Computer Science Journal of Moldova, vol.**4**, no.3(12), 1996

Replicable functions: a computational approach

Mihai Cipu*

Abstract

Methods for investigating replicable functions and a computer program which implements these methods are under development by the author. This research announcement contains the theoretical background of the method and the basic ideas of implementation.

1 Introduction

Besides the attraction inherent to any mathematical items, the topic of our research is significant for several reasons.

1. The notion alluded to in the title appeared as a surprising property shared by modular functions and head representations of the largest sporadic simple group. This connection between automorphic functions and finite simple groups is just the tip of a deep phenomenon explained by some work due to I.B.Frenkel, J.Lepowsky and A.Meurman and R.E.Borcherds.

2. The central notion and the problem itself arose in a manner called by several people numerology: some numbers appearing in distinct reasearch areas are strikingly close and the fact calls for an explanation. The first remarks of this kind are due to J.McKay in 1978. Thompson has noticed further relations and passed them to other people working on the classification of finite simple groups.

*Supported by a grant from International Centre for Theoretical Physics Trieste (Italy)

> They were convinced that the numbers mirror a hidden unifying structure lying deep enough to escape the experts in each field. Revealing the ultimate explanation seemed to be the privilege of those who succeed to master both fields. Actually, it turned out that a completely different research area has provided the tools needed to clarify the connections.

3. It is one of the first manifestations of the present direction mathematics is moving in, that of an experimental science. Essentially, mathematical research means making conjectures and providing proofs for them. Since very powerful computers are generally available, they may be helpful in the first phase of this simplified scheme. Looking at many computer-generated examples and noticing patterns, mathematicians can infer new properties of known objects or the existence of other interesting concepts.

The paper is organized as follows. First, we recall some of the notions needed to introduce the concept and the problem we are interested in. The second section contains several characterizations and properties of replicable functions, as well as the statement of Norton's conjecture aiming to give another description of replicability. The approach we took to prove there are only finitely many non-trivial replicable functions is presented in Section 3. The algorithm description rests at a conceptual level, without implementation details–these will be deferred to another paper. Section 3 also contains results obtained so far. The next section is devoted to an independent proof of Norton's theorem asserting that all replicable functions are determined by 12 of the first 23 coefficients of their q-expansions. Since our approach heavily relies on Norton's result, we strived for a proof which is suitable for direct and efficient implementation in a programming language. Finally we note some of the conclusions of the work developed so far and discuss possible improvements for the implementation of the algorithm, as well as ideas for further work.

2 Preliminaries

As mentioned above, replicable functions emerged in between two old and very respectable research areas: the theory of modular forms and group theory. We briefly review here some of the concepts needed to understand the native environment of the problem we are dealing with.

2.1 Modular functions

A very important tool in complex analysis is represented by lattices in the complex plane. Each of this is described as $\{m\omega_1 + n\omega_2 \ : \ m, n \in \mathbb{Z}\}$ for two periods ω_1 , $\omega_2 \in \mathbb{C}$. The basis ω_1 , ω_2 can be replaced by any other pair ω_1' , ω_2' provided that $\omega_1' = a\omega_1 + b\omega_2$, $\omega_2' = c\omega_1 + d\omega_2$ for some integers a, b, c, d. To obtain precisely the same lattice, one has to impose the condition $ad - bc = 1$. However, in many questions what really matters is the shape of the lattice, not its orientation or its size. So, if one doesn't distinguish two rotated or dilated versions of the same lattice, the shape is described by the complex number $\tau = \omega_1/\omega_2$ as well as by $\tau' = \omega_1'/\omega_2'$. If one works it out, one finds

$$\tau' = \frac{a\tau + b}{c\tau + d} \ .$$

Thus a quotient space arises naturally and the discussion sketched above will be formalized and detailed below.

