Canad. J. Math. Vol. **51** (5), 1999 pp. 1020–1034

On Functions Satisfying Modular Equations for Infinitely Many Primes

Dmitry N. Kozlov

Abstract. In this paper we study properties of the functions which satisfy modular equations for infinitely many primes. The two main results are:

1) every such function is analytic in the upper half plane;
2) if such function takes the same value in two different points z_1 and z_2 then there exists an f-preserving analytic bijection between neighbourhoods of z_1 and z_2.

1 Introduction

We study the analytic properties of functions which satisfy modular equations for infinitely many primes. Such functions appear most naturally in the context of *Monstrous Moonshine*. This area arose from McKay's observation that the degree of the first non-trivial irreducible character of the Monster group (the largest sporadic group), which is 196883, differs only by 1 from the first coefficient in the power series of the j function, which in its turn plays a fundamental role in analytic number theory. The paper of J. H. Conway and S. P. Norton [6] revealed more relations, which were mostly observed empirically at the time, initiating a large body of research.

We make use of certain polynomials $F_n(x, y)$ which we call *modular polynomials*. These polynomials are symmetric in both variables and have degree $n\prod_{p|n}(1 + 1/p)$. A good overview of their theory can be found in a long paper by K. Mahler [9]. We say that the function f satisfies a modular equation of degree n (or "for n"), if $F_n\Big(f\big((az+r)/d\big), f(z)\Big) = 0$, whenever $ad = n$, $0 \leq r < d$ and $(a, r, d) = 1$ (Definition 3.2). The guiding observation is that a completely replicable function of order 1 satisfies modular equations for all n (Proposition 3.3).

The main results of this paper are:

- if a function satisfies modular equations for infinitely many primes, then it is analytic in the upper half plane;
- furthermore, if such function takes the same value in two different points z_1 and z_2, then there exists an f-preserving analytic bijection between neighbourhoods of z_1 and z_2.

These results have been used in [7].

Briefly, the plan of the paper is the following:

Section 2. We recall the setting of completely replicable functions in terms of S. P. Norton's bivarial transform;

Received by the editors August 12, 1998.
AMS subject classification: 11Mxx.

Section 3. We show that completely replicable functions of order 1 satisfy modular equations for all n;
Section 4. We prove the two main theorems mentioned above.

Acknowledgments I am deeply indebted to A. Meurman for guiding me to this project and providing his help many times along the way. I would also like to thank J. McKay and the referee for many valuable comments which led to a substantially better paper.

2 The Bivarial Transform and the Definition of Completely Replicable Functions

Let $f(z) = q^{-1} + H_1 q + H_2 q^2 + \cdots$, where $q = e^{2\pi i z}$, coefficients are arbitrary complex numbers and the power series is purely formal. This needs a few words of explanation. When one considers usual examples, this function f is analytic in the unit circle (or in the upper half plane if one prefers to use z as variable). We do not assume that here as well as we do not assume that H_i's are integers (which is also most often the case). However we do use usual notations, though purely formally. We also use without further warning the formal rational powers of q, for example the expression $f(\frac{z+1}{4})$ means $f(i \cdot q^{1/4})$ and $f(\frac{az+r}{d})$ means $f(e^{\pi i r/d} q^{a/d})$.

Following [12] we give two definitions.

Definition 2.1 Let

$$\sum_{m,n=1}^{\infty} H_{m,n} q^m r^n = \log(r^{-1} - q^{-1}) - \log\bigl(f(y) - f(z)\bigr)$$

$$= -\log\Bigl(1 - qr \sum_{i=1}^{\infty} H_i (q^{i-1} + q^{i-2} r + \cdots + r^{i-1})\Bigr),$$

where $r = e^{2\pi i y}$. We call the sequence $\{H_{m,n}\}_{m,n=1}^{\infty}$ the *bivarial transform* of $\{H_i\}_{i=1}^{\infty}$ (equivalently of f).

Clearly, $H_{1,n} = H_n$ and $H_{m,n} = H_{n,m}$. One calls a function f *replicable* if $H_{a,b} = H_{c,d}$, whenever $ab = cd$ and $(a, b) = (c, d)$.

Definition 2.2 The function f (given by formal power series as above) is called *completely replicable of order k*, if there exists a sequence of formal power series

$$\{f^{(s)} = q^{-1} + H_1^{(s)} q + H_2^{(s)} q^2 + \cdots, \text{ where } q = e^{2\pi i z}\}, \quad s = 1, 2, 3, \ldots,$$

called the replicates of f, such that

(1) $f^{(s)} = f^{((s,k))}$, $f = f^{(1)}$;
(2) if $\{H_{m,n}^{(s)}\}_{m,n=1}^{\infty}$ is obtained as a bivarial transform of $f^{(s)}$ then, for all integers m, n, $s \geq 1$,

$$H_{m,n}^{(s)} = \sum_{t|(m,n)} \frac{1}{t} H_{mn/t^2}^{(st)}.$$

In particular, one can see that if f is completely replicable of order k, then for any s, $f^{(s)}$ is completely replicable of order $k/(s,k)$. Namely, one can simply define $f^{(s)(t)} = f^{(st)}$ and verify all the properties of this sequence of formal series. Also any completely replicable function is of course replicable (as easiest it can be deduced from (2) with $s = 1$), but not vice versa, take for example $-j(z+1/2)$.

Influenced by experimental observations on Monster group characters, J. H. Conway and S. P. Norton defined in [6] abstract replicability with the help of collection of functional equations. The following polynomial plays an important role in their approach.

