J. reine angew. Math. **392** (1988), 1—15

Journal für die reine und angewandte Mathematik

The l-adic representations attached to a certain noncongruence subgroup

By *A. J. Scholl* at Durham

Introduction

In this paper we elaborate on a result which was proved in [S], following the extensive computations of [A-SwD]. Let Γ be the unique subgroup of the modular group $\mathrm{PSL}_2(\mathbb{Z})$ of index 9 which has a cusp of width 7 at ∞ and inequivalent cusps of width 1 at ± 2. (This subgroup is denoted Γ_{711} in [A-SwD].) Let

$$f(\tau) = \sum_{n \geqq 1} a(n) e^{2\pi i n \tau/7}, \qquad a(n) \in \mathbb{R}$$

be the unique cusp form of weight 4 on Γ with $a(1) = 1$.

Theorem A. (i) *For every $n \geqq 1$, we have*

$$a(n) = 64^{(n-1)/7} b(n) \quad \textit{with} \quad b(n) \in \mathbb{Z}[1/14].$$

(ii) *For each prime $p \neq 2, 7$ there is an integer A_p, with $|A_p| < 2p^{3/2}$, such that if $n \equiv 0 \pmod{p^\alpha}$ then*

$$a(np) - A_p a(n) + p^3 a(n/p) \equiv 0 \begin{cases} \bmod p^{3(\alpha+1)} & \textit{if} \quad p \neq 3; \\ \bmod 3^{3\alpha+2} & \textit{if} \quad p = 3. \end{cases}$$

Here the congruences are to be interpreted as in § 5. 2 of [A-SwD] or § 5. 4 of [S]. It is clear that (ii) uniquely determines A_p, except possibly for $p = 3$. In fact more can be said about $\{A_p\}$; there exists a strictly compatible system of l-adic representations

$$\varrho_l : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{Q}_l),$$

such that if $p \notin \{2, 7, l\}$ then ϱ_l is unramified at p, and the characteristic polynomial of a Frobenius element at p is $T^2 - A_p T + p^3$.

This theorem (first conjectured in [A-SwD]) was proved in [S], apart from the determination of the exceptional set of "bad" primes $\{2, 7\}$. In §§ 1, 2 below we show how this set may be obtained. The representations ϱ_l occur in the l-adic cohomology of certain algebraic varieties, and using the Lefschetz fixed-point formula it is relatively easy to find a closed formula for the numbers A_p; this is described in § 3 below. The formula is similar to those of Ihara [I], although we have to take care of the singular values $j = 0{,}1728$ as well here. (In contrast, the computation of the Fourier coefficients $a(n)$ seems rather difficult.)

Now let

$$F(\tau) = \frac{1}{8}\,\eta(\tau)\,\eta(2\tau)\,\eta(7\tau)\,\eta(14\tau)\,\{14P(14\tau) - 7P(7\tau) + 2P(2\tau) - P(\tau)\}$$
$$= \sum_{n \geqq 1} B_n e^{2\pi i n\tau},$$

where

$$P(\tau) = 1 - 24 \sum_{n \geqq 1} \sigma(n) e^{2\pi i n\tau}$$

is the Ramanujan series, and $\eta(\tau)$ denotes Dedekind's η-function. Then $B_1 = 1$, $B_n \in \mathbb{Z}$ for all n, and $F(\tau)$ is a newform of weight 4 on $\Gamma_0(14)$; see § 4 below. Our main result is:

Theorem B. *$A_p = B_p$ for $p \neq 2, 7$.*

By Deligne's construction [D 1], associated to F is a strictly compatible system of 2-dimensional l-adic representations $\{\varrho'_l\}$, such that for $p \notin \{2, 7, l\}$ the characteristic polynomial of a Frobenius element at p is $T^2 - B_p T + p^3$. We accordingly prove that ϱ_l and ϱ'_l are isomorphic. By the strict compatibility it suffices to prove this for one prime l. In § 5 we describe how a method due to Serre (making explicit a special case of Faltings' result on l-adic representations, [F], Satz 5) can be used to prove that $\varrho_2 \cong \varrho'_2$, knowing only the values of A_p, B_p for a small number of primes p. We are particularly grateful to Serre for explaining how to apply his method in this situation.

In the first three sections of this paper, we have described a considerably more general setting than we actually require. This requires little extra effort, and should be useful in future applications. We have particularly tried to avoid restricting to the case in which the "field of definition" is $\mathbb{Q}$.

We view our result as follows. Associated to the cusp form f is a certain motive M_f (in the sense of absolute Hodge cycles, see [D4]) whose l-adic realisations are $\{\varrho_l\}$. (For the construction of M_f, see forthcoming work of U. Jannsen.) The standard conjectures on L-functions of motives, together with Weil's characterisation of Dirichlet series attached to modular forms, would imply that the L-series $L(M_f, s)$ was the Mellin transform of a newform of weight 4 on $\Gamma_0(2^\alpha 7^\beta\}$ for some α, β.

Theorem B is thus a verification of this conjectured relationship in this special case. (In general the representations associated to cusp forms on noncongruence subgroups will not decompose into two-dimensional pieces, and one must expect other automorphic L-series to arise.)

§ 1. The l-adic representations associated to cusp forms

1. 1. Let N be a natural number. We denote by $X(N)$ the moduli scheme over $\mathbb{Q}$ parameterising generalised elliptic curves with arithmetic level N structure ($\mathscr{A} \otimes \mathbb{Q}$ in the notations of [D-R], V. 4.4). Thus $X(N)$ is a smooth, proper and geometrically irreducible curve over $\mathbb{Q}$. The j-function identifies $X(1)$ with the projective line; we write

$$X(1)^\circ = X(1) - \{j = 0{,}1728,\ \infty\}$$

and for any morphism $p: Y \to X(1)$ we set $Y^\circ = p^{-1}(X(1)^\circ)$. Let $f: E \to X(1)^\circ$ be the elliptic curve with affine equation

$$y^2 + xy = x^3 - (36x + 1)/(j - 1728), \tag{1. 1}$$

whose j-invariant is j (see [T]). We write

$$\mathscr{F}_l = R^1 f_* \mathbb{Q}_l.$$

1. 2. We consider the following situation: V is a smooth and proper curve over $\mathbb{Q}$, connected (but not necessarily geometrically connected), and $\pi: V \to X(1)$ is a finite morphism, étale over $X(1)^\circ$. Assume further that the ramification degrees of π at points over $j = 0$ (respectively $j = 1728$) divide 3 (respectively 2).

