Can. J. Math. Vol. 47 (6), 1995 pp. 1201–1218

RATIONAL HAUPTMODULS ARE REPLICABLE

C. J. CUMMINS AND S. P. NORTON

ABSTRACT. It is shown that if f is a Hauptmodul with rational integer coefficients for a group $G < \mathrm{PGL}_2(\mathbb{Q})^+$, of genus zero, containing a $\bar{\Gamma}_0(N)$ with finite index and $z \longmapsto z+k$ precisely when k is an integer, then f is replicable. Examples of such functions are given by the Moonshine functions described by Conway and Norton [CN].

1. **Introduction.** The modular group $\Gamma = \mathrm{SL}_2(\mathbb{Z})$ acts on H^*, the extended upper half plane $H \cup \mathbb{Q} \cup \{i\infty\}$, by fractional linear transformations. The normalized generator, or *Hauptmodul*, of the function field of H^*/Γ is the j function,

$$j(z) = q^{-1} + 744 + 196884q + 21493760q^2 + 864299970q^3 + \cdots$$

where $q = \exp(2\pi i z)$. In this paper we will normalize Hauptmoduls to have zero constant term, so we take $J = j - 744$ as the normalized Hauptmodul for Γ. As noted by McKay the coefficient 196884 is almost the dimension of the smallest nontrivial complex representation of the Monster group $\mathbb{M}$, moreover other coefficients are the dimensions, d_n, of representations V_n of $\mathbb{M}$. Other series are be obtained by replacing the d_n by character values on V_n of other conjugacy classes of $\mathbb{M}$ (Thompson [T]). For example for the class $2B$ we obtain the series

$$t_{2B} = q^{-1} + 276q - 2048q^2 + 11202q^3 + \cdots$$

which is the Hauptmodul for the function field of the congruence subgroup $\Gamma_0(2)$. Conway and Norton [CN] made a number of remarkable conjectures about these series which they termed "Monstrous Moonshine":

CONJECTURE 1.1. *Each rational conjugacy class in* $\mathbb{M}$ *gives rise to a Hauptmodul for a genus zero subgroup of* $\mathrm{PGL}_2(\mathbb{Q})^+$ *containing a normal subgroup* $\bar{\Gamma}_0(N)$, *for some* N, *of finite index.*

This conjecture has now been proved by Borcherds [B1]. Conway and Norton also conjectured that the power map structure of $\mathbb{M}$ is mirrored in certain relationships between the Moonshine functions. More generally Norton [N1] initiated the study of q-series of the form:

$$f(z) = q^{-1} + H_1 q + H_2 q^2 + H_3 q^3 + \cdots \tag{1.1}$$

Work supported by NSERC and FCAR grants.

Received by the editors November 24, 1993.
AMS subject classification: 11F03, 11F22, 30F35.

where $H_i \in \mathbb{Q}, i = 1, 2, \ldots$, for which a "power map" structure like that of the Moonshine functions can be defined as follows: Given a q-series of the form (1.1) define the n-th replicate of f iteratively by

$$f^{(n)}(nz) = -\sum_{\substack{ad=n\\0\leq b<d}}' f^{(a)}\Big(\frac{az+b}{d}\Big) + Q_n(f) \tag{1.2}$$

where the primed sum means that the term with $a = n$ is omitted and Q_n is the unique polynomial in $f(z)$ with q expansion

$$Q_n(f) = q^{-n} + \text{ terms of degree} > 0.$$

This definition may produce replicates such that the q-expansion of $f^{(n)}(z)$ has terms with fractional powers of q. If however we have that for all $n, f^{(n)}(z)$ has q-expansion

$$f^{(n)}(z) = q^{-1} + H_1^{(n)}q + H_2^{(n)}q^2 + \cdots$$

then we say that f is replicable. As mentioned above it was conjectured by Conway and Norton [CN] that in the case of the Moonshine functions $f^{(n)}(z)$ coincides with the function on the n-th power of the conjugacy class corresponding to $f(z)$ and again this has now been proved by Borcherds [B1]. We note that the sum in equation (1.2) is, in many cases, a Hecke operator for an appropriate group. We shall not make use of this fact.

Norton [N1] defines the bivarial transformation of f to be:

$$\sum_{m,n\geq 1} H_{n,m}p^n q^m = -\log\Big(1 - pq\sum_{i=1}^{\infty} H_i \frac{p^i - q^i}{p - q}\Big) \tag{1.3}$$

so that the $H_{m,n}$ are polynomials in the H_i. He then calls a function *replicable* if it satisfies $H_{m,n} = H_{r,s}$ whenever $mn = rs$ and $(m, n) = (r, s)$. In the appendix it is shown that these two definitions coincide (see also [ACMS]). The latter definition is more convenient for numerical calculations and was used in [ACMS] to calculate all the replicable functions with rational integer coefficients which have only a finite number of distinct replicates, which are themselves replicable; a property that holds for Monstrous Moonshine functions. There are, excluding the trivial cases $q^{-1} + aq$, 326 of them, of which 171 are Monstrous functions. (Note: it is believed that the "finiteness" condition is redundant in the non-trivial cases.)

Norton conjectured the following:

CONJECTURE 1.2. *A function $f = q^{-1} + \sum_{i\geq 1} H_i q^i$ with rational integer coefficients is replicable if and only if either f is trivial or it is the Hauptmodul for a group $G <$ $\mathrm{PGL}_2(\mathbb{Q})^+$ satisfying*

1. *G has genus zero,*
2. *G contains a $\bar{\Gamma}_0(N)$ with finite index,*
3. *G contains $z \longmapsto z + k$ if and only if $k \in \mathbb{Z}$.*

This conjecture has also been extended to include the case of irrational coefficients [N2] and even to the case of higher genus [Sm, N2]. In this paper we shall prove part of this conjecture:

THEOREM 1.3. *If f is a Hauptmodul with rational coefficients for a group $G < \mathrm{PGL}_2(\mathbb{Q})^+$, of genus zero, containing a $\bar{\Gamma}_0(N)$ with finite index and $z \mapsto z+k$ precisely when k is an integer, then f is replicable.*

Some partial results have been obtained by Ferenbaugh [F], Koike [K] and Norton [N2]. The last of these deals with the case of replication by an index prime to N, and extends to irrational coefficients and higher genus. The idea of the proof of Theorem 1.3 is as follows. From the first definition of replicability, f is replicable if we can iteratively define its replication powers $f^{(n)}$. Suppose all lower replicates have been constructed. Then the obstruction to constructing $f^{(n)}$ is that the q series

$$t(z) = -\sum_{\substack{ad=n\\ 0\le b<d}}{}' f^{(a)}\left(\frac{az+b}{d}\right) + Q_n(f)$$

may not be a series in q^n, so we have to show $t(z) = t(z+\frac{1}{n})$. However we can inductively show that both $t(z)$ and $t(z+\frac{1}{n})$ are modular functions for some congruence group, G, with singularities only on $\mathbb{Q}$ and $\{i\infty\}$. We show that $t(z) - t(z+\frac{1}{n})$ is bounded on some fundamental domain of G and hence that $t(z) = t(z+\frac{1}{n})$.

The structure of the rest of the paper is as follows. In Section 2 we derive some results on the Galois action on the coefficients of f. Details of the proof of Theorem 1.3 are in Section 3. In the appendix we give some properties of replicable functions.

