

SPONTANEOUS GENERATION OF MODULAR INVARIANTS

HARVEY COHN AND JOHN MCKAY

ABSTRACT. It is possible to compute $j(\tau)$ and its modular equations with no perception of its related classical group structure except at ∞ . We start by taking, for p prime, an unknown “ p -Newtonian” polynomial equation $g(u, v) = 0$ with arbitrary coefficients (based only on Newton’s polygon requirements at ∞ for $u = j(\tau)$ and $v = j(p\tau)$). We then ask which choice of coefficients of $g(u, v)$ leads to some consistent Laurent series solution $u = u(q) \approx 1/q$, $v = u(q^p)$ (where $q = \exp 2\pi i\tau$). It is conjectured that if the same Laurent series $u(q)$ works for p -Newtonian polynomials of two or more primes p , then there is only a bounded number of choices for the Laurent series (to within an additive constant). These choices are essentially from the set of “replicable functions,” which include more classical modular invariants, particularly $u = j(\tau)$. A demonstration for orders $p = 2$ and 3 is done by computation. More remarkably, if the same series $u(q)$ works for the p -Newtonian polygons of 15 special “Fricke-Monster” values of p , then $(u =)j(\tau)$ is (essentially) determined uniquely. Computationally, this process stands alone, and, in a sense, modular invariants arise “spontaneously.”

1. INTRODUCTION

Deferring definitions for later, we note the classical result [9] that the modular function $j(\tau)$ determines a modular equation (polynomial relation between $j(\tau)$ and $j(N\tau)$ for $1 < N \in \mathbf{Z}$). In a neoclassical mode, the process can be reversed and the modular equation can be used to determine the modular function by substituting Laurent series with undetermined coefficients (see Lehmer [11], Mahler [12]).

We further show how the *precise* modular equation need not be known as a prelude to finding the modular function, only general information of orders of magnitude. It is as though the modular equations arise without the usual structure of elliptic curves, Eisenstein series, and modular groups, indeed as though through “spontaneous generation.”

The goal of treating modular equations as the primary unknown might be reasonable in view of the current “reconstruction” of modular equations caused by work of Conway, McKay, Norton and others (see [1,7,8,14]) on the characters of the Monster group, and in a more specialized context by work of Cohn [5] on determination of modular equations by class-field theoretic properties.

Received by the editor January 13, 1995.

1991 *Mathematics Subject Classification*. Primary 11F11, 20D08.

Key words and phrases. Modular functions, modular equations, replicable functions.

To quickly review definitions, the modular group Γ acting on the upper half-plane H^+ is defined by

$$(1.1a) \quad H^+ : \Re\tau > 0, \quad \Gamma = SL_2(\mathbf{Z}) = \left\{ \tau \rightarrow \frac{A\tau + B}{C\tau + D}, A, B, C, D \in \mathbf{Z}, AD - BC = 1 \right\}.$$

The fundamental domain for H^+/Γ is the region

$$(1.1b) \quad |z| \geq 1, \quad |\Re z| \leq 1/2,$$

with boundary identifications based on the generators of Γ :

$$(1.1c) \quad \Gamma = \langle \tau \rightarrow \tau + 1, \tau \rightarrow -1/\tau \rangle.$$

Then with suitable compactification, inherent in the local parameter

$$(1.2a) \quad q = \exp 2\pi i\tau,$$

a global uniformizing parameter (*Hauptmodul*) is introduced,

$$(1.2b) \quad j(\tau) = 1/q + 744 + 196884q + 21493760q^2 + \dots,$$

which maps the fundamental domain in (1.1b) uniquely onto the j -plane. The observation of McKay that these coefficients occur in a character table of the Monster group was the first clue to a long series of related results.

Suppose we want to find the modular equation (of prime order p only)

$$(1.3a) \quad \Phi_p(j(\tau), j(p\tau)) = 0.$$

We note that for a given value of $u = j(\tau)$, the following set of $p + 1$ functions,

$$(1.3b) \quad v_\infty = j(p\tau), \quad v_k = j\left(\frac{\tau + k}{p}\right) \quad (k = 0, \dots, p-1),$$

is invariant under (1.1c). It is easy to see this for $\tau \rightarrow \tau + 1$, while for $\tau \rightarrow -1/\tau$, we need only show that $v_k \rightarrow v_{k^*}$ for $kk^* + 1 \equiv 0 \pmod{p}$. It follows that there is a polynomial equation $\Phi_p(u, v) = 0$ for which, when $u = j(\tau)$, the solutions in v are (1.3b) (namely the modular equation of order p). It is irreducible and symmetric in u and v , by comparison of v_∞ and $v_0 (= j(\tau/p))$, and of degree $p + 1$ in either variable separately.

Indeed, if $\Im\tau \rightarrow +\infty$, then $q \rightarrow 0$ and $j(\tau) \approx 1/q$, so the set (1.3b) satisfies

$$(1.4a) \quad v_\infty \approx u^p, \quad v_k \approx u^{(1/p)} \rho^k \quad (k = 0, \dots, p-1).$$

(Here $u^{(1/p)}$ is a principal root and ρ is a primitive p th root of unity.) The relations as $q \rightarrow 0$ can be rewritten symmetrically as

$$(1.4b) \quad v \approx u^p, \quad u \approx v^p.$$

1.5 **Lemma** (Mahler). *A symmetric polynomial $g_p(u, v)$ of degree $p + 1$ in each variable which satisfies the relation (1.4b) for all branches as u or v approach ∞ must have the form*

$$(1.5a) \quad g_p(u, v) = u^{p+1} + v^{p+1} - u^p v^p + \sum_{i,j=0}^p a_{i,j} u^i v^j, \quad a_{i,j} = a_{j,i}, a_{p,p} = 0.$$

We shall call such a polynomial a “ p -Newtonian (modular) polynomial.” As $|u| + |v| \rightarrow \infty$,

$$(1.5b) \quad g_p(u, v) \approx u^{p+1} + v^{p+1} - u^p v^p.$$

Note that if $g_p(u, v) = 0$, the relations (1.4b) must follow from (1.5b).

