\phi}^p = \tilde{\psi}, \quad \text{avec} \quad \psi = \sum_{(p,n)=1} \sigma_{h-1}(n)q^n,$$

et on vérifie facilement que

$$\psi \equiv \theta^{h-1}\left(\sum_{n=1}^{\infty} \sigma_1(n)q^n\right), \quad \text{où} \quad \theta = q\, d/dq \quad \text{(cf. [27])}.$$

Pour tirer de là une contradiction, distinguons deux cas :

(i) $p \geqslant 5$.

On a alors

$$\tilde{\psi} = -\frac{1}{24}\,\theta^{h-1}(\tilde{P}) = -\frac{1}{24}\,\theta^{p-2}(\tilde{E}_{p+1}),$$

d'où $\tilde{\psi} \in \tilde{M}^{\circ}$, vu les propriétés de l'opérateur θ (cf. [20], [27]). L'équation $\tilde{\phi} - \tilde{\phi}^p = \tilde{\psi}$ montre que $\tilde{\phi}$ est <u>entier</u> sur $\tilde{M}^{\circ}$, donc appartient à $\tilde{M}^{\circ}$, puisque $\tilde{M}^{\circ}$ est intégralement clos; cela contredit le lemme de [20], p.416-11.

(ii) $p = 2$ ou 3.

On a alors $\tilde{\psi} = \tilde{\Delta}$, comme le montrent les congruences donnant $\tau(n)$ modulo 6. Or $\tilde{M} = \mathbf{F}_p[\tilde{\Delta}]$, et l'équation $X - X^p = \tilde{\Delta}$ est évidemment irréductible sur le corps $\mathbf{F}_p(\tilde{\Delta})$. On obtient encore une contradiction.

<u>Remarques</u>

1) Le fait que $\tilde{\phi}$ ne puisse pas appartenir au corps des fractions de $\tilde{M}^{\circ}$ peut aussi se démontrer par un argument de <u>filtration</u>, généralisant celui de [20], <u>loc</u>.<u>cit</u>.

2) Il serait intéressant de décrire géométriquement le revêtement cyclique de degré p de la courbe Y° (ou de la courbe Y) défini par l'équation $X - X^p = \tilde{\psi}$.

1.4. <u>Formes modulaires</u> p-<u>adiques</u>

a) <u>Le groupe</u> X

Soit m un entier ≥ 1 (resp. ≥ 2 si $p = 2$). Posons

$$X_m = \mathbf{Z}/(p-1)p^{m-1}\mathbf{Z} = \mathbf{Z}/p^{m-1}\mathbf{Z} \times \mathbf{Z}/(p-1)\mathbf{Z} \quad \text{si} \quad p \neq 2$$

et $$X_m = \mathbf{Z}/2^{m-2}\mathbf{Z} \quad \text{si} \quad p = 2.$$

Lorsque $m \to \infty$, les X_m forment de façon naturelle un <u>système projectif</u>; nous désignerons par X la limite projective de ce système. On a

$$X = \varprojlim X_m = \begin{cases} \mathbf{Z}_p \times \mathbf{Z}/(p-1)\mathbf{Z} & \text{si} \quad p \neq 2 \\ \mathbf{Z}_2 & \text{si} \quad p = 2, \end{cases}$$

où $\mathbf{Z}_p$ est l'anneau des entiers p-adiques. Le groupe X est un groupe de Lie p-adique compact de dimension 1. L'homomorphisme canonique $\mathbf{Z} \to X$

est injectif; nous l'utiliserons pour identifier $\mathbf{Z}$ à un sous-groupe dense de X.

Il y a souvent intérêt à considérer les éléments de X comme des caractères (p-adiques) du groupe $\mathbf{Z}_p^*$ des unités p-adiques. De façon plus précise, soit V_p le groupe des endomorphismes continus de $\mathbf{Z}_p^*$, muni de la topologie de la convergence uniforme. On vérifie facilement que l'application naturelle de $\mathbf{Z}$ dans V_p se prolonge en un homomorphisme continu $\varepsilon : X \to V_p$. Cet homomorphisme est injectif si $p = 2$, et bijectif si $p \neq 2$. Si $k \in X$, et $v \in \mathbf{Z}_p$, on note v^k le transformé de v par l'endomorphisme $\varepsilon(k)$ de $\mathbf{Z}_p$. Si l'on écrit $k = (s,u)$, avec $s \in \mathbf{Z}_p$, $u \in \mathbf{Z}/(p-1)\mathbf{Z}$, et si l'on décompose v en v_1v_2, avec $v_1^{p-1} = 1$ et $v_2 \equiv 1$ (mod.p), on a $v^k = v_1^k v_2^k = v_1^u v_2^s$.

Un élément $k \in X$ est dit pair s'il appartient au sous-groupe 2X, i.e. si $(-1)^k = 1$. Lorsque $p \neq 2$, cela signifie que la seconde composante u de k est un élément pair de $\mathbf{Z}/(p-1)\mathbf{Z}$; lorsque $p = 2$, cela signifie que k appartient à $2\mathbf{Z}_2$.

b) Définition des formes modulaires p-adiques

Une forme modulaire p-adique est une série formelle

$$f = \sum_{n=0}^{\infty} a_n q^n,$$

à coefficients $a_n \in \mathbf{Q}_p$, possédant la propriété suivante :

(*) Il existe une suite f_i de formes modulaires à coefficients rationnels, de poids k_i, telle que $\lim.f_i = f$.

(Rappelons, cf. n° 1.1, que $\lim.f_i = f$ signifie que $v_p(f_i - f)$ tend vers $+\infty$, i.e. que les coefficients des f_i tendent uniformément vers ceux de f.)

Remarque. La définition ci-dessus est la définition originale donnée dans [21]. On en trouvera une interprétation "géométrique" (ainsi qu'une généralisation) dans le texte de Katz [12].

c) Poids d'une forme modulaire p-adique

THÉORÈME 2. Soit f une forme modulaire p-adique $\neq 0$, et soit (f_i) une suite de formes modulaires de poids (k_i), à coefficients rationnels, ayant pour limite f. Les k_i ont alors une limite dans le groupe $X = \varprojlim X_m$; cette limite dépend de f, mais pas de la suite (f_i) choisie.

Par hypothèse, on a $v_p(f_i - f_j) \to +\infty$; d'autre part, les $v_p(f_i)$ sont égaux à $v_p(f)$ pour i assez grand. En appliquant le th.1, on en déduit que, pour tout $m \geqslant 1$, l'image de la suite k_i dans X_m est stationnaire; cela signifie que les k_i ont une limite k dans X. Le fait que cette limite ne dépende pas de la suite choisie est immédiat.

La limite k des k_i est appelée le poids de f; c'est un élément pair de X. On convient que 0 est de poids k, quel que soit $k \in 2X$. Avec cette convention, les formes modulaires p-adiques de poids donné forment un Q_p-espace vectoriel (et même un espace de Banach p-adique pour la norme définie par v_p).

Si des formes modulaires p-adiques f_i, de poids $k_i \in 2X$, tendent vers une série formelle f, celle-ci est une forme modulaire p-adique. De plus, si $f \neq 0$, les k_i ont une limite k dans X, et f est de poids k; cela se déduit du th.2, en approchant les f_i par des formes modulaires au sens usuel.

Exemple. Si p = 2,3,5, on a $Q \equiv 1 \pmod{p}$, d'où

$$\frac{1}{Q} = \lim_{m \to \infty} Q^{p^m - 1},$$

ce qui montre que 1/Q est modulaire p-adique, de même que la série $1/j = \Delta/Q^3$, qui est de poids 0. Il n'est d'ailleurs pas difficile de démontrer que (pour p = 2,3,5) une série f est modulaire p-adique de poids 0 si et seulement si elle s'écrit sous la forme

$$f = \sum_{n=0}^{\infty} b_n/j^n = \sum_{n=0}^{\infty} b_n \Delta^n Q^{-3n},$$

avec $b_n \in \mathbf{Q}_p$ et $v_p(b_n) \to +\infty$, et l'on a alors $v_p(f) = \inf. v_p(b_n)$.

Plus généralement, on aurait pu définir l'algèbre des formes modulaires p-adiques de poids 0 comme l'algèbre "de Tate" de la droite projective privée des disques ouverts de rayon 1 centrés aux valeurs "supersingulières" de j; c'est le point de vue adopté par Katz [12].

1.5. Premières propriétés des formes modulaires p-adiques

Si f est une forme modulaire p-adique, on a $v_p(f) \neq -\infty$, i.e. il existe une puissance p^N de p telle que $p^N f \in \mathbf{Z}_p[[q]]$; cela résulte de la définition, et du fait analogue pour les formes modulaires usuelles. De plus, le th.1 reste valable :

THÉORÈME 1'. *Soit* m *un entier* ≥ 1. *Soient* f *et* f' *deux formes modulaires p-adiques, non nulles, de poids* k, $k' \in X$ *respectivement. Si*

$$v_p(f - f') \geq v_p(f) + m,$$

k *et* k' *ont même image dans* X_m.

On écrit f (resp. f') comme limite de formes modulaires usuelles f_i (resp. f_i') de poids k_i (resp. k_i'). Pour i assez grand, on a

$$v_p(f_i) = v_p(f) = v_p(f') = v_p(f_i')$$

et
$$v_p(f_i - f_i') \geq v_p(f) + m,$$

ce qui, d'après le th.1, montre que k_i et k_i' ont même image dans X_m; le théorème en résulte.

COROLLAIRE 1. *Soit* $f = a_o + a_1 q + \dots + a_n q^n + \dots$ *une forme modulaire p-adique de poids* $k \in X$. *Soit* m *un entier* ≥ 0 *tel que l'image de* k *dans* X_{m+1} *soit* $\neq 0$. *On a alors*

$$v_p(a_o) + m \geq \inf_{n \geq 1} v_p(a_n).$$

(En d'autres termes, si les a_n sont p-entiers pour $n \geq 1$, il en est de même de $p^m a_o$.)

Si $a_o = 0$, il n'y a rien à démontrer. Sinon, la fonction constante $f' = a_o$ est de poids 0, et l'on a

$$v_p(f - f') = \inf_{n \geq 1} v_p(a_n).$$

Comme les poids de f et f' ont des images différentes dans X_{m+1}, le th.1' montre que $v_p(f) + m + 1 > v_p(f - f')$, d'où le résultat cherché puisque $v_p(a_o) \geq v_p(f)$.

Remarque. Lorsque k n'est pas divisible par p-1, i.e. n'appartient pas au sous-groupe $\mathbf{Z}_p$ de X, on peut prendre m = 0 dans le corollaire précédent, et l'on en déduit que, si les a_n sont p-entiers pour $n \geq 1$, il en est de même de a_o.

COROLLAIRE 2. *Soit*

$$f^{(i)} = \sum_{n=0}^{\infty} a_n^{(i)} q^n$$

une suite de formes modulaires p-*adiques*, *de poids* $k^{(i)}$. *Supposons que* :

(a) *les* $a_n^{(i)}$, $n \geq 1$, *tendent uniformément vers des* $a_n \in \mathbf{Q}_p$;

(b) *les* $k^{(i)}$ *tendent dans* X *vers une limite* $k \neq 0$.

Alors les $a_o^{(i)}$ *ont une limite* $a_o \in \mathbf{Q}_p$, *et la série*

$$f = a_o + a_1 q + \ldots + a_n q^n + \ldots$$

est une forme modulaire p-*adique de poids* k.

Vu l'hypothèse $\lim . k^{(i)} \neq 0$, on peut supposer qu'il existe un entier m tel que tous les $k^{(i)}$ aient une même image non nulle dans X_m. D'autre part, vu (a), il existe $t \in \mathbf{Z}$ tel que $v_p(a_n^{(i)}) \geq t$ pour tout $n \geq 1$, et tout i. D'après le cor.1, on a donc $v_p(a_o^{(i)}) > t - m$ pour tout i. Les $a_o^{(i)}$ forment donc une partie relativement compacte de $\mathbf{Q}_p$. Si (i_j) est une suite extraite de (i) telle que $a_o^{(i_j)}$ converge vers un élément a_o de $\mathbf{Q}_p$, la série

$$f = \lim . f^{(i_j)} = a_o + a_1 q + \ldots + a_n q^n + \ldots$$

est évidemment modulaire p-adique de poids k. De plus, si $(i_j^!)$ est une autre suite extraite de (i) telle que $a_o^{(i_j^!)}$ converge vers $a_o^!$, la série $f' = a_o^! + a_1 q + \ldots + a_n q^n + \ldots$ est également modulaire p-adique de poids k, et il en est de même de $f - f' = a_o - a_o^!$. Comme $a_o - a_o^!$ est aussi de poids 0, ce n'est possible que si $a_o = a_o^!$. Ainsi, a_o ne dépend pas du choix de la suite (i_j), ce qui montre bien que $a_o^{(i)}$ est une suite convergente.

1.6. <u>Exemple</u> : <u>séries d'Eisenstein</u> p-<u>adiques</u>

Soit $k \in X$. Si n est un entier $\geqslant 1$, nous noterons $\sigma_{k-1}^*(n)$ l'entier p-adique défini par

$$\sigma_{k-1}^*(n) = \sum d^{k-1},$$

la somme étant étendue aux diviseurs positifs d de n qui sont <u>premiers à</u> p. Cela a un sens, puisqu'un tel élément d est une unité p-adique, ainsi que d^{k-1}, cf. n° 1.4, a).

Supposons maintenant que k soit <u>pair</u>. Choisissons une suite d'entiers pairs $k_i \geqslant 4$ qui tende vers l'infini au sens usuel (ce que nous écrirons $|k_i| \to \infty$), et qui tende vers k dans X; c'est évidemment possible. On a alors

$$\lim . \sigma_{k_i - 1}(n) = \sigma_{k-1}^*(n) \quad \text{dans } \mathbf{Z}_p;$$

en effet $d^{k_i - 1}$ tend vers 0 si d est divisible par p (puisque $|k_i| \to \infty$) et tend vers d^{k-1} sinon (puisque $k_i \to k$ dans X). De plus, la convergence est uniforme en n. Or les $\sigma_{k_i-1}(n)$ sont les coefficients d'indice ≥ 1 de la série d'Eisenstein

$$G_{k_i} = - b_{k_i}/2k_i + \sum_{n=1}^{\infty} \sigma_{k_i-1}(n)q^n,$$

et le terme constant de cette série est $- b_{k_i}/2k_i$, qui est égal, comme on sait, à $\frac{1}{2}\zeta(1 - k_i)$. Appliquant alors le cor.2 au th.1', on en déduit que, si $k \neq 0$, les G_{k_i} <u>ont une limite</u> G_k^* qui est une forme modulaire p-adique de poids k :

$$G_k^* = a_o + \sum_{n=1}^{\infty} \sigma_{k-1}^*(n)q^n, \quad \text{où} \quad a_o = \frac{1}{2} \lim_{i \to \infty} \zeta(1 - k_i).$$

Il est clair que cette limite ne dépend pas du choix de la suite k_i; nous l'appellerons la <u>série d'Eisenstein</u> p-<u>adique de poids</u> k; son terme constant a_o sera noté $\frac{1}{2}\zeta^*(1 - k)$, de sorte que l'on a

$$G_k^* = \frac{1}{2}\zeta^*(1 - k) + \sum_{n=1}^{\infty} \sigma_{k-1}^*(n)q^n \qquad (k \in X, \ k \text{ pair} \neq 0).$$

Cela définit une fonction ζ^* sur les éléments impairs de $X - \{1\}$; le cor.2 au th.1' montre que cette fonction est <u>continue</u> (en fait, la série G_k^* elle-même dépend continûment de k). Nous allons voir que ζ^* est essentiellement la <u>fonction zêta</u> p-<u>adique de Kubota-Leopoldt</u> [16]. De façon plus précise:

THÉORÈME 3. (i) <u>Si</u> $p \neq 2$, <u>et si</u> (s,u) <u>est un élément impair</u> $\neq 1$ <u>de</u> $X = \mathbf{Z}_p \times \mathbf{Z}/(p-1)\mathbf{Z}$ <u>on a</u>

$$\zeta^*(s,u) = L_p(s; \omega^{1-u}),$$

<u>où</u> $L_p(s; \chi)$ <u>désigne la fonction</u> L p-<u>adique d'un caractère</u> χ (Iwasawa [11], p.29-30) <u>et</u> ω <u>désigne le caractère défini dans</u> [11], p.18.

(ii) <u>Si</u> $p = 2$, <u>et si</u> s <u>est un élément impair</u> $\neq 1$ <u>de</u> $X = \mathbf{Z}_2$, on a $\zeta^*(s) = L_2(s;\ \chi^\circ)$, cf. [11], p.29-30.

Notons ζ' la fonction

$$(s,u) \longmapsto L_p(s;\ \omega^{1-u}) \quad \text{si} \quad p \neq 2$$

$$s \longmapsto L_p(s;\ \chi^\circ) \quad \text{si } p = 2.$$

Il résulte de [11], loc.cit., que ζ' est continue, et que

$$\zeta'(1-k) = (1-p^{k-1})\ \zeta(1-k) \quad \text{si} \quad k \in 2\mathbf{Z}, \quad k \geqslant 2.$$

Si $k \in 2X$, $k \neq 0$, et si (k_i) est une suite convergeant vers k comme ci-dessus, on a

$$\zeta'(1-k) = \lim_{i\to\infty}.\zeta'(1-k_i) = \lim_{i\to\infty}.(1-p^{k_i-1})\ \zeta(1-k_i).$$

Mais, comme $|k_i|$ tend vers $+\infty$, on a $\lim\limits_{i\to\infty}.(1-p^{k_i-1}) = 1$, d'où

$$\zeta'(1-k) = \lim_{i\to\infty}.\zeta(1-k_i) = \zeta^*(1-k),$$

ce qui démontre bien que $\zeta' = \zeta^*$.

Exemple

Supposons que $p \equiv 3 \pmod{4}$ et $p \neq 3$. Prenons pour k l'élément $(1, \frac{p+1}{2})$ de $\mathbf{Z}_p \times \mathbf{Z}/(p-1)\mathbf{Z}$. On peut montrer que

$$G_k^* = \tfrac{1}{2}h(-p) + \sum_{n=1}^{\infty} \sum_{d|n} \left(\frac{d}{p}\right) q^n,$$

où $h(-p)$ est le nombre de classes du corps $\mathbf{Q}(\sqrt{-p})$.

Remarques

1) Lorsque k est un entier pair $\geqslant 2$, on vient de voir que

$$\zeta^*(1-k) = (1-p^{k-1})\ \zeta(1-k);$$

c'est la valeur en $1-k$ de la fonction zêta "débarrassée de son p-ième facteur". On a en outre

$$G_k^* = G_k - p^{k-1}\ G_k|V, \qquad \text{cf. n° 2.1.}$$

2) La fonction ζ^* n'est pas définie au point $s = 1$: elle a un <u>pôle simple</u> en ce point [7], [11], [16].

3) Lorsque k est divisible par p-1, on a $v_p(\zeta^*(1-k)) < 0$, de sorte que la série

$$E_k^* = 2G_k^*/\zeta^*(1-k) = 1 + \frac{2}{\zeta^*(1-k)} \sum_{n=1}^{\infty} \sigma_{k-1}^*(n)q^n$$

est à coefficients p-entiers, et $E_k^* \equiv 1 \pmod{p}$. Plus précisément, si l'image de k dans X_m est nulle, on a

$$E_k^* \equiv 0 \pmod{p^m}.$$

En particulier, E_k^* tend vers 1 lorsque k tend vers 0; cela conduit à poser $E_o^* = 1$.

4) Lorsque k n'est pas divisible par p-1, il est congru mod.(p-1) à un entier a compris entre 2 et p-3, et l'on a

$$\zeta^*(1-k) \equiv -b_a/a \pmod{p},$$

en vertu des congruences de Kummer. En particulier, si p est <u>régulier</u>, on a $\zeta^*(1-k) \not\equiv 0 \pmod{p}$, et la fonction ζ^* ne s'annule nulle part.

Par contre, si p est irrégulier, il peut se faire que $\zeta^*(1-k) = 0$ pour certaines valeurs de k; la série G_k^* correspondante est alors "parabolique" : son terme constant est nul.

§2. Opérateurs de Hecke

2.1. Action de T_ℓ, U, V, θ sur les formes modulaires p-adiques

Si

$$f = \sum_{n=0}^{\infty} a_n q^n$$

est une série formelle à coefficients dans $\mathbf{Q}_p$, on pose :

$$f|U = \sum_{n=0}^{\infty} a_{pn} q^n \quad \text{et} \quad f|V = \sum_{n=0}^{\infty} a_n q^{pn}.$$

Si ℓ est un nombre premier $\neq p$, et si $k \in X$, on pose :

$$f|_k\, T_\ell = \sum_{n=0}^{\infty} a_{\ell n} q^n + \ell^{k-1} \sum_{n=0}^{\infty} a_n q^{\ell n}.$$

Lorsque k est sous-entendu, on écrit $f|T_\ell$ au lieu de $f|_k\, T_\ell$.

THÉORÈME 4. Si f est une forme modulaire p-adique de poids k, il en est de même de $f|U$, $f|V$ et des $f|_k\, T_\ell$ (ℓ premier $\neq$ p).

Choisissons une suite $f_i = \sum a_{n,i} q^n$ de formes modulaires (au sens usuel), à coefficients rationnels, telle que

$$\lim_{i \to \infty} f_i = f.$$

Quitte à remplacer f_i par $f_i E_{(p-1)p^i}$, on peut supposer que les poids k_i des f_i sont tels que $|k_i| \to \infty$. Pour tout nombre premier ℓ, on sait (cf. par exemple [3], [22]) que le transformé $f_i|T_\ell$ de f_i par l'opérateur de Hecke T_ℓ est une forme modulaire de poids k_i, donnée par la formule :

$$f_i|T_\ell = \sum a_{\ell n,i}\, q^n + \ell^{k_i-1} \sum a_{n,i}\, q^{\ell n}.$$

On a $\lim\limits_{i\to\infty} \ell^{k_i-1} = \ell^{k-1}$ si $\ell \neq p$ (car alors ℓ est une unité p-adique), et $\lim\limits_{i\to\infty} \ell^{k_i-1} = 0$ si $\ell = p$ (puisque $|k_i| \to \infty$). On en conclut que les $f_i|T_\ell$ tendent vers $f|T_\ell$ si $\ell \neq p$, et vers $f|U$ si $\ell = p$; cela montre bien que les séries $f|T_\ell$ et $f|U$ sont des formes modulaires p-adiques, de poids $\lim\limits_{i\to\infty} k_i = k$. Appliquant ce résultat à f_i, on voit que $f_i|U$ est modulaire p-adique de poids k_i; comme $f_i|T_p$ est aussi modulaire de poids k_i, on en conclut que $f_i|V = p^{1-k_i}(f_i|T_p - f_i|U)$ est modulaire p-adique de poids k_i; comme $f|V = \lim\limits_{i\to\infty} f_i|V$, il en résulte bien que $f|V$ est modulaire p-adique de poids k.

<u>Remarque</u>. On peut également définir les opérateurs de Hecke T_m pour tout entier m premier à p, au moyen des formules usuelles. Ces opérateurs commutent entre eux, commutent à U et V, et l'on a

$$T_m T_n = T_n T_m = T_{mn} \quad \text{si} \quad (m,n) = 1,$$

$$T_\ell\, T_{\ell^n} = T_{\ell^{n+1}} + \ell^{k-1}\, T_{\ell^{n-1}} \quad \text{si } \ell \text{ est premier et } n \geqslant 1.$$

<u>Exemples</u>

On a $G_k^*|T_\ell = (1 + \ell^{k-1})G_k^*$ et $G_k^*|U = G_k^*$.

Si k est un entier pair $\geqslant 2$, un calcul immédiat montre que

$$G_k^* = G_k - p^{k-1}G_k|V = G_k|(1 - p^{k-1}V).$$

On en déduit

$$G_k = G_k^*|(1 - p^{k-1}V)^{-1} = G_k^* + p^{k-1}G_k^*|V + \ldots + p^{m(k-1)}G_k^*|V^m + \ldots$$

Pour $k = 2$, cette formule montre que $G_2 = -P/24$ est somme d'une série convergente de formes modulaires p-adiques de poids 2. On en conclut que P <u>est une forme modulaire</u> p-<u>adique de poids</u> 2.

THÉORÈME 5. <u>Soit</u> $f = \sum a_n q^n$ <u>une forme modulaire</u> p-<u>adique de poids</u> k.

(a) <u>La série</u>

$$\theta f = q\, df/dq = \sum n\, a_n\, q^n$$

<u>est une forme modulaire</u> p-<u>adique de poids</u> k + 2.

(b) <u>Pour tout</u> $h \in X$, <u>la série</u>

$$f|R_h = \sum_{(n,p)=1} n^h\, a_n\, q^n$$

<u>est une forme modulaire</u> p-<u>adique de poids</u> k + 2h.

Soit (f_i) une suite de formes modulaires, à coefficients rationnels, telle que $\lim. f_i = f$, et soit k_i le poids de f_i. On sait (cf. [20], [27]) que $\theta f_i = k_i P f_i/12 + g_i$, où g_i est une forme modulaire de poids $k_i + 2$. Puisque P est modulaire p-adique de poids 2, il en résulte que θf_i est modulaire p-adique de poids $k_i + 2$, et en passant à la limite cela montre bien que θf est modulaire p-adique de poids $k + 2$.

Choisissons maintenant une suite d'entiers positifs h_i telle que

$$h_i \to h \quad \text{dans} \quad X \qquad \text{et} \qquad |h_i| \to \infty.$$

Vu ce qui précède, $\theta^{h_i} f$ est modulaire p-adique de poids $k + 2h_i$. Comme $\theta^{h_i} f$ tend vers $f|R_h$ lorsque $i \to \infty$, on voit bien que $f|R_h$ est modulaire p-adique de poids $k + 2h$.

<u>Remarque</u>

On a les formules : $(\theta f)|U = p\theta(f|U)$, $f|R_h|U = 0$,

$$\theta(f|V) = p(\theta f)|V, \quad (\theta f)|_{k+2}\, T_\ell = \ell\, \theta(f|_k\, T_\ell), \quad f|V|R_h = 0,$$

et
$$(f|R_h)|_{k+2h}\, T_\ell = \ell^h\, (f|_k\, T_\ell)|R_h$$

pour tout ℓ premier $\neq$ p.

Exemples

Pour h = 0, on a

$$f|R_o = \lim_{m \to \infty} \theta^{(p-1)p^m} f = f|(1 - UV) = \sum_{(n,p)=1} a_n q^n.$$

Pour $h = (0, \frac{p-1}{2}) \in \mathbf{Z}_p \times \mathbf{Z}/(p-1)\mathbf{Z}$, $p \geq 3$, on a :

$$f|R_h = \lim_{m \to \infty} \theta^{(p-1)p^m/2} f = \sum \left(\frac{n}{p}\right) a_n\, q^n.$$

2.2. Une propriété de contraction

Les opérateurs de Hecke T_ℓ et T_p laissent stable l'espace M_k des formes modulaires de poids k à coefficients p-entiers. Par réduction (mod.p) ils opèrent donc sur $\widetilde{M}_k$; comme $T_p \equiv U$ (mod.p), on en conclut que U opère sur $\widetilde{M}_k$, donc aussi sur les espaces

$$\widetilde{M}^\alpha = \bigcup_{k \in \alpha} \widetilde{M}_k \qquad (\alpha \in \mathbf{Z}/(p-1)\mathbf{Z}, \qquad \text{cf. n° 1.2}).$$

En fait, U "contracte" les $\widetilde{M}_k$. De façon plus précise, nous allons démontrer le théorème suivant, en rapport étroit avec des résultats d'Atkin [2], Koike [15] et Dwork :

THÉORÈME 6.

(i) Si $k > p + 1$, U applique $\widetilde{M}_k$ dans $\widetilde{M}_{k'}$, avec $k' < k$.

(ii) La restriction de U à $\widetilde{M}_{p-1}$ est bijective.

Lorsque p = 2 ou 3, on a $\widetilde{M} = \mathbf{F}_p[\widetilde{\Delta}]$, et $\widetilde{M}_k$ est l'espace des polynômes en $\widetilde{\Delta}$ de degré $\leq k/12$. Utilisant la formule $(g^p f)|U \equiv g.(f|U)$ (mod.p), on vérifie que $\tilde{\Delta}^i|U = 0$ si $i \not\equiv 0 \pmod{p}$ et $\tilde{\Delta}^i|U = \tilde{\Delta}^{i/p}$ sinon. On en conclut que U applique $\tilde{M}_k$ dans $\tilde{M}_{k'}$, avec $k' = [k/p]$, d'où le théorème dans ce cas.

Supposons maintenant $p \geq 5$. Si f est un élément d'un $\tilde{M}^\alpha$, notons w(f) la <u>filtration</u> de f (cf. [20], [27]), i.e. la borne inférieure des k tels que $f \in \tilde{M}_k$.

LEMME 1.

(a) <u>On a</u> $w(\theta f) \leq w(f) + p+1$, <u>et il y a égalité si et seulement si</u> $w(f) \not\equiv 0 \pmod{p}$.

(b) <u>On a</u> $w(f^i) = i\, w(f)$ <u>pour tout</u> $i \geq 1$.

L'assertion (a) est démontrée dans [27], Lemme 5 et dans [20], cor.3 au th.5.

Pour prouver (b), on peut supposer $f \neq 0$, i.e. $w(f) \neq -\infty$. Ecrivons alors f comme polynôme isobare $F(\tilde{Q},\tilde{R})$ en $\tilde{Q},\tilde{R}$, de poids $k = w(f)$. Le polynôme F n'est pas divisible par le polynôme $\tilde{A}$ du n° 1.2 ([27], <u>loc. cit.</u>). Comme $\tilde{A}$ est sans facteur multiple, il en résulte que F^i n'est pas non plus divisible par $\tilde{A}$, d'où le fait que $f^i = F^i(\tilde{Q},\tilde{R})$ est de filtration ik.

LEMME 2.

(i) <u>On a</u> $w(f|U) \leq p + (w(f) - 1)/p$.

(ii) <u>Si</u> $w(f) = p-1$, <u>on a</u> $w(f|U) = p-1$.

On a l'identité

$$(f|U)^p = f - \theta^{p-1}f \quad \text{pour tout} \quad f \in \mathbf{F}_p[[q]].$$

Si l'on pose $k = w(f)$ et $k' = w(f|U)$, le lemme 1 montre que

$$w((f|U)^p) = pk' \quad \text{et} \quad w(\theta^{p-1}f) \leq k + p^2 - 1.$$

On en conclut que $pk' \leq \mathrm{Sup}(k, k + p^2 - 1) = k + p^2 - 1$, ce qui démontre (i).

Supposons maintenant que $k = p-1$. Si l'on calcule $\theta^2 f$ au moyen de la formule $12\theta = kP + \partial$ (cf. [27] pour la définition de la dérivation ∂), on trouve que $12^2\theta^2 f = Qf + \partial^2 f$, d'où $\theta^2 f \in \widetilde{M}_{p+3}$. La filtration h de $\theta^2 f$ est donc $-\infty$, 4 ou $p+3$. Dans le premier cas, on aurait $\theta^2 f = 0$, d'où $\theta^{p-1} f = 0$ et f serait égal à $(f|U)^p$, ce qui est absurde, puisque la filtration de f n'est pas divisible par p. Dans le cas $h = 4$, $\theta^2 f$ serait multiple non nul de Q, ce qui est également absurde puisque son terme constant est nul. On a donc nécessairement $w(\theta^2 f) = p+3$. Appliquant le Lemme 1, on en conclut que

$$w(\theta^i \theta^2 f) = p + 3 + i(p+1) \qquad \text{pour} \qquad 0 \leq i \leq p-3.$$

(Observer que $p + 3 + i(p + 1)$ n'est pas divisible par p si $i \leq p-4$.)

En particulier, on a $w(\theta^{p-1} f) = p + 3 + (p - 3)(p+1) = p(p - 1)$, d'où $w((f|U)^p) = p(p-1)$, et $w(f|U) = p-1$.

Le théorème 6 est maintenant immédiat. L'assertion (i) résulte du Lemme 2 (i), compte tenu de ce que $p + (k - 1)/p$ est $< k$ si $k > p + 1$. D'autre part, si f est un élément non nul de $\widetilde{M}_{p-1}$, on a, soit $w(f) = 0$, et f est une constante, d'où $f|U = f \neq 0$, soit $w(f) = p-1$ et le Lemme 2 (ii) montre que $w(f|U) = p-1$, d'où $f|U \neq 0$; ainsi, la restriction de U à $\widetilde{M}_{p-1}$ est injective, donc bijective, puisque $\widetilde{M}_{p-1}$ est de dimension finie.

Le th.6 entraîne aussitôt le résultat suivant :

COROLLAIRE. <u>Soit</u> α <u>un élément pair de</u> $\mathbf{Z}/(p-1)\mathbf{Z}$, $p \geq 5$.

(i) <u>On peut décomposer</u> $\widetilde{M}^\alpha$ <u>de façon unique en</u> $\widetilde{M}^\alpha = \widetilde{S}^\alpha \oplus \widetilde{N}^\alpha$, <u>de telle sorte que</u> U <u>soit bijectif sur</u> $\widetilde{S}^\alpha$ <u>et localement nilpotent sur</u> $\widetilde{N}^\alpha$. <u>On a</u> $\widetilde{S}^\alpha \subset \widetilde{M}_j$, <u>où</u> $j \in \alpha$ <u>est tel que</u> $4 \leq j \leq p+1$; <u>en particulier</u>, $\widetilde{S}^\alpha$ <u>est de dimension finie</u>.

(ii) <u>Pour</u> $\alpha = 0$, <u>on a</u> $j = p - 1$ <u>et</u> $\widetilde{S}^0 = \widetilde{M}_{p-1}$.

Lorsque $p = 2$ ou 3, on a une décomposition analogue de $\tilde{M} = \mathbf{F}_p[\tilde{\Delta}]$ en $\tilde{M} = \tilde{S} \oplus \tilde{N}$, avec $\tilde{S} = \tilde{M}_o = \mathbf{F}_p$ et $\tilde{N} = \tilde{\Delta}.\tilde{M}$; l'endomorphisme U est l'identité sur $\tilde{S}$, et est localement nilpotent sur $\tilde{N}$.

Remarque

Lorsque $\alpha \neq 0$, il peut se faire que $\tilde{S}^{\alpha}$ soit distinct de $\tilde{M}_j$, i.e. que la restriction de U à $\tilde{M}_j$ admette 0 pour valeur propre; c'est le cas pour $\alpha = j = 16$ et $p = 59$. On a toutefois $\tilde{S}^{\alpha} = \tilde{M}_j$ dans chacun des cas suivants :

$\alpha = 2$, $j = p+1$; les seules valeurs propres de U sur $\tilde{M}_{p+1}$ sont en effet ± 1, cf. n° 3.3, cor. au th.11.

$\alpha = j = 4, 6, 8, 10, 14$; $\tilde{M}_j$ est alors réduit aux multiples de la série d'Eisenstein $\tilde{G}_j$, et celle-ci est invariante par U.

Pour $\alpha = j = 12$ (et $p > 11$), les valeurs propres de U sur $\tilde{M}_j$ sont 1 et $\tau(p)$. On a donc $\tilde{S}^{\alpha} \neq \tilde{M}_j$ si et seulement si $\tau(p) \equiv 0 \pmod{p}$; d'après M.Newman, c'est le cas pour $p = 2411$.

2.3. Application au calcul du terme constant d'une forme modulaire p-adique

Si f est une série formelle en q, nous conviendrons de noter $a_n(f)$ son n-ième coefficient; nous dirons que f est parabolique si son terme constant $a_o(f)$ est nul.

