*Herrn C.L. Siegel gewidmet*

# ON $\ell$-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 $\ell$-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

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

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 $\nu$th 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.

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

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

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

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

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

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

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 $\Delta$, 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 $\ell$-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 $\ell$ be a prime number; denote by $K_\ell$ the maximal algebraic extension of $\mathbb{Q}$ ramified only at $\ell$, and by $K_\ell^{ab}$ the maximal subfield of $K_\ell$ abelian over $\mathbb{Q}$. For any prime $p \neq \ell$ denote by Frob(p) the conjugacy class of Frobenius elements of p in $\mathrm{Gal}(K_\ell/\mathbb{Q})$; 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 $\ell$-adic units; and this induces a canonical character

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

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*

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

*Then there is a continuous homomorphism*

$$\rho_\ell : \mathrm{Gal}(K_\ell/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{Z}_\ell),$$

*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, $\Delta$ 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 $\rho_\ell$ is small enough, a knowledge of the determinant of an element of the image will imply some $\ell$-adic information about the trace of that element; and so in particular a knowledge of p (or even an appro-

ximate $\ell$-adic knowledge of p) will imply some $\ell$-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 $\rho_\ell$, 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 $\rho_\ell$.

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

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

By (9) the image of $\det \circ \rho_\ell$ is just the (k-1)th powers in $\mathbb{Z}_\ell^*$; so to find the image of $\rho_\ell$ a major step will be to find its intersection with $SL_2(\mathbb{Z}_\ell)$. In particular, if this intersection is the whole of $SL_2(\mathbb{Z}_\ell)$ then the image of $\rho_\ell$ will be the entire inverse image of $(\mathbb{Z}_\ell^*)^{k-1}$ in $GL_2(\mathbb{Z}_\ell)$. 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 $GL_2(\mathbb{Z}_\ell)$ which is closed in the $\ell$-adic topology. If the image of G under reduction mod $\ell$ contains $SL_2(\mathbb{F}_\ell)$ then G contains $SL_2(\mathbb{Z}_\ell)$.

PROOF. For each $n > 0$, denote by $G_n$ the image of G in $GL_2(\mathbb{Z}/\ell^n\mathbb{Z})$. Since G is closed, to prove the lemma it is enough to prove that $G_n \supset SL_2(\mathbb{Z}/\ell^n\mathbb{Z})$ 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

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

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 $SL_2(\mathbb{Z})$, whence there is an element $\sigma$ in G such that $\sigma \equiv I + u \bmod \ell$, that is

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

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

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

since all the other terms which occur when the powers of $(u + \ell v)$ are written out in full either contain a factor $\ell^2$ 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 $\sigma$ of G such that

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

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

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

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

COROLLARY. Suppose that $\ell > 3$; then $\ell$ 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 $\ell$ 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 $\chi_\ell$ and whose image contains $SL_2(\mathbb{F}_\ell)$. He further conjectures that for any $\ell$ such a homomorphism is always connected in an obvious sense with a modular form mod $\ell$ 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 $\ell$ between p and $a_p$; and for each exceptional prime $\ell$ 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 $\ell$; 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 $\ell$ the position is less satisfactory, primarily because at present we lack a structure theorem for modular forms mod $\ell^\nu$. 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 $\rho_2$, 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 $\ell$ 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 $\ell^2$ 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 $GL_2(\mathbf{F}_\ell)$. If the order of G is divisible by $\ell$, then either G is contained in a Borel subgroup of $GL_2(\mathbf{F}_\ell)$ or G contains $SL_2(\mathbf{F}_\ell)$. If the order of G is prime to $\ell$, let H be the image of G in $PGL_2(\mathbf{F}_\ell)$; 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) $\ell$ must be odd; in case (iii) $\ell$ must be prime to 6,6 or 30 respectively.