The case $p = 5$ is shown in Figure 1. The coefficients $a_{i,j}$ are present at the heavy dots (i, j), but they are redesignated as explained in §2 below. These dots lie in the polygonal envelope shown (called “Newton’s polygon”) determined by slopes $-p$ and $-1/p$ corresponding to (1.4ab) and (1.5b).

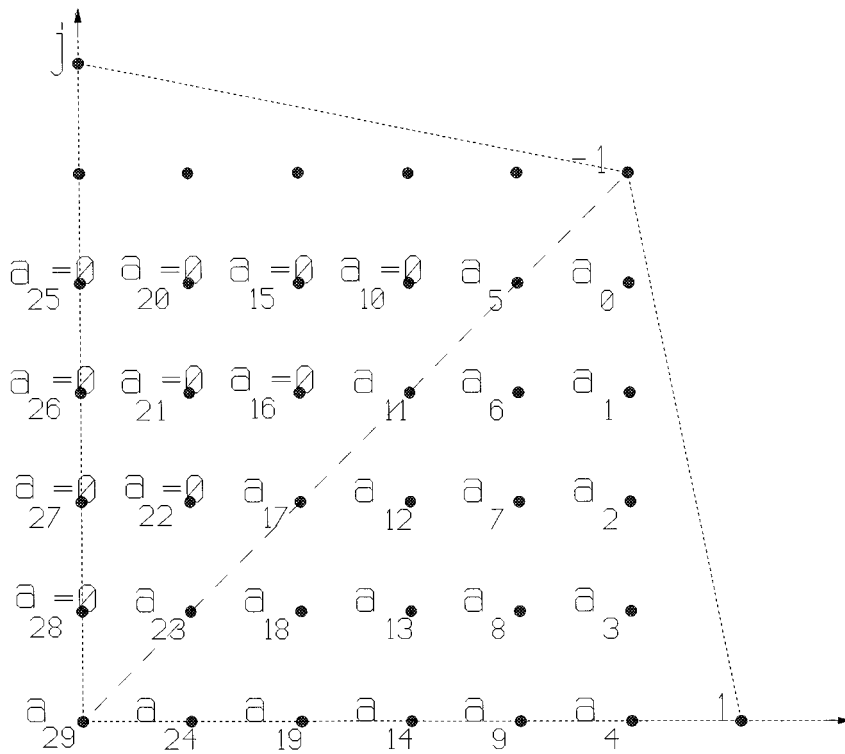


FIGURE 1. Coefficient display for the 5-Newtonian polynomial

The numbering of a_n proceeds down by row and left by column starting with $a_{5,4} = a_0$. We find, however, that gaps in the numbering of a_n must occur when

$j > i$, since, by symmetry, $a_{i,j} = a_{j,i}$ (which has already been designated). Thus, after $a_{4,0} = a_9$, we next arrive at $a_{3,4} = a_{4,3}$, which has been designated “ a_6 ,” so we designate the gap as the next coefficient “ $a_{10} = 0$.” Also note the renumbering ignores the coefficient -1 in $-u^5v^5$ and 1 in u^6 (also in v^6 , not shown).

The main exercise is to take an arbitrary (formal) Laurent series

$$(1.5c) \quad u(q) = 1/q + c_0 + c_1q + c_2q^2 + c_3q^3 + \dots,$$

and inquire if (as an identity in q)

$$(1.5d) \quad g_p(u(q), u(q^p)) = 0$$

for $g_p(u, v)$ a p -Newtonian polynomial. Clearly, $j(\tau)$ in (1.2b) must work (for the correct modular equation (1.5a)), and these trivial expansions also work for “trivial” p -Newtonian polynomials (as seen by elementary algebra):

$$(1.5e) \quad u(q) = 1/q, 1/q + q, 1/q - q \ (p \neq 2).$$

All solutions to the p -Newtonian equation (1.5a) have the property that the symmetric functions of the roots (1.3b) are polynomials in $u(q)$. In particular, in (1.5d) we could also write

$$(1.5f) \quad g_p(u(q), u(q^{1/p}\rho^k)) = 0 \quad (k = 0, \dots, p - 1).$$

Therefore, the Hecke transform on $(u(q) =)f(\tau)$, namely

$$(1.5g) \quad T_p(f(\tau)) = f(p\tau) + \sum_{k=0}^{p-1} f\left(\frac{\tau + k}{p}\right),$$

is a polynomial of degree p in $f(\tau)$ (or in $u(q)$).

1.6 Main conjecture (McKay). *If a specific Laurent series $u(q)$ in (1.5c) having integral coefficients satisfies two p -Newtonian polynomial equations (1.5a) (for two distinct prime values of p), then the series $u(q) - c_0$ is restricted to a bounded class of functions (independent of the two primes).*

Either the series (1.5c) is trivial (as in (1.5e)) or else it comes from a (bounded) class of “extended” modular functions (as defined in §4 below) which are “Hauptmoduls” (global uniformizing parameters).

To complicate this exposition, these Hauptmoduls were recently tabulated from the study of a more recondite (finite) set of “replicable” functions (see [1,7])! These functions arose in the character theory of the Monster group and will be avoided here except for the remark that they come from equations based on a variant of the property of the Hecke transform (1.5g) (also see [13]).