The typical example of this situation is the following: Let Γ be a subgroup of $\mathrm{PSL}_2(\mathbb{Z})$ of finite index, and X a model for the modular curve $\Gamma \backslash \mathfrak{H}^*$ defined over an algebraic number field K, such that the modular function j belongs to $K(X)$. We may then take V to be the curve obtained from X by restriction of scalars to $\mathbb{Q}$, and $\pi: V \to X(1)$ the map induced by the inclusion of Γ in $\mathrm{PSL}_2(\mathbb{Z})$.

Write π_0 for the restriction of π to V°, and i for the inclusion $V^\circ \hookrightarrow V$. For an even integer $k \geqq 0$, define

$$W_{k,l} = H^1(V \otimes \bar{\mathbb{Q}},\ i_* \pi_0^* \operatorname{Sym}^k \mathscr{F}_l),$$

which is a finite-dimensional l-adic representation of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$.

1. 3. Proposition. *If Γ is a subgroup of* $\mathrm{PSL}_2(\mathbb{Z})$ *defined over $\mathbb{Q}$, and (V, π) is a model for Γ (as in* § 5. 1 *of* [S]) *then $W_{k,l}$ is isomorphic to the representation ϱ_l of* § 5. 3 *of loc. cit.*

Proof. We recall the definition of ϱ_l. Let

$$G(N) = \mathrm{SL}(\boldsymbol{\mu}_N \times \mathbb{Z}/N)$$

(a finite group scheme over $\mathbb{Q}$). Assuming $N \geqq 3$, let

$$f^{\mathrm{univ}}: E^{\mathrm{univ}} \to X(N)^\circ$$

be the restriction of the universal elliptic curve to $X(N)^\circ$. Then $G(N)$ acts on $X(N)$, E^{univ} and on the $\mathbb{Q}_l$-sheaf

$$\mathscr{F}_l^{\mathrm{univ}} = R^1 f_*^{\mathrm{univ}} \mathbb{Q}_l.$$

Let $V(N)$ denote the normalisation of the fibre product

$$V \underset{X(1)}{\times} X(N),$$

on which $G(N)$ acts via the second factor. We have a commutative diagram:

$$\begin{array}{ccccc}
V(N) & \xleftarrow[i_N]{\qquad} & V(N)^\circ & \xrightarrow{\qquad} & V^\circ \\
\downarrow{\scriptstyle \pi'} & & \downarrow{\scriptstyle \pi'_0} & & \downarrow{\scriptstyle \pi_0} \\
X(N) & \xleftarrow{\qquad} & X(N)^\circ & \xrightarrow[g]{\qquad} & X(1)^\circ
\end{array}$$

in which the right-hand square is Cartesian (since π_0 is étale). Then ϱ_l is the representation of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ on

$$H^1(V(N) \otimes \bar{\mathbb{Q}},\, i_{N*}\pi_0'^{*}\,\mathrm{Sym}^k \mathscr{F}_l^{\mathrm{univ}})^{G(N)}.$$

To identify this space with $W_{k,l}$ is suffices to demonstrate the following claim:

Claim. $\mathrm{Sym}^k(g^*\mathscr{F}_l) \cong \mathrm{Sym}^k \mathscr{F}_l^{\mathrm{univ}}$ as $G(N)$-sheaves, if k is even.

(Note that k must be even here, since $-1 \in G(N)$ acts trivially on $g^*\mathscr{F}_l$, but non-trivially on $\mathscr{F}_l^{\mathrm{univ}}$.)

To see this, consider the pullback

$$E' = E \underset{X(1)^\circ}{\times} X(N)^\circ$$

on which $G(N)$ acts via the second factor.

Write

$$Z = \mathrm{Isom}_{X(N)^\circ}(E', E^{\mathrm{univ}}).$$

By Proposition 5. 3 of [D2] the structural morphism $q : Z \to X(N)^\circ$ is an étale covering of degree 2. We therefore have $q_*\mathbb{Q}_l = \mathbb{Q}_l \oplus \mathscr{L}$ where $\mathscr{L}$ is a rank one $G(N)$-sheaf on $X(N)^\circ$ with $\mathscr{L}^{\otimes 2} \cong \mathbb{Q}_l$. Then since $q^*g^*\mathscr{F}_l \cong q^*\mathscr{F}_l^{\mathrm{univ}}$ we have

$$g^*\mathscr{F}_l \subset \mathscr{F}_l^{\mathrm{univ}} \oplus \mathscr{F}_l^{\mathrm{univ}} \otimes \mathscr{L}.$$

As $\mathscr{F}_l^{\mathrm{univ}}$ is irreducible, the remark immediately following the claim implies that

$$g^*\mathscr{F}_l \cong \mathscr{F}_l^{\mathrm{univ}} \otimes \mathscr{L}$$

and the claim follows.

1. 4. We recall here that the Atkin-Swinnerton-Dyer congruences relate $W_{k,l}$ to the Fourier coefficients of cusp forms of weight $k+2$; and in particular, that the dimension of $W_{k,l}$ is twice the dimension of the space of such cusp forms.

§ 2. The ramified primes

2. 1. We keep the notations of the previous section, and write ϱ_l for the representation of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ on $W_{k,l}$; by 1. 3 this does not conflict with our earlier notation. Let $\mathfrak{o}_p$ denote the localisation of the ring $\mathbb{Z}[j]$ at the prime ideal (p); it is a valuation ring of the function field $\mathbb{Q}(j)$ of $X(1)$. Denote by $\mathfrak{O}_p$ the integral closure of $\mathfrak{o}_p$ in $\mathbb{Q}(V)$, the function field of V. We say that a prime p is *good* if $\mathfrak{O}_p$ is unramified over $\mathfrak{o}_p$.