Soit f une forme modulaire p-adique de poids $k \in X$. Nous allons voir que, si $k \neq 0$, $a_o(f)$ peut se "calculer" en fonction des $a_n(f)$, $n \geq 1$. Commençons par un cas particulier simple :

THÉORÈME 7. *Si f est une forme modulaire p-adique de poids $k \neq 0$, et si $p = 2, 3, 5$ ou 7, on a*

$$(*) \qquad a_o(f) = \tfrac{1}{2}\zeta^*(1-k) \lim_{n\to\infty} a_{p^n}(f).$$

Comme p est régulier, on a $\zeta^*(1-k) \neq 0$, cf. n° 1.6, et la série d'Eisenstein p-adique G_k^* a un terme constant $\neq 0$. On peut donc écrire f comme somme d'une forme parabolique et d'un multiple de G_k^*. On est ainsi ramené à démontrer le th.7 dans les deux cas suivants :

a) $f = G_k^*$.

On a alors $a_o(f) = \frac{1}{2}\zeta^*(1-k)$ et $a_{p^n}(f) = \sigma_{k-1}^*(p^n) = 1$; la formule est évidente.

b) f est parabolique.

On doit prouver que $a_{p^n}(f)$ tend vers 0. Comme $a_{p^n}(f) = a_1(f|U^n)$, il suffit de prouver :

LEMME 3. Si f est parabolique, et $p \leqslant 7$, on a

$$\lim_{n \to \infty} f|U^n = 0.$$

Quitte à faire une homothétie sur f, on peut supposer que $v_p(f) = 0$. Soit $\tilde{f}$ la réduction (mod.p) de f, et soit α l'image de k dans $\mathbf{Z}/(p-1)\mathbf{Z}$; on a $f \in \widetilde{M}^\alpha$. Utilisons la décomposition $\widetilde{M}^\alpha = \widetilde{S}^\alpha \oplus \widetilde{N}^\alpha$ fournie par le corollaire au th.6. Du fait que $p \leqslant 7$, l'entier j correspondant est $\leqslant 8$, et $\widetilde{S}^\alpha$ est simplement l'ensemble des multiples de $\widetilde{E}_k$; il en résulte que $\widetilde{N}^\alpha$ est l'ensemble des éléments paraboliques de M. On a donc $\tilde{f} \in \widetilde{N}^\alpha$, et il existe un entier $m \geqslant 1$ tel que $\tilde{f}|U^m = 0$, i.e.

$$v_p(f|U^m) \geqslant 1.$$

Appliquons ce résultat à la forme parabolique $\frac{1}{p} f|U^m$. On en déduit qu'il existe un entier $m' \geqslant 1$ tel que

$$v_p(f|U^{m+m'}) \geqslant 2.$$

D'où, par une récurrence évidente, le fait que $v_p(f|U^n)$ tend vers l' infini avec n, ce qui démontre le lemme (et le th.7).

Remarque

Lorsque $p \geqslant 11$, la formule (*) reste valable pourvu que l'on ait

$k \equiv 4, 6, 8, 10, 14 \pmod{(p-1)}$; la démonstration est la même. Le cas $p = 11$, $f = \Delta$ montre qu'une hypothèse sur k est nécessaire.

Nous allons maintenant établir une formule analogue à (*), valable pour tout k divisible par p-1.

THÉORÈME 8. Il existe un polynôme H en U et les T_ℓ, à coefficients entiers, tel que, pour tout $k \in X$ divisible par p-1, on ait :

(i) $E_k^*|H = c(k)\, E_k^*$, avec c(k) inversible dans $\mathbf{Z}_p$,

(ii) $\lim\limits_{n \to \infty} f|H^n = 0$

pour toute forme modulaire p-adique f de poids k qui est parabolique.

(Noter que H ne dépend pas de k, mais que son action sur f en dépend; lorsque l'on désire mettre ce fait en évidence, on écrit $f|_k H$ au lieu de $f|H$.)

COROLLAIRE. Pour toute forme modulaire p-adique f, de poids $k \neq 0$, avec $k \equiv 0 \pmod{(p-1)}$, on a

$$(**) \qquad a_o(f) = \tfrac{1}{2}\zeta^*(1-k) \lim_{n \to \infty} c(k)^{-n}\, a_1(f|H^n).$$

En effet, il suffit de vérifier la formule (**) lorsque $f = E_k^*$ et lorsque f est parabolique; dans le premier cas elle résulte de (i), et dans le second de (ii).

(On notera que, pour k fixé, $a_1(f|H^n)$ est combinaison $\mathbf{Z}_p$-linéaire des $a_m(f)$, $m \geq 1$; la formule (**) donne donc bien un procédé de calcul de $a_o(f)$ en fonction des $a_m(f)$.)

Démonstration du théorème 8

Si $p = 2, 3, 5, 7$ on prend $H = U$, cf. th.7. On peut donc supposer que $p \geq 11$. Tout revient à construire un polynôme $\widetilde{H}$ en U et les T_ℓ, à coefficients dans $\mathbf{F}_p$, tel que :

(i)' $1|\widetilde{H} = c$, avec $c \neq 0$ dans $\mathbf{F}_p$.

(ii)' $f \mapsto f|\widetilde{H}$ est localement nilpotent sur l'ensemble $\widetilde{P}^o$ des éléments

<u>paraboliques de</u> $\widetilde{M}^o$.

En effet, si l'on dispose d'un tel $\widetilde{H}$, on prend pour H un polynôme à coefficients entiers dont la réduction (mod.p) est égale à $\widetilde{H}$. Comme $E_k^*|U = E_k^*$ et $E_k^*|T_\ell = (1 + \ell^{k-1})E_k^*$, on a

$$E_k^*|H = c(k)\, E_k^*, \quad \text{avec} \quad c(k) \in \mathbf{Z}_p;$$

de plus, l'image de c(k) dans $\mathbf{F}_p$ est égale à c, ce qui montre que c(k) est inversible dans $\mathbf{Z}_p$, d'où (i). Le fait que (ii)' entraîne (ii) se démontre par l'argument utilisé pour le th.7.

<u>Construction de</u> $\widetilde{H}$

Faisons opérer U et les T_ℓ sur l'espace vectoriel $\widetilde{S}^o = \widetilde{M}_{p-1}$, cf. cor. au th.6. Ces opérateurs commutent entre eux et respectent la décomposition de $\widetilde{M}_{p-1}$ en $\mathbf{F}_p \oplus \widetilde{P}_{p-1}$, où $\widetilde{P}_{p-1}$ désigne le sous-espace des formes paraboliques. Les valeurs propres de U et T_ℓ sur le sous-espace $\widetilde{M}_o = \mathbf{F}_p$ sont respectivement 1 et $1 + \ell^{-1}$.

Par contre :

LEMME 4. <u>Il n'existe pas d'élément</u> $f \neq 0$ <u>de</u> $\widetilde{P}_{p-1}$ <u>tel que</u>

$$f|U = f \quad \underline{\text{et}} \quad f|T_\ell = (1 + \ell^{-1})f$$

<u>pour tout</u> ℓ <u>premier</u> $\neq$ p.

En effet, supposons qu'un tel f existe, et écrivons-le $f = \sum_{n=1}^{\infty} a_n q^n$.

On a par hypothèse

$$a_{pn} = a_n, \quad a_{\ell n} = (1 + \ell^{-1})a_n \quad \text{si} \quad n \not\equiv 0 \pmod{\ell},$$

$$a_{\ell n} = (1 + \ell^{-1})a_n - \ell^{-1}a_{n/\ell} \quad \text{si} \quad n \equiv 0 \pmod{\ell}.$$

Ces formules permettent de calculer par récurrence a_n à partir de a_1. On trouve $a_n = a_1\sigma^*_{-1}(n) = a_1\, \sigma_{p-2}(n)$, i.e. $f = a_1\, \widetilde{\phi}$, où

$$\phi = \sum_{n=1}^{\infty} \sigma_{p-2}(n) q^n .$$

Mais, d'après le lemme de [20], p.416-11, la série $\tilde{\phi}$ n'appartient pas à $\tilde{M}^o$; on obtient donc une contradiction.

Le lemme suivant est élémentaire :

LEMME 5. Soient k un corps commutatif, Y un k-espace vectoriel de dimension finie, $(U_i)_{i \in I}$ une famille d'endomorphismes de Y, et $(\lambda_i)_{i \in I}$ une famille d'éléments de k. On suppose que les U_i commutent entre eux, et qu'il n'existe aucun élément $y \neq 0$ de Y tel que $U_i y = \lambda_i y$ pour tout $i \in I$. Il existe alors un polynôme $F \in k[(X_i)_{i \in I}]$ tel que $F((U_i)_{i \in I}) = 0$ et $F((\lambda_i)_{i \in I}) \neq 0$.

Appliquons ce lemme aux endomorphismes U et T_ℓ de l'espace $Y = \tilde{P}_{p-1}$, et aux scalaires 1 et $1 + \ell^{-1}$, cf. lemme 4. On en déduit l'existence d'un polynôme F en U et les T_ℓ dont la restriction à $\tilde{P}_{p-1}$ est nulle, et qui ne s'annule pas sur $\mathbf{F}_p$. Le polynôme $\tilde{H} = U.F$ répond alors à la question. En effet, il vérifie évidemment (i)'. D'autre part, on a $\tilde{P}^o = \tilde{P}_{p-1} \oplus \tilde{N}^o$, et F est nul sur $\tilde{P}_{p-1}$, tandis que U est localement nilpotent sur $\tilde{N}^o$, cf. cor.au. th.6; comme U et F commutent, il en résulte que $U.F$ est localement nilpotent sur $\tilde{P}^o$, ce qui achève la démonstration.

Exemples

$p < 11$: $H = U$ et $c(k) = 1$;

$p = 13$: $H = U(U + 5)$ et $c(k) = 6$; $H = U(T_2 - 2)$ et $c(k) = 2^{k-1}-1$;

$p = 17$: $H = U(T_2 + 5)$ et $c(k) = 2^{k-1} + 6$.

Passons maintenant au cas d'un poids non divisible par p-1. Faute de mieux, je me bornerai à un théorème d'existence :

THÉORÈME 9. Soit k un élément pair de X, non divisible par $p-1$. Il existe une suite $(\lambda_{m,n})_{m,n \geq 1}$ d'éléments de $\mathbf{Z}_p$ telle que :

a) pour tout n, on a $\lambda_{m,n} = 0$ pour m assez grand;

b) si l'on pose

$$u_n(f) = \sum_{m=1}^{\infty} \lambda_{m,n}\, a_m(f),$$

on a

(***) $$a_o(f) = \lim_{n \to \infty} u_n(f)$$

pour toute forme modulaire p-adique f de poids k.

(Précisons que les coefficients $\lambda_{m,n}$ dépendent du poids k choisi.)

Notons M(k) le $\mathbf{Q}_p$-espace vectoriel des formes modulaires p-adiques de poids k.

LEMME 6. Soit Y un sous-espace de dimension finie de M(k). Il existe des éléments $(\lambda_m)_{m \geq 1}$ de $\mathbf{Z}_p$, nuls sauf un nombre fini d'entre eux, tels que

$$a_o(f) = \sum_{m=1}^{\infty} \lambda_m\, a_m(f) \quad \text{pour tout} \quad f \in Y.$$

Soit Y_o le sous-$\mathbf{Z}_p$-module de Y formé des éléments f tels que $v_p(f) \geq 0$. Il est facile de voir que Y_o est un $\mathbf{Z}_p$-module libre de rang r = dim.V. Soit $f_1,\ldots,f_r$ une base de Y_o. On peut trouver r indices $m_1, \ldots, m_r \geq 1$ tels que

$$\det(a_{m_i}(f_j)) \not\equiv 0 \pmod{p}.$$

Sinon en effet il existerait des $c_j \in \mathbf{Z}_p$, non tous divisibles par p, tels que

$$a_m\Big(\sum_{j=1}^{r} c_j f_j\Big) \equiv 0 \pmod{p} \quad \text{pour tout} \quad m \geq 1;$$

si l'on pose $$f = \sum_{j=1}^{r} c_j f_j,$$

le cor.1 au th.1' du n° 1.5 montrerait que $v_p(f) \geq 1$, contrairement au fait que les c_j ne sont pas tous divisibles par p. Ceci étant, il est clair que les formes linéaires $a_{m_1},\dots a_{m_r}$ forment une base du dual du $\mathbf{Z}_p$-module Y_o, et comme a_o est une forme linéaire sur Y_o, on peut écrire a_o sous la forme

$$a_o = \sum_{i=1}^{r} \lambda_i \, a_{m_i}, \quad \text{avec} \quad \lambda_i \in \mathbf{Z}_p,$$

d'où le lemme.

Soit maintenant $M(k)_o$ l'ensemble des $f \in M(k)$ tels que $v_p(f) \geqslant 0$. Si α est l'image de k dans $\mathbf{Z}/(p-1)\mathbf{Z}$, on a $M(k)_o/pM(k)_o \subset \widetilde{M}^\alpha$ (il y a même égalité), et par suite l'ensemble $M(k)_o/pM(k)_o$ est <u>dénombrable</u>. Il en résulte que l'on peut trouver dans M(k) une suite croissante

$$V_1 \subset V_2 \subset \dots \subset V_n \subset \dots$$

de $\mathbf{Q}_p$-sous-espaces vectoriels de dimensions finies dont la réunion est dense dans M(k). Pour chacun des V_n, le lemme 6 montre qu'il existe une combinaison $\mathbf{Z}_p$-linéaire u_n des $a_m (m \geqslant 1)$ telle que $a_o(f) = u_n(f)$ pour tout $f \in V_n$. Comme la famille des u_n est équicontinue, le fait qu'elle converge vers a_o sur une partie dense de M(k) entraîne qu'elle converge partout, et l'on a donc bien

$$a_o(f) = \lim_{n \to \infty} u_n(f) \quad \text{pour tout} \quad f \in M(k).$$

<u>Remarques</u>

1) La démonstration ci-dessus peut aussi s'exprimer en disant que le $\mathbf{Z}_p$-module engendré par les $a_m (m \geqslant 1)$ est <u>faiblement dense</u> dans la boule unité du dual de l'espace de Banach p-adique M(k).

2) Dans le cas archimédien (i.e. pour les formes modulaires usuelles de poids $k > 0$), le problème consistant à exprimer $a_o(f)$ à partir des $a_n(f)$, $n \geqslant 1$, a une solution très simple, due à Hecke : on forme la

série de Dirichlet

$$\phi_f(s) = \sum_{n=1} a_n(f)\, n^{-s},$$

on la prolonge en une fonction méromorphe dans $\mathbf{C}$, et l'on prend sa valeur $\phi_f(0)$ au point $s = 0$: c'est $-\ a_o(f)$.

§3. Formes modulaires sur $\Gamma_o(p)$

Le but de ce § est de justifier le principe suivant, bien connu expérimentalement : toute forme modulaire sur $\Gamma_o(p)$ est p-adiquement sur $SL_2(\mathbf{Z})$. La méthode suivie est due à Atkin; elle repose sur les propriétés des coefficients des séries d'Eisenstein. Une autre méthode, basée sur un théorème de Deligne ([6], §7), est exposée dans Katz [12] et Koike [15].

3.1. Rappels

a) Notation

Soit f une fonction sur le demi-plan de Poincaré $H = \{z | \mathrm{Im}(z) > 0\}$; soient $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ une matrice réelle de déterminant > 0, et k un entier; on définit une fonction $f|_k\gamma$ sur H par la formule

$$(f|_k\gamma)(z) = \det(\gamma)^{k/2}\ (cz + d)^{-k}\ f\left(\frac{az + b}{cz + d}\right).$$

On a $(f|_k\gamma)|_k\gamma' = f|_k\gamma\gamma'$ et $f|_k\gamma = f$ si γ est une homothétie > 0. Lorsque k est sous-entendu, on écrit $f|\gamma$ au lieu de $f|_k\gamma$.

b) Formes modulaires sur $\Gamma_o(p)$

Le groupe $\Gamma_o(p)$ est défini comme le sous-groupe de $SL_2(\mathbf{Z})$ formé des matrices $\binom{a\ b}{c\ d}$ telles que $c \equiv 0 \pmod{p}$; il est d'indice $p + 1$ dans $SL_2(\mathbf{Z})$; il est normalisé dans $GL_2(\mathbf{Q})$ par la matrice $W = \begin{pmatrix} 0 & -1 \\ p & 0 \end{pmatrix}$.

Soit k un entier. Une <u>forme modulaire de poids</u> k sur $\Gamma_o(p)$ est une fonction holomorphe f sur H telle que :

(i) $f|_k\gamma = f$ <u>pour tout</u> $\gamma \in \Gamma_o(p)$;

(ii) f <u>est holomorphe aux pointes de</u> $\Gamma_o(p)$.

En fait, $\Gamma_o(p)$ n'a que deux pointes, ∞ et 0, qui sont permutées par W. La condition (ii) équivaut donc à la suivante :

(ii') <u>Les fonctions</u> f <u>et</u> $f|_kW$ <u>ont des développements en série</u>

$$f = \sum_{n=0}^{\infty} a_n q^n, \qquad f|_kW = \sum_{n=0}^{\infty} b_n q^n$$

$$(q = e^{2\pi i z}, \quad a_n \in \mathbf{C}, \quad b_n \in \mathbf{C})$$

<u>qui convergent pour tout</u> $z \in H$ (i.e. pour tout q tel que $|q| < 1$).

Si f est modulaire, il en est de même de $f|W$, et $f|W^2 = f$.

Lorsque k est < 0, ou impair, toute forme modulaire de poids k est nulle. Dans ce qui suit, nous supposerons donc k pair $\geqslant 0$.

c) <u>Trace d'une forme modulaire sur</u> $\Gamma_o(p)$

Soit f une forme modulaire de poids k sur $\Gamma_o(p)$. Choisissons des représentants $\gamma_1, \ldots, \gamma_{p+1}$ de l'espace homogène $\Gamma_o(p)\backslash SL_2(\mathbf{Z})$, et posons

$$\mathrm{Tr}(f) = \sum_{j=1}^{p+1} f|_k\gamma_j .$$

On vérifie immédiatement que $\mathrm{Tr}(f)$ ne dépend pas du choix des γ_j, et que c'est une forme modulaire de poids k sur $SL_2(\mathbf{Z})$; on l'appelle la <u>trace</u> de f. Nous aurons besoin de son développement en série :

LEMME 7. <u>Si</u> $f = \sum a_n q^n$ <u>et</u> $f|_kW = \sum b_n q^n$, <u>on a</u>

$$\mathrm{Tr}(f) = \sum a_n q^n + p^{1-k/2} \sum b_{pn} q^n = f + p^{1-k/2}(f|_kW)|U.$$

On choisit pour représentants $\gamma_j = \begin{pmatrix} 0 & -1 \\ 1 & j \end{pmatrix}$, $1 \leqslant j \leqslant p$, et $\gamma_{p+1} = 1$. Le terme $f|_k\gamma_{p+1}$ donne f. Pour calculer les autres termes, posons $g = f|_k W$, et écrivons $\gamma_j (1 \leqslant j \leqslant p)$ sous la forme $W\beta_j$, où $\beta_j = \begin{pmatrix} 1/p & j/p \\ 0 & 1 \end{pmatrix}$. On a

$$\sum_{j=1}^{p} f|_k \gamma_j = \sum_{j=1}^{p} g|_k \beta_j ;$$

c'est la fonction

$$z \longmapsto p^{-k/2} \sum_{j=1}^{p} g\left(\frac{z+j}{p}\right).$$

Or un calcul simple montre que

$$\sum_{j=1}^{p} g\left(\frac{z+j}{p}\right) = p(g|U)(z).$$

D'où le lemme.

Remarques

1) Le calcul ci-dessus s'applique plus généralement aux fonctions modulaires de poids k, non nécessairement holomorphes; la seule différence est que les séries considérées peuvent avoir des exposants négatifs.

2) Le lemme 7, appliqué à $f|_k W$ donne

$$\mathrm{Tr}(f|_k W) = f|_k W + p^{1-k/2} f|U,$$

ce qui montre que $f|U$ est une forme modulaire de poids k sur $\Gamma_0(p)$.

Si de plus f est modulaire sur $SL_2(\mathbf{Z})$, on a $f|_k W = p^{k/2} f|V$ comme on le voit en écrivant $W = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix}$ et en remarquant que f est invariant par $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$. D'où :

$$\mathrm{Tr}(f|_k W) = p^{k/2} f|V + p^{1-k/2} f|U = p^{1-k/2} f|_k T_p$$

On a ainsi ramené l'opérateur de Hecke T_p à l'opérateur Tr.

3) Supposons $k > 4$. Les formes modulaires f de poids k sur $\Gamma_o(p)$ telles que $Tr(f) = Tr(f|_k W) = 0$ ne sont autres que les combinaisons linéaires des "new forms" d'Atkin-Lehner [3].

d) Propriétés de rationalité et d'intégralité

Soit $j_p = j|V$ la fonction $z \longmapsto j(pz)$. On sait que le corps des fonctions modulaires (de poids 0) sur $\Gamma_0(p)$ est le corps $\mathbf{C}(j, j_p)$ et que j et j_p sont liés par une équation absolument irréductible à coefficients dans $\mathbf{Q}$. En d'autres termes, la courbe complexe $Y_{\mathbf{C}}$ compactifiée de $H/\Gamma_o(p)$ provient par extension des scalaires d'une courbe Y définie sur $\mathbf{Q}$, caractérisée par le fait que son corps des fonctions rationnelles est $\mathbf{Q}(j, j_p)$. Si F est un sous-corps de $\mathbf{C}$, on peut donc parler d'une fonction (ou d'une forme différentielle) sur $Y_{\mathbf{C}}$ qui est rationnelle sur F. Ceci s'applique en particulier aux formes modulaires de poids k, identifiables à des formes différentielles de poids k/2 par $f \longmapsto f(dq/q)^{k/2}$. Comme j et j_p ont des développements en série à coefficients rationnels, on vérifie facilement qu'une forme modulaire $f = \sum a_n q^n$ est rationnelle sur F si et seulement si ses coefficients a_n appartiennent à F. De plus, le corps de rationalité de $f|W$ est le même que celui de f; cela résulte de ce que l'automorphisme W de $Y_{\mathbf{C}}$ est rationnel sur $\mathbf{Q}$.

Il résulte de ceci que les formes modulaires de poids k sur $\Gamma_o(p)$ ont une base formée de fonctions rationnelles sur $\mathbf{Q}$. En fait, il existe même une base formée de fonctions dont les coefficients a_n sont entiers; ce résultat, nettement moins évident, peut se démontrer, soit en utilisant l'existence d'un modèle de Y sur $\mathbf{Z}$ pour lequel q est une uniformisante à l'infini (Igusa, Deligne), soit en se ramenant au fait que les valeurs propres des opérateurs de Hecke sont des entiers algébriques (Shimura [22], p.85, th.3.52). Une conséquence de ceci est que, si $f = \sum a_n q^n$ est une forme modulaire à coefficients rationnels, les dénominateurs des a_n sont bornés. (On notera que, si les coefficients a_n de f sont entiers, il n'en est pas nécessairement de même des coefficients b_n de

$f|_k W$: les b_n sont rationnels, mais peuvent avoir pour dénominateurs des puissances de p.)

3.2. Passage de $\Gamma_o(p)$ à $SL_2(\mathbf{Z})$

THÉORÈME 10. Soit $f = \sum a_n q^n$ une forme modulaire de poids k sur $\Gamma_o(p)$. Supposons que les coefficients a_n soient rationnels. Alors f est une forme modulaire p-adique de poids k (au sens du n° 1.4).

(En d'autres termes, f est limite de formes modulaires f_m sur $SL_2(\mathbf{Z})$ dont les poids k_m tendent vers k dans l'espace X du n° 1.4.)

Choisissons un entier pair $a \geqslant 4$, divisible par p-1. Posons

$$g = E_a - p^{a/2} E_a|_a W = E_a - p^a E_a|V,$$

où E_a est la série d'Eisenstein de poids a, cf. n° 1.1. Il est clair que g est une forme modulaire de poids a sur $\Gamma_o(p)$, cf. n° 3.1. De plus :

LEMME 8. On a $g \equiv 1 \pmod{p}$ et $g|_a W \equiv 0 \pmod{p^{1+a/2}}$.

(Précisons que, dans ces congruences, on considère g et $g|_a W$ comme des séries en q, à coefficients rationnels.)

Le fait que $g \equiv 1 \pmod{p}$ provient de ce que $E_a \equiv 1 \pmod{p}$. D'autre part, on a

$$g|_a W = E_a|_a W - p^{a/2} E_a = p^{a/2}(E_a|V - E_a).$$

Comme $E_a \equiv 1 \equiv E_a|V \pmod{p}$, on en déduit bien que $g|_a W$ est congru à $0 \pmod{p^{1+a/2}}$.

Passons maintenant à la démonstration du th.10. L'hypothèse faite sur f signifie que f est rationnelle sur **Q**, et il en est de même de $f|_k W$, cf. n° 3.1. Si m est un entier $\geqslant 0$, la fonction fg^{p^m} est une forme modulaire sur $\Gamma_o(p)$, de poids $k_m = k + ap^m$, et rationnelle sur **Q**.

Sa <u>trace</u> $f_m = \mathrm{Tr}(fg^{p^m})$ est donc une forme modulaire sur $SL_2(\mathbf{Z})$, à coefficients rationnels, et de poids k_m. Comme les k_m tendent vers k dans X, le théorème sera démontré si l'on prouve que $\lim. f_m = f$, i.e. que $v_p(f_m - f)$ tend vers l'infini avec m. Or cela résulte du lemme plus précis suivant :

LEMME 9. <u>On a</u> $v_p(f_m - f) \geqslant \mathrm{Inf}(m + 1 + v_p(f),\ \ p^m + 1 + v_p(f|_k W) - \frac{k}{2})$.

(Noter que, si $f \neq 0$, $v_p(f)$ et $v_p(f|_k W)$ sont <u>finis</u>, puisque les séries f et $f|_k W$ ont des coefficients à dénominateurs bornés, cf. n° 3.1.)

Ecrivons $f_m - f$ sous la forme $(f_m - fg^{p^m}) + f(g^{p^m} - 1)$. D'après le lemme 8, on a $g \equiv 1 \pmod{p}$ d'où $g^{p^m} \equiv 1 \pmod{p^{m+1}}$, et

$$v_p(f(g^{p^m} - 1)) \geqslant m + 1 + v_p(f).$$

D'autre part, le lemme 7 montre que

$$f_m - fg^{p^m} = p^{1-k_m/2}(fg^{p^m}|_{k_m} W)|U,$$

d'où $\quad v_p(f_m - fg^{p^m}) \geqslant 1 - k_m/2 + v_p(f|_k W) + p^m v_p(g|_a W);$

en appliquant le lemme 8, on en déduit :

$$v_p(f_m - fg^{p^m}) \geqslant 1 - (k + ap^m)/2 + v_p(f|_k W) + p^m(1 + a/2)$$

$$\geqslant p^m + 1 + v_p(f|_k W) - k/2.$$

Le lemme 9 résulte de ces formules et de l'inégalité évidente :

$$v_p(f_m - f) \geqslant \mathrm{Inf}(v_p(f_m - fg^{p^m}),\ \ v_p(f(g^{p^m} - 1))).$$

Remarque

Nous avons supposé f holomorphe aux deux pointes ∞ et 0. Il suffirait en fait que f soit holomorphe en ∞ et méromorphe en 0. La démonstration est la même que ci-dessus; on remarque que la forme g s'annule en 0, donc que fg^{p^m} est une forme modulaire pour m assez grand, et l'on a ici encore $f = \lim.\mathrm{Tr}(fg^{p^m})$.

Ainsi, si l'on pose

$$j = Q^3/\Delta = q^{-1} + \sum_{n=0}^{\infty} c(n)\, q^n,$$

on peut appliquer le th.10 à la fonction $f = j|U = \sum c(pn)\, q^n$, qui a un pôle d'ordre p à la pointe 0. On en conclut que $j|U$ est une forme modulaire p-adique de poids 0; on retrouve - sous une forme plus faible - un théorème de Deligne ([6], §7).

3.3. Réduction (mod.p) des formes de poids 2 sur $\Gamma_o(p)$

Le th.10 montre que la réduction (mod.p) d'une forme modulaire sur $\Gamma_o(p)$, à coefficients p-entiers, est une forme modulaire (mod.p) sur $SL_2(\mathbf{Z})$, au sens du n° 1.2. Dans le cas du poids 2, on peut donner un résultat plus précis :

THÉORÈME 11. On suppose $p \geq 3$. Soit f une forme modulaire de poids 2 sur $\Gamma_o(p)$, à coefficients rationnels p-entiers.

(a) On a $f|_2 W = - f|U$; c'est une forme à coefficients p-entiers.

(b) La réduction $\tilde{f}$ de f (mod.p) appartient à l'espace $\widetilde{M}_{p+1}$ du n° 1.2.

(c) Inversement, tout élément de $\widetilde{M}_{p+1}$ est réduction (mod.p) d'une forme modulaire de poids 2 sur $\Gamma_o(p)$, à coefficients p-entiers.

(En d'autres termes, il y a identité entre :

réduction (mod.p) des formes modulaires de poids 2 sur $\Gamma_o(p)$

et

réduction (mod.p) des formes modulaires de poids p+1 sur $SL_2(\mathbf{Z})$.)

L'assertion (a) est bien connue (Hecke [8], p.777). On la démontre en remarquant que toute forme de poids 2 sur $SL_2(\mathbf{Z})$ est nulle, et que l'on a donc $Tr(f|_2 W) = 0$; or d'après le lemme 7, $Tr(f|_2 W)$ est égal à $f|_2 W + f|U$.

Démontrons (b) et (c) en supposant d'abord $p \geqslant 5$. Posons

$$g = E_{p-1} - p^{(p-1)/2} E_{p-1}|W = E_{p-1} - p^{p-1} E_{p-1}|V,$$

cf. démonstration du th.10. La fonction fg est une forme modulaire de poids p+1 sur $\Gamma_o(p)$, à coefficients p-entiers; sa trace Tr(fg) appartient à M_{p+1}. De plus, le lemme 9 du n° 3.2, appliqué à m = 0 et k = 2, montre que $v_p(Tr(fg) - f) \geqslant 1$, i.e. que

$$f \equiv Tr(fg) \quad (\text{mod}.p),$$

d'où $\tilde{f} \in \tilde{M}_{p+1}$, ce qui démontre (b) pour $p \geqslant 5$. Soit maintenant N le sous-espace vectoriel de $\tilde{M}_{p+1}$ formé des fonctions telles que $\tilde{f}$. La dimension de N est égale à la dimension de l'espace des formes modulaires de poids 2 sur $\Gamma_o(p)$, i.e. $1 + g(Y)$ où $g(Y)$ désigne le genre de la courbe Y définie par $\Gamma_o(p)$. La valeur de g(Y) est bien connue (cf. par exemple Hecke [8], p.810) : si l'on écrit $p = 12a + b$, avec $b = 1,5,7,11$, on a $g(Y) = a - 1, a, a, a + 1$ respectivement. D'autre part, on sait que

$$\dim.M_k = \begin{cases} [k/12] & \text{si } k \equiv 2 \pmod{12} \\ 1 + [k/12] & \text{si } k \not\equiv 2 \pmod{12}. \end{cases} \qquad (k \text{ pair} \geqslant 0)$$

On en déduit que $\dim.\tilde{M}_{p+1} = 1 + g(Y) = \dim.N$, d'où le fait que $N = \tilde{M}_{p+1}$, ce qui démontre (c) dans le cas $p \geqslant 5$.

Reste le cas p = 3. L'espace $\tilde{M}_4$ a pour base $\tilde{Q} = 1$. D'autre part, on a $g(Y) = 0$, et les formes de poids 2 sur $\Gamma_o(3)$ sont simplement les multiples de la série d'Eisenstein $E_2^* = P - 3P|V$, cf. Hecke [8], p.817.

Comme $\widetilde{E}_2^* = \widetilde{P} = 1$, les assertions (b) et (c) sont évidentes.

COROLLAIRE. Les valeurs propres de U sur $\widetilde{M}_{p+1}$ sont égales à ± 1.

En effet, le th.11 montre que $\widetilde{f}|U^2 = \widetilde{f}|W^2 = \widetilde{f}$ pour tout $\widetilde{f} \in \widetilde{M}_{p+1}$.

Remarque. Cette démonstration a également été obtenue par Atkin.

Exemples

1) Pour p = 11, 17, 19, le genre de Y est 1. Il existe une unique forme parabolique de poids 2 sur $\Gamma_0(p)$:

$$f_p = a_1 q + a_2 q^2 + \dots, \quad \text{avec} \quad a_1 = 1.$$

La série de Dirichlet correspondante $\sum a_n/n^s$ est essentiellement la fonction zêta de Y ([22], p.182). D'après le th.11, f_p est congru (mod.p) à une forme parabolique de poids 12, 18, 20 sur $SL_2(\mathbf{Z})$; on en déduit les congruences :

$$f_{11} \equiv \Delta \pmod{11}; \quad f_{17} \equiv R\Delta \pmod{17}; \quad f_{19} \equiv Q^2\Delta \pmod{19}.$$

La première de ces congruences peut aussi se déduire de l'identité :

$$f_{11} = q \prod_{n=1}^{\infty} (1 - q^n)^2 (1 - q^{11n})^2, \qquad \text{cf. [22], p.49.}$$

2) Pour p = 23, 31, le genre de Y est 2. Le nombre de classes du corps $\mathbf{Q}(\sqrt{-p})$ est 3. Soit χ un caractère d'ordre 3 du groupe des classes d'idéaux de ce corps, et posons

$$g_p = \sum \chi(\mathfrak{a})\, q^{N\mathfrak{a}} = \begin{cases} q - q^2 - q^3 + q^6 + \dots & (p = 23) \\ q - q^2 - q^5 - q^7 + \dots & (p = 31) \end{cases},$$

la sommation étant étendue à tous les idéaux entiers $\mathfrak{a}$. Il n'est pas difficile de voir que $g_p = \frac{1}{2}(\theta_1 - \theta_2)$, où θ_1 (resp. θ_2) est la série thêta associée à la forme binaire $m^2 + mn + \frac{p+1}{4} n^2$ (resp. à la forme $2m^2 + mn + \frac{p+1}{8} n^2$). Il en résulte (cf. [8], p.478-479) que g_p est une forme modulaire de poids 1 sur $\Gamma_o(p)$, de "Nebentypus" au sens de Hecke (cf. n° 3.4 ci-après). Son carré est une forme de poids 2, commençant par le terme q^2. Appliquant le th.11, on en déduit les congruences

$$g_{23}^2 \equiv \Delta^2 \pmod{23} \quad \text{et} \quad g_{31}^2 \equiv Q^2\Delta^2 \pmod{31},$$

d'où, en extrayant les racines carrées,

$$g_{23} \equiv \Delta \pmod{23} \quad \text{et} \quad g_{31} \equiv Q\Delta \pmod{31}.$$

La première de ces congruences peut aussi se déduire de l'identité

$$g_{23} = q \prod_{n=1}^{\infty} (1 - q^n)(1 - q^{23n});$$

elle est due à Wilton; voir là-dessus [27], p.34.

3.4. <u>Formes de "Nebentypus" sur</u> $\Gamma_o(p)$

On suppose $p \geqslant 3$. Soit ε un caractère (mod.p), i.e. un homomorphisme du groupe multiplicatif $(\mathbf{Z}/p\mathbf{Z})^*$ dans $\mathbf{C}^*$. Si n est un entier de réduction mod.p égale à $\tilde{n}$, on pose

$$\varepsilon(n) = 0 \text{ si } \tilde{n} = 0 \quad \text{et} \quad \varepsilon(n) = \varepsilon(\tilde{n}) \quad \text{sinon.}$$

On étend ε à $\Gamma_o(p)$ par :

$$\varepsilon(\gamma) = \varepsilon(a)^{-1} = \varepsilon(d) \quad \text{si} \quad \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

Cela a un sens puisque $ad \equiv 1 \pmod{p}$.

Soit $k \in \mathbf{Z}$. Une fonction f sur H est appelée <u>une forme modulaire de</u>

<u>type</u> (k, ε) sur $\Gamma_o(p)$ si elle est holomorphe sur H et vérifie les deux conditions :

(i) $f|_k\gamma = \varepsilon(\gamma)f$ <u>pour tout</u> $\gamma \in \Gamma_o(p)$;

(ii) f <u>est holomorphe aux pointes de</u> $\Gamma_o(p)$.