PROOF. Suppose first that the order of G is divisible by $\ell$, and choose $\sigma$ in G of order exactly $\ell$; then there is a unique one-dimensional subspace W of V which is an eigenspace of $\sigma$. If every element of G has W as an eigenspace, then G is contained in the Borel subgroup associated with W. If not, let $\sigma_1$ 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 $\ell$ 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 $SL_2(\mathbf{F}_\ell)$, 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 $\ell$. The analo-

gous 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 $\ell$, 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 $\sigma_1$ and $\sigma_2$ 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 $\ell$, contrary to hypothesis.

The set of eigenvectors of non-trivial elements of H is finite and invariant under H; let $\xi_1,\ldots,\xi_\nu$ be representatives of the orbits under H and for each $\xi_i$ let $\mu_i > 1$ be the number of elements of H which fix $\xi_i$. If h is the order of H then the orbit of $\xi_i$ contains $h/\mu_i$ 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

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

which can be rewritten as

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

An easy calculation shows that the solutions of this, with each $\mu_i$ 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 $\xi_3$ 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 $\xi_3$ 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 $\xi_2$ 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 $\mu_i$ 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 $\rho_\ell$ be any continuous homorphism $\mathrm{Gal}(K_\ell/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{Z}_\ell)$ such that $\det \circ \rho_\ell = \chi_\ell^{k-1}$ for some even integer k. Let $G \subset \mathrm{GL}_2(\mathbb{F}_\ell)$ be the image of $\tilde{\rho}_\ell$ and let H be the image of G in $\mathrm{PGL}_2(\mathbb{F}_\ell)$. Suppose that G does not contain $\mathrm{SL}_2(\mathbb{F}_\ell)$. Then*

(i) *G is contained in a Borel subgroup of $\mathrm{GL}_2(\mathbb{F}_\ell)$; 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 $\ell$, 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 $\sigma$ of

$\mathrm{Gal}(K_\ell/\mathbb{Q})$ which corresponds to complex conjugation under some complex embedding of $K_\ell$. 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 :

$$\begin{array}{ccc} \mathrm{Gal}(K_\ell/\mathbb{Q}) & \to & G \xrightarrow{\det} \mathbb{F}_\ell^* \\ & & \downarrow \qquad\quad \downarrow \\ & & H \to \mathbb{F}_\ell^*/\mathbb{F}_\ell^{*2} \sim \{\pm 1\} \end{array}$$

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*

$$\rho_\ell : \mathrm{Gal}(K_\ell/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{Z}_\ell)$$

*be the continuous homomorphism given by Theorem* 1. *Suppose that the image of* $\tilde{\rho}_\ell$ *does not contain* $\mathrm{SL}_2(\mathbb{F}_\ell)$, *so that* $\ell$ *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* $\ell$.

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

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

PROOF. In case (i) we may without loss of generality suppose that the Bo-

rel subgroup involved consists of the upper triangular matrices; thus for any $\sigma$ 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 $\alpha$ 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 $\mathrm{GL}_2(\mathbf{F}_2)$ 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 $\ell$. Now let $\alpha$ be an element of N not in C; after a field extension if necessary, $\alpha$ 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 $\alpha$ has zero trace. Hence $a_p \equiv 0 \bmod \ell$ whenever p is a quadratic non-residue mod $\ell$, 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 $\mu^2, \mu^4, \mu^6$ or $\mu^8$ 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 $\ell$. 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 $\ell$ and satisfy

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

## 3. Modular forms mod $\ell$.

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 $(2\nu)$th Bernoulli number; and

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

For $\nu > 1$ these are different normalizations of the Eisenstein series of weight $2\nu$. This $G_2$ is essentially the $\eta_2$ 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,

$$1728\Delta = Q^3 - R^2; \qquad (11)$$

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

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

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

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

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

$$3\theta Q - PQ = -R, \quad 2\theta R - PR = -Q^2,$$
$$12\theta P - P^2 = -Q, \quad \theta\Delta - P\Delta = 0 \quad . \tag{14}$$

We can reformulate lemma 3 in terms of the operator $\partial$ defined by

$$\partial = 12\theta - kP \quad \text{on modular forms of weight } k. \tag{15}$$

COROLLARY. $\partial$ <u>is the derivation on the graded algebra of modular forms such that</u> $\partial Q = -4R$ <u>and</u> $\partial R = -6Q^2$.