Definition 2.3 Let $P_n(x, y_1, \dots, y_{n-1})$ be the polynomial in n variables uniquely determined by the property that, for any formal power series $f(q) = q^{-1} + H_1 q + H_2 q^2 + \cdots$, the formal power series $P_n\big(f(q), H_1, H_2, \dots, H_{n-1}\big) - q^{-n}$ contains only positive powers of q. For example $P_3(x, y_1, y_2) = x^3 - 3y_1 x - 3y_2$.

We recall here how these two definitions are related.

Lemma 2.4 *For all positive integers n,*

$$n \cdot \sum_{m=1}^{\infty} H_{m,n} q^m + q^{-n} = P_n\big(f(q), H_1, \dots, H_{n-1}\big).$$

Proof It is enough to show that the left hand side is a polynomial in $f(q)$ and $H_1, \dots, H_{n-1}$. As a matter of fact it is n times the coefficient of r^n in the following expression:

$$\begin{aligned} &-\log(1 - r/q) + \log(1/r - 1/q) - \log\big(f(r) - f(q)\big) \\ &\quad = -\log(r) - \log\big(f(r) - f(q)\big) \\ &\quad = -\log\Big(1 - \Big(f(q) - \sum_{i=1}^{\infty} H_i r^{i+1}\Big)\Big), \end{aligned}$$

which is obviously a polynomial in $f(q)$ and $H_1, \dots, H_{n-1}$ as power series expansion of the logarithm function shows. ■

To make our formulae more concise we need the following notations:

$$\mathcal{A}_n = \{(a, r, d) \mid ad = n, 0 \le r < d\},$$
$$\mathcal{B}_n = \{(a, r, d) \mid ad = n, 0 \le r < d, (a, r, d) = 1\}.$$

Proposition 2.5 *The following are equivalent:*

(a) *f is completely replicable of order k, with replicates $f^{(s)}$;*
(b) *The sequence $(f^{(s)})_{s=1}^{\infty}$ satisfies*
  (1) $f^{(s)} = f^{((s,k))}$, $f = f^{(1)}$;
  (2) *for all $s \ge 1$, $n \ge 2$,*

https://doi.org/10.4153/CJM-1999-045-x Published online by Cambridge University Press

$$\sum_{(a,r,d)\in\mathcal{A}_n} f^{(sa)}\Big(\frac{az+r}{d}\Big) = P_n\big(f^{(s)}(q), H_1^{(s)}, \dots, H_{n-1}^{(s)}\big). \tag{2.1}$$

The formulae (2.1) are usually called the *replication formulae*.

Proof $(a) \Rightarrow (b)$.

(1) Obvious.
(2) We have

$$\begin{aligned}\sum_{(a,r,d)\in\mathcal{A}_n} f^{(sa)}\Big(\frac{az+r}{d}\Big) &= \sum_{d|n}\sum_{0\le r<d} f^{(sn/d)}\Big(\frac{nz/d+r}{d}\Big)\\ &= q^{-n} + \sum_{d|n} d\cdot(H_d^{(sn/d)}q^{n/d} + H_{2d}^{(sn/d)}q^{2n/d}+\cdots)\\ &= q^{-n} + \sum_{d|n}\frac{n}{d}(H_{n/d}^{(sd)}q^d + H_{2n/d}^{(sd)}q^{2d}+\cdots)\\ &= \sum_{k=1}^{\infty} c_k q^k + q^{-n},\end{aligned}$$

where $c_k = n\cdot\sum_{d|(k,n)}\frac{1}{d}H^{(sd)}_{kn/d^2} = nH^{(s)}_{k,n}$. Using Lemma 2.4 we get

$$\sum_{(a,r,d)\in\mathcal{A}_n} f^{(sa)}\Big(\frac{az+r}{d}\Big) = n\cdot\sum_{m=1}^{\infty} H^{(s)}_{m,n}q^m + q^{-n} = P_n\big(f^{(s)}(q), H_1^{(s)}, \dots, H_{n-1}^{(s)}\big).$$

$(b) \Rightarrow (a)$. Similar to the above. ∎

3 Completely Replicable Functions of Order 1

In this section we prove that completely replicable functions of order 1 satisfy modular equations for all n.

We need the following notations

$$T_n^m(f)(z) = \sum_{(a,r,d)\in\mathcal{A}_n} f^m\Big(\frac{az+r}{d}\Big), \quad \tilde{T}_n^m(f)(z) = \sum_{(a,r,d)\in\mathcal{B}_n} f^m\Big(\frac{az+r}{d}\Big).$$

The following fact is immediate.

Lemma 3.1 $T_n^m(f)(z) = \sum_{\alpha^2|n}\tilde{T}^m_{n/\alpha^2}(f)(z)$. ∎

https://doi.org/10.4153/CJM-1999-045-x Published online by Cambridge University Press

Reformulating the Proposition 2.5, f is a completely replicable function of order 1 if and only if it satisfies the following infinite system of functional equations:

$$T_2^1(f)(z) = f(2z) + f\Big(\frac{z}{2}\Big) + f\Big(\frac{z+1}{2}\Big) = f^2(z) - 2H_1,$$

$$T_3^1(f)(z) = f(3z) + f\Big(\frac{z}{3}\Big) + f\Big(\frac{z+1}{3}\Big) + f\Big(\frac{z+2}{3}\Big) = f^3(z) - 3H_1 f(z) - 3H_2,$$

$$T_4^1(f)(z) = f(4z) + f\Big(\frac{2z}{2}\Big) + f\Big(\frac{2z+1}{2}\Big) + f\Big(\frac{z}{4}\Big) + f\Big(\frac{z+1}{4}\Big) + f\Big(\frac{z+2}{4}\Big) + f\Big(\frac{z+3}{4}\Big)$$
$$= f^4(z) - 4H_1 f(z)^2 - 4H_2 f(z) - 4H_3 + 2H_1^2, \ldots$$

where $f(z) = q^{-1} + H_1 q + H_2 q^2 + \cdots$, $q = e^{2\pi i z}$.