The group $SL_2(\mathbb{R})$ of real 2×2 matrices of determinant 1 acts on the upper half-plane

$$H := \{z \in \mathbb{C} : \Im z > 0\} \tag{1}$$

by fractional linear transformations

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot z = \frac{az + b}{cz + d}. \tag{2}$$

The action of $SL_2(\mathbb{Z})$ on $\overline{\mathbb{R}} := \mathbb{R} \cup \{\infty\}$ is transitive and only ± 1 fixes as many as 3 points. A matrix δ is called *parabolic* if it fixes a

unique point of $\overline{\mathbf{R}}$, and the fixed-point is called a *cusp of G*. For instance, if x is a non-zero real number, then the translation $\delta = \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}$ is parabolic and the cusp is ∞. The cusps of $SL_2(\mathbb{Z})$ are the rationals $\mathbb{Q} \cup \infty$ on which $SL_2(\mathbb{Z})$ acts transitively. Thus we can take ∞ as the representative set of the orbit space $SL_2(\mathbb{Z})/\mathbb{Q} \cup \{\infty\}$ whose compactification is a sphere.

A subgroup $G \subseteq SL_2(\mathbf{R})$ is *commensurable* with $SL_2(\mathbb{Z})$ if $G \cap SL_2(\mathbb{Z})$ has finite index in both G and $SL_2(\mathbb{Z})$. If G is commensurable with $SL_2(\mathbb{Z})$, then G is discrete (*i.e.* the natural topology of $SL_2(\mathbf{R})$ induces the discrete topology on G), G has only finitely many orbits on its cusps, and adjoining these to the quotient space H/G yields a compact Riemann surface $X_G := \overline{H/G}$. Unlike the case of $SL_2(\mathbb{Z})$ itself, the genus of X_G will in general not be zero.

Example. For any positive integer N one denotes by $\Gamma(N)$ the kernel of the epimorphism $SL_2(\mathbb{Z}) \longrightarrow SL_2(\mathbb{Z}/N\mathbb{Z})$, while $\Lambda(N)$ denotes the normalizer of the group

$$\Gamma_0(N) := \{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) : c \equiv 0 \bmod N\}$$

in $SL_2(\mathbf{R})$. It is not hard to see that $\Lambda(N)$ is commensurable with $SL_2(\mathbb{Z})$, as indeed is any subgroup intermediate between $\Gamma_0(N)$ and $\Lambda(N)$.

Given G commensurable with $SL_2(\mathbb{Z})$, one associates to it the compactification X_G of the quotient space H/G and the field $K(X_G)$ consisting of all meromorphic functions $f : X_G \longrightarrow \mathbb{C} \cup \{\infty\}$. The compact Riemann surface X_G has genus zero precisely when the field $K(X_G)$ is a purely transcendental extension of $\mathbb{C}$, $K(X_G) = \mathbb{C}(t)$ for an indeterminate t. In such a case we say that G is a *genus 0 group* and any homeomorphism $f : X_G \longrightarrow \mathbb{C} \cup \{\infty\}$ is called a *Hauptmodul* for G. Clearly, a generator for the field $K(X_G)$ is determined up to rational transformations. If f is a Hauptmodul then,being one-to-one, it has a unique pole, and such a pole is necessarily simple. One may chose f so that the pole is at ∞, and the residue is 1.

All discrete groups G will contain some $\Gamma_0(N)$. In particular, they contain the translation map $z \mapsto z+1$ given by the matrix $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, so that we may take ∞ as a cusp. One usually identifies ∞ with $\lim_{y\to+\infty} iy$, so that under the map $q : z \mapsto \exp 2\pi iz$ which maps H onto the interior of the unit disk, ∞ is mapped to the origin. In the complex structure of X_G one may take q as a local parameter at the point ∞. Thus any G-invariant function $f \in K(X_G)$, being meromorphic at each point of X_G, has a Laurent expansion about ∞ in terms of q: $f(q) = \sum_{n\geq n_0} a_n q^n$, $a_{n_0} \neq 0$.

If f is a Hauptmodul, its q-expansion looks like

$$f = q^{-1} + a_0 + \sum_{n=1}^{\infty} a_n q^n \ .$$

The constant term a_0 will vary according to the location of the unique zero of f, which once specified determines f uniquely. We may normalize it so that its zero is at 0.