The Main Conjecture shall be verified for the pair $p = 2, 3$ (in §§3 and 4) and applied (in §5) to:

1.7 Main theorem (Computational Result). *If some nontrivial Laurent series in integral coefficients simultaneously satisfies some p -Newtonian polynomial equations for 15 special values of p , the so-called “Fricke-Monster” primes (see §4 below):*

$$(1.7a) \quad p = 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 41, 47, 59, 71,$$

then the Laurent series must be $j(\tau)$ (to within an additive constant).

The reader is reassured at this point that the theoretical results needed on extended modular functions shall be cited in §4, and no theoretical result from the theory of replicable functions is used.

It is probably true that the restriction to “integral coefficients” need not be made, but the computational burden would be tremendously increased without it.

2. THE LAURENT SERIES MANIPULATION

It is necessary to reorganize the coefficients of $g_p(u, v)$ into a more computer-friendly sequence (compare [12]). Figure 1 (for $p = 5$) serves as a convenient model for general p . There are

$$(2.1a) \quad P = p(p + 3)/2$$

distinct coefficients $a_{i,j}$, as we see by counting lattice points on or below the diagonal. We renumber the $a_{i,j}$ by columns starting on the upper right and going down and left. Putting this process into symbols, we now designate a single-index system by

$$(2.1b) \quad a_{i,j} := a_{Q-pi-j} \quad (0 \leq i \leq p + 1, 0 \leq j \leq p),$$

where i is the number of the column counting left, and j is the number of the row counting down, and the highest numbered index is

$$(2.1c) \quad Q = p^2 + p - 1$$

(making for $Q + 1$ single-indexed coefficients). Also, there are

$$(2.1d) \quad D = Q + 1 - P (= p(p - 1)/2)$$

double indices (i, j) which lie above the diagonal and have no coefficient $a_{i,j}$ associated. Now for these D coefficients, we define

$$(2.1e) \quad a_t := 0 \text{ for } t \in A = \{2p; 3p, 3p + 1; 4p, 4p + 1, 4p + 2; \dots; p^2, p^2 + 1, \dots, p^2 + p - 2\}.$$

Thus, $\text{card}(A) = D$. Observe the following table:

p	2	3	5	7	...	71
P	5	9	20	35	...	2627
Q	5	11	29	55	...	5111
D	1	3	10	21	...	2485

We finally expand (1.5d) as

$$(2.2a) \quad G_p(q) := g_p(u(q), u(q^p)) = \frac{\sum_{i=0}^{\infty} \gamma_i q^i}{q^Q}.$$

Note the principal part of the expansion is a pole of order Q . Actually expanding $G_p(q)$, we find the single-indexing of coefficients produces the following simple set of relations:

$$(2.2b) \quad \gamma_0 = a_0 - pc_0,$$

$$(2.2c) \quad \gamma_i = a_i - pc_i + h_i \quad (1 \leq i \leq Q),$$

where

$$(2.2d) \quad h_i \in \mathbf{Z}[a_0, \dots, a_{i-1}; c_0, \dots, c_{i-1}].$$

Also, since $G_p(q)$ must vanish identically (or $\gamma_i = 0$), we see how the coefficients c_j of a given Laurent series determine the coefficients a_t of the polynomial $g_p(u, v)$. Indeed, $a_t = 0$ for $t \in A$, so for these t , c_t is determined by the *earlier* coefficients, i.e.,

$$(2.2e) \quad c_t \in \mathbf{Z}[1/p, c_i \ (0 \leq i < t)], \text{ for } t \in A.$$

There are D such identities among the c_t for $0 < t < Q$. For $t > Q$, essentially the undefined a_t can be taken as 0, so

$$(2.2f) \quad c_t \in \mathbf{Z}[1/p, c_i \ (0 \leq i \leq Q)], \text{ for } t > Q.$$

We now think of the Q coefficients c_i for $0 \leq i \leq Q$ (with $i \notin A$) as determining both the p -Newtonian polynomial $g_p(u, v)$ and the Laurent series $u(q)$. Then we can eliminate the coefficients a_i completely and rewrite (2.2a) as

$$(2.2g) \quad G_p(q) = \frac{\sum_{i=0}^{\infty} m_i q^i}{q^Q},$$

where there are D nonvanishing m_i for $0 < i < Q$.

Before considering examples, we shall agree to eliminate the additive constants by setting $c_0 = 0$.

ORDER 2: $P = 5, Q = 5, D = 1$

Here,

$$(2.3a) \quad g_2(u, v) = u^3 + v^3 - u^2v^2 + a_5 + a_3(u+v) + a_2uv + a_1(u^2+v^2) + a_0(u^2v+v^2u).$$

We next compute $G_2(q) := g_2(u(q), u(q^2))$, with $u(q)$ given by (1.5c), as

$$(2.3b) \quad \begin{aligned} G_2(q) = & a_0/q^5 + (a_0 + a_1 - 2c_1)/q^4 + (a_2 + 1 + a_0c_1 - 2c_2)/q^3 \\ & + (c_1 - 2c_3 - c_1^2 + a_3 + a_1 + a_0(2c_1 + c_2))/q^2 \\ & + (a_2c_1 - 2c_4 - 2c_1c_2 + a_0(c_3 + 2c_1 + 2c_2) + 3c_1 + a_3)/q \\ & + (4a_1c_1 + 4c_2 - 4c_1^2 - 2c_5 - c_2^2 - 2c_1c_3 \\ & \quad + a_0(c_1 + 2c_3 + c_1^2 + c_4) + a_2c_2 + a_5) \\ & + O(q). \end{aligned}$$

So we substitute the values of a_0, \dots, a_5 required for the vanishing of $G_2(q)$:

$$(2.3c) \quad \begin{aligned} a_0 &= 0, & a_1 &= 2c_1, & a_2 &= 2c_2 - 1, & a_3 &= 2c_3 + c_1^2 - 3c_1, \\ a_5 &= -4c_1^2 - 3c_2 + 2c_5 - c_2^2 + 2c_1c_3. \end{aligned}$$