Definition 3.2 We say that a function f satisfies n-th *modular equation*, $n \geq 2$, if there exists a polynomial $F_n(x, y)$ such that

$$F_n\big(x, f(z)\big) = \prod_{(a,r,d)\in B_n} \Big(x - f\Big(\frac{az+r}{d}\Big)\Big).$$

Clearly, the term of the highest degree in x in $F_n(x, y)$ is $x^{|B_n|}$, where $|B_n| = n\prod_{p|n}(1+1/p)$, p is a prime.

Proposition 3.3 *Let f be a completely replicable function of order 1, then f satisfies modular equations for all $n \geq 2$.*

Example $F_2(x, y) = x^3 + y^3 - x^2y^2 + 2H_1(x^2 + y^2) + (2H_2 - 1)xy + (2H_4 - 2H_1)x + (2H_3 + H_1^2 - 3H_1)y + 2H_5 + 2H_1H_3 - H_2^2 - 3H_2 - 4H_1^2$ [9, p. 90].

Proof To prove the existence of the polynomial above, it is clearly enough to prove that any symmetric polynomial in $f\big((az + r)/d\big)$, $(a, r, d) \in B_n$ is a polynomial in $f(z)$. On the other hand, the power sums $\tilde{T}_n^m(f)(z)$ generate the ring of symmetric polynomials, hence it is enough to prove that for any m and n, $\tilde{T}_n^m(f)(z)$ is a polynomial in $f(z)$. Furthermore, by Lemma 3.1, it is enough to show that for any m and n, $T_n^m(f)(z)$ is a polynomial in $f(z)$.

We proceed by induction on m. For $m = 1$ the statement is the consequence of Proposition 2.5, so assume $m \geq 2$. Let us now take the m-th functional equation for $f(z)$, replace z in it with $(az + r)/d$, for $(a, r, d) \in A_n$, and sum up all these equations. On the right hand side we get $T_n^m(f) + R$, where R is a sum consisting of terms of the form $T_n^{m'}(f)\cdot$ (some constant depending on $H_1, H_2, \ldots$), for $m' < m$. So, by the assumption of induction, R is a polynomial in f. Hence, what we have to prove reduces to showing that the following expression is a polynomial in $f(z)$:

$$\sum f\left(\frac{a_1\big((a_2z + r_2)/d_2\big) + r_1}{d_1}\right) = \sum f\left(\frac{a_1a_2z + a_1r_2 + d_2r_1}{d_1d_2}\right), \tag{3.1}$$

where both sums are taken over all $(a_1, r_1, d_1) \in \mathcal{A}_m$, $(a_2, r_2, d_2) \in \mathcal{A}_n$.

Denote the right hand side of (3.1) by S_{d_1,d_2}. Now fix d_1 and d_2 for a while. Take $t = (a_1, d_2)$, and let $a_1' = a_1/t$, $d_2' = d_2/t$. Then, canceling t gives

$$S_{d_1,d_2} = \sum f\left(\frac{a_1'a_2z + a_1'r_2 + d_2'r_1}{d_1d_2'}\right),$$

the sum is taken over all $0 \le r_1 < d_1$, $0 \le r_2 < d_2$.

Let us show the equality

$$S_{d_1,d_2} = t \cdot \sum_{0 \le r < d_1d_2'} f\left(\frac{a_1'a_2z + r}{d_1d_2'}\right).$$

For that we have to prove that for all $0 \le r < d_1d_2'$ the equation

$$a_1'r_2 + d_2'r_1 \equiv r \pmod{d_1d_2'}$$

has exactly t solutions (r_1, r_2), $0 \le r_1 < d_1$, $0 \le r_1 < d_2'$. As we totally have exactly $t \cdot d_1 \cdot d_2'$ pairs (r_1, r_2), it is enough to prove that for each fixed pair (r_1, r_2) there are exactly t solutions (r_1', r_2') to

$$a_1'r_2 + d_2'r_1 \equiv a_1'r_2' + d_2'r_1' \pmod{d_1d_2'}.$$

If the above congruence is satisfied we get

$$d_1d_2' \mid a_1'(r_2 - r_2') + d_2'(r_1 - r_1'), \tag{3.2}$$

hence $d_2' \mid a_1'(r_2 - r_2')$, but $(a_1', d_2') = 1$, so $d_2' \mid r_2 - r_2'$. Write $r_2' = r_2 - s \cdot d_2'$. Canceling d_2' in (3.2) we get $d_1 \mid a_1's + r_1 - r_1'$, so each choice of s gives uniquely defined r_1'. Since s can be chosen in exactly t different ways we prove our statement. Observe that $d_1d_2'a_1'a_2 = mn/t^2$.

So S_{d_1,d_2} is equal to t times the part of Hecke operator T_{mn/t^2}, corresponding to the chosen divisor $d = d_1d_2/t$. We know that the whole operator $T_{mn/t^2}(f)$ is a polynomial in f, hence we only need to prove that for each t dividing (m, n), all the parts of the Hecke operator T_{mn/t^2} appears exactly t times in the sum (3.1). Let us fix t and d the divisor of mn/t^2. When does the corresponding part of Hecke operator appear in the sum (3.1)? The necessary and sufficient conditions for d_1 and d_2 are:

(1) $d_1 \mid m,\ d_2 \mid n$;
(2) $d_1 \cdot d_2 = d \cdot t$;
(3) $t = (\frac{m}{d_1}, d_2)$.