2. **Galois action on automorphic functions.** We start with some notation and observations. Let

$$\Gamma_0(N) = \left\{\begin{pmatrix} a & b\\ c & d\end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \mid c \equiv 0 \pmod N\right\}$$

and

$$\Gamma(N) = \left\{\begin{pmatrix} a & b\\ c & d\end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \mid b \equiv c \equiv 0 \pmod N\right\}.$$

Denote by $\bar{\Gamma}_0(N)$ and $\bar{\Gamma}(N)$ the images of $\Gamma_0(N)$ and $\Gamma(N)$ in $\mathrm{PSL}_2(\mathbb{Z}) = \mathrm{SL}_2(\mathbb{Z})/\{\pm I\}$. Up to isomorphism $\mathrm{PSL}_2(\mathbb{Z})$ is a subgroup of $\mathrm{PGL}_2(\mathbb{Q})^+ = \mathrm{GL}_2(\mathbb{Q})^+/\{\mathbb{Q}^* I\}$ (the superscript denotes positive determinants). Similarly $\mathrm{PGL}_2(\mathbb{Q})^+$ is, up to isomorphism, a subgroup of $\mathrm{PGL}_2(\mathbb{R})^+ \simeq \mathrm{PSL}_2(\mathbb{R})$. We identify these subgroups with their images and so we refer, for example, to $\bar{\Gamma}_0(N)$ and $\bar{\Gamma}(N)$ as subgroups of $\mathrm{PGL}_2(\mathbb{R})^+$. It will be convenient to make a distinction between matrices and the corresponding element of $\mathrm{PGL}_2(\mathbb{R})^+$. The former are written with round brackets and the latter with angular brackets. If α is a matrix we shall also write $\langle\alpha\rangle$ for the corresponding element of $\mathrm{PGL}_2(\mathbb{R})^+$.

A subgroup G of $\mathrm{PGL}_2^+(\mathbb{R})$ is a congruence group if it contains a $\bar{\Gamma}(N)$ with finite index. A point of $\mathbb{R} \cup \{i\infty\}$ is called a *cusp* of G if it is fixed by a parabolic element of G. If G is a congruence group, it follows ([Sh] Proposition 1.30) that the set of cusps of G is the same as that of $\mathrm{PSL}_2(\mathbb{Z})$, *i.e.* $\mathbb{Q} \cup \{i\infty\}$. Clearly if w is a cusp and $m \in G$ then $m(w)$ is also a cusp. It is not difficult to use this fact to show that any element of G is a multiple of a matrix with rational entries. Thus G is in fact a subgroup of $\mathrm{PGL}_2(\mathbb{Q})^+$ and we may define $|m|$ as the determinant of m when written as a matrix over $\mathbb{Z}$ in its lowest terms.

In the rest of this paper we shall consider only the following case: G will be a subgroup of $\mathrm{PGL}_2(\mathbb{Q})^+$ containing a $\bar{\Gamma}_0(N)$ with finite index and $z \longmapsto z+k$ precisely when $k \in \mathbb{Z}$. We will also take G to be genus zero with Hauptmodul f. In section 3 we shall restrict further to the case where f has rational q-coefficients. Our aim in the rest of this section is to derive a relation between elements of the group G and $G * k$, the fixing group of the modular function $f * k$ obtained from f by applying the Galois transformation $*k$ to the Fourier coefficients of f. We start by reviewing the results of [Sh] which we shall require.

Let $\mathcal{F}_N$ be the field of modular functions of level N with Fourier coefficients in $\mathbb{Q}\big(\exp(2\pi i/N)\big)$. In Sections 6.1 to 6.5 of [Sh] it is shown that:

a $\mathcal{F}_N = \mathbb{Q}\big(j, f_a \mid a \in (\mathbb{Z}/N\mathbb{Z})^2\big)$. The functions $f_a(z)$ are related to the elliptic curve $\mathbb{C}/(\mathbb{Z}+z\mathbb{Z})$.

b $\mathcal{F}_N$ is a Galois extension of $\mathbb{Q}(j) = \mathcal{F}_1$ with Galois group $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm I\}$. The action of $\alpha \in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ is given by $f_a \longmapsto f_{a\alpha}$. If $\alpha \in \mathrm{SL}_2(\mathbb{Z})$ then $f_a \circ \alpha = f_{a\alpha}$.

c Let k be an integer coprime to N and $*k$ the corresponding element of the group $\mathrm{Gal}\Big(\mathbb{Q}\big(\exp(2\pi i/N)\big)/\mathbb{Q}\Big)$. Then $\begin{pmatrix} 1 & 0 \\ 0 & k \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ acts on $\mathcal{F}_N$ by $f \longmapsto f * k$ where $f * k$ is obtained from f by applying $*k$ to the coefficients of f.

d Let $U = \prod_p \mathrm{GL}_2(\mathbb{Z}_p) \times \mathrm{GL}_2(\mathbb{R})^+$. For every $u \in U$ and every N, there exists an element α of $M_2(\mathbb{Z}) \cap \mathrm{GL}_2(\mathbb{Q})^+$ such that $u_p \equiv \alpha \bmod N \cdot M_2(\mathbb{Z}_p)$. Set $au = a\alpha$ for all $a \in (\mathbb{Z}/N\mathbb{Z})^2$. Then $f_a \longmapsto f_{au}$ defines an element of $\mathrm{Gal}(\mathcal{F}_N/\mathcal{F}_1)$, call it $\tau(u)$.

LEMMA 2.1. *If $M \in G$ then any prime p dividing $|M|$ also divides N.*

PROOF. Suppose, to the contrary, that p divides $|M|$ but not N. Let M' be a matrix corresponding to M which is written in lowest terms over $\mathbb{Z}$. Then the rank of M' considered as a matrix over $\mathrm{GF}(p)$, is 1. As $(p,N) = 1$, $\Gamma(N)$ projects onto the whole of $\mathrm{PSL}_2(p)$ when read modulo p, so that we can find matrices B and C in $\Gamma(N)$ such that $BM'C \equiv \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ (mod p). This implies that for any $i \in \mathbb{Z}^{\geq 0}$ the matrix $(BM'C)^i$ is not zero mod p, but p divides $\det\big((BM'C)^i\big)$ and so the cosets $\langle (BM'C)^i \rangle \bar{\Gamma}(N)$, $i \in \mathbb{Z}^{\geq 0}$ are all distinct and so the index of $\bar{\Gamma}(N)$ in G is infinite, which is a contradiction. ∎

THEOREM 2.2 ([SH] P. 147). *(a) For every $\alpha \in \mathrm{GL}_2(\mathbb{Q})^+$ and every $h \in \mathcal{F}_N$, $h \circ \alpha \in \mathcal{F}_{N'}$ for some N'.*

(b) If $\alpha \in \mathrm{GL}_2(\mathbb{Q})^+$, $\beta \in \mathrm{GL}_2(\mathbb{Q})^+$, $u \in U$, $v \in U$ and $\alpha u = v\beta$ then $(j \circ \alpha)^{\tau(u)} = j \circ \beta$ and $(f_a \circ \alpha)^{\tau(u)} = f_{av} \circ \beta$.