Lorsque $\varepsilon = 1$ ("Haupttypus" de Hecke [8], p.809), on retrouve la notion de forme modulaire de poids k, au sens du n° 3.1; le cas $\varepsilon \neq 1$ est celui appelé "Nebentypus" par Hecke.

Si $f \neq 0$, on a $k \geq 0$, et $\varepsilon(-1) = (-1)^k$; autrement dit, k est pair si $\varepsilon(-1) = 1$ et impair si $\varepsilon(-1) = -1$.

Une telle forme f a un développement en série

$$\sum_{n=0}^{\infty} a_n\, q^n,$$

avec $a_n \in \mathbf{C}$. Notons μ_{p-1} le groupe des racines (p-1)-ièmes de 1. Nous allons voir que, si les a_n appartiennent au corps $\mathbf{Q}(\mu_{p-1})$, la série f "est" une forme modulaire p-adique (ce qui généralisera le th.10). De façon plus précise, on sait que p se décompose complètement dans $\mathbf{Q}(\mu_{p-1})$ en idéaux premiers de degré 1 :

$$\mathfrak{p}_1, \ldots, \mathfrak{p}_r \quad \text{avec} \quad r = \phi(p-1) = [\mathbf{Q}(\mu_{p-1}) : \mathbf{Q}].$$

Choisissons un de ces idéaux premiers, ce qui définit un plongement σ de $\mathbf{Q}(\mu_{p-1})$ dans le corps p-adique $\mathbf{Q}_p$; comme le groupe des racines (p-1)-ièmes de l'unité de $\mathbf{Q}_p$ s'identifie canoniquement à $(\mathbf{Z}/p\mathbf{Z})^*$ ("représentants multiplicatifs"), on voit que σ définit un <u>isomorphisme de</u> μ_{p-1} <u>sur</u> $(\mathbf{Z}/p\mathbf{Z})^*$, et tout isomorphisme est obtenu ainsi (en choisissant convenablement $\mathfrak{p}_i$). En composant $\varepsilon : (\mathbf{Z}/p\mathbf{Z})^* \to \mu_{p-1}$ et $\sigma : \mu_{p-1} \to (\mathbf{Z}/p\mathbf{Z})^*$ on obtient un endomorphisme de $(\mathbf{Z}/p\mathbf{Z})^*$, qui est nécessairement de la forme $x \mapsto x^\alpha$, avec $\alpha \in \mathbf{Z}/(p-1)\mathbf{Z}$. Avec ces notations, on a :

THÉORÈME 12. <u>Soit</u> $f = \sum a_n q^n$ <u>une forme modulaire de type</u> (k, ε) <u>sur</u> $\Gamma_o(p)$, <u>telle que</u> $a_n \in \mathbf{Q}(\mu_{p-1})$ <u>pour tout</u> n. <u>Alors la série</u>

$$f^{\sigma} = \sum a_n^{\sigma} q^n, \quad \underline{\text{à coefficients}} \quad a_n^{\sigma} \in \mathbf{Q}_p,$$

<u>est une forme modulaire</u> p-<u>adique de poids</u> $k + \alpha$.

(Précisons que α est identifié à l'élément $(0, \alpha)$ du groupe des poids $X = \mathbf{Z}_p \times \mathbf{Z}/(p-1)\mathbf{Z}$, et $k + \alpha$ à $(k, k+\alpha)$. On peut supposer $f \neq 0$, d'où $\varepsilon(-1) = (-1)^k$, et il en résulte que $k + \alpha$ est un élément <u>pair</u> de X.)

Lorsque $\varepsilon = 1$, f est combinaison $\mathbf{Q}(\mu_{p-1})$-linéaire de formes modulaires de poids k (au sens du n° 3.1) à coefficients rationnels, et le th.12 résulte du th.10; nous pouvons donc supposer $\varepsilon \neq 1$.

Commençons par un cas particulier :

LEMME 10. <u>Si</u> $k \geqslant 1$, <u>et</u> $\varepsilon(-1) = (-1)^k$, <u>la série</u>

$$G_k(\varepsilon) = \frac{1}{2} L(1 - k, \varepsilon) + \sum_{n=1}^{\infty} \Big(\sum_{d|n} \varepsilon(d)\, d^{k-1} \Big) q^n$$

<u>est une forme modulaire de type</u> (k, ε) <u>sur</u> $\Gamma_o(p)$. <u>Ses coefficients appartiennent à</u> $\mathbf{Q}(\mu_{p-1})$, <u>et l'on a</u>

$$G_k(\varepsilon)^{\sigma} = G_h^{*},$$

<u>où</u> G_h^{*} <u>est la série d'Eisenstein</u> p-<u>adique de poids</u> $h = k + \alpha$, <u>au sens du</u> n° 1.6.

Le fait que $G_k(\varepsilon)$ soit de type (k, ε) résulte de la détermination par Hecke des séries d'Eisenstein de niveau p (cf. [8], p.461-486, ainsi que l'<u>Appendice</u> du §5). De façon plus précise, avec les notations de [8], <u>loc.cit</u>., on vérifie que $G_k(\varepsilon)$ est égale, à un facteur scalaire près, à la fonction

$$\sum_{\lambda \in (\mathbf{Z}/p\mathbf{Z})^{*}} \varepsilon(\lambda)^{-1}\, G_k(z;0,\lambda,p);$$

comme $G_k(z;0,\lambda,p)|_k \begin{pmatrix} a & b \\ c & d \end{pmatrix} = G_k(z;0,d\lambda,p)$ si $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_o(p)$, on en déduit, par un calcul immédiat, que $G_k(\varepsilon)|_k \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \varepsilon(d)\ G_k(\varepsilon)$, ce qui montre bien que $G_k(\varepsilon)$ est de type (k, ε). Ses coefficients appartiennent au corps engendré par les valeurs de ε, qui est contenu dans $\mathbf{Q}(\mu_{p-1})$. Montrons maintenant que $G_k(\varepsilon)^\sigma$ est égale à G_h^*. Si $n \geqslant 1$, le n-ième coefficient a_n^σ de $G_k(\varepsilon)^\sigma$ est égal à $\sum \varepsilon(d)^\sigma\ d^{k-1}$, la sommation portant sur les diviseurs d de n qui sont premiers à p. Ecrivons d dans $\mathbf{Q}_p$ sous la forme $\omega(d)\ \langle d \rangle$, avec $\omega(d)^{p-1} = 1$, et $\langle d \rangle \equiv 1 \pmod{p}$, cf. Iwasawa [11], p.18. On a alors $\varepsilon(d)^\sigma = \omega(d)^\alpha = d^\alpha$, vu la définition de α. D'où

$$a_n^\sigma = \sum d^{k+\alpha-1} = \sigma_{h-1}^*(n),$$

ce qui est bien le n-ième coefficient de G_h^*. D'autre part, $L(1-k, \varepsilon)^\sigma$ est égal à $-b_k(\omega^\alpha)/k = L_p(1-k, \omega^{k+\alpha})$, avec les notations de [11], §3. Vu le th.3 du n° 1.6, on a donc

$$L(1-k, \varepsilon)^\sigma = \zeta^*(1-k, 1-k-\alpha) = \zeta^*(1-h);$$

le terme constant de $G_k(\varepsilon)^\sigma$ est égal à celui de G_h^*, ce qui achève la démonstration du lemme.

Revenons maintenant au th.12. Choisissons une suite d'entiers $k_n \geqslant 1$ tendant vers α dans X, et tels que $k_n - \alpha \in (p-1)X$ pour tout n. Posons

$$g_n = \lambda_n^{-1} G_{k_n}(\varepsilon^{-1}),$$

où λ_n est le terme constant de la série $G_{k_n}(\varepsilon^{-1})$, cf. lemme 10. Le produit fg_n est une forme modulaire sur $\Gamma_0(p)$ de type $(k + k_n, 1)$; il en résulte, comme on l'a dit plus haut, que $f^\sigma g_n^\sigma$ est une forme modulaire p-adique de poids $k + k_n$. D'autre part, d'après le lemme 10 appliqué à k_n et ε^{-1}, on a $g_n^\sigma = E_{h_n}^*$, où $h_n = k_n - \alpha$. Comme h_n tend vers 0 dans X, il en résulte que g_n^σ tend vers $E_0^* = 1$, d'où $\lim. f^\sigma g_n^\sigma = f^\sigma$, ce qui montre que f^{σ} est modulaire p-adique de poids $k + \alpha = \lim.(k + k_n)$ et achève la démonstration.

Remarque

Sous les hypothèses du th.12, on peut démontrer que $f|_k W$ est de type (k, ε^{-1}) ; on a $f|_k W^2 = \varepsilon(-1)f$.

§4. Familles analytiques de formes modulaires p-adiques

4.1. L'algèbre d'Iwasawa (p ≠ 2)

a) Notations

Si $n \geq 1$, on note U_n le sous-groupe de $\mathbf{Z}_p^*$ formé des entiers p-adiques u tels que $u \equiv 1 \pmod{p^n}$. On sait que

$$U_1 \simeq \varprojlim (U_1/U_n)$$

est isomorphe à $\mathbf{Z}_p$. Si $s \in \mathbf{Z}_p$ et $u \in U_1$, on définit de façon évidente $u^s \in U_1$, cf. n° 1.4, a).

On note F l'algèbre des fonctions sur $\mathbf{Z}_p$, à valeurs dans $\mathbf{Z}_p$. Si $u \in U_1$, on note f_u la fonction $s \longmapsto u^s$. Les $f_u (u \in U_1)$ engendrent un sous-$\mathbf{Z}_p$-module L de F, qui est une sous-algèbre. D'après le théorème d'indépendance des caractères (Dedekind), les f_u forment une base de L, et l'on peut identifier L à l'algèbre $\mathbf{Z}_p[U_1]$ du groupe U_1. Un élément de L s'écrit donc, de façon unique, sous la forme

$$s \longmapsto f(s) = \sum_{u \in U_1} \lambda_u u^s, \quad \text{avec} \quad \lambda_u \in \mathbf{Z}_p,$$

les λ_u étant presque tous nuls.

b) L'algèbre $\overline{L}$

On définit $\overline{L}$ comme l'adhérence de L dans F, pour la topologie de la convergence uniforme. Notons d'ailleurs que les éléments de L sont équicontinus : si $f \in L$ et $n \geq 0$, on a

$$s \equiv s' \pmod{p^n} \Longrightarrow f(s) \equiv f(s') \pmod{p^{n+1}}.$$

La même propriété est donc vraie pour $\overline{L}$; de plus, sur $\overline{L}$, la topologie de la convergence uniforme coïncide avec celle de la convergence simple sur un sous-espace dense, et cette topologie fait de $\overline{L}$ un espace compact.

c) L'algèbre Λ

C'est l'algèbre $\mathbf{Z}_p[[U_1]] = \varprojlim . \mathbf{Z}_p[U_1/U_n]$, cf. [10], [11]. On sait qu'elle est isomorphe à l'algèbre $\mathbf{Z}_p[[T]]$ des séries formelles en une indéterminée T. L'isomorphisme s'obtient en choisissant un générateur topologique $u = 1 + \pi$ de U_1, avec $v_p(\pi) = 1$, et en associant à l'élément f_u de $\mathbf{Z}_p[U_1]$ l'élément $1 + T$ de $\mathbf{Z}_p[[T]]$.

L'anneau Λ est un anneau local régulier de dimension 2; il joue un rôle essentiel dans les travaux d'Iwasawa sur les classes d'idéaux des extensions cyclotomiques (le groupe U_1 intervenant alors comme un groupe de Galois). On notera que Λ est compact pour la topologie définie par les puissances de son idéal maximal; lorsqu'on identifie Λ à $\mathbf{Z}_p[[T]]$, cette topologie devient celle de la convergence simple des coefficients; le groupe topologique Λ est donc isomorphe à un produit infini de groupes $\mathbf{Z}_p$.

d) Identification de $\overline{L}$ à Λ.

Les algèbres $\overline{L}$ et Λ contiennent toutes deux $L = \mathbf{Z}_p[U_1]$ comme sous-algèbre dense. Il s'impose de les comparer :

LEMME 11. Il existe un unique isomorphisme d'algèbres topologiques

$$\varepsilon : \Lambda \to \overline{L}$$

<u>dont la restriction à</u> $\mathbf{Z}_p[U_1]$ <u>soit l'identité</u>.

L'unicité de ε résulte de ce que $\mathbf{Z}_p[U_1]$ est dense dans Λ. Pour en montrer l'existence, identifions comme ci-dessus Λ à $\mathbf{Z}_p[[T]]$ au moyen du choix d'un générateur topologique u de U_1. Si $f = \sum a_n T^n$ est un élément de Λ, on définit $\varepsilon(f)$ comme la fonction

$$s \longmapsto f(u^s - 1) = \sum a_n (u^s - 1)^n,$$

ce qui a un sens car $u^s - 1 \equiv 0 \pmod{p}$. Il est clair que ε est un homomorphisme continu de Λ dans F, et que $\varepsilon(f_u) = f_u$; il en résulte que ε est l'identité sur L; par continuité, on a donc $\varepsilon(\Lambda) = \bar{L}$. Le fait que ε soit injectif est immédiat; comme Λ est compact, c'est un homéomorphisme.

<u>Remarques</u>

1) Dans ce qui suit, nous identifierons Λ à $\bar{L}$ au moyen de ε. Comme on vient de le voir, cela revient à passer d'une série en T à une fonction de s par le "changement de variables"

$$T = u^s - 1 = vs + \dots + v^n s^n/n! + \dots, \quad \text{où} \quad v = \log(u).$$

2) Il y a une troisième interprétation de Λ, due à B.Mazur, qui est souvent utile : c'est l'algèbre des "distributions" (ou "mesures") à valeurs dans $\mathbf{Z}_p$ sur l'espace U_1. On appelle ainsi toute fonction $U \longmapsto \mu(U)$, définie sur les ouverts compacts de U_1, simplement additive, et à valeurs dans $\mathbf{Z}_p$; une telle mesure se prolonge par continuité en une forme linéaire

$$f \longmapsto \int_{U_1} f(u)\mu(u)$$

sur l'espace des fonctions continues sur U_1 à valeurs dans $\mathbf{Z}_p$. Si l'on associe à μ la fonction $s \longmapsto \int_{U_1} u^s\ \mu(u)$, on obtient un élément de Λ; tout élément de Λ s'obtient ainsi, de manière unique; les éléments de L correspondent aux mesures discrètes.

e) Zéros d'un élément de Λ

Tout élément $f \neq 0$ de $\Lambda = \mathbf{Z}_p[[T]]$ a une "décomposition de Weierstrass" canonique :

$$f = p^{\mu}(T^{\lambda} + a_1 T^{\lambda-1} + \dots + a_{\lambda})\, u(T),$$

avec λ, $\mu \geqslant 0$, $v_p(a_i) \geqslant 1$, et u inversible dans Λ. En particulier, le nombre de zéros de f(s) est fini et $\leqslant \lambda$.

Comme application, signalons :

LEMME 12. *Soit* $f_1,\dots,f_n,\dots$ *une suite d'éléments de* Λ. *On suppose que* $\lim. f_n(s)$ *existe pour tout élément* s *d'une partie infinie* S *de* $\mathbf{Z}_p$. *Alors les* f_n *convergent uniformément sur* $\mathbf{Z}_p$ *vers une fonction* f *appartenant à* Λ.

Sinon, vu la compacité de Λ, on pourrait extraire de la suite (f_n) deux suites convergeant vers des éléments distincts f' et f" de Λ. La fonction f' - f" s'annulerait sur S, donc aurait une infinité de zéros, contrairement à ce que l'on vient de voir.

(La famille Λ se comporte comme une "famille normale" au sens de Montel.)

4.2. L'algèbre d'Iwasawa (p = 2)

On définit encore U_n comme le sous-groupe de $\mathbf{Z}_p^*$ formé des entiers 2-adiques u tels que $u \equiv 1 \pmod{2^n}$. On a

$$\mathbf{Z}_p^* = U_1 = \{\pm 1\} \times U_2$$

et U_2 est isomorphe à $\mathbf{Z}_2$; si $u \in U_1$, on note $\omega(u)$ sa composante dans $\{\pm 1\}$ et $\langle u \rangle$ sa composante dans U_2, cf. [11], p.18.

On définit les algèbres L et Λ au moyen du groupe U_2 (et non plus du groupe U_1). De façon plus précise, L est l'algèbre engendrée par les fonctions $f_u : s \longmapsto u^s$, avec $u \in U_2$. On montre, comme au n° 4.1, que l'adhérence $\bar{L}$ de L s'identifie à l'algèbre d'Iwasawa

$$\Lambda = \mathbf{Z}_2[[U_2]] = \varprojlim \mathbf{Z}_2[U_2/U_n].$$

Ici encore, cette algèbre est isomorphe à $\mathbf{Z}_2[[T]]$, l'isomorphisme s'obtenant en choisissant un générateur topologique u de U_2 et en associant à l'élément f_u de $\mathbf{Z}_2[U_2]$ l'élément $1 + T$ de $\mathbf{Z}_2[[T]]$, cf. [11], p.69.

Les autres résultats du n° 4.1 se transposent de manière évidente au cas $p = 2$.

4.3. Caractérisation des éléments de Λ par leurs développements en série

Nous allons voir que les fonctions f appartenant à Λ peuvent être caractérisées comme des séries de Taylor convergentes

$$f(s) = \sum_{n=0}^{\infty} a_n s^n,$$

dont les coefficients a_n vérifient certaines congruences. Pour écrire commodément ces congruences, définissons des entiers c_{in} $(1 \leqslant i \leqslant n)$ par l'identité

$$\sum_{i=1}^{n} c_{in} Y^i = Y(Y-1)(Y-2) \dots (Y-n+1) = n! \binom{Y}{n}.$$

On a alors :

THÉORÈME 13. Pour qu'une fonction $f \in F$ appartienne à Λ, il faut et il suffit qu'il existe des entiers p-adiques b_n $(n = 0,1,\dots)$ tels que

a) $$f(s) = \sum_{n=0}^{\infty} b_n p^n s^n/n! \quad \underline{\text{pour tout}} \quad s \in \mathbf{Z}_p,$$

b) $$v_p\Big(\sum_{i=1}^{n} c_{in} b_i\Big) \geq v_p(n!) \quad \underline{\text{pour tout}} \quad n \geq 1.$$

(Si $p = 2$, on doit modifier a) en remplaçant p^n par 4^n.)

Remarques

1) Comme $c_{nn} = 1$, la condition b) équivaut à dire que chacun des b_n est congru (mod. $n!\mathbf{Z}_p$) à une certaine combinaison $\mathbf{Z}$-linéaire des b_j, $j < n$.

2) On a

$$v_p(b_n p^n/n!) \geq n - v_p(n!) \geq n\frac{p-2}{p-1} \quad \text{si} \quad p \neq 2$$

$$v_2(b_n 4^n/n!) \geq 2n - v_2(n!) \geq n \quad \text{si} \quad p = 2.$$

Il en résulte que la série entière donnant f converge dans un disque p-adique strictement plus grand que le disque unité; a fortiori, elle converge sur $\mathbf{Z}_p$, ce qui donne un sens à a).

Démonstration du th.13

Je me borne au cas $p \neq 2$; le cas $p = 2$ est analogue.

(i) Le développement

$$T = vs + \ldots + v^n s^n/n! + \ldots, \quad \text{avec} \quad v_p(v) = 1,$$

donné au n° 4.1 montre que T, ainsi que ses puissances, a un développement en série du type a). Par linéarité et passage à la limite, on voit qu'il en est de même de toute fonction f de Λ. De plus les coefficients $b_n = b_n(f)$ de f dépendent continûment de f. On en conclut que l'application $f \longmapsto (b_n(f))$ est un isomorphisme du groupe compact Λ sur un certain sous-module fermé S_Λ du $\mathbf{Z}_p$-module produit $S = (\mathbf{Z}_p)^N$ des suites

$(b_n)_{n \geq 0}$. Tout revient donc à montrer que S_Λ coïncide avec le sous-module S_b de S défini par les congruences b).

(ii) Tout élément u de U_1 s'écrit $\exp(py)$, avec $y \in \mathbf{Z}_p$. On en conclut que

$$u^s = \exp(pys) = \sum_{n=0}^{\infty} y^n p^n s^n/n!,$$

i.e. que $b_n(f_u) = y^n$. Or la suite (y^n) appartient à S_b. On a en effet

$$\sum c_{in} y^n = y(y-1)\dots(y-n+1) = n! \binom{y}{n},$$

et l'on sait que $\binom{y}{n}$ est un entier p-adique; cela montre bien que $\sum c_{in} y^n$ est divisible par $n!$ dans $\mathbf{Z}_p$.

Par linéarité et passage à la limite on conclut de là que S_Λ est contenu dans S_b. Il reste à voir que S_Λ est égal à S_b; vu ce qui précède, cela équivaut à dire que les suites de la forme (y^n), avec $y \in \mathbf{Z}_p$, engendrent un sous-$\mathbf{Z}_p$-module <u>dense</u> de S_b.

(iii) Soit $m \geq 1$ et soient $b_o, \dots, b_m \in \mathbf{Z}_p$ satisfaisant aux congruences b) pour $n \leq m$. Nous allons montrer qu'il existe $f \in \Lambda$ tel que $b_i(f) = b_i$ pour $0 \leq i \leq m$, ce qui achèvera la démonstration.

On procède par récurrence sur m, le cas $m = 0$ étant évident. Vu l'hypothèse de récurrence, il existe $g \in \Lambda$ tel que $b_i(g) = b_i$ pour $i \leq m-1$; tout revient à trouver $h \in \Lambda$ tel que $b_i(h) = 0$ pour $i \leq m-1$ et $b_m(h) = b_m - b_m(g)$. On est donc ramené au cas où les b_i sont <u>nuls</u> pour $i \leq m-1$; vu la congruence b) il en résulte que b_m est de la forme $m!\, z$, avec $z \in \mathbf{Z}_p$. On prend alors pour f le monôme $z(p/v)^m T^m$, avec les notations de (i); il est clair qu'il répond à la question.

COROLLAIRE. <u>Soit</u> $f \in \Lambda$, <u>et soient</u> b_n <u>les coefficients correspondants</u>. <u>On a</u> $b_n \equiv b_{n+p-1} \pmod{p}$ <u>pour tout</u> $n \geq 1$.

En effet, cette congruence est évidente lorsque la suite (b_n) est de la forme (y^n), avec $y \in \mathbf{Z}_p$, et le cas général s'en déduit par linéarité et passage à la limite. (Bien entendu, on peut aussi utiliser b).)

Remarque

Signalons une autre propriété de stabilité de l'algèbre Λ :

$$\underline{\text{si}}\quad f \in \Lambda,\quad \underline{\text{on a}}\quad \frac{df}{ds} \in p\Lambda\quad \underline{\text{si}}\quad p \neq 2\quad \underline{\text{et}}\quad \frac{df}{ds} \in 4\Lambda\quad \underline{\text{si}}\quad p = 2.$$

Cela résulte de la formule $\frac{df}{ds} = v(1 + T)\frac{df}{dT}$.

4.4. Caractérisation des éléments de Λ par des propriétés d'interpolation

Soient $s_o, s_1 \in \mathbf{Z}_p$ et $f \in F$. Posons $a_n = a_n(f) = f(s_o + ns_1)$ pour $n = 0, 1, \ldots$ et désignons par $\delta_o, \delta_1, \ldots, \delta_n, \ldots$ les différences successives de la suite (a_n) :

$$\delta_o = a_o,\quad \delta_1 = a_1 - a_o,\quad \delta_2 = a_2 - 2a_1 + a_o,\ \ldots,$$

$$\delta_n = \sum_{i=0}^{n} (-1)^i \binom{n}{i} a_{n-i}.$$

THÉORÈME 14. Posons

$$h = 1 + v_p(s_1)\quad \underline{\text{si}}\quad p \neq 2\quad \underline{\text{et}}\quad h = 2 + v_2(s_1)\quad \underline{\text{si}}\quad p = 2.$$

Si $f \in \Lambda$, on a

a) $\delta_n \equiv 0 \pmod{p^{nh}}$ pour tout $n \geq 0$,

b) $v_p(\sum_{i=1}^{n} c_{in}\delta_i p^{-ih}) \geq v_p(n!)$ pour tout $n \geq 1$.

(On rappelle que c_{in} est le coefficient de Y^i dans le polynôme $Y(Y - 1)\ldots(Y - n + 1)$, cf. n° 4.3.)

Il suffit de considérer le cas où $f(s) = u^s$ avec $u \in U_1$ (resp. avec $u \in U_2$ si $p = 2$); le cas général s'en déduira par linéarité et passage à la limite. On a alors

$$a_n = u^{s_o} u^{ns_1} \quad \text{et} \quad \delta_n = u^{s_o} (u^{s_1} - 1)^n.$$

Or $u^{s_1} - 1$ est de la forme $p^h y$, avec $y \in \mathbf{Z}_p$. On a donc $v_p(\delta_n) \geq nh$, ce qui prouve a). L'assertion b) provient de ce que

$$\sum_{i=1}^{n} c_{in}\delta_i p^{-ih} = u^{s_o}(\sum c_{in} y^i) = u^{s_o} y(y - 1)\ldots(y - n + 1)$$

$$= n!\ u^{s_o}\binom{y}{n} \quad \equiv 0 \pmod{n!\mathbf{Z}_p}.$$

COROLLAIRE. Posons $e_n = \delta_n p^{-nh}$. On a $e_n \equiv e_{n+p-1} \pmod{p}$ pour tout $n \geq 1$.

La démonstration est la même que celle du corollaire au th.13.

En fait, les congruences de th.14 caractérisent les éléments de l'algèbre d'Iwasawa Λ. De façon plus précise, prenons $s_o = 0$ et $s_1 = 1$, de sorte que $a_n = f(n)$, et que les δ_n sont les coefficients d'interpolation usuels; on sait (critère de Mahler, cf. [1]) que, si f est continue, les δ_n tendent vers 0, et que l'on a

$$f(s) = \sum_{n=0}^{\infty} \delta_n \binom{s}{n} \quad \text{pour tout} \quad s \in \mathbf{Z}_p.$$

THÉORÈME 15. Soit f une fonction continue sur $\mathbf{Z}_p$, à valeurs dans $\mathbf{Q}_p$, et soient $\delta_n = \sum (-1)^i \binom{n}{i} f(n-i)$ ses coefficients d'interpolation. Pour que f appartienne à Λ, il faut et il suffit que :

a) $\delta_n \equiv 0 \pmod{p^n}$ pour tout $n \geq 0$,

b) $v_p(\sum_{i=1}^{n} c_{in}\delta_i p^{-i}) \geq v_p(n!)$ pour tout $n \geq 1$.

(Si $p = 2$, on doit remplacer p^n par 4^n dans a), et p^{-i} par 4^{-i} dans b).)

La nécessité résulte du th.14. Prouvons la suffisance, en nous bornant au cas $p \neq 2$ (le cas $p = 2$ est analogue). Soit S_b l'ensemble des suites (b_n) d'entiers p-adiques tels que

$$v_p(\sum c_{in}b_i) \geq v_p(n!) \quad \text{pour tout} \quad n \geq 1.$$

On a vu au n° 4.2 que les suites de la forme (y^n), avec $y \in \mathbf{Z}_p$, engendrent un sous-module dense de S_b pour la topologie produit. Par hypothèse, la suite $(\delta_n p^{-n})$ appartient à S_b. Pour tout entier m on peut donc choisir des éléments λ_i, y_i de $\mathbf{Z}_p$, en nombre fini, tels que

$$\delta_n p^{-n} = \sum \lambda_i y_i^n \quad \text{pour tout} \quad n \leq m.$$

Posons $$f_m(s) = \sum \lambda_i(1 + py_i)^s.$$

On a $f_m \in \Lambda$ (et même $f_m \in L$); de plus les formules ci-dessus montrent que les coefficients d'interpolation de f_m sont les mêmes que ceux de f jusqu'à l'indice m; on a donc $f_m(n) = f(n)$ pour $n \leq m$, et la suite (f_m) tend vers f pour la topologie de la convergence simple sur l'ensembel $\mathbf{N}$ des entiers ≥ 0. Comme $\mathbf{N}$ est dense dans $\mathbf{Z}_p$, cela entraîne que $f = \lim. f_m$, cf. n° 4.1 b), et par suite on a bien $f \in \Lambda$.

4.5. Exemple : coefficients des séries d'Eisenstein p-adiques

Considérons la série

$$G_k^* = \frac{1}{2}\zeta^*(1-k) + \sum_{n=1}^{\infty} \sigma_{k-1}^*(n)\, q^n \qquad (k \in X, \ k \text{ pair} \neq 0)$$

définie au n° 1.6. Ecrivons k sous la forme $k = (s,u)$, avec :

$$s \in \mathbf{Z}_p, \quad u \in \mathbf{Z}/(p-1)\mathbf{Z}, \quad u \text{ pair (si } p \neq 2), \quad s \text{ pair (si } p = 2).$$

Les coefficients de $G_k^* = G_{s,u}^*$ sont :

$$a_o(G_{s,u}^*) = \tfrac{1}{2}\zeta^*(1 - s,\ 1 - u)$$

$$a_n(G_{s,u}^*) = \sigma_{k-1}^*(n) = \sum_{\substack{d|n \\ (d,p)=1}} d^{k-1} \quad \text{si} \quad n \geq 1.$$

Décomposons l'unité p-adique d en $\omega(d)\,\langle d\rangle$, avec

$$\omega(d)^{p-1} = 1, \quad \langle d\rangle \in U_1 \quad \text{si} \quad p \neq 2,$$

$$\omega(d) = \pm 1, \quad \langle d\rangle \in U_2 \quad \text{si} \quad p = 2.$$

On a alors :

$$a_n(G_{s,u}^*) = \sum d^{-1}\,\omega(d)^k\,\langle d\rangle^k = \sum d^{-1}\,\omega(d)^u\,\langle d\rangle^s \qquad (n \geq 1).$$

On en conclut que, pour u et n fixés (avec $n \geq 1$) la fonction

$$s \longmapsto a_n(G_{s,u}^*)$$

appartient à l'algèbre L du n° 4.1, et a fortiori à son adhérence Λ. (Noter que, si $u = 0$, cette fonction n'est définie que pour $s \neq 0$; si $p = 2$, elle n'est même définie que pour $s \in 2\mathbf{Z}_2$, $s \neq 0$.)

On a un résultat analogue, mais beaucoup moins évident, pour le terme constant $a_o(G_{s,u}^*)$:

THÉORÈME 16 (Iwasawa).

a) Si u est un élément pair $\neq 0$ de $\mathbf{Z}/(p-1)\mathbf{Z}$, la fonction

$$s \mapsto a_o(G_{s,u}^*) = \tfrac{1}{2}\zeta^*(1-s,\ 1-u)$$

appartient à l'algèbre Λ.

b) Si $u = 0$, la fonction

$$s \longmapsto a_o(G^*_{s,u}) = \tfrac{1}{2}\zeta^*(1-s,\ 1)$$

est de la forme $T^{-1}g(T)$, où g est un élément inversible de Λ.

(Dans b), on a identifié Λ à $\mathbf{Z}_p[[T]]$, cf. n^{os} 4.1 et 4.2.)

Cet énoncé est simplement une reformulation des principaux résultats de [10], compte tenu de ce que $\zeta^*(1-s,\ 1-u) = L_p(1-s;\ \omega^u)$, cf. n° 1.6, th.3 (i). Voir aussi [11], §6.

Remarques

1) Dans le cas $u \neq 0$, le th.16, combiné avec le th.14 a) redonne les classiques congruences de Kummer (cf. Fresnel [7] et Shiratani [23]); le th.14 b) donne des congruences supplémentaires, peut-être nouvelles.

2) Dans le cas $u = 0$, le th.16 montre que la fonction

$$s \longmapsto 2\zeta^*(1-s,\ 1)^{-1}$$

appartient à Λ et est divisible par T (elle a un "zéro simple" en $T = 0$). Il en résulte que les coefficients $a_n(E^*_{s,0})$ de la série

$$E^*_{s,0} = \frac{2}{\zeta^*(1-s,\ 1)}\, G^*_{s,0}$$

appartiennent à Λ et sont divisibles par T si $n \geqslant 1$.

4.6. Familles de formes modulaires p-adiques (poids non divisible par $p-1$)

Considérons une forme modulaire p-adique f_s dépendant d'un paramètre $s \in \mathbf{Z}_p$ et de poids $k(s) \in 2X$. On suppose que $k(s)$ est de la forme $(rs,\ u)$, avec $r \in \mathbf{Z}$ et $u \in \mathbf{Z}/(p-1)\mathbf{Z}$ indépendants de s. On suppose en outre que u est $\neq 0$ (ce qui entraîne $p \neq 2,\ 3$); le cas $u = 0$ sera traité au n° suivant.

THÉORÈME 17. <u>Supposons que, pour tout</u> $n \geq 1$, <u>la fonction</u> $s \longmapsto a_n(f_s)$ <u>appartienne à l'algèbre d'Iwasawa</u> Λ. <u>Il en est alors de même de la fonction</u> $s \longmapsto a_o(f_s)$.

Nous allons utiliser la série d'Eisenstein p-adique E^*_{-rs} de poids -rs, normalisée de telle sorte que son terme constant soit 1, cf. n° 1.6. Ecrivons-la sous la forme

$$E^*_{-rs} = \sum_{n=0}^{\infty} e_n(s)q^n, \quad \text{avec} \quad e_o(s) = 1.$$

On a vu au n° précédent que les coefficients de E^*_s appartiennent à Λ; il en est donc de même des $e_n(s)$; on a de plus $e_n(0) = 0$ si $n \geq 1$ puisque $E^*_o = 1$.

La fonction $f'_s = f_s E^*_{-rs}$ est une forme modulaire p-adique de poids $(0,u)$ indépendant de s. Ses coefficients sont donnés par :

$$a_m(f'_s) = e_m(s)a_o(f_s) + \sum_{i=1}^{m} e_{m-i}(s)a_i(f_s).$$

D'après le th.9 du n° 2.3, appliqué à $k = (0,u)$, il existe une suite $(\lambda_{m,n})_{m,n \geq 1}$ d'éléments de $\mathbf{Z}_p$, avec $\lambda_{m,n} = 0$ pour m assez grand (dépendant de n), telle que

$$a_o(f'_s) = \lim_{n \to \infty} \sum_m \lambda_{m,n}\, a_m(f'_s).$$

Comme f_s et f'_s ont même terme constant, ceci peut se récrire :

$$a_o(f_s) = \lim_{n \to \infty} \left(\sum_m \lambda_{m,n} e_m(s) a_o(f_s) + \sum_{m, i \geqslant 1} \lambda_{m,n} e_{m-i}(s) a_i(f_s)\right).$$

Posons $g_n(s) = \sum_m \lambda_{m,n}\, e_m(s)$. Les fonctions g_n appartiennent à Λ, qui est compact. Quitte à remplacer la suite (n) par une sous-suite, on peut donc supposer que les $g_n(s)$ convergent dans Λ vers un élément g; comme $g_n(0) = 0$ pour tout n, on a $g(0) = 0$. La formule ci-dessus peut alors se récrire :

$$(1 - g(s)) a_o(f_s) = \lim_{n \to \infty} b_n(s),$$

$$\text{avec} \quad b_n(s) = \sum_{m, i \geqslant 1} \lambda_{m,n}\, e_{m-i}(s) a_i(f_s).$$

Vu l'hypothèse faite sur les $a_i(f_s)$, les fonctions b_n appartiennent à Λ pour tout n. Comme ces fonctions convergent simplement vers la fonction

$$s \longmapsto (1 - g(s)) a_o(f_s),$$

on en déduit que cette dernière fonction appartient à Λ, cf. n° 4.1, lemme 12. Mais le fait que $g(0) = 0$ entraîne que g appartient à l'idéal maximal de Λ, et $1 - g$ est inversible dans Λ. On en conclut bien que $s \mapsto a_o(f_s)$ appartient à Λ.

4.7. <u>Familles de formes modulaires</u> p-<u>adiques</u> (<u>poids divisible par</u> p-1)

Considérons, comme au n° précédent, une forme modulaire p-adique f_s dépendant d'un paramètre s. Nous supposons maintenant que f_s est définie pour tout $s \neq 0$ de $\mathbf{Z}_p$ (resp. pour tout $s \neq 0$ de $2\mathbf{Z}_2$ si $p = 2$), et que son poids $k(s)$ est de la forme $rs = (rs, 0)$ où r est un entier non nul.