We can now define modular forms mod $\ell$. Denote by $\mathcal{O}$ the local ring of $\mathbb{Q}$ at $\ell$ - that is, the ring of rational numbers with denominator prime to $\ell$. Let $M_k$ be the $\mathcal{O}$-module of those modular forms of weight k whose q-series expansions have all their coefficients in $\mathcal{O}$; 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 $\ell$.) Then the $\mathbb{F}_\ell$-algebra of modular forms mod $\ell$ 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 $\ell$-adic nature of Bernouilli numbers.

LEMMA 4. (von Staudt-Kummer).

(i) <u>If</u> $(\ell - 1) \mid 2\nu$ <u>then</u> $\ell b_{2\nu} \equiv -1 \bmod \ell$.

(ii) <u>If</u> $(\ell - 1) \nmid 2\nu$ <u>then</u> $b_{2\nu}/2\nu$ <u>is</u> $\ell$-<u>integral and its residue class mod</u> $\ell$ <u>only depends on</u> $2\nu \bmod (\ell - 1)$.

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 $\sigma$; then $\tilde{f}$ will denote the formal power series $\sum \tilde{a}_n q^n$. Again, let $\phi(X,Y)$ be a polynomial in $\sigma[X,Y]$; then $\tilde{\phi}(X,Y)$ will denote the polynomial in $\mathbb{F}_\ell[X,Y]$ obtained from $\phi$ by reduction of the coefficients mod $\ell$. However, the natural arguments for $\phi$ 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 $\mathbf{F}_\ell$, whereas $\tilde{\phi}(\tilde{Q},\tilde{R})$ is the element of $\mathbf{F}_\ell[[q]]$ obtained from this polynomial by substitution. In particular if f is in $M_k$ then there is a unique polynomial $\phi$ such that $\phi(Q,R) = f$; for $\ell > 3$ the coefficients of $\phi$ are in $\sigma$ and $\tilde{\phi}(\tilde{Q},\tilde{R}) = \tilde{f}$. Note that the derivation $\partial$ on $\sigma[Q,R]$ induces a derivation, also written $\partial$, on $\mathbb{F}_\ell[Q,R]$, and that $\Theta$ 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 $\sigma[Q,R]$; 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

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

which extends $\sigma \to \mathbb{F}_\ell$ 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

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

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 $\mathbf{F}_\ell[Q,R]/(\tilde{A}-1)$ 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 $\ell$; 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 $\mathbf{F}_\ell$. 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 $a$ the kernel of the map $\mathbf{F}_\ell[Q,R] \to \mathbf{F}_\ell[[q]]$ obtained by substituting $\tilde{Q}$ and $\tilde{R}$ for Q and R; clearly $a$ contains $\tilde{A} - 1$, and $a$ is prime because the image is an integral domain. If $a$ were maximal then $\tilde{Q}$ and $\tilde{R}$ would be algebraic over $\mathbf{F}_\ell$, which is absurd because the coefficient of q in at least one of them is non-zero. Since $\mathbf{F}_\ell[Q,R]$ has dimension 2, in order to prove that $a = (\tilde{A} - 1)$ 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 $\phi_\nu$ is isobaric of weight $\nu$, and let $\tilde{c}$ be a primitive $(\ell - 1)^{\text{th}}$ root of unity in $\mathbf{F}_\ell$; 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 $\partial$ is an operator of weight 2 on $\tilde{M}$; and the same is true of $\Theta$ since $\tilde{P}$ is a modular form mod $\ell$ of weight 2. It is this last property which makes the theory of modular forms mod $\ell$ 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 :

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

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

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

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

$\ell = 13.$ 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$(\ell - 1)$. 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) Let f be a modular form of weight k such that $f = \phi(Q,R)$ for some $\phi$ in $\mathcal{O}[Q,R]$, and suppose that $\tilde{f} \neq 0$. Then $\omega(\tilde{f}) < k$ if and only if $\tilde{A}$ divides $\tilde{\phi}$.