Then, looking at the m_0, \dots, m_4 of (2.2g), we find ($D =$) one singular term in $G_2(q)$ for m_4 as follows:

$$(2.3d) \quad \begin{aligned} G_2(q) &= (-c_1 - 2c_4 + 2c_3 + c_1^2)/q \\ &+ (2c_1c_3 + c_1^3 + 2c_3 - 2c_1c_4 - 2c_6 + 2c_1c_2 - c_1)q \\ &+ (2c_2c_3 + 2c_1c_3 + c_1^2c_2 + c_1^3 + 3c_1c_2 - c_1^2 \\ &\quad - 2c_7 - 2c_1c_5 - c_3^2 + c_3 + 2c_4)q^2 \\ &+ (2c_3^2 + c_3c_1^2 + 3c_1c_3 + c_2^2 + 2c_5 + c_1^3 + 2c_1^2c_2 \\ &\quad - c_1^2 - c_2 - 2c_8 - 2c_4c_3 - 2c_1c_6)q^3 \\ &+ (c_4 + 2c_6 - 2c_9 + 3c_1c_4 - 2c_1c_7 + 4c_2c_3 - 2c_3c_5 \\ &\quad + 2c_4c_3 - c_4^2 + 2c_1^2c_2 + c_1^2c_4 + 2c_1c_2^2)q^4 + O(q^5). \end{aligned}$$

We find all coefficients expressible in terms of c_1, c_2, c_3, c_5 (note the omission of c_4). These equations follow from (2.3d):

$$(2.3e) \quad \begin{aligned} c_4 &= -1/2c_1 + c_3 + 1/2c_1^2, \\ c_6 &= c_3 + 1/2c_1^2 + c_1c_2 - 1/2c_1, \\ c_7 &= c_2c_3 + c_1c_3 + 1/2c_1^2c_2 + 1/2c_1^3 + 3/2c_1c_2 - c_1c_5 \\ &\quad - 1/2c_3^2 + 3/2c_3 - 1/2c_1, \\ c_8 &= c_1c_3 + 1/2c_2^2 + c_5 - 1/2c_2, \\ c_9 &= 3/2c_3 - 3/4c_1 + 3/8c_1^2 + c_2c_1 + 2c_2c_3 + 1/2c_3^2 \\ &\quad - c_5c_3 + 3/4c_1^3 - 1/2c_2c_1^2 - 1/2c_3c_1^2 + c_1c_2^2 \\ &\quad + c_1^2c_5 + 1/2c_1c_3^2 - 1/2c_2c_1^3 - c_1c_2c_3 - 3/8c_1^4, \dots \end{aligned}$$

ORDER 3: $P = 9, Q = 11, D = 3$

Here,

$$(2.4a) \quad \begin{aligned} g_3(u, v) &= u^4 + v^4 - u^3v^3 + a_{11} + a_8(u + v) + a_7uv + a_5(u^2 + v^2) \\ &+ a_4(u^2v + v^2u) + a_3u^2v^2 + a_2(u^3 + v^3) + a_1(u^3v + v^3u) \\ &+ a_0(u^3v^2 + v^3u^2). \end{aligned}$$

The requirement $G_3(q) := g_3(u(q), u(q^3)) = 0$ yields, as before,

$$\begin{aligned}
 a_0 &= 0, & a_1 &= 3c_1, & a_2 &= 3c_2, & a_3 &= 3c_3, & a_4 &= 3c_1c_2 + 3c_4, \\
 a_5 &= -4c_1 - 3c_1c_3 + 3c_2^2 + 3c_5 + c_1^3, \\
 a_7 &= -3c_3^2 - 1 + 3c_5c_1 - 9c_1^2 + 3c_4c_2 + 3c_7, \\
 a_8 &= -4c_2 + 3c_8 + 6c_5c_2 + 3c_6c_1 + 3c_1^2c_4 - 3c_1c_3c_2 - 3c_4c_3 \\
 (2.4b) \quad & - 6c_1^2c_2 - 6c_1c_4 - 9c_1c_2 + c_2^3, \\
 a_{11} &= 3c_1c_2c_6 - 3c_1c_5c_3 - 3c_2c_4c_3 - 12c_1c_4c_2 - 4c_3 + 3c_{11} - 6c_4^2 \\
 & - 12c_5c_1 + 3c_5^2 + 4c_1^2 - 9c_2^2 + 6c_2c_8 - 3c_3c_7 + 3c_6c_4 + 3c_9c_1 \\
 & - 12c_1c_2^2 + 3c_7c_1^2 + 3c_1c_4^2 + 3c_5c_2^2 \\
 & - 6c_1^2c_2^2 + c_3^3 - 4c_1^4, \dots
 \end{aligned}$$

When we substitute these values into $G_3(q)$, it becomes a series in m_t (again note the omission of identically vanishing terms):

$$(2.4c) \quad G_3(q) = \frac{m_6q^6 + m_9q^9 + m_{10}q^{10} + m_{12}q^{12} + m_{13}q^{13} + m_{14}q^{14} + \dots}{q^{11}}.$$

The $(D =)3$ singular terms have the coefficients

$$\begin{aligned}
 m_6 &= -3c_6 + 3c_1c_2 + 3c_4, \\
 m_9 &= -c_1 + 3c_5 - 3c_9 + 6c_4c_2 + 3c_1c_3 + 3c_2^2 - 6c_6c_2 + 6c_1c_2^2 + c_1^3, \\
 (2.4d) \quad m_{10} &= 3c_1c_3c_2 - c_2 + 3c_8 - 3c_{10} - 3c_5c_4 + 6c_2c_5 + 3c_1c_6 + 3c_3c_4 \\
 & - 3c_1c_8 - 3c_2c_7 + 6c_4c_1^2 + c_2^3 + 3c_2c_1^3 - 3c_6c_1^2.
 \end{aligned}$$

Thus, the series $u(q)$ and the 3-Newtonian polynomial $g_3(u, v)$ are both determined by the coefficients c_1, \dots, c_{11} (with the $D = 3$ omissions c_6, c_9, c_{10} , which are determined by equating the expressions in (2.4d) to 0).