Obviously (2) and (3) define d_1 and d_2 uniquely, namely

$$t = \left(\frac{m}{d_1}, \frac{dt}{d_1}\right) \Rightarrow d_1t = (m, dt) \Rightarrow d_1 = \left(\frac{m}{t}, d\right).$$

Take $d_2 = \frac{dt}{d_1}$. It is well defined since $d_1 \mid d$. Now it is easy to check the conditions: (2) is obvious, and

$$\left(\frac{m}{d_1}, d_2\right) = \left(\frac{m}{d_1}, \frac{dt}{d_1}\right) = \frac{(m, dt)}{(m/t, d)} = t$$

gives (3). Finally,

$$d_2 \mid n \Longleftrightarrow \frac{dt}{d_1} \mid n \Longleftrightarrow dt \mid d_1 n \Longleftrightarrow dt \mid \left(\frac{m}{t}, d\right) n \Longleftrightarrow dt \mid \left(\frac{mn}{t}, dn\right)$$

and the last statement is true as dt divides both mn/t and dn.

So we have proved that the expression in (3.1) is equal to

$$\sum_{t \mid (m,n)} t \cdot T_{mn/t^2}(f). \qquad \blacksquare$$

If a function satisfies a modular equation for some prime p, then, in the terminology used by Mahler in [9, pp. 69, 80], one can say that a completely replicable function of order 1 is a *basic S_p series*. In that case, by the Theorem 8 [9, 37, p. 107], f is a single-valued analytic function in a neighbourhood of ∞, with a simple pole of residue 1 at ∞.

Furthermore, we can show that the polynomials in the modular equations are symmetric.

Proposition 3.4 *Let f be a completely replicable function of order 1 and let F_n be the polynomials from the Proposition 3.3. Then F_n is symmetric in x and y, i.e., $F_n(x, y) = F_n(y, x)$.*

Remark As it was observed by K. Mahler, this property of the polynomials $F_n(x, y)$ yields many identities on the numbers $H_1, H_2, \ldots$, for example, for $n = 2$, we see from the example after Proposition 3.3 that $2H_4 = 2H_3 + H_1^2 - H_1$.

Proof Let n be a fixed number and pick $(a, r, d) \in \mathcal{B}_n$. Let us prove that $F_n\Big(f(z), f\big((az+r)/d\big)\Big) = 0$. Set $r' = a - r$. Then, by what we have proved before, $f\big((dz'+r')/a\big)$ is a root of $F_n\big(x, f(z')\big)$, that is $F_n\Big(f\big((dz'+r')/a\big), f(z')\Big) = 0$. Substitute $(az+r)/d$ instead of z', then

$$(dz' + r')/a = (az + r + r')/a = z + 1,$$

hence we get

$$F_n\Big(f\big((dz'+r')/a\big), f(z')\Big) = F_n\Big(f(z), f\big((az+r)/d\big)\Big).$$

This proves that $F_n\big(f(z), y\big)$ also has roots $f\big((az+r)/d\big)$, for $(a, r, d) \in B_n$. Since $f(z)$ has a simple pole at ∞ we conclude that the image of f contains an open neighbourhood of a point in $\mathbb{C}$ and that there exists t (depending on n), such that for all z, such that $\operatorname{Im} z > t$, all values $f\big((az+r)/d\big)$, for $(a, r, d) \in B_n$, are distinct. For z, such that $\operatorname{Im} z > t$, define

$Q_z(x) = F_n\big(f(z), x\big) - F_n\big(x, f(z)\big)$. Clearly $Q_z(x)$ has $|B_n|$ distinct roots. To complete the proof it is enough to show that the term of the highest degree in y in $F_n(x, y)$ is $y^{|B_n|}$. Since then $\deg Q_z(x) < |B_n|$, hence $Q_z(x) \equiv 0$ for all z, such that $\operatorname{Im} z > t$, which by the previous comments implies the polynomial identity $F_n(x, y) = F_n(y, x)$.

We have

$$F_n\big(x, f(z)\big) = \prod_{(a,r,d)\in B_n} \left(x - f\left(\frac{az + r}{d}\right)\right) = x^{|B_n|} + s_1 x^{|B_n|-1} + \cdots + (-1)^{|B_n|} s_{|B_n|},$$

where $s_1, \ldots, s_{|B_n|}$ are corresponding symmetric functions of $f\big((az + r)/d\big)$, for $(a, r, d) \in B_n$. Clearly, $s_{|B_n|} = (-1)^{2\epsilon} q^{-\alpha} + q^{-\alpha+1}\Gamma(q)$, where $\Gamma(q)$ is a formal power series with only positive powers of q, $\alpha = \sum_{(a,r,d)\in B_n} a/d$ and $\epsilon = \sum_{(a,r,d)\in B_n} r/d$. Since we know that $s_{|B_n|}$ is a polynomial in $f(z) = q^{-1} + H_1 q + \cdots$, we have $s_{|B_n|} = (-1)^{2\epsilon} f(z)^{\alpha} + R\big(f(z)\big)$, where $\deg R < \alpha$.

Next we see that

$$\alpha = \sum_{(a,r,d)\in B_n} \frac{a}{d} = \sum_{ad=n} \frac{a}{d} \frac{d}{(a, d)} \phi\big((a, d)\big) = \sum_{a|n} \frac{a}{(a, d)} \phi\big((a, d)\big) = \sum_{(d,r,a)\in B_n} 1 = |B_n|,$$

where $\phi(\sigma)$ is the number of all integers $0 < \gamma < \sigma$, such that $(\sigma, \gamma) = 1$.

Finally, observe that if $0 < r < d$, then $(a, r, d) \in B_n$ iff $(a, d - r, d) \in B_n$, hence $(-1)^{2\epsilon} = (-1)^{\tilde{\epsilon}}$, where $\tilde{\epsilon}$ is the number of all even d, such that $d \mid n$ and $(n/d, d/2) = 1$. It is easy to see that $\tilde{\epsilon} = 1$ for $n = 2$ and is even for $n > 2$. It follows that $(-1)^{|B_n|}(-1)^{2\epsilon} = 1$, for $n \geq 2$.