COROLLARY 2.3. *If $h \in \mathcal{F}_N$ and $\alpha \in \mathrm{GL}_2(\mathbb{Q})^+ \cap M_2(\mathbb{Z})$ then $h \circ \alpha \in \mathcal{F}_{N\det(\alpha)}$.*

PROOF. Consider first $f_a \in \mathcal{F}_N$. From Theorem 2.2(a), $f_a \circ \alpha$ is a modular function of some level. Moreover, since $\Gamma\big(N\det(\alpha)\big) \subset \alpha^{-1}\Gamma(N)\alpha$, $f_a \circ \alpha$ is a modular function of level $N\det(\alpha)$. We may find $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ such that $\gamma^{-1}\alpha = \alpha'$ is upper triangular. Then by comment **b** above, $f_a \circ \alpha = f_a \circ (\gamma\alpha') = f_{a\gamma} \circ \alpha'$. Since $f_{a\gamma}$ is an element of $\mathcal{F}_N$, it has a Fourier expansion with respect to $\exp(2\pi iz/N)$ with coefficients in $\mathbb{Q}\big(\exp(2\pi i/N)\big)$, thus $f_{a\gamma} \circ \alpha'$ has a Fourier expansion with respect to $\exp\big(2\pi iz/N\det(\alpha)\big)$ with coefficients in $\mathbb{Q}\Big(\exp\big(2\pi i/N\det(\alpha)\big)\Big)$ and so it, and hence $f_a \circ \alpha$, is in $\mathcal{F}_{N\det(\alpha)}$. The corresponding result for $j(z)$ is given in [Sh] Proposition 6.6 (5). Since $\mathcal{F}_N$ is generated over $\mathbb{Q}$ by the f_a and j the result follows. ∎

PROPOSITION 2.4. *Let k be coprime to N; if $\left\langle\begin{matrix} ka & b \\ c & d\end{matrix}\right\rangle \in G$ and $\gcd(ka, b, c, d) = 1$, then $\left\langle\begin{matrix} a & b \\ c & kd\end{matrix}\right\rangle \in G * k$.*

PROOF. Let $\alpha = \begin{pmatrix} ka & b \\ c & d\end{pmatrix}$, $\beta = \begin{pmatrix} a & b \\ c & kd\end{pmatrix}$ and define $u, v \in U$ by

$$u_p = \begin{cases} \begin{pmatrix} 1 & 0 \\ 0 & k\end{pmatrix} & \text{for } p \mid N \\ \beta & \text{for } p \nmid N \text{ and } p = \infty \end{cases}$$

and

$$v_p = \begin{cases} \begin{pmatrix} k & 0 \\ 0 & 1\end{pmatrix} & \text{for } p \mid N \\ \alpha & \text{for } p \nmid N \text{ and } p = \infty \end{cases}$$

Here u and v are well-defined since $\det(\beta) = \det(\alpha)$ and by Lemma 2.1 the primes which divide $\det(\alpha)$ also divide N. If N' is integer such that any prime dividing N' also divides N then since $u_p \equiv \begin{pmatrix} 1 & 0 \\ 0 & k\end{pmatrix} \bmod N' \cdot M_2(\mathbb{Z}_p)$ for all primes p we have, by comments **c** and **d** at the start of this section, that if $h \in \mathcal{F}_{N'}$ then $h^{\tau(u)} = h*k$. Then by Lemma 2.1 and Corollary 2.3 $(f_a \circ \alpha)^{\tau(u)} = (f_a \circ \alpha) * k$. Let $\delta \in \Gamma_0(N)$ be such that $\delta \equiv \begin{pmatrix} k^{-1} & 0 \\ 0 & k\end{pmatrix} \bmod N$, then for any $a \in (\mathbb{Z}/N\mathbb{Z})^2$ we have $f_{av} \circ \beta = f_{av\delta} \circ \delta^{-1}\beta = (f_a * k) \circ \delta^{-1}\beta$. Thus from Theorem 2.2 we have $(f_a \circ \alpha) * k = (f_a * k) \circ \delta^{-1}\beta$. Similarly $(j \circ \alpha) * k = j \circ \delta^{-1}\beta$. So for any $h \in \mathcal{F}_N$ we have $(h \circ \alpha) * k = (h * k) \circ \delta^{-1}\beta$. Since $f \in \mathcal{F}_N$ and $\langle\alpha\rangle$ fixes f we have $f * k = (f \circ \alpha) * k = (f * k) \circ \delta^{-1}\beta$ and so $\langle\delta^{-1}\beta\rangle \in G * k$. However it is not difficult, using the fact that $\begin{pmatrix} 1 & 0 \\ 0 & k\end{pmatrix}$ normalizes $\Gamma_0(N) \bmod N$, to show that $G * k$ also contains $\Gamma_0(N)$ and so $\langle\beta\rangle \in G * k$. ∎

3. **Replicability of rational Hauptmoduls.** As in the last section G will denote a subgroup of $\mathrm{PGL}_2(\mathbb{Q})^+$ containing some $\bar{\Gamma}_0(N)$ for some N with finite index and $z \longmapsto z+k$ precisely when $k \in \mathbb{Z}$. We will also take G to be genus zero with Hauptmodul f with rational coefficients. We use $a = b + O(1)$ to denote that the difference between a and b is bounded over some limiting process, which unless otherwise stated will be that $t \longrightarrow 0$ along the positive imaginary axis.

LEMMA 3.1. *If f and G are as above, and f is singular at r/m, where $(r,m) = 1$, then there exists $M \in G$ of the form*

$$M = \begin{pmatrix} d & e \\ -\ell m & \ell r \end{pmatrix}$$

with $\gcd(d, e, \ell m, \ell r) = 1$ *and*

$$f\Big(\frac{r}{m} + t\Big) = \exp\Big(\frac{2\pi i d}{\ell m}\Big)\exp\Big(\frac{2\pi i D}{tm^2\ell^2}\Big) + O(1)$$

where $D = |M|$. In particular D/ℓ^2 and the fractional part of $d/\ell m$ are independent of the particular choice of M. Also for any k such that $(k, \ell m) = 1$

$$f\Big(\frac{rk}{m} + t\Big) = \exp\Big(\frac{2\pi i d\bar{k}}{\ell m}\Big)\exp\Big(\frac{2\pi i D}{tm^2\ell^2}\Big) + O(1),$$

where $\bar{k}k \equiv 1 \pmod{\ell m}$.

PROOF. It is clear that the form of M is as given above if $M(r/m) = \infty$. Now since $(k, \ell m) = 1$, by left multiplication of M by a suitable translation we find

$$\begin{pmatrix} kd' & e' \\ -\ell m & \ell r \end{pmatrix} \in G$$

where $d' = \bar{k}d \pmod{\ell m}$. Since $G * k = G$ we have by Proposition 2.4 that

$$T = \begin{pmatrix} d' & e' \\ -\ell m & k\ell r \end{pmatrix} \in G.$$

So

$$\begin{aligned} f\Big(\frac{r}{m} + t\Big) &= f \circ M\Big(\frac{r}{m} + t\Big) \\ &= f\Big(-\frac{d}{\ell m} - \frac{D}{tm^2\ell^2}\Big) \\ &= \exp\Big(\frac{2\pi i d}{\ell m}\Big)\exp\Big(\frac{2\pi i D}{tm^2\ell^2}\Big) + O(1) \end{aligned}$$

and similarly

$$\begin{aligned} f\Big(\frac{rk}{m} + t\Big) &= f \circ T\Big(\frac{rk}{m} + t\Big) \\ &= f\Big(-\frac{d\bar{k}}{\ell m} - \frac{D}{tm^2\ell^2}\Big) \\ &= \exp\Big(\frac{2\pi i d\bar{k}}{\ell m}\Big)\exp\Big(\frac{2\pi i D}{tm^2\ell^2}\Big) + O(1) \end{aligned}$$

as required. ∎

LEMMA 3.2. *For any non-zero integers m and L there exists a non-zero integer s such that* $(1 + sm, L) = 1$ *and* $(s, L) = (2, L)/\big((2, L), m\big)$.