For instance, the meromorphic modular-invariant functions on H comprise precisely the field of rational functions of

$$j(z) := \frac{(1 + 240 \sum_{n>0} \sigma_3(n) q^n)^3}{q \prod_{n>0}(1-q^n)^{24}} =$$

$$q^{-1} + 744 + 196884q + 21493760q^2 + \dots \ ,$$

where

$$\sigma_3(n) := \sum_{d|n} d^3$$

is the sum of the cubes of the divisors of n.

Considering $G = \Gamma_0(2)$, one finds that H/G is a sphere with 2 points removed, so that G is a genus 0 group. The q-expansion of its normalized Hauptmodul is

$$24 + q^{-1} \prod_{q>0} (1-q^{2n+1})^{24} = q^{-1} + 276q - 2048q^2 + 11202q^3 + \dots \ .$$

Similarly $\Gamma_0(N)$ is a genus 0 group in the cases $N \leq 10$.

However, the genus of $\Gamma_0(N)$ tends to infinity as N increases (a stronger theorem has been proved by Thompson in [9]). A related result is due to Ogg [7] : the normalizer of $\Gamma_0(p)$ for prime p is a genus 0 group iff $p \in \{2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 41, 47, 59, 71\}$.

2.2 Finite simple groups

This strange set of prime numbers coincides with the prime divisors of the order of the sporadic finite simple group M whose existence has been predicted in 1973 by B.Fischer and B.Griess. By the time when Ogg obtained his result, the existence of the group M still was a matter of speculation, so this coincidence was intriguing indeed. Were it not only a mere coincidence, it would point to a unexpected relationship between automorphic functions and group theory.

The huge work deployed to construct the group M is very interesting. At least at the beginning, the approach was very similar to the reasoning usual in elementary particle physics: one infers many properties of an object before one asserts its existence.

From the very beginning it was conjectured that M has an irreducible rational character χ_2 of degree $\chi_2(1) = 196883$. Admitting this, Thompson [8] has shown that M must be unique and the entire character table has been constructed by Fischer, Livingston and Thorne [4]. They found 172 irreducible rational characters $\chi_1 = 1$, χ_2 , $\ldots, \chi_{172}$ ordered by increasing degrees (recall that $a, b \in M$ are *rationally equivalent* if there exist an element x in M and some integer s relatively prime to the order of M such that $a = xb^s x^{-1}$).

In 1978, J.McKay observed that the coefficient of q in the modified elliptic modular function $J(q) := j(q) - 744$ is $a_1 = \chi_1(1) + \chi_2(1)$. Likewise Thompson discovered that higher coefficients can be expressed as simple linear combinations

$$J(z) = q^{-1} + (\chi_1(1) + \chi_2(1))q + (\chi_1(1) + \chi_2(1) + \chi_3(1))q^2 +$$

$$(2\chi_1(1) + 2\chi_2(1) + \chi_3(1) + \chi_4(1))q^3 + \ldots \ .$$

This suggests that other interesting series might be

$$T_g(q) := q^{-1} + \sum_{n>0} T_n(g) q^n \ ,$$

where $T_n(g)$ are rational characters of M and g is an element of the Monster group. Note that $J(z)$ depends only on the rational equivalence class of g. Thus we get 172 meromorphic functions on H, with a simple pole of residue 1 at ∞ and vanishing 0-th coefficient there and with all Fourier coefficients in $\mathbb{Z}$.

2.3 Monstrous Moonshine

The mysterious connections between the biggest finite simple group M and modular forms have been investigated by many other people aware of Ogg's result and McKay's observation. J.Conway and S.P.Norton [3] made a number of remarkable conjectures concerning these series for which they coined the term "monstrous moonshine". Some of their guesses have been proved, others turned out to be false, and a few of them are still open. One of them is the following:

Conjecture 2.1 *There are only finitely many subgroups $G \leq SL_2(\mathbf{R})$ satisfying:*