Thus the highest monic term in y of $F_n(x, y)$ is $y^{|B_n|}$, on the other hand, it is clear from our argument that for $j < |B_n|$, s_j has degree (as a polynomial in $f(z)$) lower than $|B_n|$. This proves that the term of the highest degree in y in $F_n(x, y)$ is $y^{|B_n|}$. ■

4 The Analytic Properties

As it was mentioned before, K. Mahler has proved that any function that satisfies a modular equation for some prime number is analytic in some neighbourhood of ∞ and has a simple pole at ∞. In the next theorem, which is one of the two main results of this paper, we strengthen Mahler's result for the case when the function satisfies modular equations for infinitely many prime numbers.

Theorem 4.1 *Let I be an infinite subset of the set of prime numbers. Assume that f satisfies modular equations for all $p \in I$, then f is analytic in the upper half plane, i.e., whenever* $\operatorname{Im} z > 0$.

Proof Let t_0 denote the smallest real number, such that $f(z)$ is analytic in $\operatorname{Im} z > t_0$. Assume that $t_0 > 0$. Let t_1 be some real number larger then t_0, such that $f(z)$ is injective in $\operatorname{Im} z > t_1$ (or more exactly $f(z)$ is injective in the corresponding part of the strip of width 1, remember that we have assumed that $f(z)$ is periodic with period 1). That such t_1 exists follows from the fact that $f(z)$ has a simple pole at ∞.

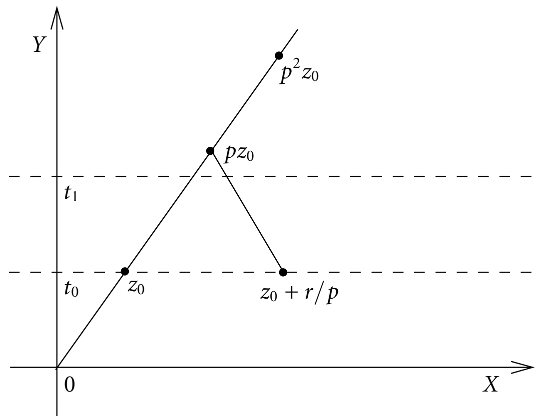

Figure 1

Since $f(z)$ is periodic with period 1, there must exist a singular point z_0 such that $\operatorname{Im} z_0 = t_0$. As otherwise for each z, such that $\operatorname{Im} z = t_0$, we would have an open neighbourhood where $f(z)$ is analytic. Because the interval $[0, 1]$ is a compact set we could then choose finitely many such neighbourhoods, which would cover the segment $[t_0 \cdot i, (1+t_0 \cdot i)]$ and hence we would get a contradiction to the minimality of t_0.

Pick a prime number $p \in I$, larger than t_1/t_0. Differentiating the equation $F_p\big(f(pz), f(p^2z)\big) = 0$ with respect to z gives

$$\begin{aligned} \frac{d}{dz} F_p\big(f(pz), f(p^2z)\big) = \frac{\partial F_p}{\partial x}&\big(f(pz), f(p^2z)\big) p f'(pz) \\ &+ \frac{\partial F_p}{\partial y}\big(f(pz), f(p^2z)\big) p^2 f'(p^2z) = 0. \end{aligned} \tag{4.1}$$

Because of the choice of p both pz_0 and p^2z_0 lie in the domain where $f(z)$ is injective, hence $f'(pz_0) \neq 0$, $f'(p^2z_0) \neq 0$.

On the other hand, if $f(z_0)$ would be a simple root of $F_p\big(f(pz_0), y\big)$, then the fact that f is analytic and injective in an open neighbourhood of pz_0 and the implicit function theorem would imply that f is analytic in an open neighbourhood of z_0, which would contradict with the singularity of f at z_0. Hence $f(z_0)$ is at least a double root of $F_p\big(f(pz_0), y\big)$.

Assume $f(z_0) = f(p^2z_0)$, then $\frac{\partial F_p}{\partial y}\big(f(pz_0), f(p^2z_0)\big) = 0$. Using the equality (4.1) we get $\frac{\partial F_p}{\partial x}\big(f(pz_0), f(p^2z_0)\big) = 0$. The polynomial F_p is symmetric according to the Proposition 3.4, hence $F_p\big(f(pz_0), f(p^2z_0)\big) = F_p\big(f(p^2z_0), f(pz_0)\big)$, which in turn implies that $f(pz_0)$ is at least a double root of $F_p\big(f(p^2z_0), x\big)$. This means that either $f(pz_0) = f(p^3z_0)$ or $f(pz_0) = f(pz_0 + r/p)$, for some $0 \leq r < p$. In both cases we get a contradiction to the injectivity of f in $\operatorname{Im} z > t_1$, since pz_0 lies above $\operatorname{Im} z = t_1$.

The only case left is when $f(z_0) = f(z_0 + r/p)$, for some $0 \leq r < p$. We have proved this for infinitely many primes $p > t_1/t_0$, so by taking larger and larger prime numbers we

https://doi.org/10.4153/CJM-1999-045-x Published online by Cambridge University Press

get a sequence $(z_i)_{i=1}^{\infty}$ of different points, such that for all i,

$$\operatorname{Im} z_i = t_0, \quad f(z_i) = c,$$

where c is some constant.