2. 2. Proposition. *If p is good and $p \neq l$, then ϱ_l is unramified at p.*

We give two proofs; the first, although only valid for $p>3$, will be useful in the next section. Fix p and l with $l \neq p$.

2. 3. Denote by R the localisation of $\mathbb{Z}$ at (p). Then $X(1)$ extends to a smooth and proper R-scheme $\mathscr{X}(1) \cong \mathbb{P}^1_R$ (the isomorphism being given by the j-function). Let $\mathscr{X}(1)^\circ$ denote the open subscheme.

$$\mathscr{X}(1)^\circ = \operatorname{Spec} R[j, 1/j(j-1728)].$$

The elliptic curve E extends to an elliptic curve $f: \mathscr{E} \to \mathscr{X}(1)^\circ$ (given by the same affine equation (1. 1)), and the sheaf $\mathscr{F}_l$ extends to a smooth $\mathbb{Q}_l$-sheaf on $\mathscr{X}(1)^\circ$, which we continue to denote $\mathscr{F}_l = R^1 f_* \mathbb{Q}_l$.

If $p>3$ then $\mathscr{X}(1)^\circ$ is the complement of disjoint sections of $\mathscr{X}(1)$ over R, and hence $\mathscr{F}_l$ is tamely ramified.

2. 4. Let $\mathscr{V}$, $\mathscr{V}^0$ be the normalisations of $\mathscr{X}(1)$, $\mathscr{X}(1)^\circ$ in $\mathbb{Q}(V)$. Then if p is good, the finite morphism $\mathscr{V} \otimes \mathbb{F}_p \to \mathscr{X}(1) \otimes \mathbb{F}_p$ is generically étale. Hence by the theorem of purity ([G], X 3. 2) $\mathscr{V}^0$ is étale over $\mathscr{X}(1)^\circ$.

If moreover $p>3$, then $\mathscr{V}$ is tamely ramified over $\mathscr{X}(1)$ along the sections $j=0,1728, \infty$ and therefore by Abhyankar's lemma ([G], XIII 5. 5) $\mathscr{V}$ is smooth over R, and $\mathscr{V}^0$ is the complement in $\mathscr{V}$ of a closed subscheme which is finite and étale over R. In a standard way (see [D1], p. 161 for a similar situation) one deduces, using the base-changing theorems in étale cohomology, that ϱ_l is unramified at p, and moreover that

$$(2.\ 1) \qquad \det(1-t\,\mathrm{Frob}_p : W_{k,l}) = \det(1-tF_p : H^1(\mathscr{V} \otimes \bar{\mathbb{F}}_p,\ i_* \pi_0^* \operatorname{Sym}^k \mathscr{F}_l)).$$

(Here by abuse of notation we use i, π_0 to denote the reductions modulo p of the morphisms in 1. 2 above.) This concludes the proof if $p>3$.

2. 5. In general we must use the other description of $W_{k,l}$ to avoid wild ramification. Choose an integer $N \geqq 3$, prime to p. Let $\mathscr{X}(N)$ denote the modular curve of level N over R (which is the normalisation of $\mathscr{X}(1)$ in the function field of $X(N)$). Normalisation defines schemes $\mathscr{V}(N)$ and $\mathscr{V}(N)^\circ$, and by the same argument as above, $\mathscr{V}(N)^\circ$ is étale over $\mathscr{X}(N)^\circ$. Now at each geometric point x of $X(N)$ for which $j(x)=0$ (respectively 1728) the covering $X(N) \to X(1)$ has ramification index exactly 3 (respectively 2). Then by Abhyankar's lemma and the purity theorem, one sees that the covering $\mathscr{V}(N) \to \mathscr{X}(N)$ is étale away from the cuspidal subscheme $j=\infty$ of $\mathscr{X}(N)$. But the cuspidal subscheme is finite and étale over R (cf. [D-R], IV. 2. 5), and so $\mathscr{V}(N)$ is tamely ramified over $\mathscr{X}(N)$. This is essentially the same setting as § 4 of [S], and ϱ_l is unramified at p. This concludes the proof for all good primes.

2. 5. Remark. Note that by Abhyankar's lemma the ramification indices of the coverings $V(N) \to X(N)$ are prime to p if p is good. We can conclude that if V comes from a subgroup $\Gamma \leqq \mathrm{PSL}_2(\mathbb{Z})$ as in 1. 2, and if p divides the width of the cusp ∞, then p cannot be good.

2. 6. We can make 2. 2 more explicit when V has genus zero, using the "j-equations" of Klein-Fricke, exploited systematically by Atkin and Swinnerton-Dyer (see [A-SwD], § 2. 3 for details). Let K be the field of constants of V. Then there is a "Hauptmodul" t (that is, a rational function on V such that $\mathbb{Q}(V)=K(t)$) satisfying equations of the form

$$(2.2)\qquad \begin{aligned} jC(t) &= A(t)\,B(t)^3, \\ (j-1728)\,C(t) &= D(t)\,E(t)^2 \end{aligned}$$

for certain polynomials A, B, C, D, E with coefficients in K. In what follows, we shall only assume that t satisfies an equation

$$(2.3)\qquad P(t)+jQ(t)=0$$

with $P, Q \in K[t]$, $\deg P = d > \deg Q$ and P monic.

2. 7. Proposition. *Let p be a prime which is unramified in K. Suppose that for each prime $\mathfrak{p}$ of K dividing p the following conditions are satisfied:*

(i) *$P(t)$, $Q(t)$ are $\mathfrak{p}$-integral, and their reductions $\tilde{P}(t)$, $\tilde{Q}(t)$ modulo $\mathfrak{p}$ are relative prime;*

(ii) *at least one of $\tilde{P}'(t)$, $\tilde{Q}'(t)$ is nonzero.*

Then p is good.