(ii) Let $\tilde{f}$ be a graded element of $\tilde{M}$; then $\omega(\theta\tilde{f}) \leqslant \omega(\tilde{f}) + \ell + 1$, (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 $\ell$ 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 $\ell$. 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 $\ell$ 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 $n \leqslant k/12$ 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 $\ell$ 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 $\Delta$ only makes use of the coefficients of $q^n$ for $n \leqslant k/12$ in $(f_1 - f_2)$, and all these are divisible by $\ell$; 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 $\partial$ 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 $\Delta$ is 1 and that $\partial\Delta = 0$.

There is as yet no satisfactory structure theory of modular forms mod $\ell^n$ where $n > 1$. At first sight it would seem natural to conjecture that for $\ell > 3$ the ideal of those elements of $\mathfrak{o}[Q,R]$ whose q-series expansion has all its coefficients divisible by $\ell^n$ is $(\ell, A - 1)^n$. It is not difficult to prove this conjecture for $n \leq \ell$; 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 $\ell$ for which there exist congruences for $\tau(n)$ or $a_n$ mod $\ell$. For we have seen in §2 that to each exceptional prime $\ell$ there correspond congruences for $a_p$ mod $\ell$; 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* $\ell$ *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

$$(\rho_\ell, \chi_\ell) : \mathrm{Gal}(K_\ell/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{Z}_\ell) \times \mathbb{Z}_\ell^* \tag{18}$$

contains $\mathrm{SL}_2(\mathbb{Z}_\ell) \times 1$. By hypothesis, the projection of the image onto the first factor contains $\mathrm{SL}_2(\mathbb{Z}_\ell)$; so the image of the commutator subgroup contains $\mathrm{Comm}(\mathrm{SL}_2(\mathbb{Z}_\ell)) \times 1$. If $\ell > 3$ this commutator subgroup is the whole of $\mathrm{SL}_2(\mathbf{Z}_\ell)$, by lemma 1 and the simplicity of $\mathrm{SL}_2(\mathbf{F}_\ell)$. If $\ell = 2$ or 3 and $\sigma$ in $\mathrm{Gal}(K_\ell/\mathbb{Q})$ is such that $\rho_\ell(\sigma)$ is in $\mathrm{SL}_2(\mathbb{Z}_\ell)$ 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 $\mathrm{GL}_2(\mathbb{Z}_\ell)$ 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 $\ell$; 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, $\ell$ and $\rho_\ell$ 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 $\ell$ 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 mod$(\ell - 1)$. 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 $0 \leqslant m < m' < \ell - 1$ 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 $\theta$ on each side has been put in to annihilate the coefficient of $q^n$ when n is divisible by $\ell$. 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 $\ell$ 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 $\omega(\theta\tilde{f}) \leqslant k + \ell + 1$. But obviously $\omega(\tilde{G}_{2\nu}) = 2\nu$ whenever $2 \leqslant 2\nu < \ell - 1$; 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

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

If $\ell > k$ then $m + m' \geqslant k - 1$ 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 $\ell$ 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

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

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 $\ell$ 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 $\theta$. 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 $\ell$ 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 $a_p \neq 0$; then if $\ell$ is an exceptional prime of this type either $\ell = p$ or $\ell$ 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 $\ell$. There are some further conditions on $\ell$ 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 $\ell$ and for which $\ell$ divides $a_p^2 - 2p^{k-1}$; since k is even, it follows that 2 is a quadratic non-residue mod $\ell$. 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 $\ell$. 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 $\theta$ on a modular form. Let f be a modular form of weight k, and write

$$f_0 = f,\ f_1 = \partial f,\ f_\nu = \partial f_{\nu-1} - (k+\nu-2)(\nu-1)Qf_{\nu-2} \text{ for } \nu > 1,$$

where we have identified f with its expression as a polynomial in Q and R. Then for any $n \geq 0$ 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 $\ell$ |
|---|---|---|---|---|---|---|---|---|---|---|---|
| $\Delta$ | 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 $\ell$ is exceptional, or the word 'No' if $\ell$ is not exceptional.