Let us again fix some prime number $p > t_1/t_0$, $p \in I$. By the symmetry of F_p the values of f at points $(pz_i)_{i=1}^{\infty}$ must be roots of $F_p(c, x)$. Since there are infinitely many points and only finitely many roots this contradicts to the injectivity of f in $\operatorname{Im} z > t_1$. ■

Note Observe that using $f(z)$ for $\operatorname{Im} z = t_0$ is strictly speaking not allowed, as $f(z)$ may not exist there. What one should do to be absolutely correct is to work with the approximations from above instead. For fixed z we can choose a sequence $(pz + ipe_k)_{k=1}^{\infty}$, where e_k is a positive real number going to 0. Such that some root of $F_p\big(f(pz), y\big)$ can be approximated by $f(z + ie_k)$ (which in its turn are roots of $F_p\big(f(pz + ipe_k), y\big)$). Then we set $f(z)$ to be this root. This setting is not unique, but sufficient for our purposes. The whole argument in the proof goes through, the technicalities are left to the reader.

With the proof of this theorem we justified our notations, so in the rest of the paper, all the formal equalities actually mean the identities for the analytic functions.

Our next goal is to show that if the function f takes the same value at two different points, then there exists an analytic bijection, which maps an open neighbourhood of the first point onto an open neighbourhood of the second point and preserves f.

Lemma 4.2 *Let f and I be as in Theorem 4.1. Assume that there exist two points z_1 and z_2 such that $f(z_1) = f(z_2)$ and $f'(z_1) = 0$, then also $f'(z_2) = 0$.*

Proof Assume $f'(z_2) \neq 0$. Take t such that $f(z)$ is injective in $\operatorname{Im} z > t$. Take $p \in I$, $(a, r, d) \in \mathcal{B}_p$. By differentiating $F_p\Big(f(z), f\big((az + r)/d\big)\Big) = 0$ we obtain

$$\frac{\partial F_p}{\partial x}\left(f(z), f\left(\frac{az+r}{d}\right)\right) f'(z) + \frac{\partial F_p}{\partial y}\left(f(z), f\left(\frac{az+r}{d}\right)\right)\frac{p}{d^2} f'\left(\frac{az+r}{d}\right) = 0. \tag{4.2}$$

This equality shows in particular that if $f'(z) = 0$ then either $f'\big((az + r)/d\big) = 0$ or $f\big((az + r)/d\big)$ is at least a double root of $F_p\big(f(z), y\big)$.

Let us prove that there exists a prime number $p \in I$, such that

- $f(pz_2)$ is a simple root to $F_p\big(f(z_2), y\big)$;
- $\operatorname{Im} pz_2 > qt$, where $q = \min I$.

Assume the contrary, then, for any large $p \in I$, $f(pz_2)$ is at least a double root of the polynomial mentioned above, hence $\frac{\partial F_p}{\partial y}\big(f(z_2), f(pz_2)\big) = 0$. From (4.2) and the assumption $f'(z_2) \neq 0$ we conclude that $\frac{\partial F_p}{\partial x}\big(f(z_2), f(pz_2)\big) = 0$. Using the symmetry of F_p we conclude that $f(z_2)$ is at least a double root to $F_p\big(f(pz_2), y\big)$. But $f(z_2) \neq f(p^2 z_2)$ as otherwise $F_p\big(f(z_2), y\big) = F_p\big(f(p^2 z_2), y\big)$ and hence $f(pz_2)$ would be at least a double root to $F_p\big(f(p^2 z_2), y\big)$. This would yield a contradiction since $F_p\big(f(p^2 z_2), y\big)$ has all its roots in a domain, where $f(z)$ is injective. So the equality $f(z_2) = f(z_2 + r/p)$, for some $0 < r < p$,

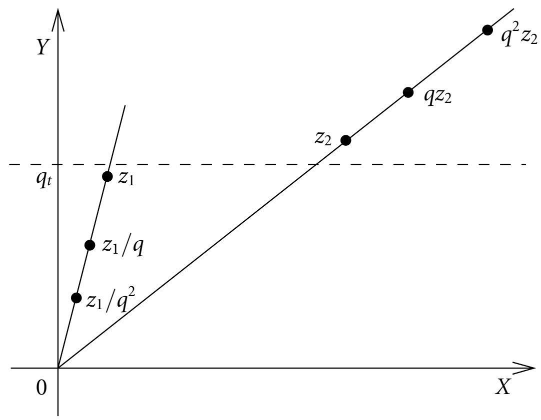

Figure 2

must take place. Taking larger and larger primes $p \in I$ we obtain a sequence of different points on $\operatorname{Im} z = \operatorname{Im} z_2$, where f takes the same value. We know that f is analytic in the upper half plane and hence we get $f \equiv f(z_2)$, a contradiction.

Take a prime number $p \in I$, such that $f(pz_2)$ is a simple root to the polynomial $F_p\big(f(z_2), y\big)$ and $\operatorname{Im} pz_2 > qt$. Observe that $F_p\big(f(z_1), y\big)$ and $F_p\big(f(z_2), y\big)$ is one and the same polynomial, hence $f(pz_2)$ is equal to the value of f at one of the following points: $pz_1, z_1/p, (z_1+1)/p, \ldots, (z_1+p-1)/p$. Denote this point by z_3. As $f(z_3) = f(pz_2)$ we obtain that $f(z_3)$ must be a simple root of $F_p\big(f(z_1), y\big)$, hence using (4.2) we can conclude that $f'(z_3) = 0$. On the other hand, $f'(pz_2) \neq 0$, as pz_2 lies in the domain where f is injective. Let us rename z_3 to z_1 and pz_2 to z_2, then all the conditions of the original assumption are satisfied and we have an extra condition that $\operatorname{Im} z_2 > qt$.