(Note that (ii) is automatic unless $p|d$.)

Proof. Let Int_K be the ring of integers of K, and let $\mathfrak{o}'_p$ denote the localisation of $\mathrm{Int}_K[j]$ at p; it is a semilocal domain. Write $S=\mathfrak{o}'_p[t]/(P(t)+jQ(t))$, which makes sense by condition (i). P being monic, S is free of rank d over $\mathfrak{o}'_p$. Since the field of fractions of S is $\mathbb{Q}(V)$, it suffices to prove that S is unramified over $\mathfrak{o}_p$. By condition (i), we have

$$S \otimes \mathbb{F}_p = \bigoplus_{\mathfrak{p}|p} (\mathrm{Int}_K/\mathfrak{p})\,(j)\,[t]/(\tilde{P}(t)+j\tilde{Q}(t)) = \bigoplus_{\mathfrak{p}|p} (\mathrm{Int}_K/\mathfrak{p})\,(t).$$

It therefore suffices to prove that for each $\mathfrak{p}$, $(\mathrm{Int}_K/\mathfrak{p})\,(t)$ is separable over $\mathbb{F}_p(j)$, which is condition (ii).

2. 8. We apply this criterion in the case of the modular curve for the subgroup $\Gamma_{711} \leqq \mathrm{PSL}_2(\mathbb{Z})$. From § 2. 4 of [A-SwD] we have, with $K=\mathbb{Q}$,

$$(2.4)\qquad (t^3+4t^2+10t+6)^3 - \frac{1}{64}\left(t^2+\frac{13}{4}t+8\right)j=0.$$

Suppose $p>2$ (so that the polynomials are p-integral). Then if $\tilde{P}, \tilde{Q}$ have a common root $\alpha \in \bar{\mathbb{F}}_p$, one calculates at once that $7\alpha=0$. Since $\tilde{Q}(0) \neq 0$ for p odd, (i) holds if $p \neq 2, 7$. For (ii), we need only check $p=3$ since $d=9$.

2. 9. Corollary. *If V is the model for the modular curve $\Gamma_{711} \backslash \mathfrak{H}^*$ given by* (2. 4), *then ϱ_l is unramified away from* $\{2, 7, l\}$.

2. 10. Taken in conjunction with the main results of [S], this implies Theorem A. We indicate here why f may be chosen such that $b(n) \in \mathbb{Z}[1/14]$ and $b(1)=1$; indeed, if this is not the case then for some choice of f we will have $b(n) \in \mathbb{Z}[1/14]$, $b(1) \equiv 0 \pmod{p}$ and some other $b(n) \not\equiv 0 \pmod{p}$, for a prime $p \neq 2, 7$. Then the reduction modulo p of f is not identically zero, but vanishes to order $\geqq 1$ at each cusp, and to order $\geqq 2$ at the cusp ∞. But the divisor of a modular form of weight 4 on Γ_{711} has degree 3, so this is impossible.

§ 3. Explicit trace formula

3. 1. Here we calculate explicitly $\operatorname{Tr} \varrho_l(\mathrm{Frob}_p^r)$ when p is a good prime, different from 2, 3 and l. To avoid complicating the notation we assume that $k>0$. In this case

$$H^i(\mathscr{V} \otimes \bar{\mathbb{F}}_p, i_* \pi_0^* \operatorname{Sym}^k \mathscr{F}_l)=0 \quad \text{if} \quad i \neq 1$$

and hence by the Lefschetz formula ([D 3], Rapport 3. 2) and (2. 1) we have, with $q=p^r$,

$$\operatorname{Tr} \varrho_l(\mathrm{Frob}_p^r) = -\sum_{x \in \mathscr{V}(\mathbb{F}_q)} \operatorname{Tr}(x)$$

where

$$\operatorname{Tr}(x) = \operatorname{Tr}(F_x : (i_* \pi_0^* \operatorname{Sym}^k \mathscr{F}_l)_x).$$

In the next four paragraphs we give explicit expressions for $\operatorname{Tr}(x)$. The proofs are outlined afterwards.

3. 2. Here we consider $x \in \mathscr{V}^0(\mathbb{F}_q)$. Let $\mathscr{E}_{\pi(x)}$ be the fibre of the elliptic curve $\mathscr{E} \longrightarrow \mathscr{X}(1)^\circ$ at $\pi(x)$, and write

$$\# \mathscr{E}_{\pi(x)}(\mathbb{F}_q) = 1 + q - \alpha_x - \bar{\alpha}_x$$

with $\alpha_x \bar{\alpha}_x = q$. Then

$$\operatorname{Tr}(x) = \sum_{-\frac{k}{2} \leqq i \leqq \frac{k}{2}} q^{\frac{k}{2}} (\alpha_x / \bar{\alpha}_x)^i.$$

3. 3. Now suppose $\pi(x)$ is the point $j=\infty$ of $\mathscr{X}(1) \otimes \mathbb{F}_q$. Then $\operatorname{Tr}(x)=1$.

3. 4. Suppose $\pi(x)$ is the point $j=0$, and let $e(x) \in \{1, 3\}$ be the ramification degree of $\mathscr{V} \otimes \mathbb{F}_q \longrightarrow \mathscr{X}(1) \otimes \mathbb{F}_q$ at x.