(ii) For these six forms, the only exceptional primes of type (ii) are $\ell = 23$ for $\Delta$ 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

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

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 $\ell$ 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 $\ell$ and to verify that $a_p$ is not divisible by $\ell$; 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 $\Delta$, 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 $\ell$ 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 $\ell$; congruences modulo higher powers of $\ell$, and the information about $\rho_\ell$ that can be derived from them, will be discussed in §5. For exceptional primes of types (ii) and (iii) however, therestill 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

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

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 Gal(K/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 $k = 16$, $\ell = 31$ 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 $\Gamma_0(\ell)$ for a certain quadratic character; so its square is a modular form of weight 2 for $\Gamma_0(\ell)$. By a theorem of Serre, proved in his lecture at this conference, any modular form of weight 2 for $\Gamma_0(\ell)$ whose q-series has integral coefficients is congruent mod $\ell$ to a modular form of weight $(\ell + 1)$ 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 $\ell$, lies in $\tilde{M}_{\ell+1}$. By lemma 6, to prove (26) or (27) it is now enough to check it for the coefficients of $q^0, q^1$ and $q^2$; and this is easy.

There remains the case $\ell = 59$ 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

$$\mathrm{Gal}(K_{59}/\mathbb{Q}) \to \mathrm{PGL}_2(\mathbb{F}_{59});$$

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 $\mathrm{PGL}_2(\mathbb{F}_{59})$ to $\mathrm{GL}_2(\mathbb{F}_{59})$ is easy; but it is not very useful because the result is too large. It is better to study not $\rho$ 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 $\mathrm{GL}_2(\mathbb{F}_{59})$ 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 $\mathrm{GL}_2(\mathbb{Z}[\sqrt{-2}])$; 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-se-

ries 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

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

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 $\ell$.

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 $\mu$,

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

is a modular form of weight 12 for $\Gamma_0(64)$, and by combining these forms we find that for any $\nu$ 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 $\Gamma_0(64)$. Such modular forms are algebraic and integral over $\mathbb{Z}[Q,R,\Delta]$, 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 $\Gamma_0(64)$; 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 $\theta$. However, $\theta$ can be expressed in terms of $\vartheta$, 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

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

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 $\rho_{23}$, 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

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

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 $\sigma$ 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 $\rho_2$ 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* $\alpha$ *in* $N$ *and* $\beta$ *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 $\rho_2$, which is described in detail in the Appendix. By a straightforward but tedious calculation one verifies that to every $\alpha$ and $\beta$ satisfying the congruence conditions above, there exist elements of $G$ with trace $\alpha$ and determinant $\beta^{11}$. 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 $\alpha$ in $\mathbb{Z}_2$ such that there is an element of $G$ with trace $\alpha$ and determinant $\beta^{11}$. It may be shown that $S(\beta)$ is a union of complete residue classes mod $2^{17}$ and that it only depends on $\beta$ 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 $\tau(p) \bmod 2^{12}$, 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.

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

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 $\phi$. If $\phi$ 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 $\phi$ 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 $\phi$ 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 $\sigma$ 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 $\sigma$ which primarily interest us. Moreover

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

will denote the trace and determinant of $\sigma$; 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 $\theta,\phi,\psi$ will be the characters of $\Delta$ mod 8 whose values are given by the following table :

| $\Delta$ mod 8 | 1 | 3 | 5 | 7 |
|---|---|---|---|---|
| $\theta$ | 1 | 1 | -1 | -1 |
| $\phi$ | 1 | -1 | 1 | -1 |
| $\psi$ | 1 | -1 | -1 | 1 |

If we have to consider several $\sigma$ 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 $\sigma$ 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

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

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

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

(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 :

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

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 $\sigma$ 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 $\sigma_o$ such that

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

Moreover with this normalization A,B,C,D are integers for every $\sigma$ 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

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

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 $\sigma$ 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 $\sigma$ runs through the elements of G. If $\sigma_1$, $\sigma_2$ are such that $2^\beta || b_1$ and $2^\gamma || c_2$ then for one of $\sigma_1$, $\sigma_2$ and $\sigma_1 \sigma_2$ we have both $2^\beta || b$ and $2^\gamma || c$; and now $4|bc$ gives $\beta + \gamma \geq 2$. 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 $\beta \geq 1$ and $\gamma \geq 1$.