3. SIMULTANEOUS MODULAR EQUATIONS

We now consider the results of the simultaneous substitution of

$$(3.1a) \quad u(q) = 1/q + c_1q + c_2q^2 + c_3q^3 + \dots$$

into two p -Newtonian modular equations (1.5d), for $p = 2$ and $p = 3$.

The easiest place to start is with the 2-Newtonian modular polynomial $g_2(u, v)$. It is determined by the quadruple c_1, c_2, c_3, c_5 from which we find c_4 and c_6, c_7, \dots as in (2.3e). So all coefficients c_t in (3.1a) are now functions of c_1, c_2, c_3, c_5 alone. (It turns out that we shall have to go as far as c_{17} for now and as far as c_{28} later on).

Turning our attention to the 3-Newtonian modular polynomial $g_3(u, v)$, we find from (2.4bcd) that $c_1, c_2, c_3, c_4, c_5, c_7, c_8, c_{11}$ determine the polynomial $g_3(u, v)$ and more importantly the *same* series (3.1a) (including c_6, c_9, c_{10}). Obviously, the process of reconciliation with the identities from $g_2(u, v)$ must involve values of the quadruple c_1, c_2, c_3, c_5 .

We go back to (2.4d) and substitute the information from (2.3e). Then coefficient m_j in (2.4cd) becomes M_j (in terms of only c_1, c_2, c_3, c_5) as follows:

$$\begin{aligned}
 m_6 &\rightarrow M_6 = 0, \\
 m_9 &\rightarrow M_9 = 5/4c_1 - 9/2c_3 + 3c_5 - 9/8c_1^2 - 3c_1c_2 + 3c_1c_3 + 3c_2^2 - 6c_3c_2 \\
 &\quad - 3/2c_3^2 + 3c_5c_3 + 3/2c_2c_1^2 + 3/2c_1^2c_3 - 3c_1c_2^2 + 3c_2c_1c_3 \\
 (3.1b) \quad &\quad - 5/4c_1^3 - 3/2c_1c_3^2 - 3c_5c_1^2 + 3/2c_2c_1^3 + 9/8c_1^4, \\
 m_{10} &\rightarrow M_{10} = 3c_2c_5c_1 + 3/2c_1 - 5/2c_2 - 3c_3 + 3c_5 - 3/2c_1^2 + 3/2c_1c_3 \\
 &\quad + 3/2c_2^2 - 15/2c_3c_2 + 3c_3^2 - 3/2c_5c_1 + 6c_5c_2 - 3c_5c_3 \\
 &\quad + 3c_2c_1^2 + 3/2c_1^2c_3 - 6c_1c_2^2 - 3/2c_1^3 + c_2^3 - 3c_3c_2^2 \\
 &\quad - 3/2c_5c_1^2 + 3/2c_2c_3^2 - 3/2c_2c_1^3 + 3/2c_1^4 - 3/2c_1^2c_2^2.
 \end{aligned}$$

For the elimination process we also need to express M_{14} and M_{17} as functions of c_1, c_2, c_3, c_5 . These formulas are found by the same procedure, but are too long to reproduce here.

The generating quadruples c_1, c_2, c_3, c_5 for $u(q)$ are, of course, found from elimination from *all* the $M_k = 0$. To obtain them, we note it is necessary (but not likely sufficient) that the quadruples are simultaneous roots of four coefficients

$$(3.2a) \quad M_9, M_{10}, M_{14}, M_{17}$$

(chosen for reasons which become clear later on).

We use the notation

$$(3.2b) \quad M_{i \times j} = c_5\text{-resultant}(M_i, M_j).$$

These are functions of c_1, c_2, c_3 only. We denote

$$(3.2c) \quad M_{i \times j \times k} = c_3\text{-resultant}(M_{i \times j}, M_{i \times k}).$$

These are functions of c_1, c_2 only.

We note that in the case $p = 3$ (by substitution of the relations (2.3e) for $p = 2$), some of the M_j will acquire an algebraic dependence. Thus, M_6 becomes identically 0 and $M_{9 \times 12}$ does not contain any information not already in $M_{9 \times 10}$. The choices in (3.2a) were discovered by trial and error to lead to independent functions of c_1, c_2, c_3

$$(3.2d) \quad M_{9 \times 10}, M_{9 \times 14}, M_{9 \times 17},$$

and to further lead to independent functions of c_1, c_2 ,

$$(3.2e) \quad M_{9 \times 10 \times 14}, M_{9 \times 10 \times 17}.$$

We might think that it is only necessary to eliminate (say) c_2 from (3.2e) to find a finite set of c_1 and work backward to the quadruple c_1, c_2, c_3, c_5 (so as to provide roots of (3.2a)). This cannot be done directly because of common factors, i.e.,

$$\begin{aligned}
 (3.3a) \quad M_{9 \times 10 \times 14} &= (c_1 - 1)^2 P_{29}(c_1, c_2) P_4(c_1, c_2)^2, \\
 M_{9 \times 10 \times 17} &= (c_1 - 1)^3 P_{34}(c_1, c_2) P_4(c_1, c_2)^3, \\
 P_4(c_1, c_2) &= 24 - 2c_1 - 35c_1^2 + 3c_1^3 + 12c_1^4 - 36c_1c_2^2 + 48c_2 + 24c_2^2.
 \end{aligned}$$

Here, $P_n(\dots)$ denotes a *nonfactorable* polynomial in $\mathbf{Z}[\dots]$ of total degree n in its variables. (Happily, in this context the degree happens to distinguish the polynomials).