Convenons de dire qu'une fonction sur $\mathbf{Z}_p - \{0\}$ (resp. sur $2\mathbf{Z}_2 - \{0\}$) <u>appartient à</u> Λ si elle est la restriction d'une fonction de Λ.

THÉORÈME 18. <u>Supposons que</u>, <u>pour tout</u> $n \geqslant 1$, <u>la fonction</u> $s \longmapsto a_n(f_s)$

<u>appartienne à</u> Λ. <u>Il en est alors de même de la fonction</u>

$$s \longmapsto 2\zeta^*(1 - rs,\ 1)^{-1}\ a_o(f_s).$$

Identifions Λ à $\mathbf{Z}_p[[T]]$ comme d'habitude. D'après le th.16, la fonction $s \longmapsto 2\zeta^*(1 - s,\ 1)^{-1}$ est de la forme $T.h(T)$, où h est un élément inversible de Λ. Comme $s \longmapsto rs$ correspond à $1 + T \longmapsto (1 + T)^r$, on en conclut que la fonction $s \longmapsto 2\zeta^*(1 - rs,\ 1)^{-1}$ est de la forme $((1 + T)^r - 1)g(T)$, avec g inversible dans Λ. D'où :

COROLLAIRE. <u>La fonction</u> $s \longmapsto a_o(f_s)$ <u>appartient au corps des fractions de</u> Λ; <u>on peut l'écrire</u> $c(T)/((1 + T)^r - 1)$, <u>avec</u> $c \in \Lambda$.

<u>Remarque</u>

Si q est la plus grande puissance de p qui divise r, on peut mettre $(1 + T)^r - 1$ sous la forme $u(T)((1 + T)^q - 1)$, où u est un élément inversible de Λ. On peut donc récrire la fonction $s \longmapsto a_o(f_s)$ comme une fraction $d(T)/((1 + T)^q - 1)$, avec $d \in \Lambda$.

<u>Démonstration du th.18</u>

Choisissons un polynôme H en U et les T_ℓ, à coefficients entiers, qui satisfasse aux conditions du th.8 du n° 2.3 : pour tout $k \in \mathbf{Z}_p$, on a

(i) $E_k^*|_k\, H = c(k)\, E_k^*$ avec $c(k)$ inversible dans $\mathbf{Z}_p$,

(ii) $\lim\limits_{n \to \infty} f|_k\, H^n = 0$ pour toute forme modulaire p-adique f de poids k qui est parabolique.

D'après le cor. au th.8, on a

$$2\zeta^*(1 - rs,\ 1)^{-1}\ a_o(f_s) = \lim_{n \to \infty} c(rs)^{-n}\ a_1(f_s|_{rs}\, H^n),$$

et tout revient à montrer que les fonctions

$$s \longmapsto c(rs)^{-n} \quad \text{et} \quad s \longmapsto a_1(f_s|_{rs} H^n)$$

appartiennent à Λ (en effet, on sait qu'une suite de fonctions de Λ qui converge en tout point d'une partie infinie de $\mathbf{Z}_p$ converge uniformément vers une fonction de Λ, cf. n° 4.1, lemme 12). Or on a le résultat suivant :

LEMME 13. Soit R un polynôme en U et les T_ℓ, à coefficients dans $\mathbf{Z}_p$. Il existe une famille de fonctions $k \longmapsto c_{ij}(R,k)_{i,j \geqslant 0}$, appartenant à sous-algèbre L de Λ (cf. n° 4.1) et telles que, pour tout $i \geqslant 0$, on ait :

a) $c_{ij}(R,k) = 0$ pour j assez grand, pour $j = 0$ si $i \geqslant 1$, et pour $j \geqslant 1$ si $i = 0$;

b) $a_i(f|_k R) = \sum_j c_{ij}(R,k)\, a_j(f)$ pour toute série formelle p-adique f, et tout $k \in 2\mathbf{Z}_p$.

Lorsque R est égal à U, ou à l'un des T_ℓ, le lemme résulte des formules donnant $f|U$ et $f|_k T_\ell$, cf. n° 2.1. Le cas général s'en déduit en remarquant que, si l'énoncé est vrai pour deux polynômes R_1 et R_2, il l'est aussi pour R_1R_2 et $R_1 + R_2$.

Revenons à la démonstration du th.18. On a

$$a_1(f_s|_{rs} H^n) = \sum_{j \geqslant 1} c_{1j}(H^n, rs)\, a_j(f_s),$$

et cette formule montre bien que $s \longmapsto a_1(f_s|_{rs} H^n)$ appartient à Λ.

On a d'autre part $c(k) = a_o(E_k^*|_k H) = c_{oo}(H,k)$, ce qui montre que $k \longmapsto c(k)$ appartient à L, et il en est de même de $s \longmapsto c(rs)$. De plus, d'après (i), les valeurs prises par $c(rs)$ sont des unités p-adiques. Si l'on écrit $s \longmapsto c(rs)$ comme une série en T, le terme constant de cette série est inversible dans $\mathbf{Z}_p$; la série elle-même est donc inversible dans $\Lambda = \mathbf{Z}_p[[T]]$, et l'on en conclut que $s \longmapsto c(rs)^{-n}$ appartient à Λ quel que soit n, ce qui achève le démonstration du théorème.

Remarque

Dans les ths.17 et 18, il n'est pas nécessaire de supposer f_s définie pour tout $s \in \mathbf{Z}_p$ (ou tout $s \neq 0$); il suffit de se donner les f_s pour s appartenant à une partie infinie S de $\mathbf{Z}_p$, et de faire l'hypothèse suivante : pour tout $n \geq 1$, la fonction $s \mapsto a_n(f_s)$ est la restriction à S d'une fonction appartenant à Λ.

§5. Fonctions zêta p-adiques

5.1. Notations

La lettre K désigne un corps de nombres algébriques totalement réel de degré r sur $\mathbf{Q}$: $K \otimes_{\mathbf{Q}} \mathbf{R}$ est isomorphe à $\mathbf{R}^r$. L'anneau des entiers de K est noté O_K, sa différente (par rapport à $\mathbf{Z}$) est notée $\mathfrak{d}$ et son discriminant d.

Si x (resp. $\mathfrak{a}$) est un élément (resp. un idéal) de K, on note Nx (resp. $N\mathfrak{a}$) sa norme, qui est un élément (resp. un élément positif) de $\mathbf{Q}$; par exemple $d = N\mathfrak{d}$. On note Tr(x) la trace de x.

Un élément x de K est dit totalement positif si $\sigma(x) > 0$ pour tout plongement $\sigma : K \to \mathbf{R}$. On écrit alors $x \gg 0$; on a $Tr(x) > 0$.

La fonction zêta de K est définie par la formule

$$\zeta_K(s) = \sum N\mathfrak{a}^{-s} = \prod (1 - N\mathfrak{p}^{-s})^{-1}$$

où $\mathfrak{a}$ (resp. $\mathfrak{p}$) parcourt l'ensemble des idéaux $\neq 0$ (resp. des idéaux premiers $\neq 0$) de O_K. Cette formule vaut pour $R(s) > 1$. On prolonge ζ_K en une fonction méromorphe sur $\mathbf{C}$, ayant pour seul pôle (simple) le point $s = 1$. La fonction

$$d^{s/2}\ \pi^{-rs/2}\ \Gamma(\tfrac{s}{2})^r\ \zeta_K(s)$$

est invariante par $s \mapsto 1 - s$ ("équation fonctionnelle"). On en déduit que, si n est un entier ≥ 1, on a

$\zeta_K(1 - n) = 0$ si n est impair (le cas $r = 1$, $n = 1$ excepté)

$\zeta_K(1 - n) \neq 0$ si n est pair.

De plus, d'après un théorème énoncé par Hecke ([8], p.387) et démontré par Siegel [24], les $\zeta_K(1 - n)$, $n \geq 1$, sont des nombres rationnels.

5.2. Formes modulaires attachées à K

Soit k un entier pair ≥ 2. Définissons une série formelle g_k

$$g_k = \sum_{n=0}^{\infty} a_n(g_k)\, q^n$$

par les formules :

$$a_o(g_k) = 2^{-r}\zeta_K(1 - k),$$

$$a_n(g_k) = \sum_{\substack{Tr(x)=n \\ x \in d^{-1} \\ x \gg 0}} \ \sum_{a | xd} (Na)^{k-1} \qquad (n \geq 1),$$

où x parcourt les éléments totalement positifs de d^{-1} de trace n, et a les idéaux de O_K contenant xd. (Il revient au même de dire que l'on somme sur les couples (x,a) tels que a soit entier, $x \in d^{-1}a$, $x \gg 0$ et $Tr(x) = n$; c'est une somme finie.)

THÉORÈME 19 (Hecke-Siegel). Mis à part le cas $r = 1$, $k = 2$, la série g_k est une forme modulaire sur $SL_2(\mathbf{Z})$ de poids rk.

(Pour $r = 1$, i.e. $K \simeq \mathbf{Q}$, on a $g_k = G_k$, d'où la nécessité d'exclure $k = 2$, cf. n° 1.1.)

Si u est un idéal fractionnaire de K, on trouve dans Siegel [25], p.93, la définition d'une certaine fonction

$$F_k(u, z_1, \ldots, z_r), \qquad \mathrm{Im}(z_i) > 0,$$

qui est une <u>série d'Eisenstein</u> du corps K, au sens de Hecke [8], p.381-404; c'est une forme modulaire de poids k par rapport au groupe $SL_2(O_K)$ opérant sur le produit H^r de r demi-plans de Poincaré. Si l'on restreint $F_k(u, z_1, \ldots, z_r)$ à la diagonale H de H^r, on obtient une fonction

$$\Phi_k(u,z) = F_k(u, z, \ldots, z),$$

qui est une forme modulaire de poids rk, au sens usuel. Les coefficients de $\Phi_k(u,z)$ sont donnés dans [25], p.94, formule (19). Les fonctions $F_k(u, z_1, \ldots, z_r)$ et $\Phi_k(u,z)$ ne changent pas lorsqu'on multiplie u par un idéal principal. Posons alors

$$\Phi_k(z) = \sum_u \Phi_k(u,z),$$

où u parcourt un ensemble de représentants des classes d'idéaux de K. Les formules (18) et (19) de [25] donnent :

$$a_n(\Phi_k) = e_k a_n(g_k) \quad \text{pour} \quad n \geq 1, \quad \text{où} \quad e_k = d^{\frac{1}{2}-k} \left(\frac{(2\pi i)^k}{(k-1)!}\right)^r,$$

ainsi que

$$a_o(\Phi_k) = \zeta_K(k),$$

et l'équation fonctionnelle de ζ_K permet de récrire cette dernière formule sous la forme :

$$a_o(\Phi_k) = e_k\, 2^{-r}\zeta_K(1-k) = e_k a_o(g_k).$$

On a donc $g_k = e_k^{-1}\Phi_k$, ce qui montre bien que g_k est modulaire de poids rk.

COROLLAIRE.

(i) Si $rk \not\equiv 0 \pmod{(p-1)}$, $\zeta_K(1-k)$ est p-entier.

(ii) Si $rk \equiv 0 \pmod{(p-1)}$, on a

$$v_p(\zeta_K(1-k)) \geqslant -1 - v_p(rk) \qquad (p \neq 2)$$

$$v_p(\zeta_K(1-k)) \geqslant r - 2 - v_p(rk) \quad (p = 2).$$

Cela résulte du cor.1 au th.1' du n° 1.5, compte tenu de ce que les coefficients $a_n(g_k)$ sont entiers pour $n \geqslant 1$. (Voir aussi [20], th.6 et th.6'.)

Remarques

1) Le corollaire ci-dessus fournit une estimation du dénominateur de $\zeta_K(1-k)$. Cette estimation est assez grossière : elle ne fait intervenir K que par l'intermédiaire de son degré r; pour k = 2, elle est moins bonne que celle donnée par la formule

$$\zeta_K(-1) = \text{caract.d'E-P. de } SL_2(O_K),$$

cf. [19], n° 3.7, prop.29-30.

2) Nous aurons besoin plus loin d'une variante du th.19, dans laquelle on modifie g_k en gardant uniquement les termes "premiers à p". De façon plus précise, soit S l'ensemble des idéaux premiers de O_K qui divisent p, et posons

$$\zeta_{K,S}(s) = \zeta_K(s) \prod_{\mathfrak{p} \in S} (1 - N\mathfrak{p}^{-s}) = \prod_{\mathfrak{p} \notin S} (1 - N\mathfrak{p}^{-s})^{-1}$$

$$= \sum_{(\mathfrak{a},p)=1} N\mathfrak{a}^{-s}.$$

Définissons une série formelle g'_k par les formules

$$a_o(g'_k) = 2^{-r}\zeta_{K,S}(1-k) = 2^{-r}\zeta_K(1-k) \prod_{p \in S} (1 - Np^{k-1})$$

et $$a_n(g'_k) = \sum_{x,a} (Na)^{k-1} \qquad (n \geq 1),$$

où la sommation porte sur les couples (x,a), avec a entier premier à p, $x \in d^{-1}a$, $x \gg 0$ et $Tr(x) = n$.

On a alors :

THÉORÈME 19'. La série g'_k est une forme modulaire sur $\Gamma_o(p)$ de poids rk (cf. n° 3.1).

(Noter qu'ici le cas $r = 1$, $k = 2$ n'est plus exclu.)

La démonstration est analogue à celle du th.19, à cela près que l'on doit utiliser des séries d'Eisenstein de niveau p, cf. Kloosterman [14] et Siegel [26]. Pour plus de détails, voir l'exemple 2) de l'Appendice placé à fin de ce §.

5.3. La fonction zêta p-adique du corps K

Soit k un élément pair de X tel que $rk \neq 0$. Nous allons associer à k une forme modulaire p-adique g^*_k, de poids rk, par passage à la limite à partir des formes g_k du n° 5.2. Le procédé est le même que celui utilisé au n° 1.6 dans le cas de $\mathbf{Q}$. On choisit une suite d'entiers pairs $k_i \geq 4$ tels que $|k_i| \to \infty$ et $k_i \to k$ dans X. Si u est un entier p-adique, on a

$$\lim_{i \to \infty} u^{k_i} = 0 \quad \text{si} \quad u \equiv 0 \pmod{p}, \text{ et } \quad \lim_{i \to \infty} u^{k_i} = u^k \quad \text{sinon},$$

la convergence étant uniforme en u. On en conclut que

$$\lim_{i \to \infty} a_n(g_{k_i}) = \sum_{x,a} (Na)^{k-1}, \qquad (n \geq 1),$$

où la sommation porte sur les couples $(x,\mathfrak{a})$, avec $\mathfrak{a}$ idéal de O_K premier à p, $x \in \mathfrak{d}^{-1}\mathfrak{a}$, $x \gg 0$ et $Tr(x) = n$; de plus, la convergence est uniforme en n. Appliquant alors le cor.2 au th.1' du n° 1.5, on en déduit que les g_{k_i} <u>ont une limite</u> g_k^* <u>qui est une forme modulaire</u> p-<u>adique de poids</u> rk, <u>indépendante de la suite</u> k_i <u>choisie</u>. Le terme constant de g_k^* sera noté $2^{-r}\zeta_K^*(1-k)$, de sorte que l'on a

$$a_o(g_k^*) = 2^{-r}\zeta_K^*(1-k) = 2^{-r} \lim_{i \to \infty} \zeta_K(1-k_i),$$

$$a_n(g_k^*) = \sum_{\substack{Tr(x)=n \\ x \in \mathfrak{d}^{-1} \\ x \gg 0}} \sum_{\substack{\mathfrak{a} | x\mathfrak{d} \\ (\mathfrak{a},p)=1}} (N\mathfrak{a})^{k-1}, \qquad n \geq 1.$$

La fonction ζ_K^* ainsi définie sera appelée la <u>fonction zêta</u> p-<u>adique</u> du corps K; elle prend ses valeurs dans $\mathbf{Q}_p$.

THÉORÈME 20. <u>Si</u> k <u>est un entier pair</u> ≥ 2, <u>on a</u>

$$\zeta_K^*(1-k) = \zeta_{K,S}(1-k) = \zeta_K(1-k) \prod_{\mathfrak{p} \in S} (1 - N\mathfrak{p}^{k-1}).$$

(Rappelons que S est l'ensemble des idéaux premiers $\mathfrak{p}$ qui divisent p.)

En effet, revenons à la série g_k' du n° précédent. D'après le th.19', cette série est une forme modulaire sur $\Gamma_o(p)$ de poids rk, donc aussi une forme modulaire p-adique de poids rk, cf. n° 3.2, th.10. Comme $a_n(g_k') = a_n(g_k^*)$ pour $n \geq 1$, on en déduit que $a_o(g_k') = a_o(g_k^*)$, d'où le théorème.

<u>Remarque</u>

Il est immédiat que ζ_K^* est <u>continue</u> sur l'ensemble des $1-k$, avec k pair et $rk \neq 0$. Le th.20 en fournit donc une caractérisation : c'est le prolongement par continuité de la fonction

$$m \longmapsto \zeta_{K,S}(m),$$

définie sur l'ensemble des entiers impairs < 0. (En particulier, lorsque K est abélien sur $\mathbf{Q}$, ζ_K^* coïncide avec la fonction zêta p-adique de K au sens de Kubota-Leopoldt, cf. [11], p.62, puisque cette dernière a la même propriété.)

En fait, ζ_K^* est même analytique. De façon plus précise, décomposons $k \in X$ en (s,u), avec $s \in \mathbf{Z}_p$, $u \in \mathbf{Z}/(p-1)\mathbf{Z}$, de sorte que la condition $rk \neq 0$ signifie simplement que $s \neq 0$ ou $ru \neq 0$. Ecrivons $\zeta_K^*(1-k)$ sous la forme $\zeta_K^*(1-s, 1-u)$. On a alors :

THÉORÈME 21. Soit u un élément pair de $\mathbf{Z}/(p-1)\mathbf{Z}$, $p \neq 2$.

(a) Si $ru \neq 0$, la fonction $s \longmapsto \zeta_K^*(1-s, 1-u)$ appartient à l'algèbre d'Iwasawa $\Lambda = \mathbf{Z}_p[[T]]$ du §4.

(b) Si $ru = 0$, la fonction $s \longmapsto \zeta_K^*(1-s, 1-u)$ est de la forme $h(T)/((1+T)^r - 1)$, avec $h \in \Lambda$.

THÉORÈME 21'. Si $p = 2$, la fonction $s \longmapsto \zeta_K^*(1-s)$ est de la forme $2^r h(T)/((1+T)^r - 1)$, avec $h \in \Lambda$.

(Noter que, pour $p = 2$, $\zeta_K^*(1-s)$ est défini pour $s \in 2\mathbf{Z}_2$, $s \neq 0$.)

Posons $k = (s,u)$. Si $n \geq 1$, la fonction $s \longmapsto a_n(g_k^*)$ est somme de fonctions de la forme $s \longmapsto (N\mathfrak{a})^{k-1}$, où $N\mathfrak{a}$ est une unité p-adique. En décomposant $N\mathfrak{a}$ à la façon habituelle (cf. n° 4.5) en $\omega(N\mathfrak{a})\langle N\mathfrak{a}\rangle$, on a

$$(N\mathfrak{a})^{k-1} = N\mathfrak{a}^{-1}\,\omega(N\mathfrak{a})^u\,\langle N\mathfrak{a}\rangle^s,$$

ce qui montre que $s \longmapsto a_n(g_k^*)$ appartient à l'algèbre L du n° 4.1. Les théorèmes 21 et 21' résultent alors des ths.17 et 18 du §4, appliqués à la famille (g_k^*).

COROLLAIRE 1. Si $ru \neq 0$ et $p \neq 2$, la fonction $s \longmapsto \zeta_K^*(1-s, 1-u)$ est holomorphe (au sens strict) dans un disque strictement plus grand que le disque unité.

En effet, le th.21 (a), combiné au th.13 du n° 4.3, montre que la fonction en question est donnée par une série de Taylor

$$\sum_{n=0}^{\infty} c_n s^n, \quad \text{avec} \quad v_p(c_n) \geq n\frac{p-2}{p-1}.$$

Une telle série converge dans un disque strictement plus grand que le disque unité.

COROLLAIRE 2. Si $ru = 0$, la fonction $s \mapsto \zeta_K^*(1 - s, 1 - u)$ est méromorphe (au sens strict) dans un disque strictement plus grand que le disque unité; si elle n'est pas holomorphe, elle a pour unique pôle le point $s = 0$, et c'est un pôle simple.

Cela se démontre de la même manière, en tenant compte du dénominateur $(1 + T)^r - 1 = u^{rs} - 1$, où u est un générateur topologique de U_1 (resp. de U_2 si $p = 2$); on vérifie en effet que $u^{rs} - 1$ peut s'écrire sous la forme $s/\phi(s)$, où ϕ est une série de Taylor convergeant dans un disque strictement plus grand que le disque unité.

COROLLAIRE 3. Soient a et b des entiers positifs. On suppose que a est pair ≥ 2, $ra \not\equiv 0 \pmod{(p-1)}$, et $b \equiv 0 \pmod{(p-1)}$. Les différences successives δ_n de la suite $a_n = \zeta_{K,S}(1 - a - nb)$ satisfont alors aux congruences

$$\delta_n \equiv 0 \pmod{p^n} \quad \underline{\text{et}} \quad \sum_{i=1}^{n} c_{in}\delta_i p^{-i} \equiv 0 \pmod{n!\mathbf{Z}_p}, \quad \text{cf. n° 4.4.}$$

(Le fait que $\delta_n \equiv 0 \pmod{p^n}$ est une généralisation des congruences de Kummer.)

Vu le th.20, on a $a_n = \zeta_K^*(1 - a - nb, 1 - a)$. Le corollaire résulte de là, et des ths.21 et 14.

5.4. Complément : calcul de $\zeta_K^*(1 - k, 1 - u)$ pour k entier ≥ 1

On suppose u pair et $p \neq 2$. Le cas où $k \equiv u \pmod{(p-1)}$ est réglé par le th.20 : on a $\zeta_K^*(1 - k, 1 - u) = \zeta_{K,S}(1 - k)$. On va voir qu'il y a un résultat analogue dans le cas général, la fonction zêta étant remplacée par une fonction L.

De façon plus précise, soit ε un homomorphisme de $(\mathbf{Z}/p\mathbf{Z})^*$ dans $\mathbf{C}^*$ tel que $\varepsilon(-1) = (-1)^k$. Si a est un idéal premier à p, posons $\varepsilon_K(a) = \varepsilon(Na)$; la fonction ε_K définit un <u>caractère</u> du corps de nombres K; l'ensemble des idéaux premiers où ce caractère est ramifié est un sous-ensemble S_ε de S. Nous aurons besoin de la fonction $L(s,\varepsilon_K)$ de ε_K, ainsi que de la fonction $L_S(s, \varepsilon_K)$ déduite de $L(s, \varepsilon_K)$ par suppression des facteurs non premiers à p; on a :

$$L_S(s, \varepsilon_K) = \prod_{p \notin S} (1 - \varepsilon_K(p)Np^{-s})^{-1}$$

$$= L(s, \varepsilon_K) \prod_{p \in S-S_\varepsilon} (1 - \varepsilon_K(p)Np^{-s}).$$

Choisissons maintenant un plongement σ du corps $\mathbf{Q}(\mu_{p-1})$ dans $\mathbf{Q}_p$, cf. n° 3.4, de sorte que ε devient $x \longmapsto x^\alpha$, avec $\alpha \in \mathbf{Z}/(p-1)\mathbf{Z}$.

THÉORÈME 22. <u>On a</u> $L_S(1 - k, \varepsilon_K)^\sigma = \zeta_K^*(1 - k, 1 - u)$, <u>où</u> $u = k + \alpha$.

(Pour u, k et σ donnés, il existe un ε et un seul tel que $u = k + \alpha$; le th.22 fournit donc bien un procédé de calcul de $\zeta_K^*(1 - k, 1 - u)$.)

Considérons la série $f_{k,\varepsilon}$ donnée par :

$$a_o(f_{k,\varepsilon}) = 2^{-r} L_S(1 - k, \varepsilon_K),$$

$$a_n(f_{k,\varepsilon}) = \sum_{x,a} \varepsilon_K(a)\, Na^{k-1}, \qquad n \geq 1,$$

où la sommation porte comme ci-dessus sur les (x, a), avec a premier à p, $x \in d^{-1}a$, $x \gg 0$ et $\mathrm{Tr}(x) = n$. La série $f_{k,\varepsilon}$ est une forme modulaire sur $\Gamma_o(p)$ de type (rk, ε^r) au sens du n° 3.4, cf. <u>Appendice</u>, Exemple 3). D'après le th.12 du n° 3.4, il en résulte que la série p-adique $f^\sigma_{k,\varepsilon}$ est une forme modulaire p-adique de poids $rk + r\alpha$. Or, si $n \geq 1$, on a

$$a_n(f_{k,\varepsilon}^{\sigma}) = \sum_{x,a} \varepsilon_K(a)^{\sigma} (Na)^{k-1} = \sum_{x,a} \omega(Na)^{\alpha} (Na)^{k-1}$$

$$= \sum_{x,a} (Na)^{k+\alpha-1} = a_n(g_{k+\alpha}^{*}), \qquad \text{cf. n° 5.3.}$$

Comme $g_{k+\alpha}$ et $f_{k,\varepsilon}^{\sigma}$ ont même poids, et que ce poids est non nul, les formules ci-dessus entraînent $g_{k+\alpha}^{*} = f_{k,\varepsilon}^{\sigma}$. On a donc

$$2^{-r} L_S(1-k, \varepsilon_K)^{\sigma} = a_o(f_{k,\varepsilon}^{\sigma}) = a_o(g_{k+\alpha}^{*}) = 2^{-r}\zeta_K^{*}(1-k-\alpha),$$

d'où le théorème.

Remarque

Il résulte de l'équation fonctionnelle des séries L que l'on a $L(1-k, \varepsilon_K) \neq 0$. Vu la formule liant L et L_S on en conclut que $\zeta_K^{*}(1-k, 1-u)$ est nul si et seulement si $k = 1$ et s'il existe $p \in S - S_{\varepsilon}$ tel que $\varepsilon_K(p) = 1$. (L'existence d'un tel zéro pour ζ_K^{*} m'a été suggérée par J.Coates - voir aussi [4], th.1.1.)

5.5. Complément : une propriété de périodicité de ζ_K^{*}

On suppose $p \neq 2$. Soit $K(\mu_p)$ le corps obtenu en adjoignant à K les racines p-ièmes de l'unité, et posons $b = [K(\mu_p) : K]$. Du fait que K est réel, b est pair, et divise p-1.

THÉORÈME 23. On a $\zeta_K^{*}(1-s, 1-u) = \zeta_K^{*}(1-s, 1-u')$ si $u' \equiv u$ (mod.b).

Notons Y_b le sous-groupe de $\mathbf{Z}/(p-1)\mathbf{Z}$ engendré par b, et identifions Y_b à un sous-groupe de X. Il s'agit de prouver que $\zeta_K^{*}(1-k) = \zeta_K^{*}(1-k')$ si $k' \equiv k$ (mod.Y_b).

Si a est un idéal de K premier à p, on vérifie (soit directement, soit par la théorie du corps de classes) que $Na^b \equiv 1$ (mod.p), i.e. que $\omega(Na)$ appartient au noyau de $z \longmapsto z^b$ dans $(\mathbf{Z}/p\mathbf{Z})^{*}$. Il en résulte que, si $k' \equiv k$ (mod.Y_b), on a $(Na)^{k'} = (Na)^k$, d'où $a_n(g_{k'}^{*}) = a_n(g_k^{*})$ pour $n \geq 1$. On a d'autre part $p - 1 = ab$, où a est le degré du corps $K \cap \mathbf{Q}(\mu_p)$; il en résulte que a divise $r = [K:\mathbf{Q}]$, et, si $t \in Y_b$, on a $rt = 0$. Les séries g_k^* et $g_{k'}^*$ ont donc même poids rk. Vu les formules ci-dessus, on a donc $g_k^* = g_{k'}^*$, d'où le théorème.

Remarque

Notons $\mathbf{Q}(\mu)$ le corps engendré sur $\mathbf{Q}$ par toutes les racines p^n-ièmes de l'unité ($n = 1,2, \ldots$). Le degré de $K \cap \mathbf{Q}(\mu)$ est de la forme $a\,p^m$, avec $m \geq 0$. On peut montrer (par un argument analogue à celui du th.23) que, pour tout u, la fonction

$$s \longmapsto \zeta_K^*(1 - s,\ 1 - u)$$

appartient au corps des fractions de $\mathbf{Z}_p[[T_m]]$, où $T_m = (1 + T)^{p^m} - 1$. Si $ru \neq 0$, cette fonction appartient même à $\mathbf{Z}_p[[T_m]]$.

5.6. Questions

1) Comportement de $\zeta_K^*(1 - s,\ 1 - u)$ pour $s = 0$

Supposons d'abord $ru \neq 0$, de sorte que $\zeta_K^*(1 - s,\ 1 - u)$ est défini en $s = 0$. Peut-on calculer ce nombre (en termes de logarithmes p-adiques d'unités de $K(\mu_p)$, par exemple) ? C'est le cas lorsque K est abélien sur $\mathbf{Q}$, en vertu d'un résultat de Leopoldt ([11], §5).

Lorsque $ru = 0$, on aimerait savoir si $s = 0$ est effectivement un pôle. Il paraît probable que ce n'est le cas que si $au = 0$, où a est le degré de $K \cap \mathbf{Q}(\mu_p)$, cf. n° 5.5; cela résulterait en tout cas des conjectures faites dans [19], n° 3.7 et dans [4].

Lorsque $au = 0$ (ou $u = 0$, cela revient au même d'après le th.23), on peut espérer que le résidu de $\zeta_K^*(1 - s,\ 1 - u)$ en $s = 0$ est lié au régulateur p-adique de K par la même formule que dans le cas abélien ([11], loc.cit.); en outre, on devrait pouvoir remplacer le dénominateur $(1 + T)^r - 1$ du th.21 par $(1 + T)^{p^m} - 1$, où p^m est la plus grande puissance de p divisant le degré de $K \cap \mathbf{Q}(\mu)$, cf. n° 5.5.

2) Généralisations

Le cas traité ici est seulement celui des fonctions zêta. Il y a certainement des résultats analogues pour les fonctions L (abéliennes d'abord, puis non abéliennes). Il devrait être possible de les démontrer en utilisant des formes modulaires p-adiques sur d'autres groupes que $SL_2(\mathbf{Z})$, cf. Katz [12]. Pour obtenir des résultats vraiment satisfaisants (et en particulier pour se débarrasser des pôles parasites, cf. ci-dessus), il sera sans doute nécessaire de travailler sur le groupe modulaire du corps K (et non plus de $\mathbf{Q}$), i.e. d'utiliser les fonctions $F_k(u, z_1, \ldots, z_r)$ et non pas seulement les fonctions d'une variable obtenues en faisant $z_1 = \ldots = z_r$. Le groupe $\mathbf{Z}_p^*$ (ou son sous-groupe U_1) serait remplacé par le groupe de Galois G d'une certaine extension abélienne de K (non nécessairement cyclotomique); l'espace X serait remplacé par l'espace des caractères p-adiques de G, et l'algèbre Λ par $\mathbf{Z}_p[[G]]$.

3) Relations avec la théorie d'Iwasawa

Du point de vue développé dans [10], [11], les éléments de Λ apparaissent, non pas comme des fonctions, mais comme des relations entre éléments de certains modules galoisiens. Pour un corps K abélien sur $\mathbf{Q}$, on a des relations canoniques, les "relations de Stickelberger" qui conduisent aux fonctions zêta et L p-adiques (Iwasawa [10]). Dans le cas général, on ne dispose que de relations définies à multiplication par un élément inversible près (ce qui permet de parler de leurs zéros, cf. Coates-Lichtenbaum [4]). Il est probable que ces relations (ou fonctions) sont essentiellement les mêmes que celles considérées ici; il serait intéressant de le démontrer.

4) Corps non totalement réels

Si K n'est pas totalement réel, on a $\zeta_K(1 - n) = 0$ pour tout entier $n \geqslant 2$; ce fait pourrait laisser croire que K ne possède pas de fonction zêta p-adique "intéressante". Cependant, pour $K = \mathbf{Q}(i)$, Hurwitz [9] a défini des nombres rationnels qui jouissent de propriétés analogues à celles des nombres de Bernoulli; les résultats de Hurwitz, ainsi que d'autres plus récents ([5], [17]), laissent penser que les nombres en question conduisent, eux aussi, à des fonctions analytiques p-adiques. Peut-être existe-t-il, plus généralement, une théorie p-adique des fonctions L à Grössencharaktere de type (A_o), au sens de Weil [28] ?

Appendice

Séries d'Eisenstein de niveau $\mathfrak{f}$

Notations

On se donne un idéal $\mathfrak{f} \neq 0$ de O_K, le conducteur. On note $S_{\mathfrak{f}}$ l'ensemble des diviseurs premiers de $\mathfrak{f}$, et l'on écrit

$$\mathfrak{f} = \prod_{p \in S_{\mathfrak{f}}} p^{f(p)}, \quad \text{avec} \quad f(p) \geqslant 1.$$

Si $\alpha \in K^*$, on dit que α est congru à 1 (mod. $\mathfrak{f}$), et on écrit $\alpha \equiv 1$ $(\text{mod}^\times\, \mathfrak{f})$, si $v_p(\alpha - 1) \geqslant f(p)$ pour tout $p \in S_{\mathfrak{f}}$, où v_p désigne la valuation discrète attachée à p.

Soient a et b deux idéaux fractionnaires de K, premiers à $\mathfrak{f}$. On dit que a et b appartiennent à la même classe (mod. $\mathfrak{f}$) s'il existe $\alpha \in K^*$, $\alpha \gg 0$, $\alpha \equiv 1$ $(\text{mod}^\times\, \mathfrak{f})$, tel que a soit le produit de b par l'idéal principal (α). Le groupe des classes d'idéaux (mod. $\mathfrak{f}$) sera noté $C_{\mathfrak{f}}$; c'est un groupe fini.

Fonction zêta d'une classe

Soit $c \in C_{\mathfrak{f}}$. On lui associe la fonction zêta "partielle"

$$\zeta_{K,c}(s) = \sum_{a \in c} Na^{-s},$$

où la sommation porte sur tous les idéaux de O_K appartenant à la classe c. Cette fonction se prolonge en une fonction méromorphe dans tout **C**, et ses valeurs aux entiers négatifs sont des nombres <u>rationnels</u> (Siegel [26], p.19).

Plus généralement, soit λ une fonction sur $C_{\mathfrak{f}}$ à valeurs complexes; on identifie λ de façon évidente à une fonction sur les idéaux fractionnaires premiers à $\mathfrak{f}$. On pose

$$\zeta_{K,\lambda}(s) = \sum_{c \in C_{\mathfrak{f}}} \lambda(c)\, \zeta_{K,c} = \sum_{(\mathfrak{a},\mathfrak{f})=1} \lambda(\mathfrak{a}) N\mathfrak{a}^{-s}.$$

Ici encore, cette fonction se prolonge à tout **C**; ses valeurs aux entiers négatifs sont des combinaisons **Q**-linéaires des $\lambda(c)$. (Il y a parfois intérêt à considérer des fonctions λ à valeurs, non plus dans **C**, mais dans une **Q**-algèbre E - par exemple un corps p-adique - et à <u>définir</u> $\zeta_{K,\lambda}(1-k) \in E$ comme la somme des $\lambda(c)\, \zeta_{K,c}(1-k)$.)

Nous dirons que λ est <u>paire</u> si

$\lambda((\alpha)\mathfrak{a}) = \lambda(\mathfrak{a})$ pour tout $\mathfrak{a}$ et tout $\alpha \equiv 1 \pmod{^{\times}\mathfrak{f}}$,

et que λ est <u>impaire</u> si

$\lambda((\alpha)\mathfrak{a}) = \mathrm{sgn}(N\alpha)\lambda(\mathfrak{a})$ pour tout $\mathfrak{a}$ et tout $\alpha \equiv 1 \pmod{^{\times}\mathfrak{f}}$.