PROOF. Let $m' = m/\big((2,L), m\big)$ and take $s = k(2,L)/\big((2,L), m\big)$ where

$$k \equiv \begin{cases} 1 & (\bmod p) \text{ if } p \mid L, p \mid m \text{ and } p \neq 2\,; \\ -2m'^{-1}(2,L)^{-1} & (\bmod p) \text{ if } p \mid L, p \nmid m \text{ and } p \neq 2; \\ 1 & \big(\bmod (2,L)\big). \end{cases}$$

Then s has the required properties. ∎

LEMMA 3.3. *With G as above, if*

$$M = \begin{pmatrix} d & e \\ -\ell m & \ell r \end{pmatrix} \in G$$

is written in lowest terms, then $\ell \mid (2/(2,m),\ell)d$.

PROOF. If $m = 0$ then $r = 1$ (recall $(r,m) = 1$) and by [Sh] Proposition 1.17 all elements of G that fix ∞ are either parabolic or the identity and we must have $\ell = d$. If $r = 0$ then we consider instead $M\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. Thus we may assume $mr \neq 0$. Then by Lemma 3.2 there exists a non-zero integer s such that $(1+sm,\ell m) = 1$ and $(s,\ell) \mid (2,\ell m)/\big((2,\ell m),m\big) \mid 2/(2,m)$, and so $(s,\ell) \mid \big(2/(2,m),\ell\big)$. Let k be such that $k(1+sm) = 1 \pmod{\ell m}$. In the notation of Lemma 3.1,

$$f\Big(\frac{rk}{m}+t\Big) = f\Big(\frac{r}{m}+t\Big) = \exp\Big(\frac{2\pi i d}{\ell m}\Big)\exp\Big(\frac{2\pi i D}{tm^2\ell^2}\Big) + O(1)$$

and also by Lemma 3.1:

$$f\Big(\frac{rk}{m}+t\Big) = \exp\Big(\frac{2\pi i d(1+sm)}{\ell m}\Big)\exp\Big(\frac{2\pi i D}{tm^2\ell^2}\Big) + O(1).$$

Hence $\ell \mid sd$ and so $\ell \mid (s,\ell)d$ and the result follows. ∎

LEMMA 3.4. *If $M \in G$ then, written in lowest terms,*

$$M = \begin{pmatrix} \psi\lambda\delta & \epsilon \\ -\psi\lambda\phi\nu & \lambda\phi\alpha \end{pmatrix}$$

where $(\delta,\phi\nu) = (\alpha,\psi\nu) = (\psi,\phi) = 1$, *and* $(2,\nu)\psi\phi \mid 2$. *Also if* $2 \mid \psi\phi$ *then* $2 \mid \lambda$.

PROOF. Write

$$M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

Let $\lambda = \big((a,c),(d,c)\big)$, $\phi = (c,d)/\lambda$ and $\psi = (a,c)/\lambda$ so $(\phi,\psi) = 1$. Then l.c.m. $(\lambda\phi,\lambda\psi) = \lambda\phi\psi \mid c$ and so set $\nu = -c/\lambda\phi\psi$ and also $\alpha = d/(c,d)$ and $\delta = a/(a,c)$. Then M has the required form with $(\delta,\phi\nu) = (\alpha,\psi\nu) = (\psi,\phi) = 1$.

G also contains

$$M^{-1} = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}.$$

Applying Lemma 3.3 to M and M^{-1} we find using the properties above that $\phi \mid 2/(2,\nu)$ and also $\psi \mid 2/(2,\nu)$ and so $(2,\nu)\psi\phi \mid 2$, since $(\phi,\psi) = 1$. Finally to show that if $2 \mid \psi\phi$ then $2 \mid \lambda$, first consider the case $\phi = 2$, then $\psi = 1$ and $(2,\nu) = (2,\delta) = 1$ hence

$$\begin{pmatrix} \psi\lambda\delta & \epsilon \\ -\psi\lambda\phi\nu & \lambda\phi\alpha \end{pmatrix} \equiv \begin{pmatrix} \lambda & \epsilon \\ 0 & 0 \end{pmatrix} \pmod 2$$

and 2 divides $|M|$ so, using the same argument as in the proof of Lemma 2.1, $2 \mid \lambda$. A similar argument gives the result in the case that $\psi = 2$. ∎

Before proceeding to the main result we shall first derive some results on sums of roots of unity using modular functions.

In what follows for $r/m \in \mathbb{Q}$ define $m' = m/(r,m)$ and $r' = r/(r,m)$ and $\tau(r,m) = x/m'$ for some x such that $xr' = 1 \pmod{m'}$ and $x \equiv 1 \pmod 2$, we shall not need this second condition until Lemma 3.12. Note that different choices of x change τ by an integer which does not change $\exp\bigl(2\pi i\tau(r,m)\bigr)$ which is all we shall require.

LEMMA 3.5.

$$\sum_{\substack{ad=n\\0\leq b<d\\(ar+bm,dm)=g}} \exp\bigl(2\pi i\tau(ar+bm,dm)\bigr) = \begin{cases}\exp\bigl(2\pi in\tau(r,m)\bigr) & \text{if } g=(r,m)n;\\ 0 & \text{otherwise.}\end{cases}$$

PROOF. The j function satisfies the identity,

$$\sum_{\substack{ad=n\\0\leq b<d}} j\Bigl(\frac{az+b}{d}\Bigr) = Q_n\bigl(j(z)\bigr).$$

Evaluating at $\frac{r}{m}+t$ and examining the singularity at $t=0$ gives

$$Q_n\Bigl(j\Bigl(\frac{r}{m}+t\Bigr)\Bigr) = \exp\bigl(2\pi ni\tau(r,m)\bigr)\exp\Bigl(\frac{2\pi\tau(m,r)^2n}{tm^2}\Bigr)+O(1)$$

and

$$\sum_{\substack{ad=n\\0\leq b<d}} j\Bigl(\frac{ar+bm}{dm}+\frac{at}{d}\Bigr) = \sum_g \sum_{\substack{ad=n,\\0\leq b<d\\(ar+bm,dm)=g}} \exp\bigl(2\pi i\tau(ar+bm,dm)\bigr)\exp\Bigl(\frac{2\pi ig^2}{tnm^2}\Bigr)$$

and the result follows by comparing coefficients. ∎

LEMMA 3.6. *Let $s(n,g) = \sum_{d\mid n}(-1)^{n/d}\mu(d/g)$ where $\mu(x)$ is the Möbius function, defined to be zero for non-integral values of x. Then $s(n,g) = -\delta_{n,g}+2\delta_{n,2g}$ (Kronecker delta).*

PROOF. Consider first $s(n,1)$. If n is odd then

$$s(n,1) = \sum_{d\mid n}(-1)^{n/d}\mu(d) = -\sum_{d\mid n}\mu(d) = -\delta_{n,1}$$

as required. If $4 \mid n$ then

$$s(n,1) = \sum_{d\mid n,\ 4\nmid d}(-1)^{n/d}\mu(d) + \sum_{d\mid n,\ 4\mid d}(-1)^{n/d}\mu(d) = \sum_{d\mid n}\mu(d) = 0$$

as required. If 2 exactly divides n then

$$\begin{aligned} s(n,1) &= \sum_{d\mid n,\ 2\nmid d}(-1)^{n/d}\mu(d) + \sum_{d\mid n,\ 2\mid d}(-1)^{n/d}\mu(d)\\ &= \sum_{d\mid(n/2)}\mu(d) - \sum_{d\mid n,\ 2\mid d}\mu(d)\\ &= \delta_{n/2,1} - (\delta_{n,a} - \delta_{n/2,1})\\ &= 2\delta_{n/2,1} = 2\delta_{n,2}\end{aligned}$$

as required.