1. *G contains some $\Gamma_0(N)$*
2. *G is a genus 0 group*
3. *the translation $z \mapsto z + k$ is in G exactly when k is an integer*
4. *the coefficients in the canonical Hauptmodul for G are algebraic integers.*

The main conjecture in Conway and Norton's paper has been finally proved by Borcherds: each rational conjugacy class in M gives rise to a Hauptmodul for a genus 0 subgroup of $SL_2(\mathbf{R})$. His result relies on previous work done by I.B.Frenkel, J.Lepowsky and A.Meurman:

Theorem 2.2 *([5]) There exists an infinite dimensional $\mathbb{Z}$ -graded representation $V = \bigoplus V_n$ of the Monster simple group such that the dimension of V_n is equal to the coefficient a_n of the elliptic modular function J.*

Theorem 2.3 *([2]) Suppose that V is the graded representation of M constructed by Frenkel et.al.. Then for any element g of the Monster group the Thompson series $T_g(q) = \sum_{n\in\mathbb{Z}} Tr(g \mid V_n)q^n$ is a Haupt-modul for a genus 0 subgroup of $SL_2(\mathbb{R})$.*

3 Replicable functions

3.1 Definition, characterizations

Let f be a function having q-expansion

$$f(z) = q^{-1} + a_1 q + a_2 q^2 + a_3 q^3 + \dots \ , \tag{3}$$

where $q = \exp 2\pi\sqrt{-1}z$. Such a function is called *replicable* if there are replicate functions $\{f^{(u)}\}_{u\geq 1}$ such that for all $n \geq 1$, the expression

$$P_n(f) := \sum_{\substack{ud=n \\ 0\leq b<d}} f^{(u)}(\frac{uz+b}{d}) \tag{4}$$

is a polynomial in f with q-expansion

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

i.e.

$$P_n(f) \equiv q^{-n} \bmod q\mathbb{Z}[q] \ .$$

One can show that $P_n(f)$ is given by a unique monic polynomial from $\mathbb{Z}[a_1, a_2, \dots, a_{n-1}][t]$.

The prototypical replication relation is that for Thompson series $T_g(z)$ for $g \in M$. The u^{th} replicate for $T_g(z)$ is $T_{g^u}(z)$. Here one notes that all replicates are replicable as well (some people would phrase this

property: the monstrous moonshine functions are *completely replicable*). In particular, the modular elliptic function J is replicable. However, the simplest example of replicable function is $q^{-1} + aq$.

Admittedly, definition (4) seems intricate. It looks more natural as soon as one introduces the twisted Hecke operator which acts linearly on q-coefficients yet takes the function $f(z)$ to $\frac{1}{n}P_n(f)$. A very useful description has been provided by Norton [6]. In that paper it is shown that the generating function for all twisted Hecke operators is

$$\sum_{n\geq 1} \frac{P_n(t)}{n} q^n = -\ln(q(f(z)-t)) \ .$$

This relation yields recursively the polynomials invoked in the definition of replicable functions:

$$P_1(t) = t, P_2(t) = t^2 - 2a_1 \ , P_3(t) = t^3 - 3a_1 t - 3a_2 \ , \ldots \ .$$

One finds also that P_n's satisfy the recurrence relation

$$tP_{n-1}(t) = na_{n-1} + \sum_{k=-1}^{n-2} a_k P_{n-k-1}(t) \ , r \geq 1 \ , v \tag{5}$$

with initial condition $P_0(t) = 1$.

Following Norton [6], let us consider the coefficients $\{H_{m,n}\}_{m,n\geq 1}$ introduced by

$$P_n(f) = q^{-n} + n \sum_{n\geq 1} H_{m,n} q^m \ , \text{ for } n \geq 1$$

and the slightly modified ones

$$h_{m,n} := (m+n)H_{m,n} \ .$$

From (5) it readily follows that $h_{m,n}$'s are given recursively by

$$h_{m,n} = (m+n)a_{m+n-1} + \sum_{r=1}^{m-1} \sum_{s=1}^{n-1} a_{r+s-1} h_{m-r,n-s} \ . \tag{6}$$

The result quoted below provides an alternative description for replicable functions, more convenient for numerical computations.