If $p \equiv 1 \pmod 3$, write $p = \beta\bar{\beta}$ in $\mathbb{Z}[\sqrt[3]{1}]$ with $\beta \equiv 1 \pmod 3$. Then for $e(x)=1$, we have

$$\text{(3. 1)} \qquad \operatorname{Tr}(x) = \sum_{-\frac{k}{6} \leqq i \leqq \frac{k}{6}} q^{\frac{k}{2}} (\beta/\bar{\beta})^{3ir};$$

for $e(x)=3$ we can write $\hat{\mathcal{O}}_{\mathscr{V} \otimes \mathbb{F}_q, x} = \mathbb{F}_q[[\sqrt[3]{j/b}]]$ for some $b \in \mathbb{F}_p^*$, and

$$\text{(3. 2)} \qquad \operatorname{Tr}(x) = \sum_{-\frac{k}{2} \leqq i \leqq \frac{k}{2}} q^{\frac{k}{2}} (\beta/\bar{\beta})^{ir} \left(\frac{b}{\beta}\right)_3^{ir}.$$

If $p \equiv 2 \pmod 3$, then

$$\text{(3. 3)} \qquad \operatorname{Tr}(x) = \begin{cases} (-q)^{\frac{k}{2}} & \text{if } r \text{ is odd,} \\ \left(1 + 2\left[\dfrac{k\,e(x)}{6}\right]\right) q^{\frac{k}{2}} & \text{if } r \text{ is even.} \end{cases}$$

3. 5. Finally suppose $\pi(x)$ is the point $j = 1728$, so $e(x) \in \{1, 2\}$.

If $p \equiv 1 \pmod 4$, write $p = \gamma\bar{\gamma}$ in $\mathbb{Z}[i]$ with $\gamma \equiv 1 \pmod{2(1+i)}$. Then for $e(x)=1$,

$$\operatorname{Tr}(x) = \sum_{-\frac{k}{4} \leqq i \leqq \frac{k}{4}} q^{\frac{k}{2}} (\gamma/\bar{\gamma})^{2ir};$$

for $e(x)=2$, we have

$$\hat{\mathcal{O}}_{\mathscr{V} \otimes \mathbb{F}_q, x} = \mathbb{F}_q[[\sqrt{(j-1728)/c}]]$$

for some $c \in \mathbb{F}_p^*$ and

$$\operatorname{Tr}(x) = \sum_{-\frac{k}{2} \leqq i \leqq \frac{k}{2}} q^{\frac{k}{2}} (\gamma/\bar{\gamma})^{ir} \left(\frac{c}{p}\right)_2^{ir}.$$

If $p \equiv 3 \pmod 4$, then

$$\operatorname{Tr}(x) = \begin{cases} (-q)^{\frac{k}{2}} & \text{if } r \text{ is odd,} \\ \left(1 + \left[\dfrac{k\,e(x)}{4}\right]\right) q^{\frac{k}{2}} & \text{if } r \text{ is even.} \end{cases}$$

3. 6. The proof of 3. 2 is clear; indeed, if $x \in \mathscr{V}^{\circ}(\mathbb{F}_q)$ we have

$$\begin{aligned} (i_* \pi_0^* \operatorname{Sym}^k \mathscr{F}_l)_x &= \operatorname{Sym}^k \mathscr{F}_{l, \pi(x)} \\ &= \operatorname{Sym}^k H^1(\mathscr{E}_{\pi(x)} \otimes \bar{\mathbb{F}}_q, \mathbb{Q}_l). \end{aligned}$$

For the remaining points, we must analyse the local Galois representations attached to the elliptic curve $\mathscr{E} \otimes \mathbb{F}_p \to \mathscr{X}(1)^\circ \otimes \mathbb{F}_p$ at the points $j = 0, 1728, \infty$.

3. 7. We first introduce some notation. If $x \in \mathscr{V}(\mathbb{F}_q)$, let k be the function field of the connected component of $\mathscr{V} \otimes \mathbb{F}_q$ containing x. (Recall that by 2. 4 above $\mathscr{V} \otimes \mathbb{F}_q$ is smooth, since $p > 3$.) Thus k is a finite extension of $\mathbb{F}_q(j)$. Let v be the discrete valuation of k corresponding to x, and k_v the completion. Let G_v be the absolute Galois group $\mathrm{Gal}(k_v^{\mathrm{sep}}/k_v)$, I_v the inertia group, and F_v a geometric Frobenius.

Finally write A_v for the elliptic curve $\mathscr{E} \otimes k_v$, and $H_v = H^1(\mathscr{E} \otimes k_v^{\mathrm{sep}}, \mathbb{Q}_l)$. Then H_v is a G_v-module, and

$$\mathrm{Tr}(x) = \mathrm{Tr}(F_v : (\mathrm{Sym}^k H_v)^{I_v}).$$

3. 8. The model (1. 1) of the elliptic curve A_v has j-invariant $j \in k_v$, and discriminant $\Delta = j^2 (j - 1728)^{-3}$. The behaviour of the Néron model of A_v can be read off from the table in § 6 of [T]. If $v(j) = v(j - 1728) = 0$ then $x \in \mathscr{V}^0(\mathbb{F}_q)$ and the position is described in 3. 6 above.

3. 9. If $v(j) < 0$ then $\pi(x) = \infty$. Tate's algorithm shows that the identity component of the special fibre of the Néron model is $\mathbf{G}_m$ (untwisted). The image of I_v in $\mathrm{GL}(H_v)$ is a non-trivial group of unipotent matrices, and F_v acts trivially on $H_v^{I_v}$ and by multiplication by q on $H_v/H_v^{I_v}$. Therefore $(\mathrm{Sym}^k H_v)^{I_v}$ is a 1-dimensional space with a trivial G_v-action, and 3. 3 follows.

3. 10. If $v(j) > 0$, there are various cases to consider, according as whether $p \equiv 1$ or $2 \pmod 3$ and whether $k/\mathbb{F}_q(j)$ is ramified at v. We first consider the unramified case $v(j) = 1$; then $k_v = \mathbb{F}_q((j))$. As $v(\Delta) = 2$ in this case, Tate's algorithm and the criterion of Néron-Ogg-Shafarevich imply that the image of I_v in $\mathrm{GL}(H_v)$ has order 6. Since $\Lambda^2 H_v \cong \mathbb{Q}_l(-1)$ is unramified, in terms of a suitable basis $\{X, Y\}$ for $H_v \otimes \bar{\mathbb{Q}}_l$ the image of I_v becomes

$$\left\{ \begin{pmatrix} \zeta & 0 \\ 0 & \zeta^{-1} \end{pmatrix} : \zeta \in \boldsymbol{\mu}_6(\bar{\mathbb{Q}}_l) \right\}.$$

Therefore $(\mathrm{Sym}^k H_v)^{I_v}$ is spanned by the monomials $(XY)^{k/2} (X/Y)^{3i}$ with $i \in \mathbb{Z}$,

$$-(k/6) \leqq i \leqq (k/6).$$

Now if $p \equiv 1 \pmod 3$, then $\boldsymbol{\mu}_6 \subset k_v^*$, and the image of G_v in $\mathrm{GL}(H_v)$ is therefore abelian. We must have

$$F_v(X) = \beta^r X, \quad F_v(Y) = \bar{\beta}^r Y$$

for an algebraic integer β with $\beta\bar{\beta} = p$. (Recall that $q = p^r$.) Since $j \equiv 0 \pmod v$ we have $\beta \in \mathbb{Z}[\sqrt[3]{1}]$. Formula (3. 4. 1) follows immediately (note that the choice of β is irrelevant at this point).