<u>Forme modulaire définie par une fonction</u> λ

On se donne un entier $k \geq 1$, et une fonction λ sur $C_{\mathfrak{f}}$ comme ci-dessus. On suppose que λ <u>et</u> k <u>ont même parité</u>; on exclut les cas ($k = 1$, $\mathfrak{f} = O_K$) et ($k = 2$, $r = 1$, $\mathfrak{f} = O_K$), cf. [19], p.48.

On associe à k,λ la série formelle $G_{k,\lambda} = \sum_{n=0}^{\infty} a_n(G_{k,\lambda})q^n$ définie par :

$$a_0(G_{k,\lambda}) = 2^{-r}\, \zeta_{K,\lambda}(1-k)$$

$$a_n(G_{k,\lambda}) = \sum_{x,\mathfrak{a}} \lambda(\mathfrak{a})\, N\mathfrak{a}^{k-1}, \qquad n \geq 1,$$

où la sommation porte sur les couples $(x,\mathfrak{a})$ tels que $\mathfrak{a}$ soit un idéal de O_K premier à $\mathfrak{f}$, $x \in \mathfrak{d}^{-1}\mathfrak{a}$, $x \gg 0$ et $\mathrm{Tr}(x) = n$.

Soit d'autre part f le générateur > 0 de l'idéal $\mathfrak{f} \cap \mathbf{Z}$ de $\mathbf{Z}$. Notons $\Gamma_o(f)$ le sous-groupe de $SL_2(\mathbf{Z})$ formé des matrices $\binom{\alpha\ \beta}{\gamma\ \delta}$ telles que $\gamma \equiv 0$ (mod.f), et $\Gamma_1(f)$ le sous-groupe de $\Gamma_o(f)$ formé des matrices $\binom{\alpha\ \beta}{\gamma\ \delta}$ telles que $\alpha \equiv \delta \equiv 1$ (mod.f).

THÉORÈME 24 (Kloosterman-Siegel).

(i) <u>La série</u> $G_{k,\lambda}$ <u>définie ci-dessus est une forme modulaire de poids</u> rk <u>sur</u> $\Gamma_1(f)$.

(ii) <u>Si</u> $\binom{\alpha\ \beta}{\gamma\ \delta}$ <u>appartient à</u> $\Gamma_o(f)$, <u>on a</u>

$$G_{k,\lambda}|_{rk} \begin{pmatrix}\alpha & \beta\\ \gamma & \delta\end{pmatrix} = G_{k,\lambda_\delta},$$

<u>où</u> λ_δ <u>est définie par la formule</u> $\lambda_\delta(a) = \mathrm{sgn}(\delta)^{rk}\,\lambda((\delta)a)$.

<u>Remarque</u>

La définition de λ_δ peut aussi se présenter de la manière suivante : on a un homomorphisme naturel $\rho : (\mathbf{Z}/f\mathbf{Z})^* \to C_{\mathfrak{f}}$ obtenu en associant à un élément $\xi \in (\mathbf{Z}/f\mathbf{Z})^*$ l'idéal principal (x) engendré par un élément positif x de ξ. Comme δ est inversible mod.f, on peut donc parler de $\rho(\delta) \in C_{\mathfrak{f}}$, et la définition de λ_δ donnée ci-dessus équivaut simplement à

$$\lambda_\delta(c) = \lambda(\rho(\delta)c) \quad \text{pour tout} \quad c \in C_{\mathfrak{f}}.$$

<u>Exemples</u>

1) Prenons $\mathfrak{f} = (1)$, $\lambda = 1$, et k pair $\geqslant 2$ (resp. $\geqslant 4$ si r = 2). La série $G_{k,\lambda}$ n'est autre que la série g_k du n° 5.2; comme f = 1, on en déduit que g_k est une forme modulaire sur le groupe $SL_2(\mathbf{Z})$: on retrouve le th.19.

2) Prenons $\mathfrak{f} = (p)$, $\lambda = 1$ et k pair $\geqslant 2$. On a f = p. La série $G_{k,\lambda}$ est égale à la série g'_k du n° 5.2. Comme $\lambda_\delta = \lambda$ pour tout δ premier à p, on en déduit que g'_k est une forme modulaire sur $\Gamma_o(p)$.

3) Les notations étant celles du n° 5.4, prenons $\mathfrak{f} = (p)$, et choisissons pour λ la fonction $a \to \varepsilon_K(a) = \varepsilon(Na)$; prenons $k \geqslant 1$ tel que

$\varepsilon(-1) = (-1)^k$, ce qui assure que k et λ ont même parité. La série $G_{k,\lambda}$ coïncide avec la série $f_{k,\varepsilon}$ introduite dans la démonstration du th.22 du n° 5.4. Comme on a $\lambda_\delta = \varepsilon(\delta)^r\lambda$, on en déduit que $f_{k,\varepsilon}$ est une forme modulaire de type (rk, ε^r) sur $\Gamma_o(p)$.

Démonstration du th.24

Je me bornerai à indiquer comment on le déduit des résultats de Siegel [26]. Choisissons des représentants $b_1,\ldots,b_h$ des éléments de $C_\mathfrak{f}$, et posons $a_i = b_i d^{-1}\mathfrak{f}^{-1}$. A chaque a_i, Siegel attache une certaine forme modulaire $\phi_i = \phi_{a_i}$, cf. [26], p.48, formule (98). Posons :

$$\phi_\lambda = \sum_{i=1}^{h} \lambda(b_i)\ \phi_i.$$

D'après [26], p.49, ϕ_λ est une forme modulaire de poids rk sur un certain sous-groupe de congruence de $SL_2(\mathbf{Z})$. Son terme constant (avec les notations de [26], loc.cit.) est

$$a_o(\phi_\lambda) = \sum_i \lambda(b_i)Q_k(a_i) = \zeta_{K,\lambda}(1-k), \qquad \text{cf. [26], p.48 et 19.}$$

D'autre part, un calcul sans grande difficulté, basé sur les formules (101) de [26], p.48, montre que l'on a

$$a_n(\phi_\lambda) = 2^r\ a_n(G_{k,\lambda}) \quad \text{pour} \quad n \geqslant 1.$$

On en déduit que $G_{k,\lambda} = 2^{-r}\phi_\lambda$.

Si maintenant $M = \begin{pmatrix}\alpha & \beta\\ \gamma & \delta\end{pmatrix}$ est un élément de $\Gamma_o(f)$, on vérifie facilement que $\phi_{\delta a}|M = \text{sgn}(\delta)^{rk}\ \phi_a$. Or, on peut écrire

$$\phi_\lambda = \sum_i \lambda(\delta b_i)\phi_{\delta a_i},$$

puisque les δb_i sont des représentants de $C_\mathfrak{f}$. On en déduit :

$\phi_\lambda|M = \text{sgn}(\delta)^{rk} \sum_i \lambda(\delta b_i)\ \phi_{a_i} = \phi_{\lambda_\delta}$, ce qui établit (i) et (ii).

BIBLIOGRAPHIE

[1] Y.AMICE - Interpolation p-adique, Bull.Soc.math.France, 92, 1964, p.117-160.

[2] A.O.L.ATKIN - Congruences for modular forms, Computers in math. research (R.F.Churchhouse et J-C.Herz ed.), p.8-19, North-Holland, Amsterdam, 1968.

[3] A.O.L.ATKIN et J.LEHNER - Hecke operators on $\Gamma_o(m)$, Math.Ann., 185, 1970, p.134-160.

[4] J.COATES et S.LICHTENBAUM - On ℓ-adic zeta functions, Ann. of Math., 98, 1973, p. 498-550

[5] R.M.DAMERELL - L-functions of elliptic curves with complex multiplication I, Acta Arith., 17, 1970, p.287-301.

[6] B.DWORK - p-adic cycles, Publ.Math.I.H.E.S., 37, 1969, p.27-115.

[7] J.FRESNEL - Nombres de Bernoulli et fonctions L p-adiques, Ann. Inst.Fourier, 17, 1967, p.281-333.

[8] E.HECKE - Mathematische Werke, Vandenhoeck und Ruprecht, Göttingen, 1959 (zw.Aufl. 1970).

[9] A.HURWITZ - Über die Entwicklungskoeffizienten der lemniskatischen Funktionen, Math.Ann., 51, 1899, p.196-226 (Math.Werke, II, p.342-373).

[10] K.IWASAWA - On p-adic L functions, Ann.of Math., 89, 1969, p.198-205.

[11] K.IWASAWA - Lectures on p-adic L functions, Ann.Math.Studies 74, Princeton Univ.Press, 1972.

[12] N.KATZ - p-adic properties of modular schemes and modular forms, ce volume.

[13] H.KLINGEN - Über die Werte der Dedekindschen Zetafunktion, Math. Ann., 145, 1962, p.265-272.

[14] H.D.KLOOSTERMAN - Theorie der Eisensteinschen Reihen von mehreren Veränderlichen, Abh.Math.Sem. Hamb., 6, 1928, p.163-188.

[15] M.KOIKE - Congruences between modular forms and functions and applications to a conjecture of Atkin, J. Fac. Science Univ. Tokyo, 20, 1973, p.129-169

[16] T.KUBOTA et H.W.LEOPOLDT - Eine p-adische Theorie der Zetawerte, J.Crelle, 214-215, 1964, p.328-339.

[17] H.LANG - Kummersche Kongruenzen für die normierten Entwicklungskoeffizienten der Weierstrass'schen $\wp$ -Funktion, Abh.Math. Sem.Hamburg., 33, 1969, p.183-196.

[18] H.W.LEOPOLDT - Eine Verallgemeinerung der Bernoullischen Zahlen, Abh.Math.Sem.Hamburg., 22, 1958, p.131-140.

[19] J-P.SERRE - Cohomologie des groupes discrets, Ann.Math.Studies 70, p.77-169, Princeton Univ.Press, 1971.

[20] J-P.SERRE - Congruences et formes modulaires (d'après H.P.F. Swinnerton-Dyer), Sém.Bourbaki, 1971/72, exposé 416.

[21] J-P.SERRE - Résumé des cours 1971/72, Annuaire du Collège de France, 1972/73, Paris, p.55-60.

[22] G.SHIMURA - Introduction to the arithmetic theory of automorphic functions, Princeton, 1971.

[23] K.SHIRATANI - Kummer's congruence for generalized Bernoulli numbers and its application, Mem.Kyushu Univ., 26, 1972, p.119-138.

[24] C.L.SIEGEL - Über die analytische Theorie der quadratischen Formen III, Ann.of Math., 38, 1937, p.212-291 (Gesam.Abh. I, p.469-548).

[25] C.L.SIEGEL - Berechnung von Zetafunktionen an ganzzahligen Stellen, Gött.Nach., 10, 1969, p.87-102.

[26] C.L.SIEGEL - Über die Fourierschen Koeffizienten von Modulformen, Gött.Nach., 3, 1970, p.15-56.

[27] H.P.F.SWINNERTON-DYER - On ℓ-adic representations and congruences for coefficients of modular forms, ce volume.

[28] A.WEIL - On a certain type of characters of the idèle-class group of an algebraic number field, Proc.Int.Symp. Tokyo-Nikko, 1955, p.1-7.

International Summer School on Modular Functions
ANTWERP 1972

Certains calculs numériques relatifs à l'interpolation p-adique des séries de Dirichlet

par P.CARTIER (Bures-sur-Yvette) et Y.ROY (Strasbourg)

Table des Matières

Introduction

Soient K un corps de nombres, totalement réel et abélien, et p un nombre premier. Kubota et Leopoldt [12] ont construit une fonction analytique p-adique qui interpole les nombres $\zeta_K^{(p)}(1-k)$ pour $k \equiv 0 \mod. p-1$, $k \geq 1$; on a noté $\zeta_K^{(p)}$ la fonction zêta du corps K débarrassée de son facteur local en p . On renvoie le lecteur à l'excellent petit livre d'Iwasawa [9] pour l'exposé de cette théorie. Lorsque le corps K n'est plus abélien, on savait par Siegel que les nombres $\zeta_K(1-k)$ sont rationnels pour $k \geq 1$ entier; Klingen [10] a étendu ce résultat aux fonctions zêta associées aux classes d'idéaux, en interprétant les nombres $\zeta_K(1-k)$ comme termes constants de certains formes modulaires. Sa méthode a été approfondie par Serre, et l'on trouvera ses résultats dans ce même volume.

Au début de ses recherches, en février 1971, Serre nous avait suggéré d'étudier numériquement les fonctions zêta de certains corps non abéliens, et d'en inférer la possibilité d'étendre à ce cas les résultats de Kubota-Leopoldt et Iwasawa. A cette époque, Y.Roy venait de mettre au point un système (écrit en langage assembleur) pour traiter des grands entiers ($< 10^{600}$) sur ordinateur. Le problème de Serre nous sembla un excellent test de l'efficacité de ce système. Les calculs furent donc entrepris sur l'ordinateur modèle IBM 360/44 du centre de calcul de l'Esplanade à Strasbourg, et durèrent de mars 1971 à avril 1972.

Les premiers résultats sur le corps cubique de discriminant 148 dépassèrent nos espérances, et nous firent entreprendre une étude systématique. Dès juillet 1971, nous disposions de tables étendues sur les corps cubiques. La critique de Weil, exprimée dans une lettre dosant artistement le chaud et le froid, nous poussa à sortir franchement du cas abélien en étudiant certains corps de degré 4 ou 5 à groupe de Galois non résoluble. Dans les 80 cas étudiés, les résultats sont frappants; ils semblent avoir encouragé Serre dans sa recherche, et suggèrent plus que la théorie ne sait établir actuellement.

Le plan de ce rapport est le suivant. La première partie est un résumé des résultats théoriques connus, y compris ceux de Serre. La deuxième partie décrit les résultats et la troisième la méthode de nos calculs. Enfin nous donnons en annexe un extrait de nos tables, qui font environ 600 pages.

Nos remerciements chaleureux vont à J.-P.Serre pour l'enthousiasme avec lequel il a suivi nos efforts, et le soin qu'il a pris à nous instruire de cette théorie. Ils vont aussi à W.Mercouroff qui n'a démantelé le centre de calcul de Strasbourg qu'après l'achèvement de ce travail.

Notations générales.

On note $\mathbf{Z}$ l'anneau des entiers rationnels

$\mathbf{Q}$ le corps des nombres rationnels

$\mathbf{R}$ le corps des nombres réels

$\mathbf{C}$ le corps des nombres complexes

$\mathrm{Re}\ s$ la partie réelle du nombre complexe s

p un nombre premier

$\mathbf{F}_p$ le corps des entiers modulo p

$\mathbf{Z}_p$ l'anneau des entiers p-adiques

$\mathbf{Q}_p$ le corps des nombres rationnels p-adiques

$\mathbf{C}_p$ la complétion d'une clôture algébrique de $\mathbf{Q}_p$

$\mathcal{O}_p$ l'anneau des entiers de $\mathbf{C}_p$

K	un corps de nombres algébriques totalement réel
D	le discriminant de K
r	le degré de K (sur $\mathbf{Q}$) (supposé fini)
$A[[T]]$	l'algèbre des séries formelles à coefficients dans l'anneau A.
$A[T]$	l'algèbre des polynômes à coefficients dans l'anneau A.

§1. Sur la théorie des fonctions zêta p-adiques

1. Nombres de Bernoulli.

Ils sont définis par la série génératrice

(1) $$\sum_{n=0}^{\infty} B_n \frac{X^n}{n!} = \frac{X}{e^X-1},$$

d'où les premiers nombres de la suite

(2) $$B_0 = 1, \ B_1 = -\frac{1}{2}, \ B_2 = \frac{1}{6}, \ B_3 = 0, \ B_4 = -\frac{1}{30}.$$

D'après un résultat fameux d'Euler, on a

(3) $$\sum_{n=1}^{\infty} \frac{1}{n^{2k}} = (-1)^{k+1} \frac{(2\pi)^{2k}}{2.(2k)!} B_{2k}$$

pour $k = 1,2,..$ et en particulier $\sum_{n=1}^{\infty} \frac{1}{n^2} = \frac{\pi^2}{6}$. La formule précédente donne le signe et une bonne valeur approchée de B_{2k} : lorsque $k \geqslant 10$ par exemple, la somme de la série $\sum_{n=1}^{\infty} \frac{1}{n^{2k}}$ diffère de 1 de moins de 10^{-6}. Noter aussi qu'on a $B_{2k+1} = 0$ pour $k \geqslant 1$.

Le résultat précédent s'explique par la fonction zêta de Riemann, définie par $\zeta(s) = \sum_{n=1}^{\infty} n^{-s}$ lorsque $\mathrm{Re}\, s > 1$. La formule (3) montre en particulier que $\pi^{-2k}\zeta(2k)$ est un nombre rationnel pour $k \geqslant 1$. Pour se débarrasser des puissances de π, on utilise le prolongement analytique de $\zeta(s)$ et l'équation fonctionnelle bien connue

(4) $$\zeta(1-s) = 2.(2\pi)^{-s}\,\Gamma(s) \cos\frac{\pi s}{2}\, \zeta(s).$$

Les résultats du premier alinéa sont alors contenus dans la formule d'Euler

(5) $$\zeta(1-k) = -B_k/k \qquad \text{pour } k \geqslant 2 \text{ entier.}$$

Autrement dit, les valeurs de la fonction ζ aux entiers négatifs sont des nombres rationnels, que l'on peut calculer facilement au moyen de relations de récurrence déduites de la série génératrice des nombres de Bernoulli

Plus généralement, soit χ un caractère primitif de Dirichlet, de conducteur f . La fonction L associée est définie par $L(s;\chi) = \sum_{n=1}^{\infty} \chi(n)n^{-s}$ lorsque $\operatorname{Re} s > 1$. Lorsque $f = 1$, on retrouve la fonction ζ de Riemann; sinon, $L(s;\chi)$ se prolonge en une fonction holomorphe sur $\mathbf{C}$, dont la valeur aux entiers négatifs est donnée par la formule de Leopoldt [13]

$$(6) \qquad L(1-k;\chi) = -B_{k,\chi}/k, \text{ pour } k \geq 1.$$

Le polynôme de Bernoulli $B_n(X)$ est égal comme d'habitude à $\sum_{j=0}^{n} \binom{n}{j} B_j X^{n-j}$ <u>et les nombres de Bernoulli généralisés</u> sont définis comme suit

$$(7) \qquad B_{k,\chi} = \frac{1}{f} \sum_{a=1}^{f} \chi(a) f^k B_k(\tfrac{a}{f}).$$

2. <u>Interpolation</u> <u>p-adique</u>.

Avant de pouvoir formuler les résultats de Kubota-Leopoldt, Iwasawa et Serre, nous devrons rappeler les principes généraux de l'interpolation p-adique.

Choisissons un nombre premier p et notons $\mathbf{C}_p$ la complétion d'une clôture algébrique du corps p-adique $\mathbf{Q}_p$; on normalise la valeur absolue dans $\mathbf{C}_p$ par $|p| = p^{-1}$ et l'on note $\mathcal{O}_p$ l'anneau des éléments x de $\mathbf{C}_p$ tels que $|x| \leq 1$.

Soit par ailleurs $b = (b_0, b_1, ..)$ une suite d'éléments de $\mathbf{C}_p$. On définit comme d'habitude les différences itérées de cette suite par les formules

$$(8) \qquad \Delta^0 b_k = b_k \qquad (k \geq 0)$$

(9) $$\Delta^n b_k = \Delta^{n-1} b_{k+1} - \Delta^{n-1} b_k \qquad (n \geq 1,\ k \geq 0)$$

et l'on définit les coefficients d'interpolation $c_n = \Delta^n b_0$, soit plus explicitement

(10) $$c_n = \sum_{j=0}^{n} (-1)^{n-j} \binom{n}{j} b_j .$$

Pour tout entier $n \geq 0$, on a inversement

(11) $$b_k = \sum_{n=0}^{\infty} c_n \binom{k}{n} .$$

On a alors le <u>critère de Mahler</u> : <u>pour qu'il existe une fonction continue</u> $f : \mathbf{Z}_p \to \mathbf{C}_p$ <u>telle que</u> $f(k) = b_k$ <u>pour tout entier</u> $k \geq 0$, <u>il faut et suffit</u> qu'on ait $\lim\limits_{n\to\infty} |c_n| = 0$. La fonction f est définie par le développement binomial

(12) $$f(x) = \sum_{n=0}^{\infty} \frac{c_n}{n!} (x)_n ,$$

avec la définition usuelle des "puissances binomiales" (sous la forme "descendante")

(13) $$(x)_n = x(x-1)\ldots(x-(n-1)).$$

Pour déduire de là un développement en série de puissances pour f(x), introduisons les nombres de Stirling $S_n^{(m)}$ (pour $0 \leq m \leq n$) par l'identité

(14) $$(X)_n = \sum_{m=0}^{n} S_n^{(m)} X^m$$

on calcule ces entiers par la formule de récurrence usuelle

(15) $$S_{n+1}^{(m)} = S_n^{(m-1)} - n\, S_n^{(m)} \qquad (1 \leq m \leq n)$$

et les conditions aux limites $S_0^{(0)} = 1$, $S_n^{(0)} = 0$ et $S_n^{(n)} = 1$ pour $n \geq 1$.

Posons alors $q = p$ si $p \neq 2$ et $q = 4$ si $p = 2$; de plus, posons

$R = p^{\frac{p-2}{p-1}}$ si $p \neq 2$ et $R = 2$ si $p = 2$. Supposons que les coefficients d'interpolation c_n satisfassent à la congruence

$$c_n \equiv 0 \mod q^n \mathcal{O}_p. \tag{16}$$

On peut alors définir de nouveaux coefficients a_m par la série convergente

$$a_m = \sum_{n=m}^{\infty} S_n^{(m)} c_n/n! \tag{17}$$

et la fonction f d'interpolation définie par (12) admet le développement en série de Taylor

$$f(x) = \sum_{m=0}^{\infty} a_m x^m \tag{18}$$

de rayon de convergence $\geq R$. Autrement dit, si l'on a $c_n \equiv 0 \mod. q^n \mathcal{O}_p$ pour tout $n \geq 0$, il existe une fonction f analytique dans le disque ouvert $\{x \in \mathbf{C}_p \mid \|x\| < R\}$ de $\mathbf{C}_p$ et telle que $f(k) = b_k$ pour $k \geq 0$.

Les méthodes d'Iwasawa [8] suggèrent une notion plus restrictive d'analyticité qui a été étudiée systématiquement par Serre [15]. Notons U_1 le groupe multiplicatif des éléments x de $\mathbf{Z}_p$ tels que $x \equiv 1 \mod q\, \mathbf{Z}_p$. Choisissons un isomorphisme de groupes topologiques $\phi : \mathbf{Z}_p \to U_1$, par exemple $\phi(x) = (1+q)^x = \sum_{n=0}^{\infty} \frac{q^n}{n!} (x)_n$ ou $\phi(x) = \exp qx = \sum_{n=0}^{\infty} \frac{q^n}{n!} x^n$.
D'après Serre on appelle algèbre d'Iwasawa l'ensemble des fonctions $f : \mathbf{Z}_p \to \mathbf{C}_p$ de la forme

$$f(x) = F(\phi(x)-1) \quad \text{avec } F \in \mathcal{O}_p[[T]]. \tag{19}$$

On voit facilement que l'algèbre d'Iwasawa ne dépend pas du choix de l'isomorphisme ϕ.

On dira par abus de langage que la suite $b = (b_0, b_1, ..)$ d'éléments de $\mathbf{C}_p$ appartient à l'algèbre d'Iwasawa s'il existe une fonction $f : \mathbf{Z}_p \to \mathbf{C}_p$

de la forme (19) et telle que $f(k) = b_k$ pour tout entier $k \geq 0$. Il revient au même de dire qu'il existe une série formelle $F \in \mathcal{O}_p[[T]]$ telle que $b_k = F(\gamma^k - 1)$ pour tout $k \geq 0$, le nombre p-adique γ étant choisi de la forme $\gamma = 1 + q\,u$ avec une unité p-adique u. Par une généralisation facile des résultats de Serre [15], on obtient le critère suivant : <u>la suite b appartient à l'algèbre d'Iwasawa si et seulement si l'on a les congruences</u> $c_n \equiv 0 \bmod. q^n \mathcal{O}_p$ <u>déjà rencontrées plus haut, et si de plus les éléments</u> $d_n = \sum_{m=0}^{n} S_n^{(m)} c_m/q^m$ <u>de</u> $\mathcal{O}_p$ <u>sont divisibles par</u> $n!$ <u>dans</u> $\mathcal{O}_p$. En particulier, la classe de $c_n/q^n \bmod. p\mathcal{O}_p$ ne dépend alors que de la classe de n mod.p-1 (pour $n \geq 1$).

3. <u>Les fonctions zêta p-adiques des corps abéliens totalement réels</u>.

Tout repose sur les propriétés arithmétiques des nombres de Bernoulli. Il est bien connu ("congruences de Kummer") que si n n'est pas divisible par p-1, le nombre rationnel B_n/n est p-entier (autrement dit, de la forme a/b avec $b \not\equiv 0 \bmod. p$) et que sa classe modulo p ne dépend que de la classe de n modulo p-1. Plus généralement, posons $\zeta^{(p)}(s) = (1-p^{-s})\zeta(s)$ et considérons les p-2 "sous-séries" formées des valeurs de $\zeta^{(p)}(-n)$ sur les progressions arithmétiques de période p-1 à l'exception de la progression $-n \equiv 1 \bmod. p-1$, soit

$$\zeta^{(p)}(0),\ \zeta^{(p)}(1-p),\ \zeta^{(p)}(2-2p),\ \zeta^{(p)}(3-3p),\ldots$$

$$\zeta^{(p)}(-1),\ \zeta^{(p)}(-p),\ \zeta^{(p)}(1-2p),\ \zeta^{(p)}(2-3p),\ldots$$

- -

$$\zeta^{(p)}(3-p),\ \zeta^{(p)}(4-2p),\ \zeta^{(p)}(5-3p),\ \zeta^{(p)}(6-4p),\ldots\ .$$

<u>Iwasawa a prouvé que chacune des sous-séries précédentes appartient à l'algèbre d'Iwasawa</u>. Pour la sous-série restante, il faut une petite modification; c'est <u>la suite des nombres</u> $(\gamma^{(1+k)(p-1)}-1)\zeta^{(p)}(1-(k+1)(p-1))$ pour $k \geq 0$ qui <u>appartient à l'algèbre d'Iwasawa</u>.

On peut généraliser ceci aux séries $L(s;\chi)$. Choisissons un isomorphisme $x \mapsto x^\sigma$ du corps $\bar{\mathbf{Q}}$ des nombres algébriques dans le corps algébriquement clos $\mathbf{C}_p$. Il existe alors un unique caractère ω_p, de conducteur q, tel que $\omega_p(x)^\sigma \equiv x \mod q\,\mathcal{O}_p$ pour tout x entier. De plus, si $L(s) = \sum_{n=1}^{\infty} a_n n^{-s}$ est une série de Dirichlet, on note $L^{(p)}(s)$ la série de Dirichlet $\sum_{(n,p)=1} a_n n^{-s}$ d'où l'on a ôté les termes $a_n n^{-s}$ avec $n \equiv 0$ mod.p. En particulier, on a $\zeta^{(p)}(s) = (1-p^{-s})\,\zeta(s)$ comme plus haut et $L^{(p)}(s,\chi) = (1-\chi(p)p^{-s})\,L(s;\chi)$. Avec ces notations, Iwasawa a montré que <u>si le caractère</u> χ <u>est distinct de</u> ω_p^{-1}, <u>la suite des nombres</u> $L^{(p)}(-k;\chi\,\omega_p^{-k})^\sigma$ <u>pour</u> $k = 0,1,2,..$ <u>appartient à l'algèbre d'Iwasawa</u>. On en déduit que si χ est distinct du caractère ω_p^{-j}, la suite des éléments $L^{(p)}(1-j-n(p-1);\chi)^\sigma$ pour $n = 0,1,2,..$ appartient à l'algèbre d'Iwasawa (pour $j = 1,2,..,p-1$ fixé).

Soit K un corps de nombres totalement réel, <u>abélien</u> et de degré r sur le corps $\mathbf{Q}$ des nombres rationnels et soit ζ_K la fonction zêta du corps K. D'après la théorie du corps de classes, il existe r caractères $\chi_1,\ldots,\chi_r$ dont le conducteur divise le discriminant D de K, et tels que $\zeta_K(s) = \prod_{j=1}^{r} L(s;\chi_j)$. Posons $L(s) = \zeta_K(s)/\zeta(s)$. Ce qui précède montre alors que pour $k \geqslant 0$, le nombre $L(-k)$ est rationnel et n'a en dénominateur que des nombres premiers divisant le discriminant D de K. De plus, si p ne divise pas D, les p-1 sous-séries formées des nombres $L^{(p)}(1-j-k(p-1))$ pour $k = 0,1,2,..$ (on fixe $j = 1,2,..,p-1$) appartiennent à l'algèbre d'Iwasawa.

4. <u>Les résultats de Serre</u> [15].

Serre considère un corps K, totalement réel de degré r sur $\mathbf{Q}$, et les nombres rationnels $\zeta_K(1-k)$ pour $k = 1,2,..$. Les résultats sont de deux ordres.

<u>THÉORÈME D'INTÉGRALITÉ</u> : a) <u>Si</u> $k \geq 1$ <u>est pair et</u> $rk \not\equiv 0$ mod.p-1, <u>alors</u> $\zeta_K(1-k)$ <u>est</u> p-<u>entier</u> .

b) <u>Si</u> $k \geq 1$ <u>est pair et</u> $rk \equiv 0$ mod.p-1, <u>alors</u> $prk\,\zeta_K(1-k)$ <u>est</u> p-<u>entier pour</u> $p \neq 2$.

c) <u>Si</u> $k \geq 1$ <u>est pair</u>, <u>le nombre</u> $2^{2-r}rk\zeta_K(1-k)$ <u>est</u> 2-<u>entier</u>.

<u>INTERPOLATION p-ADIQUE</u> : Supposons d'abord $p \neq 2$. Choisissons un générateur topologique γ de $U_1 = 1 + q\,\mathbf{Z}_p$, et un entier pair j compris entre 1 et $p-1$.

a) <u>Si</u> $rj \not\equiv 0$ mod.p-1, <u>il existe une série formelle</u> $F_j \in \mathbf{Z}_p[[T]]$ <u>telle que</u> $\zeta_K^{(p)}(1-k) = F_j(\gamma^k - 1)$, <u>pour tout entier</u> $k \geq 2$ <u>tel que</u> $k \equiv j$ mod.p-1.

b) <u>Si</u> $rj \equiv 0$ mod.p-1, <u>il existe une série formelle</u> $F_j^* \in \mathbf{Z}_p[[T]]$ <u>telle que</u> $\zeta_K^{(p)}(1-k) = \dfrac{F_j^*(\gamma^k-1)}{\gamma^{rk}-1}$ <u>pour tout entier</u> $k \geq 2$ <u>tel que</u> $k \equiv j$ mod.p-1.

Supposons maintenant $p = 2$. Il existe alors une série $F \in \mathbf{Z}_2[[T]]$ telle que $2^{-r}\zeta_K^{(2)}(1-k) = \dfrac{F^*(\gamma^k-1)}{\gamma^{rk}-1}$ pour $k \geq 2$ pair.

Avec les notations de Serre, on a dans le cas a) $\zeta_K^*(1-x;1-u) = F_j(\gamma^x-1)$ pour $x \in \mathbf{Z}_p$, en notant u la classe de j modulo p-1. Il faut remplacer $F_j(T)$ par $\dfrac{F_j^*(T)}{(1+T)^r-1}$ dans le cas b); modification analogue pour $p = 2$.

§2. Résultats numériques

5. Description des corps étudiés.

Nous donnons d'abord la description précise des 63 corps totalement réels de degré 3,4 ou 5 que nous avons étudiés.

A) Corps cycliques de degré 3 et discriminant < 900.

Si K est un tel corps, son discriminant est un carré $D = d^2$, le corps K est contenu dans le corps cyclotomique $\mathbf{Q}(e^{2\pi i/d})$ et il existe un sous-groupe H du groupe multiplicatif $(\mathbf{Z}/d\mathbf{Z})^\times$ avec les propriétés suivantes :

a) la classe de -1 modulo d appartient à H ;

b) il n'existe aucun diviseur $d' \neq d$ de d tel que H contienne toutes les classes modulo d des entiers a premiers à d et tels que $a \equiv 1$ mod.d';

c) H est d'indice 3 dans $(\mathbf{Z}/d\mathbf{Z})^\times$;

d) notons $C_0 = H$, C_1 et C_2 les classes de $(\mathbf{Z}/d\mathbf{Z})^\times$ modulo H, et posons $z_j = \sum_{a \in C_j} e^{2\pi i a/d}$ pour $j = 0,1,2$. Si d n'est pas divisible par 3, alors (z_0,z_1,z_2) est une base sur $\mathbf{Z}$ de l'anneau des entiers de K.

Les propriétés a), b) et c) montrent que d est de l'une des formes $3^2\, p_1 \cdots p_r$ ou $p_1 \cdots p_r$, où $p_1,\ldots,p_r$ sont des nombres premiers congrus à 1 modulo 6, et deux à deux distincts. Les nombres premiers $p \equiv 1$ mod.6 au plus égaux à 30 sont 7, 13, 19 et par suite les discriminants $D < 900$ sont $3^4 = 81$, $7^2 = 49$, $13^2 = 169$, $19^2 = 361$. Dans chacun de ces cas, le groupe $(\mathbf{Z}/d\mathbf{Z})^\times$ est cyclique et contient donc un seul sous-groupe H d'indice 3; choisissons une racine primitive g modulo d et notons C_j l'ensemble des entiers congrus modulo d à l'un des entiers g^{j+3n} pour $n \geqslant 0$. On a le tableau suivant (avec $g = 2$ pour $d \neq 7$ et $g = -2$ pour $d = 7$).

D	81	49	169	361
C_0	1	1	1,5	1,7,8
C_1	2	2	2,3	2,3,5
C_2	4	3	4,6	4,6,9

Pour chaque classe C_j, on a donné la liste des éléments a compris entre 1 et $\frac{d-1}{2}$; les autres éléments sont les nombres de la forme $nd \pm a$ avec n entier .

Le tableau précédent donne immédiatement la valeur de $x = z_0$. Nous y avons adjoint l'équation irréductible satisfaite par x.

$D = 49 \quad x = 2\cos\frac{2\pi}{7} \qquad x^3 + x^2 - 2x - 1 = 0$

$D = 81 \quad x = 2\cos\frac{2\pi}{9} \qquad x^3 - 3x + 1 = 0$

$D = 169 \quad x = 2\cos\frac{2\pi}{13} + 2\cos\frac{10\pi}{13} \qquad x^3 + x^2 - 4x + 1 = 0$

$D = 361 \quad x = 2\cos\frac{2\pi}{19} + 2\cos\frac{14\pi}{19} + 2\cos\frac{16\pi}{19} \qquad x^3 + x^2 - 6x - 7 = 0.$

On peut montrer que $(1,x,x^2)$ est une base des entiers de K .

B) Corps non abéliens de degré 3 et discriminant < 1257.

Il y a 28 corps de cette classe; la table 1 donne pour chacun d'eux le discriminant et sa décomposition en facteurs premiers, et l'équation irréductible satisfaite par un élément x tel que $K = \mathbf{Q}(x)$. On a choisi x de sorte que les monômes $1,x,x^2$ forment une base sur $\mathbf{Z}$ de l'anneau des entiers de K . La table 1 est copiée de Delone et Faddeev [6] .

C) Corps non abéliens de degré 4 ne contenant aucun sous-corps non-trivial, et de discriminant < 8069.

Il y a 9 corps de cette classe; la table 2 donne pour chacun d'eux le discriminant et sa décomposition en facteurs premiers, et une équation définissant le corps. Si L est la clôture galoisienne de K , le groupe de Galois de L sur **Q** est le groupe symétrique S_4 d'ordre 4!. Dans chacun des cas, le générateur x de K est tel que $(1,x,x^2,x^3)$ soit une base sur **Z** de l'anneau des entiers de K.