Consider the sequence $z_2, qz_2, q^2 z_2, \ldots$. As $F_q\big(f(z_1), y\big) = F_q\big(f(z_2), y\big)$ we have two possibilities:

(1) $f(qz_2) = f(qz_1)$,
(2) $f(qz_2) = f\big((z_1 + r)/q\big), \quad 0 \le r < q.$

Assume that the first equality is true. Observe that $F_q\big(f(z_2), y\big)$ has only simple roots, as $\operatorname{Im} z_2 > qt$, hence also $f(qz_1)$ is a simple root of $F_q\big(f(z_1), y\big)$ and, using (4.2) again, we conclude that $f'(qz_1) = 0$. This allows us to rename qz_1 and qz_2 to z_1, resp. z_2 in exactly the same manner as before. On the other hand this process must obviously terminate after at most k steps, where k is such that $q^k \operatorname{Im} z_1 > t$, as after each step we get $f'(z_1) = 0$, which is impossible if f is injective in some open neighbourhood of z_1.

The argument above and the fact that we can always add an integer to z_1 allows us to assume that $f(qz_2) = f(z_1/q)$. Since f' is not identically zero, there are only finitely many points in the set S of all $1/q \le \alpha \le 1$, for which there exists z such that $f'(z) = 0$ and $\operatorname{Im} z = \operatorname{Im} \alpha z_1$. Let k be a positive integer. Consider the pair of points z_1/q and qz_2, by (4.2) we know that $f'(z_1/q) = 0$. Also $f'(qz_2) \neq 0$ and $f(z_1/q) = f(qz_2)$ hence all the original conditions are satisfied for the pair $(z_1/q, qz_2)$. This means that one of the two equalities above (with z_1/q instead of z_1 and qz_2 instead of z_2) is true. If it is the first one, then $f(q^2z_2) = f(z_1) = f(z_2)$, which is impossible. Adding some multiple of q to z_1 if necessary we obtain $f(z_1/q^2) = f(q^2z_2)$. Repeating the above argument we get

$$\begin{gathered} f(z_1) = f(z_2), \\ f(z_1/q) = f(qz_2), \\ \vdots \\ f(z_1/q^k) = f(q^kz_2), \end{gathered}$$

and $f'(z_1) = f'(z_1/q) = \cdots = f'(z_1/q^k) = 0$.

Finally note that for any $q^{k-1} \le p \le q^k$, $p \in I$, the polynomial $F_p\big(f(q^kz_2), y\big)$ has only simple roots, as all of them lie in the domain where f is injective. Further, as $F_p\big(f(q^kz_2), y\big) = F_p\big(f(z_1/q^k), y\big)$ and $f'(z_1/q^k) = 0$, we obtain from (4.2) that $f'(pz_1/q^k) = 0$. On the other hand $1/q \le p/q^k \le 1$, so $p/q^k \in S$ (note that only the real part of z_1 is ever changed, so S is well-defined and independent of p). Since I is infinite and numbers p/q^k are different for different $p \in I$ we get a contradiction. ■

Lemma 4.3 *Let $F(x, y)$ be a polynomial in two variables, and $f(z)$, $g(z)$ be analytic (say in the upper half plane) functions of z. Then, for all k,*

$$\begin{aligned} \frac{d^k}{dz^k}F\big(f(z), g(z)\big) &= \frac{\partial F}{\partial x}(f, g) f^{(k)}(z) + \frac{\partial^k F}{\partial y^k}(f, g)\big(g'(z)\big)^k \\ &\quad + \sum_{m=1}^{k-1} \frac{\partial^m F}{\partial y^m}(f, g) A_{m,k} + \sum_{m=1}^{k-1} f^{(m)}(z) B_{m,k}, \end{aligned} \tag{4.3}$$

where $A_{m,k}$ is a polynomial in $g', g'', \dots, g^{(k)}$, and $B_{m,k}$ is a polynomial, in the derivatives of f and g and partial derivatives of F.

Proof We prove (4.3) by induction. For $k = 1$ (4.3) is just the usual chain rule for derivative of the function with two parameters:

$$\frac{dF}{dz} = \frac{\partial F}{\partial x} f' + \frac{\partial F}{\partial y} g'.$$

To carry out the induction step, assume (4.3) is true for $k-1$ and differentiate with respect to z each:

$$\begin{aligned}
&\frac{d}{dz}\left(\frac{\partial F}{\partial x}f^{(k-1)}+\frac{\partial^{k-1}F}{\partial y^{k-1}}(g')^{k-1}+\sum_{m=1}^{k-2}\frac{\partial^m F}{\partial y^m}A_{m,k-1}+\sum_{m=1}^{k-2}f^{(m)}B_{m,k-1}\right)\\
&\quad=\frac{\partial F}{\partial x}f^{(k)}+f^{(k-1)}\left(\frac{\partial^2 F}{\partial x^2}f'+\frac{\partial^2 F}{\partial x\partial y}g'\right)+\frac{\partial^{k-1}F}{\partial y^{k-1}}(k-1)g''(g')^{k-2}\\
&\qquad+\frac{\partial^k F}{\partial x\partial y^{k-1}}f'(g')^{k-1}+\frac{\partial^k F}{\partial y^k}(g')^k+\sum_{m=1}^{k-2}\frac{\partial^m F}{\partial y^m}\frac{d}{dz}A_{m,k-1}+\sum_{m=1}^{k-2}\frac{\partial^{m+1}F}{\partial y^{m+1}}g'A_{m,k-1}\\
&\qquad+\sum_{m=1}^{k-2}\frac{\partial^{m+1}F}{\partial x\partial y^m}f'A_{m,k-1}+\sum_{m=1}^{k-2}f^{(m+1)}B_{m,k-1}+\sum_{m=1}^{k-2}f^{(m)}\frac{d}{dz}B_{m,k-1}\\
&\quad=\frac{\partial F}{\partial x}f^{(k)}+\frac{\partial^k F}{\partial y^k}(g')^k+\sum_{m=1}^{k-1}\frac{\partial^m F}{\partial y^m}A_{m,k}+\sum_{m=1}^{k-1}f^{(m)}B_{m,k}. \qquad\blacksquare
\end{aligned}$$

Lemma 4.4 *Let f be as in Theorem 4.1. Assume that for two points z_1 and z_2 the following is true:*

(1) $f(z_1)=f(z_2)$
(2) $f'(z_1)=f''(z_1)=\cdots=f^{(k)}(z_1)=0$
(3) $f'(z_2)=f''(z_2)=\cdots=f^{(k-1)}(z_2)=0.$

Then $f^{(k)}(z_2)=0$.