3. 11. In the ramified case, $v(j)=3$. Then if $p\equiv 1 \pmod 3$, we have by Kummer theory $k_v=\mathbb{F}_q((\sqrt[3]{j/b}))$ for some unit $b\in\mathbb{F}_q((j))$. Clearly we may take $b\in\mathbb{F}_p^*$. Let $\varpi=\sqrt[3]{j/b}$; then writing $u=\varpi^{-1}(x+1/12)$, $z=\varpi^{-2}(y+x/2)$, equation (1. 1) becomes

$$\varpi z^2=u^3-\frac{\varpi b u}{48(j-1728)}+\frac{b}{864(j-1728)}.$$

This acquires good reduction over $k_v(\sqrt{\varpi})$, with special fibre of the form

$$w^2=u^3-2\cdot 12^{-6}b. \tag{3. 4}$$

Thus I_v has image $\{\pm 1\}\subset \mathrm{GL}(H_v)$, and the eigenvalues of F_v on H_v are $\pm\alpha^r$, $\pm\bar{\alpha}^r$ where $1+p-(\alpha+\bar{\alpha})$ is the number of points on the elliptic curve (3. 4) over $\mathbb{F}_p$. By [D-H] this implies

$$\alpha=\beta\left(\frac{-8b}{\beta}\right)_6,$$

where β is chosen as in 3. 4. Since k is even, $\mathrm{Sym}^k H_v$ is unramified, so

$$\begin{aligned}\mathrm{Tr}(x)&=\sum_{i=0}^{k}(\pm\alpha^r)^i(\pm\bar{\alpha}^r)^{k-i}\\ &=\sum_{-\frac{k}{2}\leqq i\leqq\frac{k}{2}} q^{\frac{k}{2}}(\alpha/\bar{\alpha})^i\end{aligned}$$

and (3. 4) results.

3. 12. Now suppose that $v(j)>0$ and $p\equiv 2 \pmod 3$. Then A_v has potentially good and supersingular reduction. In the unramified case, since $\boldsymbol{\mu}_6\nsubseteq k_v^*$, the image of G_v in $\mathrm{GL}(H_v)$ is a semi-direct product:

$$I_v\to\left\{\begin{pmatrix}\zeta & 0\\ 0 & \zeta^{-1}\end{pmatrix}:\zeta\in\boldsymbol{\mu}_6(\bar{\mathbb{Q}}_l)\right\},$$

$$F_v\mapsto\begin{pmatrix}0 & 1\\ -p & 0\end{pmatrix}^r.$$

In the ramified case, I_v maps to $\{\pm 1\}$ and F_v acts as above. The formulae (3. 3) follow at once.

3. 13. For $v(j-1728)>0$ the proofs are completely analogous, and we omit them.

3. 14. It is now a simple matter to calculate $\mathrm{Tr}\,\varrho_l(\mathrm{Frob}_p^r)$ in a given case, if we have a set of equations defining V. In the case in which V has genus zero, given by j-equations (2. 2), the computation is particularly easy; for each $t\in\mathbb{F}_q\cup\{\infty\}$ one calculates the corresponding j, and then computes the local term using 3. 2—3. 5 above. The constants b, c of 3. 4, 3. 5 can be read off from the j-equations.

We have carried out this computation for the modular curve corresponding to Γ_{711} given by (2. 4) and $k=2$, for which ϱ_l is two-dimensional (corresponding to the one-dimensional space of cusp forms of weight 4). Here it suffices to compute $\mathrm{Tr}\,\varrho_l(\mathrm{Frob}_p^r)$ for $r=1$, since we know from § 4. 2 of [S] that $\det \varrho_l(\mathrm{Frob}_p)=p^3$. For $p=5$ and $11 \leqq p < 100$ the numbers $A_p = \mathrm{Tr}\,\varrho_l(\mathrm{Frob}_p)$ are given below.

p	5	11	13	17	19	23	29	31
A_p	−12	48	56	−114	2	−120	−54	236

37	41	43	47	53	59	61
146	126	−376	−12	174	138	380

67	71	73	79	83	89	97
−484	576	−1150	776	378	−390	−1330

§ 4. Modular forms on $\Gamma_0(14)$

4. 1. Write $M_w(N)$, $S_w(N)$ for the spaces of modular and cusp forms of weight w on $\Gamma_0(N)$. Recall the Ramanujan series

$$P(\tau) = 1 - 24 \sum_{n=1}^{\infty} \sigma(n) q^n = \frac{12}{\pi i} \frac{\eta'(\tau)}{\eta(\tau)}$$

where

$$\eta(\tau) = q^{\frac{1}{24}} \prod_{n=1}^{\infty} (1-q^n)$$

is Dedekind's η-function.