D) <u>Corps non abéliens K de degré</u> 4, <u>contenant un sous-corps quadratique</u> E, <u>et de discriminant</u> < 8112.

Il y a 18 corps de cette catégorie, décrits par la table 3. Dans chaque cas, on a donné le discriminant D de K, le discriminant d de E, un générateur η de E et un générateur x de K. Dans tous les cas, la famille $(1,\eta,x,x\eta)$ est une base sur **Z** de l'anneau des entiers du corps K, et la clôture galoisienne L de K est de degré 8 sur **Q**, de groupe de Galois diédral d'ordre 8.

E) <u>Le corps de degré</u> 5 <u>et discriminant</u> $11^4 = 14641$.

C'est la partie réelle du corps cyclotomique $\mathbf{Q}(e^{2\pi i/11})$. Il est engendré par $x = 2\cos\frac{2\pi}{11}$ dont l'équation irréductible est

$$x^5 + x^4 - 4x^3 - 3x^2 + 3x + 1 = 0.$$

L'anneau des entiers admet $(1,x,x^2,x^3,x^4)$ pour base sur **Z**.

F) <u>Corps de degré</u> 5 <u>non abéliens</u>.

Il s'agit de 3 corps, dont nous donnons le discriminant et l'équation irréductible satisfaite par un générateur x

24217	$x^5 - 5x^3 + x^2 + 5x - 1 = 0$
36497	$x^5 - 6x^3 - x^2 + 4x - 1 = 0$
38569	$x^5 - 5x^3 + 4x - 1 = 0.$

On a 24217 = 61.397 et les nombres 36497 et 38569 sont premiers. Comme le discriminant n'est pas divisible par un carré, l'anneau des entiers admet $(1,x,x^2,x^3,x^4)$ pour base sur **Z**.

Remarque 1 : Les corps de degré 4 ont été pris dans la table de Delone et Faddeev [6] pages 199-200. Cette table comprend trois erreurs d'impression :

a) Les coefficients s,p,q,n sont tels que l'équation est $x^4 - sx^3 + px^2 - qx + n = 0$ avec $+ px^2$ et non $- px^2$.

b) Pour le corps de discriminant 2225, lire $\frac{\rho^3+\rho^2+\rho}{2}$ et non $\frac{\rho^3+\rho^2+\rho^2}{2}$.

c) Pour le corps de discriminant 7625, l'équation est $x^4 - x^3 - 9x^2 + 4x + 16 = 0$ avec le terme constant 16, et non 1.

Enfin, le corps de discriminant 7260 n'existe pas; l'équation proposée n'est pas irréductible, car on a

$$x^4 - x^3 - 7x^2 + 8x - 2 = (x^2 + 2x - 2)(x^2 - 3x + 1).$$

A titre de contrôle, tous les discriminants des corps de degré 3 et 4 ont été recalculés.

Remarque 2 : Les corps de degré 5 ont été pris dans le travail de H.Cohn [5]. Pour les discriminants indiqués, cet auteur donnent d'autres équations, mais nous avons vérifié qu'elles engendraient le même corps. Nous publierons par ailleurs [3] nos résultats numériques sur les corps de degré 5, et la méthode utilisée.

6. Description des tables.

Pour chacun des 63 corps décrits ci-dessus, nos tables imprimées (dont on trouvera un extrait plus loin) contiennent les renseignements suivants :

a) La loi de décomposition explicite des nombres premiers p en idéaux du corps K, pour $p \leqslant 2500$ environ. Nous possédons des renseignements analogues pour $p \leqslant 50000$ environ, stockés sur cartes perforées.

b) Pour chaque corps K, nous avons posé $L(s) = \zeta_K(s)/\zeta(s)$, sauf dans le cas D, où nous avons posé $L(s) = \zeta_K(s)/\zeta_E(s)$. Nous avons calculé les nombres $L(-n)$ dans les limites suivantes :

- pour $1 \leq n \leq 57$ si K est de classe A, sauf pour le plus grand discriminant 361, où nous avons seulement $1 \leq n \leq 53$
- pour $1 \leq n \leq N$ si K est de classe B, l'entier N étant donné par la table 1
- pour $1 \leq n \leq 29$ si K est de classe C
- pour $1 \leq n \leq 39$ si K est de classe D
- pour $1 \leq n \leq 17$ si K est de degré 5 (classes E et F).

Noter qu'on a $L(-n) = 0$ si $n \geq 0$ est pair.

c) Pour chaque entier $L(-n)$, ses facteurs premiers < 10000 avec leur exposant.

d) Coefficients d'interpolation : on forme d'abord des sous-séries comme suit : si $p = 2$, une seule sous-série formée des nombres $L^{(2)}(-1-2n)$ pour $n = 0,1,2,..$ dans les limites de la table b). Si $p \neq 2$, soit t l'un des nombres $1,2,..,\frac{p-1}{2}$; la t-ième sous-série se compose des nombres $a_n = L^{(p)}(1-2t-n(p-1))$ pour $n = 0,1,2,..$ dans les limites de la table b). On forme les coefficients d'interpolation $c_n = \sum_{j=0}^{n} (-1)^{n-j}\binom{n}{j}a_j$, qui sont entiers si K n'est pas abélien. On détermine ensuite la plus grande puissance de p divisant c_n. La suite d'exposants obtenue peut avoir jusqu'à 29 termes pour $p = 2$ et les corps de degré 3 et discriminant assez petit.

e) Valeur extrapolée de $L^{(p)}(1)$: considérons la dernière sous-série définie par $a_{n-1} = L^{(p)}(1-n(p-1))$ pour $n = 1,2,..,N$; définissons les coefficients d'interpolation c_n comme plus haut et soit p^h la plus haute puissance de p divisant c_{N-1}. On a calculé $\ell = \sum_{n=0}^{N-1} c_n\binom{-1}{n}$ modulo p^h. Si les résultats mentionnés en 7, B) ci-dessous sont exacts, la fonction analytique p-adique L^*, telle que $L^*(1-k) = L^{(p)}(1-k)$ pour $k > 0$, $k \equiv 0$ mod.p-1, satisfait à $L^*(1) \equiv \ell \bmod p^{N-1}$ pour $p \neq 2$, et à $L^*(1) \equiv \ell \bmod 2^{3(N-1)}$ pour $p = 2$. Nous n'avons pas interprété les résultats obtenus pour ℓ, mais nous pensons qu'ils pourront servir à tester les conjectures à faire sur le régulateur p-adique dans le cas d'un corps non abélien.

7. Interprétation des résultats.

Les corps cycliques de degré 3 et le corps de degré 5 et de discriminant 11^4 sont abéliens, et la théorie d'Iwasawa fournit tous les renseignements cherchés sur eux. Nous n'avons fait les calculs de tels corps qu'à titre de contrôle de nos méthodes. En particulier, nous avons vérifié que les nombres $L(-n)$ obtenus n'étaient pas toujours entiers, mais n'avaient en dénominateur que les diviseurs premiers du discriminant.

A) Intégralité : Il faut distinguer deux cas.

A_1) Lorsque le corps K ne contient aucun sous-corps abélien $\neq \mathbf{Q}$ (classes B,C et F), les nombres $L(-n) = \zeta_K(-n)/\zeta(-n)$ sont entiers et divisibles par 2^{r-1} pour $n > 0$ entier (dans la limite des tables).

A_2) Pour les corps K de classe D, les nombres $\zeta_K(-n)/\zeta(-n)$ ne sont pas toujours entiers, mais par contre les nombres $L(-n) = \zeta_K(-n)/\zeta_E(-n)$, où E est le plus grand sous-corps abélien de K, sont entiers et divisibles par 4 (pour $n > 0$).

Dans ces deux cas, la fonction L considérée est une série L d'Artin associée à une représentation irréductible du groupe de Galois $Gal(\overline{\mathbf{Q}}/\mathbf{Q})$, de degré $\delta = 2,3,2,4$ pour les classes B,C,D,F respectivement. Ces cas suggèrent l'énoncé suivant : si L est une série d'Artin associée à une représentation du groupe de Galois $Gal(\overline{\mathbf{Q}}/\mathbf{Q})$, de degré δ, définie sur $\mathbf{Q}$, et sans composante absolument irréductible de degré 1, alors $L(-n)$ est un entier rationnel divisible par 2^δ (pour tout entier $n > 0$). Voir [4] pour des conjectures analogues.

B) Interpolation p-adique : nous nous intéressons aux corps non abéliens (classes B,C,D,F). On peut résumer comme suit les résultats obtenus :

- Supposons $p \neq 2$ et fixons l'entier $t = 1,2,..,\frac{p-1}{2}$; dans la limite des tables, on a une formule d'interpolation

(20) $$L^{(p)}(1 - 2t - n(p - 1)) = \sum_{j=0}^{\infty} p^j u_j \binom{n}{j}$$

avec $u_0, u_1, ..$ entiers.

- Supposons $p = 2$; on a une formule d'interpolation

(21) $$L^{(2)}(1 - 2n) = \sum_{j=0}^{\infty} 2^{\delta + 3j} u_j \binom{n}{j}$$

avec $u_0, u_1, ..$ entiers (dans la limite des tables).

Pour les corps K de la classe C qui contiennent $\mathbf{Q}(\sqrt{2})$, on peut même remplacer $2^{\delta + 3j}$ par $2^{\delta + 4j}$ dans (21); ceci se produit pour les corps de discriminant 2624, 4352, 7168 et 7232.

Pour $p \neq 2$, l'énoncé précédent signifie que les coefficients d'interpolation c_n de la sous-série $L^{(p)}(1-2t-k(p-1))$ (t fixé égal à $1,2,..,\frac{p-1}{2}$, k prenant les valeurs $0,1,2,..$) satisfont aux conditions $c_n \equiv 0 \bmod p^n \mathcal{O}_p$. Nous avons vérifié pour le corps cubique de discriminant 148 que les autres congruences de Serre sont satisfaites dans la limite des tables, de sorte que chaque sous-série est le début d'une suite appartenant à l'algèbre d'Iwasawa; nous projetons de vérifier systématiquement de telles propriétés sur nos tables. Il est facile en tout cas de vérifier une des conséquences de l'appartenance à l'algèbre d'Iwasawa, à savoir que si c_n est divisible par p^{n+1}, la propriété analogue a lieu dans la limite des tables pour les entiers $n' \equiv n \bmod. p-1$ (lorsque $n \geq 1$ et $n' \geq 1$).

8. Séries de Dirichlet tordues.

Si $F(s) = \sum_{n=1}^{\infty} a_n n^{-s}$ est une série de Dirichlet et χ un caractère, on définit la série de Dirichlet $F(s;\chi) = \sum_{n=1}^{\infty} a_n \chi(n) n^{-s}$ et on l'appelle la série F tordue par χ.

Le caractère ω_p est défini comme au n° 3. Serre a démontré le résultat suivant dans [15, thm. 22] ; si a est un entier pair tel que $ra \not\equiv 0$ mod.p-1, la suite des éléments $\zeta_K^{(p)}(-k;\ \omega_p^{a-k-1})^{\sigma}$ de $\mathbf{C}_p$ (pour $k = 0,1,2,..$) appartient à l'algèbre d'Iwasawa. Il en est de même de $(\gamma^{r(k+1)}-1)\zeta_K^{(p)}(-k;\ \omega_p^{a-k-1})^{\sigma}$, si $ra \equiv 0$ mod.p-1. Lorsque $K = \mathbf{Q}$, donc $r = 1$, ceci se réduit à un résultat d'Iwasawa mentionné au n° 3.

Par analogie, nous conjecturons le résultat suivant : soient K un corps de nombres totalement réel, et E le plus grand sous-corps abélien de K. Posons $L(s) = \zeta_K(s)/\zeta_E(s)$. Alors pour tout entier a, la suite des éléments $L^{(p)}(-k;\ \omega_p^{a-k-1})^{\sigma}$ de $\mathbf{C}_p$ (pour $k = 0,1,2,..$) appartient à l'algèbre d'Iwasawa. On pourrait plus généralement considérer des séries L d'Artin (?).

Examinons quelques cas particuliers de cette conjecture. Tout d'abord pour $p = 2$, on trouve que la suite des nombres entiers

$$L^{(p)}(0;\ \omega_2),\ L^{(p)}(-1),\ L^{(p)}(-2;\ \omega_2),\ L^{(p)}(-3),...$$

appartient à l'algèbre d'Iwasawa. On montre facilement que ceci entraîne que le n-ième coefficient d'interpolation de la suite $L^{(p)}(-1), L^{(p)}(-3)$, $L^{(p)}(-5),..$ est divisible par 2^{3n}. Par contre, nous n'avons pas d'explication pour la divisibilité par 2^{4n} lorsque $E = \mathbf{Q}(\sqrt{2})$ et $[K : \mathbf{Q}] = 4$.

Supposons maintenant $p \neq 2$; le caractère $\omega_p^{\frac{p-1}{2}}$ n'est autre que le caractère de Legendre $\chi_p : a \mapsto (\frac{a}{p})$, à valeurs dans $\{1,-1\}$. On a donc en particulier l'énoncé conjectural suivant : si $p \equiv 1$ mod 4, pour chacun des nombres $t = 1,2,..,\frac{p-1}{4}$, les suites

$$L^{(p)}(1-2t),\ L^{(p)}(1-2t-\tfrac{p-1}{2};\ \chi_p),\ L^{(p)}(1-2t-(p-1)),\ L^{(p)}(1-2t-3\,\tfrac{p-1}{2};\ \chi_p),..$$

$$L^{(p)}(1-2t;\ \chi_p),\ L^{(p)}(1-2t-\tfrac{p-1}{2}),\ L^{(p)}(1-2t-(p-1);\ \chi_p),\ L^{(p)}(1-2t-3\,\tfrac{p-1}{2}),..$$

appartiennent à l'algèbre d'Iwasawa; en particulier, le n-ième coefficient d'interpolation de ces suites est divisible par p^n.

Pour tenter de vérifier une telle propriété, nous avons calculé pour certains corps cubiques les nombres $L(-n;\chi_5)$ pour $1 \leq n \leq N$; voici une table des discriminants étudiés

D = 148, 229, 257, 316, 321, 404, 469, 473 N = 29

D = 564, 568, 621, 697, 733 N = 23.

Nous avons vérifié pour ces fonctions $L(s;\chi_5)$ les propriétés usuelles d'intégralité et d'interpolation p-adique (pour $p \neq 5$); de plus, nous avons formé par intercalement les deux suites suivantes (lorsque N = 29 par exemple)

$$L^{(5)}(-1),\ L^{(5)}(-3;\chi_5),\ L^{(5)}(-5),\ L^{(5)}(-7;\chi_5),\ldots,L^{(5)}(-29)$$

$$L^{(5)}(-1;\chi_5),\ L^{(5)}(-3),\ L^{(5)}(-5;\chi_5),\ L^{(5)}(-7),\ldots,L^{(5)}(-29;\chi_5)$$

et vérifié que le n-ième coefficient d'interpolation est divisible par 5^n.

Nous avons aussi calculé les nombres $L(-n;\chi_{13})$ pour $1 \leq n \leq 19$ lorsque K est le corps cubique de l'un des discriminants 148, 229, 257 et 316. Les propriétés d'intégralité et d'interpolation p-adique pour $p \neq 13$ sont comme d'habitude. Nous avons ensuite formé par intercalement les 6 sous-séries

$$L^{(13)}(-1),\ L^{(13)}(-7;\chi_{13}),\ L^{(13)}(-13),\ L^{(13)}(-19;\chi_{13})$$

$$L^{(13)}(-1;\chi_{13});\ L^{(13)}(-7),\ L^{(13)}(-13;\chi_{13}),\ L^{(13)}(-19)$$

$$L^{(13)}(-3),\ L^{(13)}(-9;\chi_{13}),\ L^{(13)}(-15)$$

$$L^{(13)}(-3;\chi_{13}),\ L^{(13)}(-9),\ L^{(13)}(-15;\chi_{13})$$

$$L^{(13)}(-5),\ L^{(13)}(-11;\chi_{13}),\ L^{(13)}(-17)$$

$$L^{(13)}(-5;\chi_{13}),\ L^{(13)}(-11),\ L^{(13)}(-17;\chi_{13})$$

et vérifié que dans chacune des sous-séries, le n-ième coefficient d'interpolation est divisible par 13^n.

§3. Calcul numérique des fonctions zêta

9. Méthode générale.

Notons K un corps de nombres totalement réel, de degré r et discriminant D. La fonction zêta de K a été définie par Dedekind au moyen de la formule

$$\zeta_K(s) = \sum_{\mathfrak{a}} (N\,\mathfrak{a})^{-s} = \prod_{\mathfrak{p}}(1-(N\,\mathfrak{p})^{-s})^{-1} \tag{22}$$

lorsque $\underline{\mathrm{Re}}\ s > 1$; la somme est étendue à tous les idéaux entiers $\mathfrak{a}$ de K et le produit à tous les idéaux premiers $\mathfrak{p}$ de K. Il est commode d'écrire le produit infini sous la forme d'un produit étendu aux nombres premiers p

$$\zeta_K(s) = \prod_p H_p(p^{-s})^{-1}; \tag{23}$$

pour chaque p, le facteur $H_p(p^{-s})$ est le produit des nombres $1-(N\,\mathfrak{p})^{-s}$ pour tous les idéaux premiers $\mathfrak{p}$ de K au-dessus de p. De plus, H_p est un polynôme de degré $\leqslant r$.

On sait par Hecke que la fonction ζ_K se prolonge en une fonction méromorphe sur $\mathbf{C}$, avec un pôle simple pour s = 1, et une équation fonctionnelle

$$\zeta_K(1-s) = D^{s-1/2} C(s)^r\ \zeta_K(s); \tag{24}$$

on a posé

$$C(s) = 2^{1-s}\ \pi^{-s}\ \Gamma(s) \cos \frac{\pi s}{2}. \tag{25}$$

Lorsque $K = \mathbf{Q}$, on retrouve la fonction zêta de Riemann et ses propriétés.

Notre but est le calcul des nombres $L(-1)$, $L(-3)$, $L(-5)$,... pour diverses fonctions L liées étroitement à la fonction ζ_K. La méthode générale est la suivante :

a) Répartition des nombres premiers en classes : dans chaque cas, on peut répartir les nombres premiers p en un nombre fini de classes $D_1,..,D_h$ et déterminer des polynômes $M_1,..,M_h$ tels que l'on ait

$$L(s) = \prod_{j=1}^{h} \prod_{p \in D_j} M_j(p^{-s})^{-1} \qquad (\mathrm{Re}\ s > 1). \tag{26}$$

b) Calcul des nombres $L(2)$, $L(4)$,... par le produit infini précédent.

c) Détermination d'une équation fonctionnelle, donnant *a priori* les nombres $\frac{L(-1)}{L(2)}$, $\frac{L(-3)}{L(4)}$, $\frac{L(-5)}{L(6)}$,... sous une forme ne dépendant que du degré et du discriminant du corps considéré, nombres qu'on peut calculer une fois pour toutes.

10. Le cas des corps abéliens.

Parmi les corps que nous avons étudiés, il y a 4 corps cycliques de degré 3 et un corps cyclique de degré 5. Dans ces cas la loi de réciprocité permet de déterminer les nombres $\zeta_K(-1)$, $\zeta_K(-3)$,.. par des calculs faciles, qui permettent le contrôle de nos méthodes.

Considérons un corps K totalement réel, cyclique, de degré 3, et reprenons les notations du n° 5, A. Il y a trois classes de nombres premiers :

a) celle des diviseurs premiers de D, soit D_1 : si p est un tel nombre, on a $(p) = \mathfrak{p}^3$ où $\mathfrak{p}$ est un idéal premier de K de norme p. Posons $M_1(T) = 1$.

b) La classe $C_0 = H = D_2$: pour p dans C_0, on a la décomposition $(p) = \mathfrak{p}_1\,\mathfrak{p}_2\,\mathfrak{p}_3$, avec trois idéaux premiers distincts $\mathfrak{p}_1$, $\mathfrak{p}_2$, $\mathfrak{p}_3$, de norme p. On pose $M_2(T) = (1-T)^2$.

c) La classe $C_1 \cup C_2 = D_3$: pour p dans $C_1 \cup C_2$, on a $(p) = \mathfrak{p}$ où $\mathfrak{p}$ est premier de norme p^3. On pose $M_3(T) = 1 + T + T^2$.
Posons $L(s) = \zeta_K(s)/\zeta(s)$ et $L_p(s) = M_j(p^{-s})^{-1}$ si $p \in D_j$. On a alors

(27) $$L(s) = \prod_p L_p(s) = L(s;\chi)\,L(s;\overline{\chi})$$

où χ est le caractère primitif de conducteur $d = D^{1/2}$ défini par $\chi(n) = \rho^{nj}$ pour $n \in C_j$ (on note $\rho \neq 1$ une racine cubique de l'unité).

Soit par ailleurs $r \neq 1$ une racine 11-ième de l'unité et $K = \mathbf{Q}(r + r^{-1})$ (degré 5, discriminant 11^4). On a de même les lois de décomposition :

a) On a $(11) = \mathfrak{p}^5$ avec $N\mathfrak{p} = 11$, et le facteur local $L_p(s) = 1$.

b) Si $p \equiv \pm 1 \bmod 11$, l'idéal (p) est produit de 5 idéaux premiers de norme p, et l'on a le facteur local $L_p(s) = (1-p^{-s})^{-4}$.

c) Dans les autres cas, (p) est premier de norme p^5 dans K, et l'on a le facteur local $L_p(s) = (1 + p^{-s} + p^{-2s} + p^{-3s} + p^{-4s})^{-1}$.
La fonction $L(s) = \zeta_K(s)/\zeta(s)$ admet alors les représentations

(28) $$L(s) = \prod_p L_p(s) = \prod_{j=1}^{4} L(s;\chi_j)$$

où χ_1, χ_2, χ_3, χ_4 sont les caractères non triviaux modulo 11 tels que $\chi_j(-1) = 1$.

Il reste à donner une méthode de calcul de $a_k = L(-k;\chi)$ pour tout entier $k \geqslant 0$ et tout caractère χ non trivial de conducteur f tel que $\chi(-1) = 1$. Le plus commode est d'utiliser la série génératrice

(29) $$\sum_{k=0}^{\infty} a_k\, X^k/k! = \frac{\sum_{n=1}^{f} \chi(n)e^{nX}}{1-e^{fX}}$$

qui fournit les relations $a_0 = a_2 = a_4 = \ldots = 0$ et les formules de récurrence

$$\begin{aligned}
\binom{2}{1} f\, a_1 &= -\sum_{n=1}^{f} \chi(n) n^2 \\
\binom{4}{1} f^3\, a_1 + \binom{4}{3} f\, a_3 &= -\sum_{n=1}^{f} \chi(n) n^4 \\
\binom{6}{1} f^5\, a_1 + \binom{6}{3} f^3\, a_3 + \binom{6}{5} f\, a_5 &= -\sum_{n=1}^{f} \chi(n) n^6 \\
\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots
\end{aligned}$$

11. Lois de décomposition, facteurs locaux, équation fonctionnelle.

Soient K un corps de nombres, r son degré, D son discriminant et $\mathcal{O}$ l'anneau de ses entiers. La répartition des nombres premiers en classes se fait comme suit :

a) p est ramifié s'il divise D et non ramifié s'il ne divise pas D ;

b) si l'on a dans K la décomposition $(p) = \mathfrak{p}_1^{e_1} \ldots \mathfrak{p}_n^{e_n}$ avec $e_1 \geq 1, \ldots, e_n \geq 1$ et des idéaux premiers distincts $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ tels que $N\mathfrak{p}_j = p^{f_j}$, on dit que p appartient à la classe $C(f_1^{e_1}, \ldots, f_n^{e_n})$.
La classe $C(f_1^{e_1}, \ldots, f_n^{e_n})$ est dite non ramifiée si l'on a $e_1 = \ldots = e_n = 1$; alors tous les nombres premiers appartenant à cette classe sont non ramifiés. Si au contraire l'un des exposants e_i est différent de 1, la classe $C(f_1^{e_1}, \ldots, f_n^{e_n})$ est dite ramifiée, elle ne se compose que de nombres premiers ramifiés.

Une classification plus grossière est fournie par les familles et sous-familles. La sous-famille $F_{s,j}$ est la réunion des classes non-ramifiées $C(f_1, \ldots, f_n)$ pour lesquelles le nombre 1 apparaît s fois et le nombre 2 apparaît j fois dans la suite $(f_1, \ldots, f_n)$; la famille F_s est la réunion des sous-familles $F_{s,0}, F_{s,1}, \ldots$. On définit de manière analogue les familles et sous-familles ramifiées $\bar{F}_s$ et $\bar{F}_{s,j}$.

Dans tous les cas, le corps étudié est donné sous la forme $K = \mathbf{Q}(x)$ où x est un entier algébrique. Notons $F(X) = X^r + c_1X^{r-1} + .. + c_r$ le polynôme minimal de x ; ses coefficients $c_1,..,c_r$ sont entiers. Posons $N = (\mathcal{O} : \mathbf{Z}[x])$; alors le discriminant du polynôme F est donné par $\Delta = N^2D$. On dira qu'un nombre premier est <u>exceptionnel</u> (pour x) s'il divise N. Soit p un nombre premier non exceptionnel, et soit F_p la réduction de F modulo p. Alors p appartient à la classe $C(f_1^{e_1},..,f_n^{e_n})$ si et seulement si F_p se décompose dans l'anneau de polynômes $\mathbf{F}_p[X]$ en $F_p = H_1^{e_1}...H_n^{e_n}$ où $H_1,..,H_n$ sont irréductibles, deux à deux distincts et où H_j est de degré f_j.

Nous examinons maintenant en détail les divers cas.

A) <u>Détermination</u> de $L(s) = \zeta_K(s)/\zeta(s)$. On a l'équation fonctionnelle

$$L(1-s) = D^{s-1/2}C(s)^{r-1}\,L(s). \tag{30}$$

Le facteur local associé à un nombre premier p de la classe $C(f_1^{e_1},..,f_n^{e_n})$ est

$$L_p(s) = \frac{1-p^{-s}}{(1-p^{-f_1s})....(1-p^{-f_ns})}. \tag{31}$$

Voir les tables 4 et 5 pour les classes et les facteurs locaux en degré 3,4 ou 5. On constate qu'en degré 3, il y a au plus une classe par famille. En degré 4, la famille F_0 contient deux classes, qui correspondent chacune à une sous-famille; pour les classes ramifiées, la famille $\overline{F}_1$ se scinde en deux sous-familles comprenant chacune une seule classe; la famille $\overline{F}_2$ contient une seule sous-famille et deux classes, mais celles-ci ont même facteur local. En degré 5, on constate aussi que les sous-familles ramifiées $\overline{F}_{1,0}$, $\overline{F}_{1,1}$, $\overline{F}_{2,0}$ et la famille $\overline{F}_3 = \overline{F}_{3,0}$ contiennent chacune deux classes; ceci n'introduit aucune ambiguïté pour le facteur local, à l'exception de la sous-famille $\overline{F}_{1,0} = C(1^5) \cup C(3,1^2)$. Ce cas se rencontre une seule fois, pour $D = p = 38569$ où p est de classe $C(3,1^2)$; il a requis le calcul du p.g.c.d. de F_p et F_p'' .

Enfin, pour tous les corps étudiés, l'anneau des entiers est $\mathbf{Z}[x]$ et il n'y a donc pas de nombre premier exceptionnel.

En résumé, <u>la connaissance des familles suffit en degré</u> 3, <u>et pour les corps étudiés de degré</u> 4 <u>et</u> 5, <u>la connaissance des sous-familles suffit à une exception près</u>.

B) <u>Séries</u> L <u>tordues</u>.

Comme en A), on pose $L(s) = \zeta_K(s)/\zeta(s)$, et l'on note $L_p(s)$ le facteur local associé à p. Soit par ailleurs d le discriminant d'un corps quadratique réel. Si l'on a $L(s) = \sum_{n=1}^{\infty} c_n n^{-s}$, la série tordue est $L(s;\chi_d) = \sum_{n=1}^{\infty} (\frac{d}{n}) c_n n^{-s}$ avec le symbole de Jacobi $(\frac{d}{n})$. Chaque classe C se décompose en 3 sous-classes C_0, C_+, C_- selon que $(\frac{d}{p})$ vaut 0, +1 ou -1; le facteur local est 1 si $p \in C_0$, c'est celui de la classe C si $p \in C_+$ et enfin, il s'obtient en changeant p^{-s} en $-p^{-s}$ si $p \in C_-$. La table 6 donne les sous-classes et les facteurs locaux lorsque K est de degré 3.

Pour obtenir l'équation fonctionnelle, on introduit les corps $K' = \mathbf{Q}(\sqrt{d})$ et $K'' = K(\sqrt{d})$, et l'on utilise la relation

$$L(s;\chi_d) = \frac{\zeta_{K''}(s)\zeta(s)}{\zeta_K(s)\zeta_{K'}(s)} \tag{32}$$

Dans les cas étudiés, d est premier au discriminant D de K ; par suite, le discriminant de K'' est D^2d^3 (et celui de K' est d). On obtient donc l'équation fonctionnelle

$$L(1-s;\chi_d) = (Dd^2)^{s-1/2} C(s)^2 \, L(s;\chi_d). \tag{33}$$

C) <u>Corps de degré</u> 4 <u>avec sous-corps quadratique</u>.

Soit K un corps totalement réel de degré 4, avec un sous-corps quadratique E ; on note D le discriminant de K et d celui de E, et l'on suppose que K n'est pas abélien sur $\mathbf{Q}$. On pose $L(s) = \zeta_K(s)/\zeta_E(s)$, d'où l'équation fonctionnelle

$$(34)\qquad L(1-s) = (D/d)^{s-1/2} C(s)^2\, L(s).$$

La répartition en classes se fait en tenant compte des lois de décomposition d'un nombre premier p à la fois dans E et dans K. On sait que la décomposition dans E est de la forme $C(1^2)$, $C(1,1)$ ou $C(2)$ selon que le symbole de Jacobi $(\frac{d}{p})$ est égal à 0, $+1$ ou -1. On ajoute donc aux symboles de classe dans K un indice 0, $+$ ou $-$ donnant le signe de $(\frac{d}{p})$, indice sous-entendu s'il n'y a pas d'ambiguïté. La table 7 a été déterminée en remarquant qu'un idéal premier p dans E a une décomposition de l'une des formes $p = P^2$, $p = PQ$ ou $p = P$ dans K.

Dans la table 3, on a donné deux nombres x et η tels que $E = \mathbf{Q}(\eta)$, $K = \mathbf{Q}(x)$ et que $(1, x, \eta, x\eta)$ soit une base sur $\mathbf{Z}$ de l'anneau des entiers de K. Il est alors facile de déterminer les <u>nombres premiers exceptionnels</u>. Comme x et η satisfont à des équations du type

$$(35)\qquad \eta^2 = a\eta + b \quad , \quad x^2 = a' + b'x + c'\eta + d'x\eta$$

on a

$$(36)\quad x^3 = (a'b' + bc'd') + (a' + b'^2 + bd'^2)x + (b'c' + a'd' + ac'd')\eta + (2b'd' + c' + ad'^2)x\eta.$$

L'indice du sous-groupe $\mathbf{Z}[x] = \mathbf{Z} + \mathbf{Z}x + \mathbf{Z}x^2 + \mathbf{Z}x^3$ dans l'anneau des entiers $\mathcal{O} = \mathbf{Z} + \mathbf{Z}x + \mathbf{Z}\eta + \mathbf{Z}x\eta$ est égal à la valeur absolue du déterminant de la matrice formée des coefficients de η et $x\eta$ dans l'expression de x^2 et x^3, d'où

$$(37)\qquad (\mathcal{O} : \mathbf{Z}[x]) = |d'(a'd' - b'c') - c'^2|.$$

Prenons par exemple le corps K de discriminant 2225, avec $\eta = \frac{1+\sqrt{5}}{2}$

et $x = \frac{\eta + \sqrt{\eta + 9}}{2}$. On a $(2x-\eta)^2 = \eta + 9$, d'où

(38) $$\eta^2 = \eta + 1 \quad , \quad x^2 = 2 + x\eta,$$

et la matrice $\begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}$ est égale à $\begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}$. On a alors $(\mathcal{O} : \mathbf{Z}[x]) = 2$ et 2 est le seul nombre premier exceptionnel. Comme 2 ne divise pas le discriminant, il n'est pas ramifié. Comme le polynôme $H^2 - H - 1$ est irréductible modulo 2, et qu'on a $x(x-\eta) \equiv 0 \bmod. 2\,\mathcal{O}$ d'après (38), en obtient immédiatement la décomposition $(2) = (x)(x-\eta)$ de (2) en produit de deux idéaux premiers de norme 2^2. Autrement dit, 2 est dans la classe $C(2,2)$ pour K ; comme on a aussi $(\frac{5}{2}) = -1$, le nombre premier 2 appartient à la classe $C(2,2)_-$.

Avec un peu de patience, on traite de manière semblable les autres corps de la table 3, et l'on obtient le tableau suivant (il n'y a pas de nombre premier exceptionnel dans les autres cas) :

Discriminant	2225	4525	5225	5725	7232	7625
Nombre premier exceptionnel	2	3	2	3	2	2
Classe	$C(2,2)_-$	$C(2,2)_-$	$C(2,2)_-$	$C(2,2)_-$	$C(1^2,1^2)_0$	$C(2,2)_-$

12. Algorithme de décomposition des polynômes modulo p.

Un tel algorithme, prévoyant tous les cas de décomposition possibles, a été mis au point par Y. Roy [14] ; il s'agit d'une modification de la méthode de Berlekamp [2] et Knuth [11, p.389], intéressante si le degré est petit et p grand. Comme on l'a noté plus haut, nous n'avons besoin que de la répartition en familles et sous-familles; nous nous contenterons donc d'exposer la partie correspondante de l'algorithme.

Soient p un nombre premier et

$$H(X) = X^r - v_1X^{r-1} - v_2X^{r-2} - \dots - v_{r-1}X - v_r$$

un polynôme de degré r à coefficients dans le corps $\mathbf{F}_p$ à p éléments.

Pour tout entier $n \geq 1$, on sait que $X^{p^n} - X$ est le produit des polynômes irréductibles (dans $\mathbf{F}_p[X]$) dont le degré divise n, chacun avec multiplicité 1. Nous voulons déterminer le nombre s de facteurs de degré 1 de H(X) et le nombre j de facteurs irréductibles de degré 2 de H(X) (compte non tenu des multiplicités). Pour tout entier $n \geq 1$, soit $G_n(X)$ le p.g.c.d. de H(X) et $X^{p^n} - X$ dans $\mathbf{F}_p[X]$, et soit g_n son degré. Il est immédiat qu'on a

$$s = g_1, \quad s + 2j = g_2, \tag{39}$$

et tout revient à déterminer g_1 et g_2. Nous décrivons maintenant les diverses parties de l'algorithme.

A) <u>Algorithme de division modifié</u>.

Il s'agit de la méthode classique, modifiée pour ne pas avoir à faire de division dans le corps $\mathbf{F}_p$. Soient

$$M(X) = m_0X^{\alpha} + m_1X^{\alpha-1} + \ldots + m_{\alpha-1} X + m_{\alpha}$$
$$N(X) = n_0X^{\beta} + n_1X^{\beta-1} + \ldots + n_{\beta-1} X + n_{\beta} \qquad (n_0 \neq 0)$$

deux polynômes dans $\mathbf{F}_p[X]$.

<u>Initialisation</u> : $S_0(X) = M(X)$

<u>Boucle</u> :
$$\begin{cases} e_i = \deg S_i - \deg N \\ \text{si } e_i < 0 \quad \text{fin de procédure} \\ \text{si } e_i \geq 0 \quad f_i \text{ coefficient dominant de } S_i(X) \\ \qquad\qquad\quad S_{i+1}(X) = n_0S_i(X) - f_iX^{e_i}\ N(X). \end{cases}$$

La procédure s'arrête pour une valeur q de i et il existe un entier $h \geq 0$ tel que $S_q(X)$ soit le reste de la division euclidienne de $n_0^h M(X)$ par N(X); on a $n_0^h \neq 0$ dans $\mathbf{F}_p$.