TABLE I. Series satisfying Newtonian equations of order 2 and 3

Case	c_1	c_2	c_3	c_4	c_5	Ident.	Genus
1	196884	21493760	864299970	20245856256	333202640600	1A	0
2	134	760	3345	12256	39350	5A	0
3	51	204	681	1956	5135	7A	0
4	17	46	116	252	533	11A	0
5	12	28	66	132	258	13A	1
6	9	10	-30	6	-25	5B	0
7	7	14	29	50	92	17A	1
8	6	10	21	36	61	19A	1
9	-6	20	15	36	0	5a	1
10	4	5	10	16	25	25A	1
11	4	7	13	19	33	23A	0
12	3	3	6	9	13	31A	1
13	3	4	7	10	17	29A	2
14	2	2	3	4	7	41A	3
15	2	3	5	6	10	35B	2
16	2	8	-5	-4	-10	7B	2
17	2	1	1	2	3	55A	1
18	2	1	2	3	4	49a	3
19	-1	0	0	1	0	25a	2
20	-1	2	1	2	-2	13B	2
21	1	0	1	1	1	95A	2
22	1	0	0	0	0	$(1/q + q)$	0
23	1	2	3	3	5	47A	1
24	1	4	6	6	10	35A	1
25	1	1	2	2	3	59A	3
26	1	1	1	1	2	71A	2
27	1	-1	1	1	0	35a	2
28	0	0	0	0	0	$(1/q)$	0
29	0	0	1	1	1	119A	3

The identifications are after the table of McKay and Strauss [14]. The genus refers to the 2-Newtonian equation in each case.

So to find the values of c_1 (in addition to the obvious $c_1 = 1$), we find the resultants of P_{29}, P_{34}, P_4 taken two at a time. In effect,

$$\begin{aligned}
 c_2\text{-resultant}(P_{29}, P_4) &= (c_1 + 1)^2(c_1 - 2)^2 P_{24}(c_1) P_{48}(c_1), \\
 c_2\text{-resultant}(P_{34}, P_4) &= (c_1 + 1)(c_1 - 2) P_{92}(c_1), \\
 c_2\text{-resultant}(P_{29}, P_{34}) &= c_1^5(c_1 - 196884)(c_1 - 134)(c_1 - 51)(c_1 - 17) \\
 &\quad (c_1 - 12)(c_1 - 9)(c_1 - 7)(c_1 - 6)(c_1 + 6) \\
 &\quad (c_1 - 4)^2(c_1 - 3)^2(c_1 - 1)^{54}(c_1 + 1)^3 \\
 &\quad (c_1 - 2)^7 P_{134}(c_1) P_{518}(c_1).
 \end{aligned}
 \tag{3.3b}$$

Thus, working backwards from the integral values of c_1 displayed as roots in (3.3b), we find c_2 from any one of the polynomials in (3.2e), c_3 likewise from (3.2d), and c_5 from (3.2a).

As a result, we find 29 *integral* cases shown in Table I, with c_4 calculated from (2.3e). (If we had not made the restriction of integrality, there would be literally *hundreds* of additional quadruples arising from the polynomials $P_n(c_1)$ in (3.3b).)

Obviously, $j(\tau) - 744$ is present (Case 1). All solutions have been assigned identifying symbols, which shall be discussed in the next section. (The genera of the corresponding 2-Newtonian modular equations are of possible interest as they show all possible values for a quartic.)

4. THE EXTENDED MODULAR FUNCTIONS AND GROUPS

To interpret the various cases in Table I, it is necessary, at the very least, to introduce “extended” modular functions and groups. This concept is assuredly not part of the “brute force” calculation in the Main Theorem (above), but it is part of the theoretical verification.

The traditional Klein modular group Γ operates on H^+ , the upper-half τ -plane so as to preserve $j(\tau)$. For a given $N \in \mathbf{Z}^+$, we next define $\Gamma^0(N)$, the subgroup of Γ which keeps $j(\tau/N)$ as well as $j(\tau)$ invariant. Then $\Gamma^0(N)$ has an extension $\Gamma^c(N)$, which was discovered by Fricke and Bessel-Hagen [10] in 1929 and proved by Atkin and Lehner [2] in 1970 to be (within equivalence) a maximal discrete normal extension group of $\Gamma^0(N)$ in $SL_2(\mathbf{R})$. In particular, $\Gamma^c(N)$ is a collection of sets of matrices S_T (over \mathbf{Z}) indexed by T , a divisor of N restricted to primary factors, i.e.,

$$(4.1a) \quad T|N, \gcd(T, N/T) = 1.$$

The matrices in S_T are represented for convenience by the linear fractional formulation $\tau' = S_T(\tau)$ with coefficients in \mathbf{Z} . Thus,

$$(4.1b) \quad \Gamma^c(N) = \{S_T\}, S_T : \{\tau' = \frac{A\tau + B}{C\tau + D}, AD - BC = T, T|\gcd(A, D), T|N|B\}.$$

Of course, $S_1 = \Gamma^0(N)$. Thus, as special cases,

$$(4.1c) \quad \{\tau' = \tau + N\} \in S_1, \{\tau' = -N/\tau\} \in S_N.$$

When N is 1, 2 or 3, the above transformations are sufficient to determine $\Gamma^c(N)$, but in general the situation is more complicated (see [4,6]). (The subgroup $\Gamma^*(N) = S_1 \cup S_N$ is more usually associated directly with Fricke [9].)