In general $s(n,g) = \sum_{d|n,\ g|d}(-1)^{n/d}\mu(d/g)$. Setting $d = gd'$ we have $s(n,g) = \sum_{gd'|n}(-1)^{n/gd'}\mu(d') = s(n/g,1)$ and the result follows from the previous calculation. ∎

LEMMA 3.7.

$$h_n(z) = \sum_{ad=n,\ 0\le b<d} (-1)^a j\Big(\frac{az+b}{d}\Big)$$

is invariant under $\Gamma_0(2)$.

PROOF. We must show that right multiplication by $M \in \Gamma_0(2)$ permutes the set of matrices of the form

$$\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}, \quad ad = n,\ 0 \le b < d$$

up to left multiplication by elements of Γ while preserving $a \pmod 2$. Let

$$M = \begin{pmatrix} \alpha & \beta \\ 2\gamma & \delta \end{pmatrix}, \quad \alpha\delta - 2\beta\gamma = 1.$$

There exist p, q, r, s with $ps - qr = 1$ such that the product

$$\begin{pmatrix} p & q \\ r & s \end{pmatrix}\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}\begin{pmatrix} \alpha & \beta \\ 2\gamma & \delta \end{pmatrix}$$

is again of the form

$$\begin{pmatrix} a' & b' \\ 0 & d' \end{pmatrix}, \quad a'd' = n,\ 0 \le b' < d'.$$

From which we deduce that

$$pa\alpha \equiv a' \pmod 2 \quad \text{and} \quad ra\alpha \equiv 0 \pmod 2$$

If $a \equiv 0 \pmod 2$ then $a' \equiv 0$. If $a \equiv 1 \pmod 2$ then $r \equiv 0 \pmod 2$ since α is odd, however $(p,r) = 1$ so $2 \not| p$ so $a' \equiv 1$. ∎

LEMMA 3.8.

$$\text{As } z \longrightarrow \infty \quad h_n(z) = (-1)^n \exp(2\pi i n z) + O(1)$$

$$\text{As } z \longrightarrow 0 \quad h_n(z) = \begin{cases} -\exp(2\pi i n/z) + O(1) & \text{if } n \text{ is odd;} \\ -\exp(2\pi i n/z) + 2\exp(\pi i n/2z) + O(1) & \text{if } n \text{ is even.} \end{cases}$$

PROOF. 1) For fixed a and d we have

$$\sum_{0\le b<d} j\Big(\frac{az+b}{d}\Big) = \sum_k dH_{dk}q^{ak}$$

so that the only negative exponent in the q expansion at infinity occurs for $d = 1, k = -1$ and $a = n$.

2) We have that as $z \longrightarrow 0$

$$j\Big(\frac{az+b}{d}\Big) = \exp\big(2\pi i\tau(b,d)\big)\exp\Big(\frac{2\pi\tau(b,d)^2}{nz}\Big) + O(1)$$

So

$$\begin{aligned} h_n(z) &= \sum_{\substack{ad=n\\ 0\le b<d}} (-1)^a \exp\big(2\pi i\tau(b,d)\big)\exp\Big(\frac{2\pi\tau(b,d)^2}{nz}\Big) + O(1)\\ &= \sum_{\substack{g\mid n\\ d\mid n}} (-1)^{n/d}\Big(\sum_{\substack{0\le b<d\\ (b,d)=g}} \exp\big(2\pi i\tau(b,d)\big)\Big)\exp\Big(\frac{2\pi i g^2}{nz}\Big) + O(1)\\ &= \sum_{g\mid n}\Big(\sum_{d\mid n}(-1)^{n/d}\mu(d/g)\Big)\exp\Big(\frac{2\pi i g^2}{nz}\Big) + O(1) \end{aligned}$$

so using Lemma 3.6

$$h_n(z) = \begin{cases} -\exp(2\pi i n/z) + O(1) & \text{if } n \text{ is odd;}\\ -\exp(2\pi i n/z) + 2\exp(\pi i n/2z) + O(1) & \text{if } n \text{ is even.}\end{cases}$$ ∎

LEMMA 3.9. *If m' is odd and n is even then*

$$\sum_{\substack{ad=n,\\ 0\le b<d\\ (ar+bm,dm)=g}} (-1)^{n/d}\exp\big(2\pi i\tau(ar+bm,dm)\big) = \begin{cases} -\exp\big(2\pi i n\tau(r,m)\big) & \text{if } g = n(m,r);\\ 2\exp\big(2\pi i h\frac{n}{2}\tau(r,m)\big) & \text{if } g = n(m,r)/2;\\ 0 & \text{otherwise.}\end{cases}$$

where $2h \equiv 1 \pmod{m'}$.

PROOF. We compute the singular part of $h_n(\frac{r}{m}+t)$ as $t \longmapsto 0$ in two ways. Write $r' = r/(m,r)$ and $m' = m/(m,r)$. Then since m' is odd we may find integers x and y such that $ym' + x(2r') = 1$ so that

$$\begin{pmatrix} m' & -r'\\ 2x & y\end{pmatrix} \in \Gamma_0(2)$$

Transforming by this element and using Lemmas 3.7 and 3.8 we find

$$\begin{aligned} h_n\Big(\frac{r'}{m'}+t\Big) &= h_n\Big(\frac{mm't}{(m,r)+2xmt}\Big)\\ &= -\exp\Big(\frac{4\pi i x n}{m'}\Big)\exp\Big(\frac{2\pi i n}{m'^2 t}\Big) + 2\exp\Big(\frac{\pi i x n}{m'}\Big)\exp\Big(\frac{\pi i n}{2m'^2 t}\Big) + O(1)\end{aligned}$$

Also

$$\begin{aligned} h_n\Big(\frac{r}{m}+t\Big) &= \sum_{\substack{ad=n\\ 0\le b<d}} (-1)^{n/d} j\Big(\frac{ar+bm}{dm}+\frac{at}{d}\Big)\\ &= \sum_{\substack{ad=n\\ 0\le b<d}} \exp\big(2\pi i\tau(ar+bm,dm)\big)\exp\Big(\frac{2\pi i g^2}{tnm^2}\Big) + O(1)\end{aligned}$$

where $g = (ar+bm, dm)$. Comparing coefficients yields the result. ∎

https://doi.org/10.4153/CJM-1995-061-1 Published online by Cambridge University Press