B) <u>Calcul du reste</u> $R_1(X)$ <u>de la division de</u> X^p <u>par</u> H(X).

On définit les matrices

$$A = \begin{pmatrix} v_1 & 1 & 0 & 0 & \cdot & \cdot & 0 & 0 \\ v_2 & 0 & 1 & 0 & \cdot & \cdot & 0 & 0 \\ v_3 & 0 & 0 & 1 & \cdot & \cdot & 0 & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ v_{r-1} & 0 & 0 & 0 & \cdot & \cdot & 0 & 1 \\ v_r & 0 & 0 & 0 & \cdot & \cdot & 0 & 0 \end{pmatrix}, \quad v = \begin{pmatrix} v_1 \\ v_2 \\ v_3 \\ \cdot \\ \cdot \\ \cdot \\ v_{r-1} \\ v_r \end{pmatrix}$$

puis l'on effectue le calcul matriciel $w = A^{p-r}\, v$. Si $w_1,\dots,w_r$ sont les éléments de w , on a

(40) $$R_1(X) = w_1X^{r-1} + w_2X^{r-2} +\dots+ w_{r-1}X + w_r.$$

Nous avons eu à considérer des nombres premiers p de l'ordre de 45000 et r vaut 3,4 ou 5. Le calcul par récurrence de la puissance A^{p-r} est très onéreux; voici une méthode qui requiert $O(\log p)$ opérations et qui nous a permis (en degré 5) de traiter en 3 minutes environ les nombres premiers contenus dans chaque tranche de 1000 nombres.

Si $p = r$, on a $w = v$. Sinon, on écrit

(41) $$p - r = \gamma_0 + 2\gamma_1 + 2^2\gamma_2 +\dots+ 2^m\gamma_m$$

avec des γ_i égaux à 0 ou 1 et $\gamma_m = 1$. On définit ensuite les matrices $B_1,\dots,B_m$ de type $r \times r$ par

$$B_1 = A,\quad B_2 = B_1^2,\dots,B_m = B_{m-1}^2,\quad B_{m+1} = B_m^2.$$

Les matrices v_0, $v_1,\dots,v_{m+1}$ de type $r \times 1$ sont définies par

$$v_0 = v,\quad v_j = \begin{cases} v_{j-1} & \text{si} \quad \gamma_{j-1} = 0 \\ B_jv_{j-1} & \text{si} \quad \gamma_{j-1} = 1. \end{cases}$$

On a finalement $w = v_{m+1}$.

C) <u>Calcul du reste</u> $R_2(X)$ <u>de la division de</u> $R_1(R_1(X))$ <u>par</u> $H(X)$.

Il s'agit en fait du schéma de Horner appliqué à l'anneau quotient $\mathbf{F}_p[X]/(H(X))$. On définit les polynômes $T_0(X), T_1(X),\ldots,T_{r-1}(X)$ de degré $\leqslant r - 1$ par

$T_0(X) = R_1(X)$,

$T_i(X)$ est le reste de la division de $X\,T_{i-1}(X)$ par $H(X)$ pour $1 \leqslant i \leqslant r-1$.

On pose ensuite, avec les notations de (40),

$$U_1(X) = w_1R_1(X) + w_2 \tag{42}$$

et si

$$U_i(X) = a_1X^{r-1} + a_2X^{r-2} +\ldots+ a_{r-1}X + a_r, \tag{43}$$

on pose

$$U_{i+1}(X) = a_1T_{r-1}(X) + a_2T_{r-2}(X) +\ldots+ a_{r-1}T_1(X) + a_rT_0(X) + w_{i+2}. \tag{44}$$

Il est immédiat que modulo $H(X)$ on a $T_i(X) \equiv X^iR_1(X)$ d'où $U_{i+1}(X) \equiv U_i(X)R_1(X) + w_{i+2}$ et donc $U_{r-1}(X) \equiv R_1(R_1(X))$. On a par conséquent $R_2 = U_{r-1}$.

D) <u>Calcul de</u> g_1 <u>et</u> g_2.

Par construction, on a $X^p \equiv R_1(X)$ mod.$H(X)$, d'où

$$G(X^p) \equiv G(R_1(X)) \quad \text{mod.}H(X) \tag{45}$$

pour tout polynôme $G(X)$ dans $\mathbf{F}_p[X]$. Remplaçons successivement $G(X)$ par X^p et $R_1(X)$; on obtient

$$X^{p^2} \equiv R_1(X)^p \quad \text{mod.}H(X) \tag{46}$$

(47) $$R_1(X^p) \equiv R_1(R_1(X)) \quad \mathrm{mod}.H(X),$$

et comme $R_1(X^p) = R_1(X)^p$, on a finalement

(48) $$X^{p^2} \equiv R_1(R_1(X)) \equiv R_2(X) \quad \mathrm{mod}.H(X).$$

Par suite, le p.g.c.d. $G_n(X)$ de $X^{p^n} - X$ et $H(X)$ est aussi celui de $R_n(X) - X$ et $H(X)$ (pour $n = 1,2$). Pour calculer $G_n(X)$, on utilise l'algorithme classique d'Euclide et l'on voit immédiatement qu'on ne change pas le résultat (à multiplication près par un élément non nul de $\mathbb{F}_p$) si l'on utilise partout l'algorithme de division "modifié" décrit en A).

13. Calcul numérique de L(1-2n).

On note K un corps totalement réel de degré r = 3,4 ou 5, et de discriminant D, et l'on suppose connue la répartition des nombres premiers en classes; on pose $L(s) = \zeta_K(s)/\zeta(s)$. Les autres cas sont analogues. Le calcul de L(1-2n) se fonde sur les formules suivantes :

(49) $$L(1-2n) = (-1)^{n(r-1)} c_n L(2n)$$

(50) $$L(2n) = \prod_{j=2}^{\infty} L_j(2n)$$

(51) $$L_j(2n) = \begin{cases} (1-p^{-2n}) \prod_{k=1}^{t} (1-p^{-2n f_k})^{-1} & \text{si } j \in C(f_1^{e_1},\dots,f_t^{e_t}) \\ 1 & \text{si } j \text{ n'est pas premier.} \end{cases}$$

(52) $$c_1 = \frac{D\sqrt{D}}{(2\pi^2)^{r-1}}$$

(53) $$c_n = \frac{D^2}{(2\pi^2)^{r-1}} B_n c_{n-1} \quad \text{avec} \quad B_n = [(n-1)(2n-1)]^{r-1}.$$

Enfin, on note $r_p(2n)$ et $s_p(2n)$ le numérateur et le dénominateur du nombre rationnel $L_p(2n)$.

Nos calculs ont été effectués en "arithmétique entière", c'est-à-dire que l'on connaît exactement la valeur de la somme, de la différence ou du produit de deux nombres entiers, et la partie entière $a \div b$ du quotient de l'entier a par l'entier b. Nous pouvions en principe traiter des entiers compris entre -10^{600} et 10^{600} ce qui excédait largement les besoins du calcul.

Détaillons maintenant les calculs et l'estimation de l'erreur. On choisit des entiers strictement positifs P,α,β,γ et l'on pose

(54) $$\varepsilon = \frac{r-1}{(2n-1)P^{2n-1}} , \quad \varepsilon^* = e^{\varepsilon} - 1.$$

On s'est arrangé pour avoir toujours $\varepsilon < \frac{1}{5000}$, ce qui permet de négliger en toute sécurité ε^2 dans les calculs qui suivent. Nous définirons des nombres $F,Z,\ldots$ dont les valeurs approchées calculées sont notées $F^*,Z^*,\ldots$

a) Calcul de $F = 10^{\alpha} L(2n)$: on tronque le produit infini en posant $L_1 = \prod_{j=2}^{P} L_j(2n)$. Si un nombre premier p appartient à la classe $C(f_1^{e_1},\ldots,f_t^{e_t})$ on a $r = \sum_{k=1}^{t} e_k f_k$, d'où $f_1 + \ldots + f_t \leq r$; de plus, on a $0 < p^{-2nf_k} < 1$ et comme $0 < t < 1$ entraîne $1 \leq \frac{1}{1-t^f} \leq \frac{1}{1-t}$, on obtient l'estimation suivante du facteur local (voir (51))

(55) $$1 - p^{-2n} \leq L_p(2n) \leq \left(\frac{1}{1-p^{-2n}}\right)^{r-1}.$$

On a $L(2n)/L_1 = \prod_{p>P} L_p(2n)$, d'où

(56) $$\left[\prod_{p>P} \frac{1}{1-p^{-2n}}\right]^{-1} \leq \frac{L(2n)}{L_1} \leq \left[\prod_{p>P} \frac{1}{1-p^{-2n}}\right]^{r-1} ;$$

or l'unicité du développement en facteurs premiers entraîne

$$\prod_{p>P} \frac{1}{1-p^{-2n}} = \sum_{a\in S} a^{-2n} \leq 1 + \sum_{a=P+1}^{\infty} a^{-2n}$$

$$\leq 1 + \int_P^{\infty} x^{-2n}dx = 1 + \frac{1}{(2n-1)P^{2n-1}} = 1 + \frac{\varepsilon}{r-1}$$

(on note S l'ensemble des entiers $a \geq 1$ sans facteur premier $\leq P$). En conclusion, on a

$$(57) \qquad (1 + \frac{\varepsilon}{r-1})^{-1} - 1 \leq \frac{L(2n)}{L_1} - 1 \leq (1 + \frac{\varepsilon}{r-1})^{r-1} - 1 .$$

La valeur approchée F^* de $10^\alpha L_1$ est calculée par le schéma

$$F_1 = 10^\alpha$$
$$F_j = [F_{j-1}\, r_j(2n)] \div s_j(2n) \qquad \text{pour } j = 2,3,\ldots,P$$
$$F^* = F_P .$$

En ajoutant à l'erreur de troncation donnée par (57) l'erreur d'arrondi due aux divisions, on obtient l'estimation suivante de l'erreur

$$(58) \qquad \left|\frac{F^*}{F} - 1\right| \leq \varepsilon^* + (1 + \varepsilon^*)\, \frac{P-1}{10^\alpha}\, \zeta(2n) .$$

b) <u>Calcul de</u> $Z = 10^\beta \sqrt{D}$: soit u la partie entière de $\sqrt{D}$, d'où $D = u^2 + v$ avec $0 \leq v \leq 2u$. On pose

$$(59) \qquad T = 10^{\beta+6} \sqrt{D} = 10^{\beta+6} u \sqrt{1 + \frac{v}{u^2}} ,$$

et l'on développe le racine carrée par la série du binôme. Voici le schéma du calcul

$$G_0 = 10^{\beta+6} u$$
$$G_k = [(3-2k) v\, G_{k-1}] \div 2ku^2 \qquad \text{pour } k \geq 1$$
N plus petit entier k tel que $G_{k+1} = 0$
$$Z^* = [G_0 + G_1 + \ldots + G_N] \div 10^6 .$$

On a l'erreur

$$(60) \qquad \left|\frac{Z^*}{Z} - 1\right| \leq \frac{1}{10^\beta \sqrt{D}} \left[\frac{7(\beta + \log_{10} u) + 50}{10^6} + 1\right] .$$

c) <u>Calcul de</u> $K = 10^\beta (2\pi^2)^{r-1}$: au moyen d'une table donnant π avec 200 décimales, on définit $U_1 = 10^{\beta+6}\pi$. On calcule successivement

$$U_2 = (2U_1^2) \div 10^{\beta+6}$$
$$U_3 = (U_2U_2) \div 10^{\beta+6}$$
$$U_4 = (U_2U_3) \div 10^{\beta+6}$$
$$U_5 = (U_2U_4) \div 10^{\beta+6}$$

et l'on pose $K^* = U_r \div 10^6$ si le degré est égal à r. On a l'erreur

(61) $$\left|\frac{K^*}{K} - 1\right| < \frac{2}{10^\beta(2\pi^2)^{r-1}} .$$

Dans les conditions usuelles, ceci signifie que $\sqrt{D}$ et $(2\pi^2)^{r-1}$ ont été calculés à $2.10^{-\beta}$ près.

d) Calcul de $C_n = 10^\gamma c_n$: on utilise les formules de récurrence (52) et (53) sous la forme suivante

$$A^* = (10^{2\beta}D^2) \div K^* \quad \text{(valeur approchée de } A = \frac{10^\beta D^2}{(2\pi^2)^{r-1}})$$
$$C_1^* = 10^\gamma DZ^* \div K^*$$
$$C_n^* = (A^*B_n\, C_{n-1}^*) \div 10^\beta .$$

L'erreur se calcule selon la formule

(62) $$\left|\frac{C_n^*}{C_n} -1\right| \leqslant n\left|\frac{K^*}{K} - 1\right| + \frac{n-1}{A} + \frac{1}{C_1} + \frac{n-1}{C_2} + \left|\frac{Z^*}{Z} - 1\right| ,$$

c'est-à-dire

(63) $$\left|\frac{C_n^*}{C_n} - 1\right| < \left\{\frac{2n}{(2\pi^2)^{r-1}} + \frac{(n-1)(2\pi^2)^{r-1}}{D^2}\right\} 10^{-\beta}$$
$$+ \left\{\frac{(2\pi^2)^{r-1}}{D^{3/2}} + \frac{(n-1)(2\pi^2)^{2r-2}}{3^{r-1}\, D^{7/2}}\right\} 10^{-\gamma} + \left\{\frac{7(\beta + \log_{10} u) + 50}{10^6} +1\right\} \frac{10^{-\beta}}{\sqrt{D}}$$

e) Calcul de $L = 10^{10}|L(1-2n)|$: on utilise l'équation fonctionnelle (49), sous la forme de la valeur approchée

(64) $$L^* = (F^*C_n^*) \div 10^{\alpha+\gamma-10}.$$

Dans les cas étudiés, on a $D \geqslant 49$ d'où $A \geqslant 6.10^{\beta}$, $C_1 \geqslant \frac{3}{4}.10^{\gamma}$, et l'on n'a considéré que le cas $n \leqslant 29$. Les nombres α, β, γ de décimales retenues sont définis en fonction de P par

$$\beta = \gamma = \alpha - 6 \quad \text{et} \quad \alpha - 9 = \text{partie entière de } \log_{10} \frac{2n-1}{r-1} + (2n-1) \log_{10} P.$$

Les formules (58) et (63) montrent que dans ces conditions et pour $P < 45000$, l'erreur d'arrondi est inférieure au dixième de l'erreur de troncation, d'où l'estimation finale de l'erreur

(65) $$\left|\frac{L^*}{L} - 1\right| < 2\varepsilon = \frac{2(r-1)}{(2n-1)P^{2n-1}} .$$

14. Caractère significatif des résultats obtenus.

Les fonctions L considérées ont un développement en série de Dirichlet

(66) $$L(s) = \sum_{n=1}^{\infty} c_n n^{-s},$$

dont les coefficients c_n sont "petits". Il en résulte que pour $s \geqslant 10$ par exemple, la série précédente converge très rapidement et a une somme très voisine de $c_1 = 1$. Mais l'équation fonctionnelle introduit un facteur $\Delta^{s-1/2}C(s)^d$ qui croît très rapidement avec s, et ceci d'autant plus que Δ et d sont plus grands. Dans certains des cas étudiés, ce facteur est de l'ordre de 10^{170}, et il nous faut donc sommer la série (66) (ou le produit infini équivalent) avec une erreur inférieure à 10^{-180}; ceci requiert environ 45000 termes de la série.

Les nombres $L(1-2n)$ ont été calculés avec 10 chiffres après la virgule, et la formule (65) montre qu'avec un P convenable (choisi en fonction de n), on peut faire en sorte que $|L^* - L| < 10^{-5}$ (sauf pour $n = 1$, où nous n'avons que $|L^* - L| < 10^{-3}$). Par suite, les 5 premiers chiffres après la virgule (sauf pour $n = 1$) sont exacts. Dans tous les cas étudiés, ces chiffres sont tous égaux à 0 ou tous égaux à 9. Autrement dit, nous avons <u>prouvé</u> que L(1-2n) diffère d'un entier de moins de 10^{-5}. Comme ces nombres sont calculés de manière indépendante, l'existence des congruences très précises sur les différences itérées ne laisse aucun doute sur l'intégralité des nombres L(1-2n).

BIBLIOGRAPHIE

[1] Y.AMICE et J.FRESNEL, Fonctions zêta p-adiques des corps de nombres abéliens réels, "Acta Arithm." 20 (1972), p.353-384.

[2] E.R.BERLEKAMP, Factoring polynomials over large finite fields, Math. Comp. 24 (1970), p.713-735.

[3] P.CARTIER et Y.ROY, On the enumeration of quintic fields with small discriminant, à paraître pour le jubilé de Hasse.

[4] J.COATES et S.LICHTENBAUM, On l-adic zêta functions, à paraître aux Annals of Mathematics.

[5] H.COHN, A numerical study of quintics of small discriminant, Comm. Pure Appl. Math. 8, (1955), p.377-385.

[6] B.N.DELONE et D.K.FADDEEV, The theory of irrationalities of the third degree, Transl. of Math. Monographs, 10, Amer. Math. Soc. Providence, 1964.

[7] J.FRESNEL, Nombres de Bernoulli et fonctions L p-adiques, Ann. Inst. Fourier, 17 (1967), p.281-333.

[8] K.IWASAWA, On p-adic L-functions, Annals of Maths, 89 (1969), p.198-205.

[9] K.IWASAWA, Lectures on p-adic L-functions, Annals Math. Studies, Princeton University Press, 1972.

[10] H.KLINGEN, Über die Werte der Dedekindschen Zetafunktionen, Math. Annalen, 145 (1962), p.265-272.

[11] D.E.KNUTH, The art of computer programming, vol.2 : Seminumerical algorithms, Addison-Wesley, Reading, 1969.

[12] T.KUBOTA et H.W.LEOPOLDT, Eine p-adische Theorie der Zetawerte, Journ. Crelle, 214/215 (1964), p.328-339.

[13] H.W.LEOPOLDT, Eine Verallgemeinerung der Bernoullischen Zahlen, Abh. Math. Sem. Hamburg, 22 (1958), p.131-140.

[14] Y.ROY, Algorithme donnant la structure de la factorisation modulo p d'un polynôme, Séminaire d'informatique de Strasbourg, 1972 (polycopié).

[15] J.-P.SERRE, Formes modulaires et fonctions zêta p-adiques, dans ce même volume.

[16] C.L.SIEGEL, Berechnung von Zetafunktionen an ganzzahligen Stellen, Göttingen Nach. 10 (1969), p.87-102.

[17] C.L.SIEGEL, Über die Fourierschen Koeffizienten von Modulformen, Göttingen Nach. 3 (1970),p.15-56.

T A B L E S

TABLE 1

Corps de degré 3 non cycliques

Discriminant	Equation	N
$148 = 2^2.37$	$x^3 - x^2 - 3x + 1$	57
229	$x^3 - 4x - 1$	55
257	$x^3 - x^2 - 4x + 3$	55
$316 = 2^2.79$	$x^3 - x^2 - 4x + 2$	53
$321 = 3.107$	$x^3 - x^2 - 4x + 1$	53
$404 = 2^2.101$	$x^3 - x^2 - 5x - 1$	53
$469 = 7.67$	$x^3 - x^2 - 5x + 4$	51
$473 = 11.43$	$x^3 - 5x - 1$	51
$564 = 2^2.3.47$	$x^3 - x^2 - 5x + 3$	51
$568 = 2^3.71$	$x^3 - x^2 - 6x - 2$	51
$621 = 3^3.23$	$x^3 - 6x - 3$	29
$697 = 17.41$	$x^3 - 7x - 5$	"
733	$x^3 - x^2 - 7x + 8$	"
$756 = 2^2.3^3.7$	$x^3 - 6x - 2$	"
761	$x^3 - x^2 - 6x - 1$	"
$785 = 5.157$	$x^3 - x^2 - 6x + 5$	"
$788 = 2^2.197$	$x^3 - x^2 - 7x - 3$	"
$837 = 3^3.31$	$x^3 - 6x - 1$	"
$892 = 2^2.223$	$x^3 - x^2 - 8x + 10$	"
$940 = 2^2.5.47$	$x^3 - 7x - 4$	"
$985 = 5.197$	$x^3 - x^2 - 6x + 1$	"
$993 = 3.331$	$x^3 - x^2 - 6x + 3$	"
$1016 = 2^3.127$	$x^3 - x^2 - 6x + 2$	"
$1076 = 2^2.269$	$x^3 - 8x + 6$	"
$1101 = 3.367$	$x^3 - x^2 - 9x + 12$	"
1129	$x^3 - 7x - 3$	"
1229	$x^3 - x^2 - 7x + 6$	"
$1257 = 3.419$	$x^3 - x^2 - 8x + 9$	"

TABLE 2

Corps de degré 4 à groupe de Galois symétrique

Discriminant	Equation
1957 = 19.103	$x^4 - 4x^2 + x + 1$
2777	$x^4 - x^3 - 4x^2 + x + 2$
3981 = 3.1327	$x^4 - x^3 - 4x^2 + 2x + 1$
5744 = 2^4.359	$x^4 - 5x^2 + 2x + 1$
6224 = 2^4.389	$x^4 - 2x^3 - 4x^2 + 2x + 2$
6809 = 11.619	$x^4 - 5x^2 + x + 1$
7053 = 3.2351	$x^4 - 2x^3 - 4x^2 + 3x + 3$
7537	$x^4 - x^3 - 5x^2 + 4x + 3$
8069	$x^4 - x^3 - 5x^2 + 5x + 1$

TABLE 3

Corps de degré 4 contenant un sous-corps quadratique

D	d	η	x	Equation
725	5	$\frac{1+\sqrt{5}}{2}$	$\frac{\eta+\sqrt{\eta+5}}{2}$	$x^4 - x^3 - 3x^2 + x + 1$
2225	5	$\frac{1+\sqrt{5}}{2}$	$\frac{\eta+\sqrt{\eta+9}}{2}$	$x^4 - x^3 - 5x^2 + 2x + 4$
2525	5	$\frac{1+\sqrt{5}}{2}$	$\frac{1+\sqrt{4\eta+9}}{2}$	$x^4 - 2x^3 - 4x^2 + 5x + 5$
2624	8	$\sqrt{2}$	$\frac{\eta+1+\sqrt{2\eta+7}}{2}$	$x^4 - 2x^3 - 3x^2 + 2x + 1$
4205	29	$\frac{1+\sqrt{29}}{2}$	$\frac{\eta+\sqrt{\eta+3}}{2}$	$x^4 - x^3 - 5x^2 - x + 1$
4352	8	$\sqrt{2}$	$\frac{\eta+\sqrt{-4\eta+10}}{2}$	$x^4 - 6x^2 + 4x + 2$
4400	5	$\frac{1+\sqrt{5}}{2}$	$\sqrt{\eta+3}$	$x^4 - 7x^2 + 11$
4525	5	$\frac{1+\sqrt{5}}{2}$	$\frac{\eta+\sqrt{\eta+13}}{2}$	$x^4 - x^3 - 7x^2 + 3x + 9$
4752	12	$\sqrt{3}$	$\frac{1+\sqrt{4\eta+9}}{2}$	$x^4 - 2x^3 - 3x^2 + 4x + 1$
5125	5	$\frac{1+\sqrt{5}}{2}$	$\frac{1+\sqrt{4\eta+13}}{2}$	$x^4 - 2x^3 - 6x^2 + 7x + 11$
5225	5	$\frac{1+\sqrt{5}}{2}$	$\frac{\eta+\sqrt{5\eta+13}}{2}$	$x^4 - x^3 - 8x^2 + x + 11$
5725	5	$\frac{1+\sqrt{5}}{2}$	$\frac{\eta+\sqrt{-3\eta+17}}{2}$	$x^4 - x^3 - 8x^2 + 6x + 11$
7168	8	$\sqrt{2}$	$\sqrt{\eta+3}$	$x^4 - 6x^2 + 7$
7232	8	$\sqrt{2}$	$\frac{\eta+1+\sqrt{2\eta+11}}{2}$	$x^4 - 2x^3 - 5x^2 + 4x + 4$
7488	12	$\sqrt{3}$	$\frac{\eta+1+\sqrt{2\eta+8}}{2}$	$x^4 - 2x^3 - 4x^2 + 2x + 1$
7600	5	$\frac{1+\sqrt{5}}{2}$	$\sqrt{\eta+4}$	$x^4 - 9x^2 + 19$
7625	5	$\frac{1+\sqrt{5}}{2}$	$\frac{\eta+\sqrt{\eta+17}}{2}$	$x^4 - x^3 - 9x^2 + 4x + 16$
8112	13	$\frac{1+\sqrt{13}}{2}$	$\sqrt{\eta+4}$	$x^4 - 5x^2 + 3$

D discriminant du corps K = $\mathbf{Q}(x)$
d discriminant du corps E = $\mathbf{Q}(\eta)$

TABLE 4

Facteurs locaux associés aux classes non ramifiées

Degré	Classe	Famille	Facteur local
$r = 3$	C(3)	F_0	$\frac{p^{2s}}{p^{2s}+p^s+1}$
	C(2,1)	F_1	$\frac{p^{2s}}{p^{2s}-1}$
	C(1,1,1)	F_3	$\frac{p^{2s}}{p^{2s}-2p^s+1}$
$r = 4$	C(4)	$F_{0,0}$ } F_0	$\frac{p^{3s}}{p^{3s}+p^{2s}+p^s+1}$
	C(2,2)	$F_{0,2}$ } F_0	$\frac{p^{3s}}{p^{3s}+p^{2s}-p^s-1}$
	C(3,1)	F_1	$\frac{p^{3s}}{p^{3s}-1}$
	C(2,1,1)	F_2	$\frac{p^{3s}}{p^{3s}-p^{2s}-p^s+1}$
	C(1,1,1,1)	F_4	$\frac{p^{3s}}{p^{3s}-3p^{2s}+3p^s-1}$
$r = 5$	C(5)	$F_{0,0}$ } F_0	$\frac{p^{4s}}{p^{4s}+p^{3s}+p^{2s}+p^s+1}$
	C(3,2)	$F_{0,1}$ } F_0	$\frac{p^{4s}}{p^{4s}+p^{3s}-p^s-1}$
	C(4,1)	$F_{1,0}$ } F_1	$\frac{p^{4s}}{p^{4s}-1}$
	C(2,2,1)	$F_{1,2}$ } F_1	$\frac{p^{4s}}{p^{4s}-2p^{2s}+1}$
	C(3,1,1)	F_2	$\frac{p^{4s}}{p^{4s}-p^{3s}-p^s+1}$
	C(2,1,1,1)	F_3	$\frac{p^{4s}}{p^{4s}-2p^{3s}+2p^s-1}$
	C(1,1,1,1,1)	F_5	$\frac{p^{4s}}{p^{4s}-4p^{3s}+6p^{2s}-4p^s+1}$

TABLE 5

Facteurs locaux associés aux classes ramifiées

Degré	Classe	Famille	Facteur local
$r = 3$	$C(1^3)$	$\overline{F}_1$	1
	$C(1^2,1)$	$\overline{F}_2$	$\frac{p^s}{p^s-1}$
$r = 4$	$C(2^2)$	$\overline{F}_0$	$\frac{p^s}{p^s+1}$
	$C(2,1^2)$	$\overline{F}_{1,1}$ ($\overline{F}_1$)	$\frac{p^{2s}}{p^{2s}-1}$
	$C(1^4)$	$\overline{F}_{1,0}$ ($\overline{F}_1$)	1
	$C(1^3,1)$	$\overline{F}_2$	$\frac{p^s}{p^s-1}$
	$C(1^2,1^2)$	$\overline{F}_2$	$\frac{p^s}{p^s-1}$
	$C(1^2,1,1)$	$\overline{F}_3$	$\frac{p^{2s}}{(p^s-1)^2}$
$r = 5$	$C(1^5)$	$\overline{F}_{1,0}$ ($\overline{F}_1$)	1
	$C(3,1^2)$	$\overline{F}_{1,0}$ ($\overline{F}_1$)	$\frac{p^{3s}}{p^{3s}-1}$
	$C(2^2,1)$	$\overline{F}_{1,1}$ ($\overline{F}_1$)	$\frac{p^{2s}}{p^{2s}-1}$
	$C(2,1^3)$	$\overline{F}_{1,1}$ ($\overline{F}_1$)	$\frac{p^{2s}}{p^{2s}-1}$
	$C(1^4,1)$	$\overline{F}_{2,0}$ ($\overline{F}_2$)	$\frac{p^s}{p^s-1}$
	$C(1^3,1^2)$	$\overline{F}_{2,0}$ ($\overline{F}_2$)	$\frac{p^s}{p^s-1}$
	$C(2,1^2,1)$	$\overline{F}_{2,1}$ ($\overline{F}_2$)	$\frac{p^{3s}}{p^{3s}-p^{2s}-p^s+1}$

TABLE 5 (suite)

Facteurs locaux associés aux classes ramifiées

Degré	Classe	Famille	Facteur local
$r = 5$	$C(1^3,1,1)$	$\overline{F}_3$	$\frac{p^{2s}}{(p^s-1)^2}$
	$C(1^2,1^2,1)$		$\frac{p^{2s}}{(p^s-1)^2}$
	$C(1^2,1,1,1)$	$\overline{F}_4$	$\frac{p^{3s}}{(p^s-1)^3}$

TABLE 6

Facteurs locaux pour $L(s;\chi_d)$ avec $L(s) = \zeta_K(s)/\zeta(s)$

Sous-classes	Facteur local
$C(3)_0$	1
$C(3)_+$	$\frac{p^{2s}}{p^{2s}+p^s+1}$
$C(3)_-$	$\frac{p^{2s}}{p^{2s}-p^s+1}$
$C(2,1)_0$	1
$C(2,1)_+$	$\frac{p^{2s}}{p^{2s}-1}$
$C(2,1)_-$	$\frac{p^{2s}}{p^{2s}-1}$
$C(1,1,1)_0$	1
$C(1,1,1)_+$	$\frac{p^{2s}}{(p^s-1)^2}$
$C(1,1,1)_-$	$\frac{p^{2s}}{(p^s+1)^2}$
$C(1^3)_0$	1
$C(1^3)_+$	1
$C(1^3)_-$	1

TABLE 6 (suite)

Facteurs locaux pour $L(s;\chi_d)$ avec $L(s) = \zeta_K(s)/\zeta(s)$

Sous-classes	Facteur local
$C(1^2,1)_0$	1
$C(1^2,1)_+$	$\frac{p^s}{p^s-1}$
$C(1^2,1)_-$	$\frac{p^s}{p^s+1}$

TABLE 7

Facteurs locaux pour $L(s) = \zeta_K(s)/\zeta_E(s)$

Classes non ramifiées	Classe du sous-corps	Facteur local
$C(4)$	$C(2)$	$\frac{p^{2s}}{p^{2s}+1}$
$C(2,2)_+$	$C(1,1)$	$\frac{p^{2s}}{(p^s+1)^2}$
$C(2,2)_-$	$C(2)$	$\frac{p^{2s}}{p^{2s}-1}$
$C(2,1,1)$	$C(1,1)$	$\frac{p^{2s}}{p^{2s}-1}$
$C(1,1,1,1)$	$C(1,1)$	$\frac{p^{2s}}{(p^s-1)^2}$
Classes ramifiées		
$C(2^2)_0$	$C(1^2)$	$\frac{p^s}{p^s+1}$
$C(2^2)_-$	$C(2)$	1
$C(2,1^2)$	$C(1,1)$	$\frac{p^s}{p^s+1}$
$C(1^4)$	$C(1^2)$	1
$C(1^2,1^2)_0$	$C(1^2)$	$\frac{p^s}{p^s-1}$
$C(1^2,1^2)_+$	$C(1,1)$	1
$C(1^2,1,1)$	$C(1,1)$	$\frac{p^s}{p^s-1}$

TABLE 8

FONCTION ZÊTA DU CORPS DE DEGRÉ 3

ET DISCRIMINANT 148

(groupe de Galois non cyclique)

1) Répartition en classes des nombres premiers < 2000

2) Valeurs de $L(1-2n)$ pour $1 \leq n \leq 29$, avec $L(s) = \zeta_K(s)/\zeta(s)$

3) Valuation des différences itérées

4) Valeurs extrapolées de $L^{(p)}(1)$

5) Valeurs de $L'(1-2n)$ pour $1 \leq n \leq 15$, avec $L'(s) = L(s;\chi_5)$

6) Valuation des différences itérées pour $L'(s)$

7) Intercalement de $L(s)$ et $L'(s)$

RÉPARTITION EN CLASSES DES NOMBRES PREMIERS INFÉRIEJRS A 2000 R= 3 D= 148 .

CLASSE (3) .

3	7	11	41	47	53	71	73	83	101	127	149	157	173	181	197	211
223	229	263	271	307	337	359	373	379	397	419	433	443	509	521	571	593
599	613	617	619	641	659	673	677	719	733	739	743	751	761	773	787	811
821	887	937	953	983	1009	1033	1039	1063	1109	1117	1151	1181	1187	1193	1217	1231
1249	1291	1321	1381	1399	1409	1427	1439	1447	1453	1459	1471	1481	1483	1487	1543	1579
1619	1621	1637	1699	1709	1723	1801	1823	1861	1871	1913	1931	1933	1949	1951	1987	1997
1999																

CLASSE (2 , 1) .

5	13	17	19	23	29	31	43	59	61	79	89	97	103	109	113	131
163	167	179	191	193	199	227	239	241	251	257	277	281	283	311	313	331
347	353	383	389	401	409	421	431	439	449	457	461	463	467	479	487	499
503	523	541	547	557	563	569	577	587	607	631	643	647	653	661	683	701
709	727	757	769	797	809	827	829	853	857	859	883	907	911	919	947	967
977	991	997	1013	1019	1021	1031	1049	1051	1087	1091	1093	1097	1123	1129	1153	1171
1201	1213	1223	1229	1277	1289	1297	1301	1303	1319	1327	1361	1367	1423	1429	1451	1493
1499	1511	1523	1531	1549	1559	1567	1571	1583	1597	1609	1613	1657	1663	1667	1697	1721
1733	1741	1747	1753	1759	1789	1811	1831	1867	1873	1879	1889	1901	1907	1979	1993	

CLASSE (1 , 1 , 1) .

67	107	137	139	151	233	269	293	317	349	367	491	601	691	823	839	863
877	881	929	941	971	1061	1069	1103	1163	1237	1259	1279	1283	1307	1373	1433	1489
1553	1601	1607	1627	1669	1693	1777	1783	1787	1847	1877	1973					

CLASSE (1^3)
2

CLASSE $(1^2,1)$
37

VALEURS DE L(1-2N) .   R= 3 D= 148 .