4.2a Definition. An extended modular function is one associated with a subgroup of some $\Gamma^c(N)$ or an equivalent. The minimum such N is the level of the extended modular function.

4.2b Lemma. For cases where $\Gamma^c(N)$ is of genus zero, the global uniformizing parameter (*Hauptmodul*) $j_N(\tau)$ satisfies a p -Newtonian modular equation (relating

$j_N(\tau)$ and $j_N(p\tau)$) if and only if $\gcd(N, p) = 1$. The same holds in $\Gamma^0(N)$ and $\Gamma^*(N)$.

A proof can be found in [6]. Some Hauptmoduls of subgroups will also enjoy the property of the p -Newtonian modular equation, but not so in general. It should be understood that “ q ” may have to be interpreted as $\exp 2\pi i\tau/N$ as the case requires (because the general translation at ∞ in $\Gamma^0(N)$ is $\tau \rightarrow \tau + N$).

4.3 Remark on replicable functions. All 29 cases in Table I are identified from the larger table [14] of replicable functions. These functions are each associated with a (generalized) level N and each has the property that it may not satisfy a p -Newtonian equation when $p|N$. To make this work more self-contained, we shall verify this property as needed (from Lemma 4.2b only).

We make more direct use of the theory of extended modular functions. There are tabulations (see [4]) of the values of N where $\Gamma^c(N)$ is of genus zero. They show 64 cases as follows:

$$(4.4a) \quad N = 2, 3, 4, 5, 6, 7, 8, 9, 10, 12, 13, 16, 18, 25,$$

where $\Gamma^0(N)$ is of genus zero to begin with; also,

$$(4.4b) \quad \begin{aligned} N = 11, 14, 15, 17, 19, 20, 21, 23, 24, 26, 27, 29, 31, 32, 35, 36, \\ 39, 41, 47, 49, 50, 59, 71, \end{aligned}$$

where $\Gamma^*(N)$ is of genus zero (Fricke’s cases) [9,3], and, finally,

$$(4.4c) \quad \begin{aligned} N = 22, 28, 30, 33, 34, 38, 42, 44, 45, 46, 51, 54, 55, 56, 60, 62, 66, 69, 70, \\ 78, 87, 92, 94, 95, 105, 110, 119, \end{aligned}$$

where $\Gamma^c(N)$ is of genus zero. (Note $\Gamma^c(N) = \Gamma^*(N)$ when N is a prime power.)

The 15 primes in (1.7a) used in the Main Theorem 1.7 are those which divide the values of N in (4.4abc). Note that they are already present in Fricke’s shorter list (4.4ab). They were first observed by Andrew Ogg to be the same as the prime divisors of the order of the Monster group.

5. COMPLETION OF THE COMPUTATION FOR THE MAIN THEOREM

In Table I we ignore the trivial Cases 22 and 28, and (the desired) Case 1, thus leaving 26 cases which we must eliminate in order to prove the Main Theorem. For these 26 cases, we invoke the condition that the series for $u(q)$ must simultaneously satisfy some other p -Newtonian modular equation for $p(> 3)$ a Fricke-Monster prime. In the identifications (from the table in [14]), the number is the level (≥ 1). The letter is more arcane, but the “ A ” denotes a Hauptmodul $j_N(\tau)$ of $\Gamma^c(N)$ and the “ B ” denotes a Hauptmodul of $\Gamma^0(N)$.

We first reduce the job by eliminating the 10 cases (out of the 26) where the identifying index is divisible by 5 in Table I. (For these cases the Hauptmoduls do not all come under Lemma 4.2b.) We now use a combination of Newtonian modular equations for $p = 2$ and 5 (as we had done before with $p = 2$ and 3). A complete computation of four *independent* eliminants M_t as in (3.2a) might require enormous

values of t , but a partial computation is effective enough. We use equations of type (2.3e) to recompute values of c_t for the 2-Newtonian modular equation (this time up to $t = 28$) as functions of the basic c_1, c_2, c_3, c_5 . Then, as in §3 (above) we expand a 5-Newtonian $g_5(u, v)$ into

$$(5.1a) \quad G_5(q) := g_5(u(q), u(q^5)) = \sum_{i=0}^{\infty} g_i q^i / q^{29}$$

(note $Q = 29$ and $D = 10$). Then the process of discovery of the $(P =)20$ coefficients of $g_5(u, v)$ will dispose of 20 coefficients of (5.1a) and leave 10 values in the principal part of (5.1a). Thus as in (2.4c), the equation (5.1a) shows 10 singular terms

$$(5.1b) \quad G_5(q) = [m_{10}q^{10} + m_{15}q^{15} + m_{16}q^{16} + m_{20}q^{20} + m_{21}q^{21} + m_{22}q^{22} + m_{25}q^{25} + m_{26}q^{26} + m_{27}q^{27} + m_{28}q^{28} + \dots] / q^{29}.$$

(Compare the coefficients $a_t = 0$ in Figure 1.) Actually, some of these m_t vanish identically as a result of the dependence of the 2-Newtonian relations (2.3e) of the c_t .

We test all 10 cases in Table I where the indicated level is divisible by 5. In these cases we substitute c_1, c_2, c_3, c_4 into the m_t present in (5.1b). Remarkably, we must go as far as m_{26}, m_{27}, m_{28} before we find any m_t (actually all three) unequal to 0 for (just) these 10 cases.

If we return to our list of genus zero cases (4.4abc), we see that removal of prime factors 2, 3, and 5 leaves us with 14 genus zero cases:

$$(5.2) \quad N = 7, 11, 13, 17, 19, 23, 29, 31, 41, 47, 49, 59, 71, 119.$$

Now there *must* be a Hauptmodul for $\Gamma^c(N)$ in each of these cases, as shown by the “A” designation (including, exceptionally “49a”). These 14 cases would necessarily be removed by the failure of the coefficients of any p -Newtonian equation for $p|N$, by Lemma 4.2b.