Theorem 3.1 *A function is replicable if and only if*

$$H_{m,n} = H_{r,s} \tag{7}$$

for all r, s, m, n positive integers satisfying

$$rs = mn \text{ and } \gcd(r,s) = \gcd(m,n). \tag{8}$$

Once one tries to check either definition or the equivalent property stated above, it readily becomes apparent that it puts strong restrictions on the function. In order to motivate this feeling, we mention the fact that a function having finite q-expansion $f = q^{-1} + \sum_{k\geq 1}^{n} a_k q^k$ is replicable exactly when $n = 1$. An even more impressive result is also due to Norton [6] :

Theorem 3.2 *Any replicable function is determined by the values of 12 of its coefficients:*

$$a_1, a_2, a_3, a_4, a_5, a_7, a_8, a_9, a_{11}, a_{17}, a_{19}, a_{23}. \tag{9}$$

3.2 The problem

In the fundamental paper [6] Norton conjectured the following statement:

Conjecture 3.3 *A function $f = q^{-1} + \sum_{n\geq 1} a_n q^n$ with integer coefficients is replicable if and only if either f is of the form $q^{-1} + aq$, or it is the Hauptmodul for a subgroup G of $PSL_2(\mathbf{R})$ of genus 0 containing a $\Gamma_0(N)$ with finite index and such that G contains a translation $z \mapsto z + k$ precisely when k is an integer.*

Admitting the truth of Conjecture (2.1), as well as the validity of Conjecture (3.3), it follows that there are only finitely many non-trivial replicable functions.

The aim of my research is to tackle the following

Question. Are there only finitely many replicable functions apart from the family $q^{-1} + aq$?

Replicable functions are important tools in the study of the so-called head representations of the Monster group. Actually, the experts of the field have put forward the statement and provided heuristic reasoning that points to a positive answer to the question.

There is additional evidence that the problem could be solved in the affirmative. Some time ago, D.Alexander, C.Cummins, J.McKay and C.Simons [1] have obtained 326 replicable functions with integer coefficients whose replicates are themselves replicable (in other words, completely replicable functions). Their approach is entirely different from ours, so their result could serve to check our solution. Recently, V.Ufnarovski [10] has announced a partial affirmative solution: there are only finitely many replicable functions modulo 2 and modulo 3.

3.3 The method

Our approach heavily relies on Norton's result (3.2). Accordingly, to settle in the affirmative the problem, it is sufficient to compute *all* solutions of a suitable system of polynomial equations in 12 indeterminates with integral coefficients. Stated this way, the problem hints to an approach using computer algebra systems.

The method consists of three major steps.

Phase 1. For t below a certain bound $Ncoef$, express a_t in terms of the 12 variables.

This is achieved by using relation (7) for integers r, s, m, n satisfying (8) and moreover

$$m + n < r + s \leq Ncoef + 1 \ . \tag{10}$$

Phase 2. Generate equations in 12 indeterminates.

More precisely, for u at most $Nnum$ one tries to decompose it as $u = rs = mn$ for r, s, m, n subject to conditions (8) and (10). Then one rewrites (7) using the expressions obtained in Phase 1.

Phase 3. Solve the system of equations previously obtained.

This step is done via a Gröbner basis computation. The lexicographic ordering is best suited for the task, since the Gröbner basis is

obtained in a triangular form. To effectively obtain the solutions, one has to factor univariate polynomials of high degree.

The above sketched algorithm has an additional advantage: in case of successful termination, it will provide us with replicable functions whose q-expansions have algebraic integers coefficients.

Actually, to answer the Question as stated above, it is sufficient to replace Phase 3 by the following step:

Phase 3′. Determine the dimension of the ideal generated by the polynomials previously obtained.

From the computational point of view, the task is now easier, since one may use a cheaper ordering instead of the lexicographic one. Moreover, there are a number of quite efficient computer algebra systems for obtaining the dimension of a polynomial ideal.

3.4 Implementation

I have written a program implementing in MATHEMATICA the algorithm sketched above.