L(-1) =	4	DIVISIBLE PAR	2(2)
L(-3) =	2308	DIVISIBLE PAR	2(2).577
L(-5) =	131 25124	DIVISIBLE PAR	2(2).19.373.463
L(-7) =	32 57915 08228	DIVISIBLE PAR	2(2)
L(-9) =	23 73928 47471 97444	DIVISIBLE PAR	2(2).43.71
L(-11) =	40 37044 12801 87261 30948	DIVISIBLE PAR	2(2).31.37
L(-13) =	138 07573 92562 97487 08699 67364	DIVISIBLE PAR	2(2).23
L(-15) =	855 77580 68859 93637 68688 37359 66468	DIVISIBLE PAR	2(2).6229
L(-17) =	8898 19213 47240 73923 64587 95526 78337 22884	DIVISIBLE PAR	2(2).1889.6763
L(-19) =	1 46270 90535 78676 01466 32391 62984 71198 49198 30788	DIVISIBLE PAR	2(2)
L(-21) =	36 26272 92815 97320 55316 93916 13438 21540 94812 07835 52004	DIVISIBLE PAR	2(2).41.67.4283
L(-23) =	1304 86468 89866 58825 06745 21804 41538 72810 65271 12017 48744 59908	DIVISIBLE PAR	2(2).19.181.587
L(-25) =	66019 45531 93938 22160 12256 45428 55744 87064 46784 87823 32305 96325 42724	DIVISIBLE PAR	2(2).83
L(-27) =	45 72462 14379 91130 75116 96021 93333 96616 66471 58773 49714 24255 36323 65057 09828	DIVISIBLE PAR	2(2).89.109.1471
L(-29) =	4237 07483 35234 88560 60239 03826 30120 36087 01505 32574 18235 66047 77644 09494 00729 83044	DIVISIBLE PAR	2(2).37.41

VALEURS DE L(1-2N) . R= 3 D= 148 .

```
L(-31) =     5 15034 10543 47877 15084 06442 27598 66995 93038
         51822 53121 17011 03749 39644 95194 81553 44077 56548  DIVISIBLE PAR   2(2).71.193.2203

L(-33) =   807 17514 91498 64882 81700 02476 11362 70182 68786
         59779 08725 19242 62665 91972 71461 07874 70957 70035
         60964                                                  DIVISIBLE PAR   2(2).157.3499

L(-35) =     1 60644 42661 30456 11048 55548 51331 70802 38773
         94424 48288 78615 61944 91707 87547 68629 87677 86978
         58580 39702 96068                                      DIVISIBLE PAR   2(2).23

L(-37) =   400 56967 65819 18056 11233 74816 15911 05807 10144
         46491 80133 58431 27712 01122 70607 96275 08493 67564
         09075 76491 88525 64484                                DIVISIBLE PAR   2(2).479

L(-39) =     1 23645 53397 21319 47860 63045 73607 74984 42144
         49034 95981 51703 42700 77018 84152 33670 21162 73676
         22199 50506 50394 39379 75737 44388                    DIVISIBLE PAR   2(2).113

L(-41) =   467 37996 08783 83635 91371 82314 35417 58555 82989
         12207 36886 18764 94131 29854 34914 59872 03228 74098
         60921 45309 17036 68903 45213 12770 81604              DIVISIBLE PAR   2(2).19.31.79.107

L(-43) =     2 14244 42871 50149 19068 79719 50096 32736 48788
         65445 86124 77201 27016 18343 40777 72540 57072 60857
         52037 09601 49023 34694 53323 07843 42507 04324 37508  DIVISIBLE PAR   2(2).137

L(-45) =  1180 43988 48751 59418 21739 63043 11266 81543 81624
         95849 46627 08419 89423 37050 04977 79054 19021 55583
         86364 76995 17745 56529 57814 54659 35801 58797 07182
         00324                                                  DIVISIBLE PAR   2(2).241

L(-47) =     7 75459 66225 78712 01110 46882 70646 68379 13810
         70807 74959 71171 43762 99710 51685 60196 45221 60219
         40770 91111 33425 20244 24012 70288 91320 29028 50937
         26130 38458 31428                                      DIVISIBLE PAR   2(2).37.79.101
```

```
VALEURS DE L(1-2N) .                                                                    R= 3  D=   148 .
------------------                                                                      --------------

L(-49) =    6028 89616 10310 16929 07710 32144 62866 06917 85092
           00933 98052 94862 48034 50340 03077 62010 08223 28925
           49975 47103 03953 33544 04192 49675 68755 68844 58156
           39692 10989 22922 08644                                DIVISIBLE PAR              2(2)

L(-51) =      55 09626 03349 94360 49434 05212 30869 63862 49630
           56940 64814 90865 38761 12806 78562 96475 03127 34372
           07413 43429 68677 26442 04596 64247 30740 06418 23309
           61245 36209 82404 99091 08177 02148                    DIVISIBLE PAR      2(2).43.349

L(-53) =   58814 51308 08922 40588 61919 57989 26143 18367 58993
           63132 22436 79920 96008 49148 50233 45004 83034 44027
           42759 40042 28921 57472 07343 91765 84762 39947 65284
           68027 20449 20248 10987 79711 24977 94564              DIVISIBLE PAR          2(2).863

L(-55) =     729 12394 64188 47995 86029 72562 73348 81326 90922
           70882 27251 06515 23463 46993 36262 48956 57690 45517
           46658 11213 12892 67874 62543 28786 14185 22764 06186
           17444 05931 83502 38161 12295 46272 90052 82033 45668  DIVISIBLE PAR     2(2).67.1259

L(-57) =      10 44073 52807 87543 43879 09754 54019 36811 96062
           37326 71249 20703 11559 66848 06129 74624 39251 22969
           79603 59029 69027 50574 31490 90627 10602 64073 15022
           49171 69337 08828 87749 66156 75980 59480 68354 80369
           52192 46084                                            DIVISIBLE PAR           2(2).23
```

DIFFÉRENCES ITÉRÉES POUR L(s)

R= 3 D= 148 .

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28
P= 2	2	8	10	12	17	18	28	24	29	30	36	36	41	42	49	48	53	54	60	60	65	66	75	72	77	78	84	84	89
P= 3	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28
P= 5	0	1	2	3	5	5	6	7	9	9	10	11	13	13	14														
	0	1	2	3	4	5	6	7	8	9	10	11	12	13															
P= 7	0	1	2	3	4	6	6	7	8	9																			
	0	1	2	3	4	5	6	7	8	9																			
	0	1	2	3	4	5	6	7	8																				
P=11	0	1	2	3	4	6																							
	0	1	2	3	4	5																							
	0	2	3	3	4	5																							
	0	1	2	3	4	5																							
	0	1	2	3	6																								
P=13	0	1	2	3	4																								
	0	1	2	3	4																								
	0	1	2	3	5																								
	0	1	2	3	5																								
	0	1	2	3	4																								
	0	1	2	3																									

```
VALEURS EXTRAPOLÉES DE LP(1)                                                    R= 3  D=  148 .
----------------------------                                                    ---------------

CES VALEURS SONT ÉCRITES EN BASE P .

P= 2   LP(1) =   110 01110 01100 11001 00100 11110 10101 01011 00011 10000 11110 11110
                10101 10000 10101 11110 11000 00100
                                                                                 MODULO  2^89

P= 3   LP(1) =   101 01012 12022 21002 01111 01001                               MODULO  3^28

P= 5   LP(1) =   420 14411 42223                                                 MODULO  5^13

P= 7   LP(1) =    13 42235                                                       MODULO  7^8

P=11   LP(1) =     3 45837                                                       MODULO  11^6

P=13   LP(1) =   9A5      (*)                                                    MODULO  13^3
```

(*) La lettre A désigne "dix" en base 13

VALEURS DE L'(1-2N) .

R= 3 D= 148 / R1= 2 D1= 5 .

L'(-1) =	648	DIVISIBLE PAR	2(3).3(4)
L'(-3) =	1849 73064	DIVISIBLE PAR	2(3).3.37.67.3109
L'(-5) =	64264 67598 84168	DIVISIBLE PAR	2(3).3.13.1021
L'(-7) =	99 45402 46475 42013 04584	DIVISIBLE PAR	2(3).3(2).37.6673
L'(-9) =	45280 62626 38921 08663 37283 56488	DIVISIBLE PAR	2(3).3.29.53.181.283.613
L'(-11) =	481 25497 35846 70990 44081 84422 73089 89704	DIVISIBLE PAR	2(3).3.661
L'(-13) =	10 28744 85398 18135 28523 28635 75289 84245 06733 53608	DIVISIBLE PAR	2(3).3(2).29
L'(-15) =	39850 16823 96219 57050 57902 75903 61482 40669 78786 66371 16424	DIVISIBLE PAR	2(3).3.409.907
L'(-17) =	2589 71476 59735 24024 83172 65772 33265 48428 24329 11022 40762 69839 31528	DIVISIBLE PAR	2(3).3.13
L'(-19) =	266 06522 70456 33541 06271 12777 22880 17329 46159 73250 42979 71541 52813 50459 72744	DIVISIBLE PAR	2(3).3(3)
L'(-21) =	41 22595 01944 25925 71724 30641 50074 97982 41340 31384 32485 70604 87193 96606 77616 99294 66248	DIVISIBLE PAR	2(3).3.37
L'(-23) =	9 27162 12591 58984 50024 22404 40432 32937 65637 31305 13001 43692 57442 07437 18401 57270 31157 19142 46664	DIVISIBLE PAR	2(3).3
L'(-25) =	2 93185 27747 54418 42587 65943 91510 02204 58860 29810 23919 46211 86651 90016 50238 79301 36172 75292 45824 62468 53768	DIVISIBLE PAR	2(3).3(2).37.107

VALEURS DE L'(1-2N) .

R= 3 D= 148 / R1= 2 D1= 5 .

```
L'(-27) =      1 26911 31878 18280 64747 42672 25427 74265 74096
           94663 14918 05784 19657 50248 09561 15035 70439 45882
           84922 46001 30700 36222 26184                          DIVISIBLE PAR        2(3).3.107.443

L'(-29) =  73501 53183 18378 87253 54416 04519 11653 51309 45666
           91914 35505 66308 71515 66487 08563 91596 52718 90451
           14044 46353 06763 32205 84157 10088                    DIVISIBLE PAR        2(3).3.13.109
```

DIFFÉRENCES ITERÉES POUR L'(s) R= 3 D= 148 / R1= 2 D1= 5 .

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
P= 2	3	7	9	12	15	18	21	24	27	30	33	36	39	42	45	48	51	54	57
P= 3	4	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
P= 5	0	1	2	3	4	5	6	7	8	9									
	0	1	2	3	5	5	6	7	9										
P= 7	0	1	2	3	4	5	6												
	0	2	2	5	5	5													
	0	1	2	3	4	7													
P=11	0	1	3	3															
	0	1	3	3															
	0	2	2	3															
	0	1	2	3															
	0	1	2																
P=13	0	1	2	3															
	0	1	2																
	1	1	2																
	0	1	2																
	0	2	2																
	0	1	2																

R = 3, D = 148

INTERCALEMENT DE L(s) ET L'(s)

Les différences itérées sont calculées sur les suites

$L^{(5)}(-1),\ L^{(5)}(-3;\chi_5),\ L^{(5)}(-5),\ L^{(5)}(-7;\chi_5)\ldots$ pour la première ligne

$L^{(5)}(-1;\chi_5),\ L^{(5)}(-3),\ L^{(5)}(-5,\chi_5),\ L^{(5)}(-7),\ldots$ pour la seconde ligne.

On a indiqué la plus haute puissance de 5, soit 5^{v_n} (resp. $5^{v'_n}$) qui divise la n-ième différence itérée.

n	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
v_n	0	1	2	3	5	5	6	7	9	9	10	11	14	13	14
v'_n	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14

Valeurs extrapolées (*) $L^{(5)}(1;\chi_5) \equiv 9412\ 97769 \mod. 5^{14}$

$L^{(5)}(1) \equiv 35194\ 74688 \mod. 5^{14}$

(*) En écriture décimale

TABLE 9

FONCTION ZÊTA DU CORPS DE DEGRÉ 4

ET DISCRIMINANT 1957

(groupe de Galois symétrique)

1) Répartition en classes des nombres premiers $\leq$ 5000

2) Valeurs de $L(1-2n)$ pour $1 \leq n \leq 15$, avec $L(s) = \zeta_K(s)/\zeta(s)$

3) Valuation des différences itérées

4) Valeurs extrapolées de $L^{(p)}(1)$

RÉPARTITION EN CLASSES DES NOMBRES PREMIERS INFÉRIEURS A 5000 R= 4 D= 1957 .

CLASSE C(4) .

2	5	11	13	29	41	79	107	167	179	191	223	233	263	269	271	277
349	389	397	463	523	593	607	641	653	673	691	727	751	761	769	797	809
823	839	859	887	919	953	983	997	1013	1019	1033	1051	1063	1087	1123	1171	1187
1223	1231	1249	1279	1291	1319	1399	1429	1453	1459	1489	1543	1567	1571	1579	1609	1619
1637	1667	1669	1709	1741	1777	1823	1861	1877	1901	1913	1933	1999	2003	2017	2053	2063
2083	2099	2113	2137	2143	2179	2243	2251	2341	2347	2377	2411	2417	2521	2671	2677	2683
2687	2693	2711	2719	2833	2909	2917	2927	2963	2971	2999	3001	3011	3023	3041	3083	3089
3109	3119	3121	3163	3181	3203	3221	3323	3361	3433	3449	3457	3499	3517	3539	3559	3593
3613	3623	3631	3659	3677	3779	3797	3881	3943	3947	4001	4093	4099	4177	4201	4217	4219
4229	4243	4259	4289	4327	4337	4357	4423	4451	4519	4523	4567	4583	4591	4673	4679	4703
4759	4789	4813	4889	4919	4933	4937	4967	4973	4993	4999						

CLASSE C(3 , 1) .

3	7	23	31	37	53	61	67	71	83	89	127	131	137	139	149	151
163	173	181	211	229	239	257	281	293	311	313	331	367	383	419	439	449
461	467	491	521	541	563	569	587	599	613	619	631	643	647	683	739	757
811	827	829	911	929	971	1031	1049	1117	1129	1153	1163	1181	1201	1259	1277	1307
1321	1327	1361	1373	1427	1447	1481	1559	1583	1597	1601	1613	1621	1657	1693	1697	1699
1723	1747	1753	1867	1871	1873	1879	1889	1931	1979	1993	1997	2027	2039	2111	2153	2161
2207	2213	2221	2293	2309	2339	2351	2357	2389	2393	2437	2441	2447	2459	2467	2503	2539
2549	2593	2609	2617	2647	2657	2659	2663	2689	2707	2713	2741	2749	2767	2801	2837	2857
2887	2897	2953	3019	3037	3061	3137	3167	3191	3209	3271	3299	3313	3329	3343	3373	3389
3407	3461	3463	3467	3529	3547	3557	3571	3583	3673	3697	3709	3761	3767	3769	3793	3821
3833	3847	3853	3877	3889	3907	3917	3923	3931	3989	4007	4027	4051	4057	4073	4129	4139
4241	4253	4273	4297	4349	4441	4447	4457	4463	4483	4517	4547	4561	4597	4643	4657	4691
4751	4783	4793	4831	4871	4931	4943	4951	4957								

CLASSE C(2 , 2) .

17	109	113	193	227	241	307	359	379	433	503	571	601	661	701	709	743
853	863	877	883	1097	1109	1151	1229	1297	1381	1433	1483	1511	1759	1783	1787	1973
2069	2131	2203	2237	2267	2269	2311	2333	2399	2423	2531	2551	2591	2729	2777	2797	2803
2819	2843	2957	3067	3253	3301	3371	3581	3607	3671	3701	3719	3733	3739	3851	3911	3967
4079	4127	4153	4157	4261	4271	4373	4391	4397	4409	4421	4493	4909				

CLASSE C(2 , 1 , 1) .

43	47	59	73	97	101	157	197	199	251	283	317	337	353	373	401	409

RÉPARTITION EN CLASSES DES NOMBRES PREMIERS INFÉRIEURS A 5000 R= 4 D= 1957 .

421	431	443	457	479	499	509	547	557	577	617	659	677	719	733	773	787
857	881	907	937	941	947	967	977	991	1009	1039	1061	1069	1091	1093	1103	1193
1213	1217	1237	1289	1301	1303	1367	1423	1439	1471	1487	1493	1499	1523	1531	1549	1553
1607	1627	1663	1721	1733	1789	1801	1831	1847	1907	1949	1951	2011	2029	2087	2089	2129
2141	2273	2287	2297	2371	2381	2383	2473	2477	2543	2557	2579	2621	2699	2753	2789	2791
2851	2861	2879	2903	2939	2969	3049	3169	3187	3217	3229	3251	3257	3259	3307	3319	3331
3359	3391	3413	3469	3491	3511	3527	3541	3617	3637	3643	3691	3727	3823	3919	3929	4013
4019	4021	4049	4091	4111	4133	4159	4211	4231	4283	4507	4549	4603	4621	4639	4649	4651
4663	4721	4723	4729	4733	4787	4801	4817	4861	4877	4903	4969	4987				

CLASSE C(1 , 1 , 1 , 1) .

347	487	821	1021	1283	1409	1451	1811	1987	2081	2239	2281	2633	2731	3079	3347	3533
3803	3863	4003	4339	4363	4481	4513	4637	4799								

CLASSE C(2 , 1^2).

19 103

VALEURS DE L(1-2N) .   R= 4 D= 1957 .

L(-1) =	- 8	DIVISIBLE PAR	2(3)
L(-3) =	1 41640	DIVISIBLE PAR	2(3).5.3541
L(-5) =	- 7 41785 07128	DIVISIBLE PAR	2(3).11
L(-7) =	346 17448 03732 09480	DIVISIBLE PAR	2(3).5.787.829
L(-9) =	-80662 46900 04692 24539 26008	DIVISIBLE PAR	2(3)
L(-11) =	668 76006 54719 97250 78936 28174 30920	DIVISIBLE PAR	2(3).5
L(-13) =	- 15 80615 01573 52846 08625 55603 36398 73910 08888	DIVISIBLE PAR	2(3).4639
L(-15) =	91118 44718 51866 66717 33919 94919 80613 75344 00815 17960	DIVISIBLE PAR	2(3).5.11.271
L(-17) =	-11413 54179 35192 31575 63220 29316 79065 94667 10041 43836 16554 51768	DIVISIBLE PAR	2(3).31.137.211.229.311
L(-19) =	2841 85840 37088 99787 56194 19479 11127 78384 56427 53295 38176 10124 93903 02600	DIVISIBLE PAR	2(3).5(2)
L(-21) =	- 1310 54838 11115 44576 86944 79598 29925 53382 12713 35723 49607 50017 75312 59333 76340 70648	DIVISIBLE PAR	2(3).181.593
L(-23) =	1056 83485 38400 34406 68632 42326 81770 38833 32717 96085 13298 18671 86977 53413 80079 09720 54822 16840	DIVISIBLE PAR	2(3).5.593
L(-25) =	- 1420 89942 78219 59418 14999 60563 26591 44038 58463 96658 15579 85865 67198 43898 66361 05352 73628 50810 06980 01528	DIVISIBLE PAR	2(3).11.41
L(-27) =	3059 68784 89801 04245 08897 69288 49491 09670 72572 35046 37056 31403 95109 72336 45379 68699 38395 72646 94113 73629 71756 92680	DIVISIBLE PAR	2(3).5.149

VALEURS DE L(1-2N) .   R= 4 D= 1957 .

```
L(-29) = -10196 41849 10142 77663 59392 65090 32924 88358 86785
          27341 20563 83289 42015 57337 45073 59563 36592 89699
          53694 57879 81280 12621 49755 00408          DIVISIBLE PAR          2(3).251
```

DIFFÉRENCES ITÉRÉES

R= 4 D= 1957 .

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
P= 2	3	9	10	13	16	19	22	25	28	31	34	37	40	43	46
P= 3	0	1	3	3	11	5	7	7	9	9	12	11	13	13	15
P= 5	0	1	3	3	4	5	8	7							
	1	1	2	3	5	5	6								
P= 7	0	1	2	4	4										
	0	1	2	3	4										
	0	1	2	3	4										
P=11	0	1	2												
	0	2	2												
	1	1	2												
	0	1	2												
	0	1	2												
P=13	0	1	2												
	0	1	3												
	0	1	2												
	0	1													
	0	2													
	0	2													

VALEURS EXTRAPOLÉES DE LP(1)

R= 4 D= 1957 .

CES VALEURS SONT ÉCRITES EN BASE P .

P= 2	LP(1) = 1010 11001 01000 00110 11110 11011 10111 01100 01000	MODULO	2^{46}
P= 3	LP(1) = 11122 22200 01111	MODULO	3^{15}
P= 5	LP(1) = 3 13100	MODULO	5^{6}
P= 7	LP(1) = 5132	MODULO	7^{4}
P=11	LP(1) = 37	MODULO	11^{2}
P=13	LP(1) = 87	MODULO	13^{2}

TABLE 10

FONCTION ZÊTA DU CORPS DE DEGRÉ 4
ET DISCRIMINANT 725

(groupe de Galois diédral)

1) Répartition en classes des nombres premiers $\leqslant 3000$

2) Valeurs de $L(1-2n)$ pour $1 \leqslant n \leqslant 20$, avec $L(s) = \zeta_K(s)/\zeta_E(s)$

3) Valuation des différences itérées

4) Valeurs extrapolées de $L^{(p)}(1)$

RÉPARTITION EN CLASSES DES NOMBRES PREMIERS INFÉRIEURS A 3000 — R= 4 D= 725 .

CLASSE C(4) .

2	3	17	37	43	47	73	97	113	127	137	157	163	193	263	293	307
317	337	367	433	443	467	503	563	577	607	617	653	677	727	733	743	757
773	797	823	827	853	887	907	947	967	983	997	1013	1033	1063	1087	1117	1123
1163	1187	1237	1297	1303	1307	1373	1423	1433	1447	1453	1487	1493	1523	1583	1597	1607
1613	1627	1663	1667	1693	1697	1723	1777	1783	1787	1867	1873	1877	1933	1987	1993	2003
2027	2143	2207	2243	2273	2293	2347	2357	2393	2417	2447	2467	2473	2477	2593	2647	2657
2683	2687	2707	2753	2767	2803	2857	2897	2903	2917	2927						

CLASSE $C(2, 2)_-$.

7	13	23	53	67	83	103	107	167	173	197	223	227	233	257	277	283
313	347	353	373	383	397	457	463	487	523	547	557	587	593	613	643	647
673	683	787	857	863	877	883	937	953	977	1093	1097	1103	1153	1193	1213	1217
1223	1277	1283	1327	1367	1427	1483	1543	1553	1567	1637	1657	1733	1747	1753	1823	1847
1907	1913	1973	1997	2017	2053	2063	2083	2087	2113	2137	2153	2203	2213	2237	2267	2287
2297	2333	2377	2383	2423	2437	2503	2543	2557	2617	2633	2663	2677	2693	2713	2777	2797
2833	2837	2843	2887	2953	2957	2963										

CLASSE $C(2, 2)_+$.

59	71	151	181	199	239	241	349	401	419	439	661	691	701	719	761	919
991	1009	1019	1031	1039	1051	1069	1451	1459	1531	1571	1579	1601	1741	1789	1811	1889
1901	1949	1979	2029	2039	2081	2089	2269	2371	2551	2609	2659	2731	2789	2851	2971	

CLASSE C(2 , 1 , 1) .

11	19	31	41	61	79	89	101	131	191	211	229	251	269	271	311	331
359	379	389	409	421	449	461	479	491	541	569	599	601	619	641	659	739
751	769	809	829	839	859	881	911	971	1061	1091	1129	1171	1181	1201	1229	1249
1259	1279	1291	1319	1361	1381	1409	1429	1439	1471	1481	1489	1511	1549	1609	1621	1699
1709	1721	1759	1801	1871	1931	1951	1999	2011	2069	2099	2129	2131	2161	2221	2251	2281
2309	2339	2341	2351	2381	2389	2399	2521	2531	2549	2579	2591	2621	2671	2689	2699	2711
2729	2741	2801	2861	2879	2939	2969	2999									

CLASSE C(1 , 1 , 1 , 1) .

109	139	149	179	281	431	499	509	521	571	631	709	811	821	929	941	1021
1049	1109	1151	1231	1289	1301	1321	1399	1499	1559	1619	1669	1831	1861	1879	2111	2141
2179	2239	2311	2411	2441	2459	2539	2719	2749	2791	2819	2909					

RÉPARTITION EN CLASSES DES NOMBRES PREMIERS INFÉRIEJRS A 3000 R= 4 D= 725 .

CLASSE$_{5}$ $C(2^2)_0$.

CLASSE$_{29}$ $C(2, 1^2)$.

VALEURS DE L(1-2N) . R= 4 D= 725 .

L(-1) =	4	DIVISIBLE PAR	2(2)
L(-3) =	2164	DIVISIBLE PAR	2(2).541
L(-5) =	117 39604	DIVISIBLE PAR	2(2)
L(-7) =	27 94444 17844	DIVISIBLE PAR	2(2).17.317
L(-9) =	19 54268 59225 16884	DIVISIBLE PAR	2(2).17
L(-11) =	31 89969 89772 00455 88724	DIVISIBLE PAR	2(2)
L(-13) =	104 72547 49299 36592 42768 65364	DIVISIBLE PAR	2(2).19.37.239
L(-15) =	623 02785 02010 54439 23709 62168 58804	DIVISIBLE PAR	2(2).109.4909
L(-17) =	6218 15867 04125 53376 30860 78776 76177 61044	DIVISIBLE PAR	2(2).59
L(-19) =	98113 90087 48401 09011 79954 10879 18543 74458 44084	DIVISIBLE PAR	2(2).43.4549
L(-21) =	23 34778 33563 36616 80812 80612 23093 50504 30065 97918 59924	DIVISIBLE PAR	2(2).73.271.379
L(-23) =	806 42358 26208 89424 51072 49831 14989 54692 99779 78519 97494 40564	DIVISIBLE PAR	2(2).17
L(-25) =	39163 56800 00781 55318 37226 76705 55165 44049 65045 61040 68168 31814 98004	DIVISIBLE PAR	2(2).17.3919.4787
L(-27) =	26 03592 46905 01493 12474 29456 11176 12474 78159 59353 56848 78483 39491 50946 24244	DIVISIBLE PAR	2(2).41.1811.5843
L(-29) =	2315 80291 45994 57098 20760 87306 77754 07835 99513 80100 19149 69357 06644 75777 41414 91284	DIVISIBLE PAR	2(2).67.151

```
VALEURS DE L(1-2N) .                                                  R= 4  D=   725 .
------------------                                                    ---------------

L(-31) =      2 70199 17853 07256 20039 28911 44393 62260 18127
          60258 14759 86773 80144 40704 98187 62418 75712 51124  DIVISIBLE PAR        2(2).19

L(-33) =    406 46990 10433 11011 34353 71115 62918 41688 90037
          72690 09068 86113 71368 90729 94780 85764 14503 17479
          35764                                                  DIVISIBLE PAR      2(2).3323

L(-35) =  77649 53254 37805 87903 10099 43295 50473 56435 47322
          17359 93337 81844 91641 62353 05771 19564 73556 72396
          81568 57204                                            DIVISIBLE PAR           2(2)

L(-37) =    185 85053 95675 59938 44765 12984 13353 38351 66084
          81248 02236 85892 97490 69312 21678 22648 14500 54326
          16249 05849 36190 07444                                DIVISIBLE PAR           2(2)

L(-39) =  55065 14214 09981 82563 27801 92166 53424 49153 05994
          97512 94667 75853 95753 60143 95624 37900 58205 25777
          44078 86597 29933 62334 58484                          DIVISIBLE PAR    2(2).17.443
```

DIFFÉRENCES ITÉRÉES

R= 4 D= 725 .

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
P= 2	2	5	8	11	14	17	20	23	26	29	32	35	38	41	44	47	50	53	56	59
P= 3	0	2	2	4	4	6	6	8	8	10	10	12	12	14	14	16	16	18	18	20
P= 5	0	1	2	3	4	5	6	7	8	9										
	0	1	2	3	4	5	6	7	8	9										
P= 7	0	1	2	4	4	5	6													
	0	4	2	3	4	5	6													
	0	1	3	4	4	5														
P=11	0	1	2	3																
	0	1	2	3																
	0	1	2	3																
	0	1	2	3																
	0	1	2	3																
P=13	0	1	2	3																
	0	1	2	3																
	0	1	2																	
	0	1	2																	
	0	1	2																	
	0	1	2																	

VALEURS EXTRAPOLÉES DE LP(1)

R= 4 D= 725 .

CES VALEURS SONT ÉCRITES EN BASE P .

P= 2	LP(1) = 1000 00001 00100 10010 11011 01001 10110 11111 00010 01110 01101 10100	MODULO 2^{59}
P= 3	LP(1) = 12212 22122 02021 22011	MODULO 3^{20}
P= 5	LP(1) = 2303 02214	MODULO 5^{9}
P= 7	LP(1) = 51422	MODULO 7^{5}
P=11	LP(1) = 246	MODULO 11^{3}
P=13	LP(1) = 24	MODULO 13^{2}

TABLE 11

FONCTION ZÊTA DU CORPS DE DEGRÉ 5

ET DISCRIMINANT 24217

1) Répartition en classes des nombres premiers $\leq$ 5000

2) Valeurs de $L(1-2n)$ pour $1 \leq n \leq 9$, avec $L(s) = \zeta_K(s)/\zeta(s)$

3) Valuation des différences itérées

4) Valeurs extrapolées de $L^{(p)}(1)$

RÉPARTITION EN CLASSES DES NOMBRES PREMIERS INFÉRIEURS A 5000 R= 5 D= 24217 .

CLASSE C(5) .

2	3	7	19	71	89	127	137	179	181	211	227	229	331	337	359	373
389	419	467	479	487	503	683	797	811	829	859	863	881	1039	1049	1201	1213
1217	1237	1297	1301	1319	1381	1433	1453	1489	1493	1499	1543	1549	1559	1613	1663	1693
1709	1787	1823	1831	1847	1877	1889	1907	1949	1999	2141	2179	2287	2377	2383	2389	2423
2531	2579	2617	2621	2633	2659	2713	2719	2767	2777	2791	2819	2887	2903	2917	2927	2999
3019	3067	3271	3361	3371	3491	3527	3529	3533	3547	3571	3623	3631	3779	3793	3797	3823
3853	3863	3881	3943	4001	4027	4079	4093	4099	4133	4201	4231	4261	4289	4327	4349	4397
4421	4457	4463	4481	4583	4723	4733	4799	4817	4861	4871	4903	4951	4993			

CLASSE C(4 , 1) .

5	23	29	37	41	43	103	109	113	151	191	199	241	269	277	283	307
347	379	383	401	443	463	499	521	523	541	563	587	593	607	613	619	631
701	769	821	823	839	853	857	877	887	911	919	937	1013	1021	1031	1033	1087
1093	1097	1109	1123	1171	1187	1223	1291	1361	1399	1447	1481	1511	1531	1597	1601	1607
1627	1657	1871	1913	1979	1993	2011	2063	2069	2111	2129	2153	2203	2213	2221	2237	2269
2273	2293	2297	2339	2347	2351	2381	2399	2411	2417	2437	2441	2459	2473	2543	2609	2677
2693	2699	2729	2741	2801	2803	2857	2939	2971	3001	3023	3037	3079	3083	3109	3119	3163
3169	3209	3221	3253	3257	3259	3299	3323	3359	3407	3469	3499	3511	3541	3559	3617	3637
3701	3727	3761	3821	3833	3847	3851	3907	3919	3947	3989	4021	4057	4073	4153	4157	4177
4219	4229	4241	4259	4271	4297	4337	4357	4409	4423	4441	4483	4493	4507	4519	4643	4649
4657	4673	4721	4729	4787	4789	4813	4877	4889	4933	4957	4969	4973				

CLASSE C(3 , 2) .

11	13	31	67	79	173	197	239	263	281	317	349	409	433	449	491	571
599	643	653	659	673	809	929	941	977	1069	1103	1117	1151	1163	1231	1303	1307
1409	1423	1439	1553	1567	1571	1583	1619	1621	1637	1721	1723	1733	1747	1753	1811	1867
1973	2017	2083	2099	2113	2131	2243	2447	2503	2521	2551	2557	2591	2647	2663	2711	2753
2789	2833	2843	2851	2861	2897	2953	3011	3041	3181	3229	3319	3347	3391	3433	3449	3461
3659	3677	3691	3697	3803	3929	3931	4049	4129	4273	4283	4363	4373	4391	4513	4517	4523
4621	4651	4663	4679	4759	4793	4801	4931	4987	4999							

CLASSE C(3 , 1 , 1) .

17	53	59	83	97	139	157	167	223	257	271	311	313	353	367	421	431
461	509	547	719	727	739	743	757	787	827	907	967	983	1061	1063	1129	1181
1279	1321	1373	1429	1451	1459	1487	1609	1697	1699	1783	1873	1879	1901	1987	2027	2029
2039	2081	2087	2089	2137	2207	2281	2309	2333	2341	2393	2467	2477	2539	2657	2687	2731

RÉPARTITION EN CLASSES DES NOMBRES PREMIERS INFÉRIEURS A 5000 R= 5 D= 24217 .

2749	2969	3049	3121	3137	3187	3301	3313	3331	3343	3373	3457	3463	3557	3583	3643	3673
3709	3719	3739	3889	3911	3923	4007	4051	4139	4159	4211	4243	4253	4547	4567	4591	4597
4603	4783	4831	4909													

CLASSE C(2 , 2 , 1) .

47	73	101	107	131	163	193	233	251	293	439	457	569	577	617	641	661
677	751	883	947	953	997	1009	1051	1153	1249	1289	1327	1367	1427	1471	1483	1667
1669	1741	1777	1789	1801	1931	1951	1997	2003	2053	2143	2239	2267	2311	2357	2549	2593
2671	2689	2707	2837	2879	2963	3061	3089	3167	3307	3413	3539	3581	3593	3613	3671	3733
3769	3877	4013	4127	4217	4339	4451	4549	4637	4751	4937	4967					

CLASSE C(2 , 1 , 1 , 1) .

149	557	601	647	691	709	733	761	773	971	991	1019	1091	1193	1229	1259	1277
1283	1523	1579	1759	1861	1933	2161	2251	2371	2683	2797	2909	2957	3191	3203	3217	3251
3389	3467	3517	3607	3767	3917	3967	4003	4019	4111	4561	4639	4691	4919	4943		

CLASSE C(1 , 1 , 1 , 1 , 1) .

3329	4091	4447	4703

CLASSE C(2 , 1^2,1).

61	397

VALEURS DE L(1-2N) . R= 5 D= 24217 .

L(-1) =	16	DIVISIBLE PAR	2(4)
L(-3) =	71 88208	DIVISIBLE PAR	2(4)
L(-5) =	29495 13678 68656	DIVISIBLE PAR	2(4)
L(-7) =	2245 03358 94871 66394 85808	DIVISIBLE PAR	2(4).9337
L(-9) =	1461 13030 11941 68101 93951 81532 80496	DIVISIBLE PAR	2(4)
L(-11) =	5168 75854 53241 83572 96341 62306 88370 35563 81808	DIVISIBLE PAR	2(4).19
L(-13) =	73920 79607 19345 66145 48012 22364 46192 36939 17224 69033 51536	DIVISIBLE PAR	2(4).257.571
L(-15) =	34 71067 10972 64948 51222 84363 94624 87950 82951 42999 57200 50834 38301 80208	DIVISIBLE PAR	2(4).23
L(-17) =	4587 20178 62789 28647 76279 52624 46655 79507 37076 19728 03165 43452 79674 85876 35136 97776	DIVISIBLE PAR	2(4).131.1039

DIFFÉRENCES ITÉRÉES

R= 5 D= 24217 .

	0	1	2	3	4	5	6	7	8
P= 2	4	7	10	13	16	19	22	25	28
P= 3	0	1	3	3	7	5	7	7	9
P= 5	0	1	2	3	4				
	0	2	2	3					
P= 7	0	1	2						
	0	1	2						
	0	1	2						
P=11	0	1							
	0	1							
	0	1							
	0	1							
	0								
P=13	0	1							
	0	1							
	0	1							
	0								
	0								
	0								

VALEURS EXTRAPOLÉES DE LP(1)

R= 5 D= 24217 .

CES VALEURS SONT ÉCRITES EN BASE P .

P= 2	LP(1) =	110 01100 00110 01111 01011 10000	MODULO 2^{28}
P= 3	LP(1) =	1200 02111	MODULO 3^{9}
P= 5	LP(1) =	13	MODULO 5^{3}
P= 7	LP(1) =	32	MODULO 7^{2}
P=11	LP(1) =	0	MODULO 11
P=13	LP(1) =	0	MODULO 13

ADDRESSES OF AUTHORS

P. CARTIER	28 rue Ronsard 91470 Limours (France)
B. DWORK	Univ. of Princeton Dept. of Math. Fine Hall Princeton, N.J.08540 (U.S.)
N. KATZ	Univ. of Princeton Dept. of Math. Fine Hall Princeton, N.J.08540 (U.S.)
Y. ROY	Centre de calcul de l'Esplanade 7 rue R.Descartes 67000 Strasbourg (France)
J-P. SERRE	6 avenue de Montespan 75116 Paris (France)
H.P.F. SWINNERTON-DYER	Univ. of Cambridge Dept. of Math. 16 Mill Lane Cambridge CB2 1SB (England)