This leaves us with only $(26-10-14=)$ two recalcitrant cases from the original 29 in Table I, namely (Case 16) “7B” and (Case 20) “13B.” Both of these are Hauptmoduls for $\Gamma^0(N)$. So by Lemma 4b, they too would be likewise removed by $p = 7$ and 13, respectively. (Note these are the only two primes > 5 which appear in (4.4a).)

The proof of the Main Theorem is now complete.

6. INDEPENDENCE OF THE PROOF OF THE MAIN THEOREM

In the course of the proof of the Main Theorem, it was interesting to be aware of McKay’s Conjecture, and it was edifying to identify and label the cases by the table in [14]. Yet the 26 cases could be eliminated independently. Indeed, the first 10 are first identified and then eliminated by checking the 5-Newtonian equation (as before). The remaining 16 cases are disposed of by the “coincidence” of 16 available Hauptmoduls (with integral coefficients), namely the 14 in (5.2) where the genus of $\Gamma^c(N)$ is 0, and the two cases $N = 7, 13$ where $\Gamma^0(N)$ has genus 0. In each case

some $p(> 5)$ divides N , and for this p no p -Newtonian equation is satisfied. (Of course, we do not *have to know* which case was which!)

Note that the proofs in §§5 and 6 do not require that the lists (4.4abc) be complete (although this is strongly believed).

7. CONCLUDING REMARKS

The main computation lies at the fringe of the SUN-Maple capacity. We can only hope that future computer algebra systems will permit the simultaneous solution of p -Newtonian modular equations for larger pairs of p (indeed up to 71). If McKay's Conjecture 1.6 holds, this would be a theoretically easy way to find all the extended modular Hauptmoduls (with integral coefficients). On the further assumption that no value of N has more than three prime divisors, it suffices to take 10 pairings of $p \in \{2, 3, 5, 7, 11\}$ to obtain a list of all Hauptmoduls. (This is a little bit closer to the capabilities of current computers.)

Also, Table I provides a possible proof that even if the lists (4.4abc) are incomplete, no more prime divisors will occur beyond those listed in (1.7a). Obviously, no other primes occur in the identifiers of Table I, and if some composite N existed for which $\Gamma^c(N)$ had genus zero, the same would be true of its prime divisors by an elementary argument on the projection of a Riemann surface to one of (necessarily) no greater genus.

Finally, the algebraic dependency among the variables M_t (as in (3.1b)) seems intractable. For instance, M_t for $t = 11, 12, 13$ are dependent on M_9 and M_{10} . It is unlikely, however, that *all* M_t can be dependent on just the four cases $t = 9, 10, 14, 17$ in (3.2a). For if so, all hundreds of irrational roots c_1 in (3.3b) would lead to legitimate Laurent series solutions of the p -Newtonian equations for $p = 2$ and 3.

REFERENCES

1. D. Alexander, C. Cummins, J. McKay, and C. Simons, *Completely replicable functions*, Groups, Combinatorics and Geometry (M.W. Liebeck and J. Saxl, eds.) (1992), 87–98; (LMS Lecture Note Series, vol. 165), Cambridge Univ. Press. MR **94g**:11029
2. A.O.L. Atkin and J. Lehner, *Hecke operators on $\Gamma_0(m)$* , Math. Ann. **185** (1970), 134–160. MR **42**:3022
3. H. Cohn, *Fricke's two-valued modular equations*, Math. of Comput. **51** (1988), 787–807. MR **89f**:11064
4. H. Cohn, *A numerical survey of the reduction of modular curve genus by Fricke's involutions* (1991), Springer Verlag, 85–104; Number Theory, New York Seminar (1989-90). MR **92f**:11060
5. H. Cohn, *How branching properties determine modular equations*, Math. of Comput. **61** (1993), 155–170. MR **93k**:11036
6. H. Cohn, *Half-step modular equations*, Math. of Comput. **64** (1995), 1267–1285. MR **96a**:11038
7. J.H. Conway and S.P. Norton, *Monstrous moonshine*, Bull. Lond. Math. Soc. **11** (1979), 308–339. MR **81j**:20028
8. D. Ford, J. McKay and S. Norton, *More on replicable functions*, Comm. in Algebra **13** (1994), 5175–5193. MR **95i**:11036
9. R. Fricke, *Lehrbuch der Algebra III (Algebraische Zahlen)*, Vieweg, Braunschweig, 1928.
10. R. Fricke, *Über die Berechnung der Klasseninvarianten*, Acta Arith. **52** (1929), 257–279.
11. D.H. Lehmer, *Properties of coefficients of the modular invariant $J(\tau)$* , Amer. J. Math. **64** (1942), 488–502. MR **3**:272c
12. K. Mahler, *On a class of non-linear functional equations connected with modular equations*, J. Austral. Math. Soc. **22A** (1976), 65–118. MR **56**:258

13. Yves Martin, *On modular invariance of completely replicable functions*, (preprint).
14. J. McKay and H. Strauss, *The q -series decompositions of monstrous moonshine and the decomposition of the head characters*, Comm. in Algebra **18** (1990), 253–278. MR **90m**:11065

DEPARTMENT OF MATHEMATICS, CITY COLLEGE (CUNY), NEW YORK, NEW YORK 10031

Current address: IDA, Bowie, Maryland 20715-4300

E-mail address: hihcc@cunyvm.edu

DEPARTMENT OF COMPUTER SCIENCE, CONCORDIA UNIVERSITY, MONTREAL, QUEBEC, CANADA
H3G 1M8

E-mail address: mckay@vax2.concordia.ca