Since the definition (6) is recursively invoked many times, the function computing $h_{r,s}$ is memorizing its value. This leads to high space requirements. The Gröbner–basis computation is also very demanding in this regard. As the modular elliptic function shows, the solutions themselves consist of large numbers, so the amount of memory needed is an inherent difficulty of the problem.

The running time is also very high. In all steps one has to manipulate very large expressions. The time needed in the worst case of a Gröbner–basis computation is doubly exponential in the number of variables. Moreover, it depends in an unpredictable way upon the ordering of the variables. Hence, it will be helpful to exercise a few of the $12! = 479001600$ permutations of 12 variables.

Due to space and time restrictions, it was not possible to obtain sufficiently many equations (*i.e.* to generate a 0–dimensional ideal). One may try to play with the value for $Nnum$ in Phase 2. The underlying idea is to obtain equations from "sporadic" pairs, hoping that they will reduce the dimension of the ideal they generate.

3.5 Results obtained so far

The cost of computations increases dramatically with the value of $Ncoef$. For no other reason than the limits of the available configuration we chose $Ncoef = 58$. The expressions giving the 46 dependent variables in terms of the independent ones occcupy 500 Kb.

As it is apparent from the example of elliptic modular function, the coefficients of a replicable function could be huge. Apart from large number of indeterminates and polynomials, this is a reason for the long time needed by the computer to manipulate expressions. Using about 20 hours on the IBM/R6000 cluster and about 150 hours running time for PC486, I have obtained 82 equations in the 12 independent variables. An amount of 1.5 Mb of memory was needed just to store these polynomials. One point should be emphasized: it is not at all clear that the equations obtained so far are sufficient in the sense that the polynomials already available form a system of generators for the ideal generated by all relations of type (7). With the present choice of $Ncoef$ there is available sufficient information to generate more equations, but due to space limitations we had to restrict ourselves to consider only 82 polynomials.

As a first attempt to simplify the computations, I have imposed the vanishing of the first 3 variables. Then I chosed 14 polynomials in the remaining 9 indeterminates, hoping that I shall obtain a 0-dimensional ideal. But the computer didn't succeed to find the Gröbner basis for the ideal (it ran out of memory).

4 Proof of Theorem (3.2)

The main idea is deceivingly simple. We record it in the next lemma for later reference.

Lemma 4.1 *If n has two distinct prime divisors, then it has two coprime divisors a and b with $1 < a < b < n$. Thus $H_{1,n} = H_{a,b}$.*

This obvious remark allows us to restrict ourselves to prime powers n. So from now on we shall assume

Standing hypothesis:
There are a prime p and a positive integer a such that $n = p^a \geq 24$.

To deal with values not covered by (4.1), one needs a refined idea. Specifically, one looks for a decomposition of $n+1$ as a sum of two integers r, s having the same product and greatest common divisor as another pair u, v whose sum is less than $n+1$. Then one can obtain a_n in terms of a_i's with $i < n$ from the relation obtained by expanding (7) according to defining relation (6). Having in view the recurrence involved in the computation of the h function, one tries to keep a summand as small as possible. Such decompositions are obtained with reasoning having a number-theoretic flavour.

As a typical case we shall examine first a simple situation:

Lemma 4.2 *If $n = 8m+5$, then $H_{2,n-1} = H_{4,(n-1)/2}$.*

Proof. Since $n-1 = 4(2m+1)$, one has $(n-1)/2 = 2(2m+1)$ and $\gcd(2, n-1) = 2 = \gcd(4, (n-1)/2)$. Clearly $n+1 = 8m+6 > 4m+6 = 4+(n-1)/2$, so one has got an admissible decomposition for $n+1$.