LEMMA 3.10. *If m' and n are even then*

$$\sum_{\substack{ad=n,\\ 0\le b<d\\ (ar+bm,dm)=g}} (-1)^{n/d}\exp\big(2\pi i\tau(ar+bm,dm)\big) = \begin{cases} \exp\big(2\pi i n\tau(r,m)\big) & \text{if } g=n(m,r);\\ 0 & \text{otherwise.}\end{cases}$$

PROOF. The argument is similar to the last Lemma. Since m' is even there exist x and y such that

$$\begin{pmatrix} x & y\\ -m' & r'\end{pmatrix} \in \Gamma_0(2)$$

So

$$\begin{aligned} h_n\Big(\frac{r'}{m'}+t\Big) &= h_n\Big(-\frac{x}{m'}-\frac{1}{m'^2t}\Big)\\ &= \exp\Big(\frac{2\pi i x n}{m'}\Big)\exp\Big(\frac{2\pi i n}{m'^2t}\Big)+O(1)\end{aligned}$$

and also

$$h_n\Big(\frac{r}{m}+t\Big)= \sum_{\substack{ad=n\\ 0\le b<d}} (-1)^{n/d}\exp\big(2\pi i\tau(ar+bm,dm)\big)\exp\Big(\frac{2\pi i g^2}{tnm^2}\Big)+O(1)$$

where once again $g=(ar+bm,dm)$. Again comparing coefficients yields the result. ∎

LEMMA 3.11. *Given $r\in\mathbb{Z}$ and $m,n\in\mathbb{Z}^{>0}$ and a divisor k of n then there exists a matrix*

$$M=\begin{pmatrix} a & b\\ 0 & d\end{pmatrix}$$

with $ad=n$ and $0\le b<d$ such that $(ar+bm,dm)=(r,m)k$.

PROOF. We can find coprime integers e and f such that $er+fm\equiv 0 \pmod n$ and hence a matrix

$$S=\begin{pmatrix} e & f\\ g & h\end{pmatrix}$$

in $SL_2(\mathbb{Z})$. Let

$$M'=\begin{pmatrix} n/k & 0\\ 0 & k\end{pmatrix}\begin{pmatrix} e & f\\ g & h\end{pmatrix}$$

and

$$M'\begin{pmatrix} r\\ m\end{pmatrix}=\begin{pmatrix} p\\ q\end{pmatrix}$$

then $(p,q)=(r,m)k$. By premultiplying by a suitable element of $SL_2(\mathbb{Z})$ we can put M' into the required form. ∎

In the following lemma we make the definitions:

$$\zeta(m)=\begin{cases}\exp(2\pi i\delta/\phi\nu) & \text{if } 1/m \text{ is on the same } G\text{-orbit as } \infty;\\ 0 & \text{otherwise.}\end{cases}$$

where in the first case, $m = \psi\nu$ and

$$M = \begin{pmatrix} \psi\lambda\delta & \epsilon \\ -\psi\lambda\phi\nu & \lambda\phi \end{pmatrix}$$

is a matrix that maps $1/m$ to ∞. Keeping the same notation, if the element $\langle M\rangle$ of G maps $1/m$ to ∞ define:

$$A(m) = 2\pi i|M|/\psi^2\lambda^2\phi^2\nu^2.$$

LEMMA 3.12. *$f^{(n)}$ exists. Also*

$$f^{(n)}\Big(\frac{r}{m}+t\Big)= \zeta(nm')^{n\tau(r,m)} \exp\big(A(nm')n^2/t\big) + O(1),$$

$f^{(n)}$ has no singularities in the upper half plane and is an automorphic function for $\Gamma(M)$ for some M.

PROOF. Induction on n. For $n = 1$ the only property that must be verified is that

$$f\Big(\frac{r}{m}+t\Big)= \zeta(m')^{\tau(r,m)} \exp\big(A(m')/t\big) + O(1)$$

When $\zeta(m')$ is a primitive m'-th root of 1 this follows from Lemma 3.1. However from Lemma 3.4 $\zeta(m')$ can be an $m'/2$-th or $2m'$-th primitive root of 1. Only the latter situation is a problem and it can only occur when m' is odd. Lemma 3.1 in this case implies that the exponent of $\zeta(m')$ is congruent to $r \pmod{m'}$ and $1 \pmod 2$, but now the result follows from our definition of $\tau(r,m)$.

Now assume that the result holds for all $a < n$ (in fact we only need that it holds for all proper divisors of n). Let

$$t_n(z) = Q_n\big(f(z)\big) - \sum_{\substack{ad=n\\0\leq b<d}}{}' f^{(a)}\Big(\frac{az+b}{d}\Big).$$

We have to show that $t_n(z) = t_n(z+\frac{1}{n})$ so $f^{(n)}(z) = t_n(z/n)$ has integral q-expansion *i.e.* the n-th replicate of f exists. From above we have

$$Q_n\Big(f\Big(\frac{r}{m}+t\Big)\Big)= \big(\zeta(m')\big)^{n\tau(r,m)} \exp\big(A(m')n/t\big) + O(1)$$

Using the inductive hypothesis,

$$\sum_{\substack{ad=n\\0\leq b<d}}{}' f^{(a)}\Big(\frac{az+b}{d}+\frac{at}{d}\Big) = \sum_{g}\sum_{\substack{ad=n\\0\leq b<d\\(ar+bm,dm)=g}} \zeta(nm/g)^{a\tau(ar+bm,dm)} \exp\big(A(nm/g)n/t\big)$$

$$- \zeta(\mu)^{n\tau(nr,m)} \exp\big(A(\mu)n/t\big) + O(1)$$

where $\mu = nm/(nr,m)$. When $\zeta(nm/g)$ is a primitive nm/g-th root of 1 we can use Lemma 3.5 and, after applying a suitable Galois automorphism, Lemma 3.11 to show that

$$\sum_{\substack{ad=n\\0\leq b<d}}{}' f^{(a)}\Big(\frac{az+b}{d}+\frac{at}{d}\Big) = \zeta(m')^{n\tau(r,m)} \exp\big(A(m')n/t\big)$$

$$- \zeta(\mu)^{n\tau(nr,m)} \exp\big(A(\mu)n/t\big) + O(1)$$

However, as noted above, it might happen that $\zeta(nm/g)$ is a $2nm/g$-th or $nm/2g$-th root of 1. However in this case $-\zeta(nm/g)$ is a primitive nm/g-th root of 1 and we can use Lemma 3.10 and 3.11 to obtain the same result (recall that $\tau(r,m)$ is odd), except in the case that n is even and m' is odd. In this case, from Lemma 3.9, we find:

$$\sum_{\substack{ad=n\\0\le b<d}}' f^{(a)}\Big(\frac{az+b}{d}\Big) = \zeta(m')^{n\tau(r,m)}\exp\big(A(m')n/t\big) - 2\zeta(2m')^{hn\tau(r,m)}\exp\big(A(m')n/t\big)$$
$$- \zeta(\mu)^{n\tau(nr,m)}\exp\big(A(\mu)n/t\big) + O(1)$$

where $2h \equiv 1 \pmod{m'}$. However, if

$$\begin{pmatrix} 2\lambda\delta & \epsilon \\ -2\lambda m' & \lambda \end{pmatrix}$$

is a matrix that maps $2m'$ to ∞, $\zeta(m') = -\exp(2\pi i\delta h/m')$ and also $A(2m') = A(m')$. So once again we find:

$$\sum_{\substack{ad=n\\0\le b<d}}' f^{(a)}\Big(\frac{az+b}{d}\Big)= \zeta(m')^{n\tau(r,m)}\exp\big(A(m')n/t\big) - \zeta(\mu)^{n\tau(nr,m)}\exp\big(A(\mu)n/t\big) + O(1)$$