4. 2. Lemma. *For any $a(d) \in \mathbb{C}$, $d|N$ such that $\sum_{d|N} d^{-1} a(d) = 0$, the function*

$$G(\tau) = \sum_{d|N} a(d)\, P(d\tau)$$

belongs to $M_2(N)$, and if $p|N$,

$$G(\tau)|W_p = \sum_{p|d} p^{-1} a(d)\, P(p^{-1} d\tau) + \sum_{p\nmid d} p a(d)\, P(p d\tau).$$

Proof. The first part is classical. One has ([H], pp. 413, 474)

$$P(\tau) = E_2(\tau) + \frac{3}{\pi\, \mathrm{Im}(\tau)}$$

where

$$E_2(\tau) = \frac{1}{2} \lim_{s\to 0} \sum_{\substack{m,n \\ (m,n)=1}} \frac{1}{(m\tau+n)^2\, |m\tau+n|^s}$$

and

$$E_2\left(\frac{a\tau+b}{c\tau+d}\right)=(c\tau+d)^2\,E_2(\tau)$$

if

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}).$$

The lemma then follows from calculating the action of the W_p-operators on $E_2(d\tau)$.

4. 3. Corollary. *If* $(\alpha, \beta)=(+1,-1), (-1,+1)$ *or* $(-1,-1)$ *then*

$$G_{\alpha,\beta}(\tau)=14P(14\tau)+7\alpha P(7\tau)+2\beta P(2\tau)+\alpha\beta P(\tau)$$

belongs to $M_2(14)$, *and*

$$G_{\alpha,\beta}|W_2=\alpha G_{\alpha,\beta}; \quad G_{\alpha,\beta}|W_7=\beta G_{\alpha,\beta}.$$

4. 4. The space $M_2(14)$ is four-dimensional, and the forms $G_{\alpha,\beta}$ span a complement to the one-dimensional subspace $S_2(14)$. A non-zero element of $S_2(14)$ is

$$K(\tau)=\eta(\tau)\,\eta(2\tau)\,\eta(7\tau)\,\eta(14\tau)$$

(cf. [N]). From the Fourier expansion one finds that

$$K|W_2=K, \quad K|W_7=-K.$$

4. 5. The space $S_4(14)$ has dimension four, and is therefore spanned by K^2 and the forms $KG_{\alpha,\beta}$. They are eigenfunctions for W_2, W_7 with eigenvalues $(+1,+1)$ and $(\alpha, -\beta)$ respectively.

4. 6. Proposition. $F(\tau)=\frac{1}{8}K(\tau)\,G_{-1,+1}(\tau)$ *is a newform in* $S_4(14)$.

Proof. From the above $F(\tau)$ is the unique element of $S_4(14)$ whose coefficient of q is 1 and for which $F|W_2=F|W_7=-F$. It suffices to show that it is not an oldform. But $S_4(2)=0$ and thus the oldforms are spanned by $H(\tau)\pm 2H(2\tau)$, where H is a non-zero element of $S_4(7)$, a one-dimensional space. The corresponding W_2, W_7 eigenvalues for these forms are $(\pm 1, \varepsilon)$ where $H|W_7=\varepsilon H$. By 4. 5 the eigenvalues $(+1,-1)$ do not occur in $S_4(14)$, hence $\varepsilon=+1$, the oldforms have W-eigenvalues $(\pm 1,+1)$, and F is a newform.

4. 7. Write

$$F(\tau)=\sum_{n\geqq 1} B_n q^n,$$

so that $B_1=1$ and $B_n\in\mathbb{Z}$ for every $n\geqq 1$. A simple calculation verifies that for $p=5$ and $11\leqq p<100$ the numbers A_p (from 3. 14 above) and B_p are equal. (In fact we only need to verify equality for $p<30$; see 5. 8 below.)

§ 5. Application of the method of Faltings and Serre

5. 1. We have considered the representations ϱ_l associated to the cusp form of weight 4 on Γ_{711}, and calculated the numbers $A_p = \mathrm{Tr}\,\varrho_l(\mathrm{Frob}_p)$ for various primes p in 3. 14. By [D 1], associated to the cuspform $F(\tau)$ of the preceding section is a system $\{\varrho_l'\}$ of 2-dimensional l-adic representations of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$, such that if $p \notin \{2, 7, l\}$ then ϱ_l' is unramified at p and

$$\mathrm{Tr}\,\varrho_l'(\mathrm{Frob}_p) = B_p, \quad \det \varrho_l'(\mathrm{Frob}_p) = p^3.$$

By Theorem 2. 3 of [R] the representations ϱ_l, ϱ_l' are irreducible.

5. 2. Theorem. *ϱ_l and ϱ_l' are isomorphic for every l.*

Theorem B is an immediate corollary. By Cebotarev's density theorem and the irreducibility, it suffices to prove 5. 2 for $l=2$. For this we shall use the following theorem of Serre. Let K be a number field, and S a finite set of primes of K. Let $\chi_1, \dots, \chi_r$ be a maximal independent set of quadratic characters of $G = \mathrm{Gal}(\bar{K}/K)$ unramified away from S, and let Σ be a subset of G such that the map

$$(\chi_1, \dots, \chi_r): \Sigma \longrightarrow (\mathbb{Z}/2)^r$$

is surjective.

5. 3. Theorem. *Let $\varrho, \varrho': G \longrightarrow \mathrm{GL}_2(\mathbb{Q}_2)$ be continuous semisimple representations, unramified away from S, whose images are pro-2-groups. If for every $\sigma \in \Sigma$*

$$\mathrm{Tr}\,\varrho(\sigma) = \mathrm{Tr}\,\varrho'(\sigma) \quad \textit{and} \quad \det \varrho(\sigma) = \det \varrho'(\sigma)$$

then ϱ, ϱ' are isomorphic.

(For the proof and a generalisation see § 4 of [L]; see also [Se].)

5. 4. *Proof of* 5. 2 *for* $l=2$. Write $\varrho = \varrho_2$, $\varrho' = \varrho_2'$. Taking $K = \mathbb{Q}$ and $S = \{2, 7\}$, we shall show that the conditions of 5. 3 are satisfied for a certain Σ. Assuming without loss of generality that the images of ϱ, ϱ' lie in $\mathrm{GL}_2(\mathbb{Z}_2)$, let us denote by

$$\tilde{\varrho}, \tilde{\varrho}': G \longrightarrow \mathrm{GL}_2(\mathbb{F}_2)$$

their reductions modulo 2.