Next we deal with the values of n congruent to 1 modulo 8. The first case is easy:

Lemma 4.3 *If $n = 2^a m + 1$ for some $a, m > 1$ and m odd, then $H_{2,n-1} = H_{2^a,2m}$.*

Lemma 4.4 *For $n = 2^{4a} + 1$ with $a > 1$ one has $n - 2 = 3^b c$ with $b \geq 1, c > 1$ and $3 \not| c$. Therefore $H_{3,n-2} = H_{3^b,3c}$.*

Proof. Clearly 3 is a divisor of $n-2$, so one must show that $n-2$ is not a power of 3. This follows from the fact that $n-2$ has residue -1 modulo 8, while the powers of 3 give residues 1 or 3 modulo 8.

Lemma 4.5 *For any $a \geq 2$, $2^{2a+1} + 1$ is not a prime power.*

Proof. Otherwise one must have $2^{2a+1}+1=3^b$ with $b\geq 3$. Taking residues modulo 8 yields $b=2c$, so that $3^c-1=2^\alpha$ and $3^c+1=2^\beta$ for positive integers α,β with sum $2a+1$. Then it follows $2=2^\beta-2^\alpha$, which is possible only for $\beta=2,\alpha=1$. This results in $a=1$, a contradiction.

Lemma 4.6 *There is no $a\geq 1$ such that $2^{4a+2}+1$ is a prime power.*

Proof. Suppose there exists $a\geq 1$ for which the statement does not hold. Then $2^{4a+2}+1=5^b$ for an integer $b\geq 1$. As above b is even, say $b=2c$, and therefore one has $5^c-1=2^\alpha$ and $5^c+1=2^\beta$. But the last equality is impossible modulo 8.

Now we shall examine the situation n congruent to 3 modulo 8. A reasoning similar to that used to prove (4.4) gives the next statement.

Lemma 4.7 *If $n=2^am+3$ with $a\geq 3$, $m>1$ and m odd, then $H_{4,n-3}=H_{2^a,4m}$.*

Lemma 4.8 *If $n=2^{4a+2}+3$, then there are coprime odd integers $b,c>1$ such that $n-1=2bc$. Hence it follows $H_{2,n-1}=H_{2b,2c}$.*

Proof. The conclusion is equivalent with the fact that $2^{4a+1}+1$ is not a prime power. This statement has been already proved in (4.5).

Lemma 4.9 *If $n=2^{4a}+3$, then $n-4=5^bc$ for some integers $b\geq 1$, $c>1$, $5\not| c$. Therefore $H_{5,n-4}=H_{5^b,5c}$.*

Proof. Clearly 5 is a divisor of $n-4=2^{4a}-1=(2^{2a}-1)(2^{2a}+1)$. Since the numbers in the parentheses are odd with difference two, they are coprime.

Lemma 4.10 *If $n=2^{4a+3}+3$, then there are odd coprime integers $b,c>1$ such that $n-1=2bc$ and $H_{2,n-1}=H_{2b,2c}$.*

Proof. See (4.6).

Lemma 4.11 *For any $a\geq 1$, $n=2^{4a+1}+3$ is not a prime power.*

Proof. Since n is a multiple of 5 and its residue modulo 8 is 3, it cannot be equal to a power of 5.

Finally, let us consider the values of n congruent to 7 modulo 8.

Lemma 4.12 *If $n = 2^a m+7$ with $a \geq 4$ and $m > 1$ odd, then $H_{8,n-7} = H_{2^a,8m}$.*

Lemma 4.13 *There is no $a \geq 1$ such that $n = 2^{2a+1} + 7$ is a prime power.*

Proof. The only possibility $n = 3^b$ is ruled out by considering the residues modulo 8.

Lemma 4.14 *If $n = 2^{4a+2} + 7$, then $n - 1$ has at least three prime divisors.*

Proof. It follows from $n - 1 = 2(2^{4a+1} + 3)$ and (4.11).

Lemma 4.15 *If $n = 2^{4a}+7$ with $a \geq 2$, then $n-3$ has at least 3 prime divisors.*

Proof. It is a consequence of the relation $n - 3 = 4(2^{4a-2} + 1)$ and of (4.6).