Combining these results we find

$$t_n(z)= \zeta(\mu)^{n\tau(nr,m)}\exp\big(A(\mu)n/t\big) + O(1).$$

It is easy to verify that this expression is invariant under the substitution $r \longmapsto rn+m$, $m \longmapsto mn$ so that $t_n(\frac{r}{m}+t) - t_n(\frac{r}{m}+\frac{1}{n}+t) = O(1)$. Hence this difference is bounded on $\mathbb{Q}$. At infinity $t_n(z) = \exp(-2\pi izn) + O\big(\exp(2\pi iz)\big)$ and so the difference is bounded at infinity. By the inductive hypothesis each term on the right hand side of

$$t_n(z) = Q_n\big(f(z)\big) - \sum_{\substack{ad=n\\0\le b<d}}' f^{(a)}\Big(\frac{az+b}{d}\Big)$$

has no poles in the upper half plane and so neither does $t_n(z)$. Also $t_n(z)$ is an automorphic function for the intersection of the fixing groups of each term in the right hand side each of which contain a principal congruence subgroup by the inductive hypothesis and so $t_n(z)$ is an automorphic function of $\Gamma(M)$ for some M. Thus $t_n(z) - t_n(z+\frac{1}{n})$ is an automorphic function for $\Gamma(n^2M)$, bounded on a fundamental domain and hence is constant. However from the q expansion of t_n we see that the constant is zero as required.

Finally we can use $f^{(n)}(z) = t_n(z/n)$ and

$$t_n(z)= \zeta(\mu)^{n\tau(nr,m)}\exp(A(\mu)n/t) + O(1)$$

to verify that

$$f^{(n)}\Big(\frac{r}{m}+t\Big)= \zeta(nm')^{n\tau(r,m)}\exp\big(A(nm')n^2/t\big) + O(1),$$

and also that $f^{(n)}$ is an automorphic function with no singularities on the upper half plane. ∎

To summarise we have now shown:

THEOREM 1.3. *If f is a Hauptmodul with rational coefficients for a group $G <$ $\mathrm{PGL}_2(\mathbb{Q})^+$, of genus zero, containing a $\bar{\Gamma}_0(N)$ with finite index and $z \longmapsto z+k$ precisely when k is an integer, then f is replicable.*

Appendix. In this appendix we shall prove some useful properties of replicable functions. As in the rest of the paper we shall take f to have rational integer coefficients.

LEMMA A.1.

$$Q_n(f) = \frac{1}{q^n} + \sum_{i=1}^{\infty} nH_{n,m}q^m.$$

PROOF. First note that any polynomial in

$$f(z) = q^{-1} + H_1 q + H_2 q^2 + H_3 q^3 + \cdots$$

whose q-expansion has only positive degree terms is zero, from which we can deduce that the $Q_n(f)$ satisfy the recurrence relation:

$$(n+1)H_n + Q_{n+1}(f) + \sum_{i=1}^{n-1} H_i Q_{n-i}(f) = fQ_n(f).$$

This leads to the generating function:

$$-\log\Big(1 - pf(z) + \sum_{i=1}^{\infty} H_i p^{i+1}\Big) = \sum_{j=1}^{\infty} \frac{1}{i} Q_i(f) p^i.$$

Comparing with equation (1.3) we see that

$$Q_n(f) = \frac{1}{q^n} + \sum_{m=1}^{\infty} nH_{n,m}q^m. \qquad \blacksquare$$

LEMMA A.2. *The function*

$$f(z) = q^{-1} + H_1 q + H_2 q^2 + H_3 q^3 + \cdots$$

is replicable if and only if the coefficients $H_{m,n}$ given by the generating function:

$$\sum_{m,n \geq 1} H_{n,m} p^n q^m = -\log\Big(1 - pq \sum_{i=1}^{\infty} H_i \frac{p^i - q^i}{p - q}\Big)$$

satisfy the conditions $H_{m,n} = H_{r,s}$ whenever $mn = rs$ and $(m,n) = (r,s)$.

PROOF. If f satisfies $H_{m,n} = H_{r,s}$ whenever $mn = rs$ and $(m,n) = (r,s)$ then set

$$f^{(k)}(z) = \sum_{i=-1}^{\infty} a_i^{(k)} q^i$$

where

$$a_i^{(k)} = k\sum_{d|k} \mu(d) H_{\frac{k}{d},dki} \quad i > 0,\ a_{-1}^{(k)} = 1,\ a_0^{(k)} = 0$$

and μ is the Möbius function. It follows that $f^{(1)} = f$. For any pair $r, s \in \mathbf{Z}^{>0}$, we find, by Möbius inversion, that

$$H_{r,rs} = \sum_{d|r} \frac{1}{d} a^{(d)}_{r^2 s/d^2}$$

and, since f satisfies $H_{m,n} = H_{r,s}$ whenever $mn = rs$ and $(m,n) = (r,s)$ this implies that

$$(A.1) \qquad H_{m,n} = \sum_{d|(m,n)} \frac{1}{d} a^{(d)}_{mn/d^2}$$

which gives, using Lemma A.1 (compare Serre [S], Chapter VII, Section 5.3)

$$(A.2) \qquad Q_n(f) = \sum_{\substack{ad=n\\ 0\le b<d}} f^{(a)}\big((az+b)/d\big).$$

Conversely if f has replicates which satisfy (A.2) it follows that the $H_{m,n}$ satisfy (A.1) and so $H_{m,n} = H_{r,s}$ whenever $mn = rs$ and $(m,n) = (r,s)$. ∎

PROPOSITION A.3. *If $f = 1/q + H_1 q + \cdots + H_k q^k$ is replicable then $f = 1/q + H_1 q$.*

PROOF. If $k = 0$ or $k = 1$ then we are done, so assume $k \geq 2$ and $H_k \neq 0$. We consider two cases, either

$$f = 1/q + H_1 q + \cdots + H_{k-i} q^{k-i} + H_k q^k$$

with $1 \leq i < k$ and $H_{k-i+1} = \cdots = H_{k-1} = 0$ and $H_{k-i} \neq 0$, or

$$(A.3) \qquad f = 1/q + H_k q^k.$$

We shall show that the former case cannot occur. Looking at the $(i + 1)$-st replication identity we have:

$$(A.4) \qquad Q_{i+1}(f) = f^{(i+1)}\big((i+1)z\big) + \sum_{\substack{ad=i+1\\ 0\le b<d}}{}' f^{(a)}\Big(\frac{az+b}{d}\Big)$$

First note that

$$\sum_{0\le b<d} f^{(a)}\Big(\frac{az+b}{d}\Big) = d(H_d^{(a)}q^a + H_{2d}^{(a)}q^{2a} + \cdots).$$

The term with second largest degree on the l.h.s. of (A.4) is $(i+1)H_{k-i}H_k^i q^{(i+1)k-i}$ and contributions from the 2-nd term on the r.h.s. to this degree would come from the j-th term with $ja = (1+i)k - i$, but $a \mid (i+1)$ so $a \mid i$ so $a = 1$ and $d = i+1$. But the degree of this sum is bounded above by $k/(i+1)$. So to have a contribution of degree $(i+1)k - i$ we would have to have $(i+1)k - i \le k/(i+1)$ which implies $k \le (i+1)/(i+2) < 1$ and so $k = 0$ a contradiction. So the sum on the r.h.s. has no terms of degree $(i+1)k - i$. Also $(i+1)k - i \equiv 1 \pmod{i+1}$ so $f^{(i+1)}\big((i+1)z\big)$ has no terms of degree $(i+1)k - i$. So we must have $(i+1)H_{k-i}H_k^i = 0$ which is a contradiction. So f must be as given in (A.3).