5. 5. Lemma. *If $p=13$ or 19, then $\tilde{\varrho}(\mathrm{Frob}_p)$ and $\tilde{\varrho}'(\mathrm{Frob}_p)$ have order two.*

Proof. If $g \in \mathrm{GL}_2(\mathbb{Z}_2)$ satisfies

$$g \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod 2$$

then by a simple calculation

$$\mathrm{Tr}(g) \equiv \det(g) + 1 \pmod 4.$$

Hence

$$\tilde{\varrho}(\mathrm{Frob}_p)=1 \Rightarrow A_p \equiv p^3+1 \pmod 4.$$

Now for $p=13$, 19 we have from 3.14 that $A_p \equiv p^3-1 \pmod 4$, whence $\tilde{\varrho}(\mathrm{Frob}_p) \neq 1$; and $\tilde{\varrho}(\mathrm{Frob}_p)^2=1$ since $A_p \equiv 0 \pmod 2$. The same applies to ϱ'.

5.6. Proposition. *The images of $\tilde{\varrho}$, $\tilde{\varrho}'$ have order exactly* 2.

Proof. Consider the composite homomorphism θ below:

$$\begin{array}{ccc} G & \xrightarrow{\tilde{\varrho}} & \mathrm{GL}_2(\mathbb{F}_2) \cong S_3 \\ & \searrow^{\theta} & \downarrow \\ & & \mathbb{Z}/2. \end{array}$$

By the preceding lemma θ is surjective. It therefore cuts out a quadratic extension M/Q, unramified away from 2 and 7, in which 13 and 19 are inert. The only possibilities are then $M=\mathbb{Q}(\sqrt{2})$ or $\mathbb{Q}(\sqrt{-7})$. If the image of $\tilde{\varrho}$ was not of order 2 then $\tilde{\varrho}$ would be surjective, which is impossible in view of the following lemma.

5.7. Lemma. *There is no S_3-extension $L/\mathbb{Q}$, unramified away from* 2 *and* 7, *whose quadratic subfield M is $\mathbb{Q}(\sqrt{2})$ or $\mathbb{Q}(\sqrt{-7})$.*

Proof. One must show that there is no idèle class character

$$\psi : J_M/M^* \twoheadrightarrow \boldsymbol{\mu}_3,$$

unramified away from $\{v : v|14\infty\}$, which satisfies $\psi^\sigma=\psi^{-1}$ for the non-trivial automorphism σ of M. Since M has class number one in either case this is a simple exercise in class field theory, which we leave to the reader.

5.8. By 5.6 the images of ϱ and ϱ' are pro-2-groups. We may take

$$\chi_1=\left(\frac{-1}{p}\right), \quad \chi_2=\left(\frac{2}{p}\right) \quad \text{and} \quad \chi_3=\left(\frac{p}{7}\right).$$

Then

$$\Sigma=\{1, c\} \cup \{\mathrm{Frob}_p : 11 \leqq p \leqq 29\}$$

(where c denotes complex conjugation) satisfies the condition of 5.2. Since

$$\det \varrho = \det \varrho' : G \longrightarrow \mathbb{Z}_2^*$$

is the cube of the cyclotomic character, we have $\mathrm{Tr}\,\varrho(c)=\mathrm{Tr}\,\varrho'(c)=0$, and by 4.7 the remaining conditions of 5.3 are satisfied. This concludes the proof of 5.2 and Theorem B.

References

[A-SwD] *A. O. L. Atkin, H. P. F. Swinnerton-Dyer*, Modular forms on noncongruence subgroups, Proc. Symp. Pure Math. A.M.S. **19** (1971), 1—25.

[D1] *P. Deligne*, Formes modulaires et représentations *l*-adiques, Sém. Bourbaki, éxp. 355, Lect. Notes in Math. **179** (1969), 139—172.

[D2] *P. Deligne*, Courbes elliptiques: Formulaire (d'après J. Tate), Modular functions of one variable IV, Lect. Notes in Math. **476** (1975), 53—73.

[D3] *P. Deligne*, Cohomologie étale (SGA $4\frac{1}{2}$), Lect. Notes in Math. **569** (1977).

[D4] *P. Deligne*, Valeurs de fonctions L et périodes d'intégrales, Proc. Symp. Pure Math. A.M.S. **33** (1979), 313—346.

[D-H] *H. Davenport, H. Hasse*, Die Nullstellen der Kongruenz-Zetafunctionen in gewissen zyklischen Fällen, J. reine angew. Math. **172** (1935), 151—182.

[F] *G. Faltings*, Endlichkeitssätze für abelsche Varietäten über Zahlkörpern, Invent. math. **73** (1983), 349—366.

[G] *A. Grothendieck*, Revêtements étales et groupe fondamental (SGA 1), Lect. Notes in Math. **244** (1971).

[H] *E. Hecke*, Mathematische Werke, Göttingen 1959.

[I] *Y. Ihara*, Hecke polynomials as congruence ζ-functions in elliptic modular case, Ann. of Math. **85** (1967), 267—295.

[L] *E. Livné*, Cubic exponential sums and Galois representations, Contemp. Math. **67** (1987), 247—261.

[N] *M. Newman*, Construction and application of a class of modular functions II, Proc. London Math. Soc. (3) **9** (1959), 373—387.

[R] *K. Ribet*, Galois representations attached to eigenforms with Nebentypus, Modular functions of one variable V, Lect. Notes in Math. **601** (1977), 17—52.

[S] *A. J. Scholl*, Modular forms and de Rham cohomology; Atkin-Swinnerton-Dyer congruences, Invent. math. **79** (1985), 49—77.

[Se] *J.-P. Serre*, Résumé de cours 1984-5, Collège de France.

[T] *J. Tate*, Algorithm for determining the type of a singular fibre in an elliptic pencil, Modular functions of one variable IV, Lect. Notes in Math. **476** (1975), 33—52.

Department of Mathematical Sciences, University of Durham, Durham DH1 3LE, England

Eingegangen 28. Juli 1987