Lemma 4.16 *If m is an odd multiple of 3 and $n = 8m + 7$, then $n - 1 = 2 \cdot 3^b \cdot c$ for some $b \geq 1$, $c > 1$ and $3 \not| c$. Therefore one gets $H_{2,n-1} = H_{2c,2\cdot 3^b}$.*

Proof. Let p be such that $m = 6p+3$. Then $n-1 = 6(8p+5)$ and $8p+5$ is an odd integer which cannot be a power of 3 (look modulo 8).

Lemma 4.17 *If $p \geq 1$, $m = 6p - 1$ and $n = 8m + 7$, then there exist $b \geq 1$, $c > 1$ such that $n - 2 = 3^b c$ and $3 \not| c$.*

Proof. We have $n - 2 = 3(16p - 1)$ and the expression in the parenthesis is congruent to 7 modulo 8, while the powers of 3 give residues 1 or 3 modulo 8.

Lemma 4.18 *If* $m = 6p + 1$ *,*$p \geq 1$*, then* $n = 8m + 7$ *is not a prime power.*

Proof. The statement holds because n is a multiple of 3 and its residue modulo 8 differs from the residues given by the powers of 3.

5 Conclusions

The algorithm consisting of Phase 1, Phase 2 and Phase 3 is intended to solve a problem more general than that stated in Section 3. Its aim is to obtain *all* replicable functions whose q-expansions have algebraic integer coefficients.

However, at the time of writing, even the successful termination of Phase $3'$ is out of reach for the MATHEMATICA implementation. The reasons have already been mentioned: huge coefficients, large expressions, high space requirements, very long running time.

Perhaps the Phase $3'$ or Phase 3 might be accomplished migrating from MATHEMATICA to a computer algebra system dedicated to computational commutative algebra. Quite recently COCOA 3.0, MACAULAY 2 and SINGULAR have been released, and each of these packages seems more adequate for the task of computing a Gröbner basis for a polynomial ideal.

Additionally, one needs a criterion to recognize when we have generated enough equations (*i.e.* a system of generators for the ideal generated by all relations of type (7)). The work needed to settle this point of theoretical interest is deferred to the near future.

References

[1] D.Alexander, C.Cummins, J.McKay, C.Simons, *Completely replicable functions*,in *Groups, Combinatorics and Geometry*, Durham 1991, (M.-W.Liebeck, J.Saxl, eds.), London Math.Soc.Lecture Note Ser., 165, Cambridge Univ.Press, 1992, pp.87-95

[2] R.Borcherds,*Monstrous Moonshine and monstrous Lie superalgebras*, Invent.Math., **109**(1992), pp.405-444

[3] J.H.Conway,S.P.Norton,*Monstrous Moonshine*, Bull. Lond. Math. Soc., **11**(1979), 308-339

[4] B.Fischer, D.Livingstone, M.P.Thorne,*The characters of the "Monster" simple group*, unpublished manuscript, Birmingham, 1978

[5] I.B.Frenkel,J.Lepowsky,A.Meurman,*Vertex operator algebras and the monster*, Academic Press, Boston, 1988

[6] S.P.Norton,*More on Moonshine*, in *Computational Group Theory* (M.D.Atkinson,ed.), Academic Press,1984,pp.185-193

[7] A.G.Ogg,*Automorphismes des courbes modulaires* , Séminaire Delange-Pisot-Poitou, 16^e année (1974/1975), no.7

[8] J.G.Thompson,*Uniqueness of the Fischer-Griess monster*, Bull. London Math.Soc., **11**(1979), 340-346

[9] J.G.Thompson,*A finiteness theorem for subgroups of* $PSL(2,\mathbf{R})$ *which are commensurable with* $PSL(2,\mathbb{Z})$, in *Proc.Symp.Pure Math.*, **37**, A.M.S., Providence, 1979, pp.533-555

[10] V.A.Ufnarovski, *BERGMAN for IBM PC and replicable functions*, in *COCOA IV, Genova, May 29 - June 2, 1995, Abstracts*, pp.26-27

Mihai Cipu,
Institute of Mathematics of the Romanian Academy
P.O.Box 1-764
RO-70700 Bucharest, Romania
e–mail: *mcipu@stoilow.imar.ro*

Received 13 July, 1996