We now show that we must have $k = 1$. Take n such that $\big(n, k(k+1)\big) = 1$ and $n > k+1$. Then

$$\begin{aligned} Q_n(f) = 1/q^n + \cdots + \binom{n}{j} H_k^j q^{-n+j(k+1)} + \cdots + H_k^n q^{nk} \\ + c_1 f^{n-1} + c_2 f^{n-2} + \cdots + c_n \end{aligned}$$

Looking at the coefficient of q^{-n+k+1}, we see we must have $c_1 = c_2 = \cdots = c_{n-k} = 0$ and $c_{n-k-1} = -nH_k$. So the coefficient of $q^{(n-k-1)k}$ is $H_k^{n-k}\Big(\binom{n}{n-k} - n\Big)$. Since $n > k+1$, $\Big(\binom{n}{n-k} - n\Big) = 0$ implies $k = 1$. So we have to check that the coefficient of $q^{k(n-k-1)}$ is zero on the r.h.s. of (A.4). Now $H_{jd}^{(a)}q^{ja}$ of degree $k(n-k-1)$ implies $a \mid k(n-k-1)$ and so $a \mid k(k+1)$ and hence $a = 1$ since $\big(n, k(k+1)\big) = 1$. But again the degree of the $a = 1$ term is bounded by $k/n < 1$ and so this term vanishes. Finally $k(n-k-1) \equiv -k(k+1) \not\equiv 0 \pmod{n}$, since $\big(n, -k(k+1)\big) = 1$, so $f^{(n)}(nz)$ has no terms of degree $k(n-k-1)$. ■

We also give a proof of the fact that any replicable function is determined by the values of 12 of its first 23 coefficients as noted by Norton [N1].

LEMMA A.4. *If $N \in \mathbb{Z}^{>0}$, then there exist $m, n, m', n' \in \mathbb{Z}^{>0}$ such that 1) $m + n = N$, 2) $mn = m'n'$, 3) $(m,n) = (m',n')$ and 4) $m' + n' < m + n$ exactly when $N \ne 1, 2, 3, 4, 5, 6, 8, 9, 10, 12, 18, 20, 24$.*

PROOF. Note first that if the lemma holds for N it holds for kN, $k \ge 1$ by taking km, kn, km', kn'. We consider cases:

i) $N = 2^k$ except 2, 4 and 8. For $N = 16$ choose $m = 1$, $n = 15$, $m' = 3$ and $n' = 5$. From the comment above we then obtain all higher powers of 2 as multiples of 16.

https://doi.org/10.4153/CJM-1995-061-1 Published online by Cambridge University Press

ii) N odd of the form 2^a+1, $a \geq 4$ (*i.e.* except 3, 5 and 9) choose $m = 2^a-2$, $n = 3$, $m' = 2^{a-1}-1$ and $n' = 6$.

iii) N odd, $N-1$ not a power of 2. In this case choose $m = N-1$, $n = 1$, $m' = 2^{-r}(N-1)$ and $n' = 2^r$, where 2^r is the exact power of 2 which divides $N-1$. Note $N-1 > 2^r \Rightarrow N > 2^r+1 \Rightarrow N(2^r-1) > 2^{2r}-1 \Rightarrow N > 2^{-r}(N-1)+2^r$.

iv) N even, not a power of 2. Then N must be a product of 2, 4 or 8 with 3, 5 or 9 since all other possibilities are multiples of the cases considered above. For 40 choose $m = 1$, $n = 39$, $m' = 3$ and $n' = 13$. For 36 choose $m = 1$, $n = 35$, $m' = 5$ and $n' = 7$ which, from the comment above, gives $m = 2$, $n = 70$, $m' = 10$ and $n' = 14$ as a solution for 72.

The only remaining cases are $N = 1,2,3,4,5,6,8,9,10,12,18,20,24$. It is easily verified that there are no solutions for m, n, m', n' in these cases. ∎

PROPOSITION A.5. *If*

$$f = q^{-1} + H_1 q + H_2 q^2 + \cdots$$

is replicable then f is determined by the values of H_1, H_2, H_3, H_4, H_5, H_7, H_8, H_9, H_{11}, H_{17}, H_{19} and H_{23}.

PROOF. If $i+1 \neq 2,3,4,5,6,8,9,10,12,18,20,24$ then by Lemma A.4 we can find m, n, m', n' such that $m+n = i+1$, $H_{m,n} = H_{m',n'}$ and $m'+n' < m+n$ (since f is replicable). The leading term of $H_{m,n}$ is H_i and so solving $H_{m,n} = H_{m',n'}$ for H_i expresses H_i in terms of the H_j with $j < i$. Iterating this process we can express all the coefficients in terms of $H_1, H_2, H_3, H_4, H_5, H_7, H_8, H_9, H_{11}, H_{17}, H_{19}$ and H_{23}. ∎

REFERENCES

[ACMS] D. Alexander, C. Cummins, J. McKay and C. Simons, *Completely replicable functions.* In: Groups, Combinatorics and Geometry, Lecture Notes in Math., (ed. M. W. Liebeck and J. Saxl), Cambridge Univ. Press, 1992, 87–95

[ATLAS] J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker and R. A. Wilson, *Atlas of finite groups*, Oxford Univ. Press, 1985.

[B1] R. E. Borcherds, *Monstrous Moonshine and monstrous Lie superalgebras*, Invent. Math. **109**(1992), 405–444.

[CN] J. H. Conway and S. P. Norton, *Monstrous Moonshine*, Bull. London Math. Soc. **11**(1979), 308–339.

[F] C. R. Ferenbaugh, *On the Modular Functions involved in "Monstrous Moonshine"*, Ph.D. thesis, Princeton University, 1992.

[K] M. Koike, *On replication formula and Hecke operators*, Nagoya University, preprint.

[N1] S. P. Norton, *More on Moonshine*. In: Computational Group Theory (ed. M. D. Atkinson), Academic Press, 1984, 185–193.

[N2] ———, *Non-monstrous Moonshine*, Proceedings of the Columbus conference on the Monster, 1993, to appear.

[Sh] G. Shimura *Introduction to the arithmetic theory of automorphic functions*, Princeton Univ. Press, 1971.

[Sm] G. W. Smith, *Higher genus Moonshine*, 1993, preprint.

[T] J. G. Thompson, *Some numerology between the Fischer-Griess monster and the elliptic modular function*, Bull. London Math. Soc. **11**(1979), 352–353.

Centre Interuniversitaire en Calcul Mathématique Algébrique
Department of Mathematics and Statistics
Concordia University
1455 de Maisonneuve Boulevard West
Montréal, Québec
H3G 1M8

Department of Pure Mathematics and Mathematical Statistics
Cambridge University
16 Mill Lane
Cambridge, CB2 1SB
England