Now choose an element $\sigma_o$ 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 $\sigma_o$ 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 $\sigma$ in G are still integral after the transformation. However we have temporarily lost all information about $\beta$ and $\gamma$.

Applying (37) to $\sigma\sigma_o$, which mod $2^{13}$ only differs from $\sigma$ 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 $2^8 \mid (a - 1)$ 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 $2^7 \mid bc$, whence $ad - bc = \Delta$ shows that $d \equiv \Delta \bmod 2^7$. With this additional help, (37) now gives $2^9 \mid bc$. With the same definition of $\beta, \gamma$ 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 $\sigma$ 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

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

Note that D and $\Delta$ 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

$$A \equiv A_1 + A_2 + 4B_1C_2,\ B \equiv B_1\Delta_2 + B_2\ ,\ C \equiv C_1 + \Delta_1C_2 \qquad (39)$$

all mod $2^7$.

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

| $\Delta \bmod 8$ | $\pm 1$ | $\pm 3$ |
|---|---|---|
| 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 $\sigma_o$ 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 $\theta$ 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,

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

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 $\sigma$ 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 $\sigma_o$. This completes the proof of the lemma.

We now complete the normalization of G. Fix an element $\sigma_3$ 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 $\lambda$ such that multiplying the last term on the right by $\lambda^2$ replaces the congruence by an equality. Now for every $\sigma$ in G multiply c by $\lambda$ and divide b by $\lambda$; this is an allowed transformation and does not affect the representation of $\sigma_o$ given by (36). So henceforth we can assume that there is a $\sigma_3$ with

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

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 $\sigma\sigma_0$, where $\sigma_0$ satisfies (36). Finally suppose that $\Delta \equiv \pm 3 \bmod 8$ and write $\sigma_1 = \sigma\sigma_3^{-1}$ where $\sigma_3$ satisfies (40); thus $\theta = \theta_1$ and $\sigma$ 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 $\sigma_1$. This last expression vanishes mod 32, and this completes the proof of the Corollary.

LEMMA 11. G is contained in $G_o$.

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 $\Delta$ 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 $\sigma_o$ 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 $\Delta$ 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 $\sigma_3$ 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,

$$A - \tfrac{1}{8}(\Delta + 50)(3\Delta + 130) - 3 + 2C^2$$

$$\equiv A_1 + A_3 + 2C_1^2 + 2\Delta_1^2C_3^2 + 2C_3(\Delta_1^2 - 1) - \tfrac{1}{8}(\Delta + 50)(3\Delta + 130) - 3$$

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

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

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 $\Delta$ 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 $\sigma$ in G with $\Delta$ equal to some fixed $\Delta_1$ are obtained from one of them by multiplication by the elements of G with $\Delta = 1$. Choose $\sigma_1$ 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 $\sigma$ with $\Delta = 1$ and

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

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 $\sigma_1$ and $\sigma_2$ 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

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

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 $\sigma$ 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 $\sigma$ in $H_{n-1}$ the map that sends $\sigma$ to $\sigma^2$ 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 $\rho_2$ and det, is $\chi_2^{11}$ 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 $\sigma$ 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 $\sigma_1$ and $\sigma_2$ 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 $\sigma$ 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 $\sigma$ 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 $\sigma$ 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 $\ell$-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 $\tau$ de Ramanujan. (Séminaire Delange-Pisot-Poitou, 1967-68, exposé 14)

[10] J.-P. SERRE: Abelian $\ell$-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.