Proof Assume $f^{(k)}(z_2)\neq 0$. The proof is similar to the one of Lemma 4.2. The only difference is that we use (4.3) instead of (4.2).

We start by proving that there exists a prime number $p\in I$ such that $f(pz_2)$ is a root of $F_p\big(f(z_2),y\big)$ of multiplicity at most k and $f'(pz_2)\neq 0$. Assume that such p does not exist. Then for all large primes $p\in I$ we have that $f(pz_2)$ is a root of $F_p\big(f(z_2),y\big)$ of multiplicity at least $k+1$. Then (4.3) gives $\frac{\partial F_p}{\partial x}\big(f(z_2),f(pz_2)\big)f^{(k)}(z_2)=0$. We assumed that $f^{(k)}(z_2)\neq 0$, so it follows that $\frac{\partial F_p}{\partial x}\big(f(z_2),f(pz_2)\big)=0$, and, because $F_p(x,y)$ is symmetric, $f(z_2)$ must be at least a double root of $F_p\big(f(pz_2),y\big)$. The same argument as in the proof of Lemma 4.2 shows that there exists $0<r<p$, such that $f(z_2)=f(z_2+r/p)$. Taking larger and larger primes $p\in I$ we obtain a contradiction.

Let us take a prime number $p\in I$ as above, that is $f(pz_2)$ is a root of $F_p\big(f(z_2),y\big)$ of multiplicity at most k and $f'(pz_2)\neq 0$ (for the last condition to be fulfilled, one has to take p large enough). Just in the same way as in the proof of Lemma 4.2 there exists $z_3\in\{pz_1,z_1/p,\dots,(z_1+p-1)/p\}$ such that $f(z_3)=f(pz_2)$. If $f'(z_3)=0$, then $f'(pz_2)\neq 0$ gives a contradiction with Lemma 4.2, so we can assume $f'(z_3)\neq 0$.

Let $l(z)$ be the linear function, which reflects how z_3 is obtained from z_1 (for example if $z_3=(z_1+4)/p$, then $l(z)=(z+4)/p$). Consider (4.3), when $F=F_p$, $g(z)=f\big(l(z)\big)$ and

https://doi.org/10.4153/CJM-1999-045-x Published online by Cambridge University Press

$f(z)$ is just our function. For $k = 1$ one gets

$$\frac{\partial F_p}{\partial y}\big(f(z_1), g(z_1)\big)g'(z_1) = 0,$$

but $g'(z_1) = (\text{non-zero const}) \cdot f'(z_1) \neq 0$, hence $\frac{\partial F_p}{\partial y}\big(f(z_1), f(z_3)\big) = 0$. For $k = 2$ (4.3) yields

$$\frac{\partial^2 F_p}{\partial y^2}\big(f(z_1), g(z_1)\big)\big(g'(z_1)\big)^2 + \frac{\partial F_p}{\partial y}\big(f(z_1), g(z_1)\big)A_1 = 0,$$

which allows us to conclude that $\frac{\partial^2 F}{\partial y^2}\big(f(z_1), g(z_1)\big) = 0$. Proceeding in the same manner we obtain

$$\frac{\partial F_p}{\partial y}\big(f(z_1), f(z_3)\big) = \frac{\partial^2 F}{\partial y^2}\big(f(z_1), f(z_3)\big) = \cdots = \frac{\partial^k F}{\partial y^k}\big(f(z_1), f(z_3)\big) = 0,$$

which means that $f(z_3)$ is a root of multiplicity at least $k+1$ of the polynomial $F_p\big(f(z_1), y\big)$. But $F_p\big(f(z_1), y\big) = F_p\big(f(z_2), y\big)$ and $f(z_3) = f(pz_2)$, hence we obtain a contradiction with the fact that p has been chosen so that $f(pz_2)$ has multiplicity at most k as a root of $F_p\big(f(z_2), y\big)$. ■

Finally we can prove the second main result of this paper.

Theorem 4.5 *Let f be as above, and assume that $f(z_1) = f(z_2)$ for some z_1 and z_2. Then the derivatives of f vanish up to the same order at the points z_1 and z_2, and in particular there exists the analytic bijection α between neighbourhoods of z_1 and z_2, such that α preserves f.*

Proof The first statement follows immediately from the previous lemma.

To prove the second one let

(1) $f(z_1) = f(z_2) = c$;
(2) $f'(z_1) = f''(z_1) = \cdots = f^{(k)}(z_1) = f'(z_2) = f''(z_2) = \cdots = f^{(k)}(z_2) = 0$;
(3) $f^{(k+1)}(z_1) \neq 0$, $f^{(k+1)}(z_2) \neq 0$.

Then there exists analytic functions $g_1(z)$ and $g_2(z)$, such that

$$f(z) = c + g_1(z)^{k+1} = c + g_2(z)^{k+1},$$

where g_1 and g_2 are analytic bijections of an open neighbourhood of z_1 resp. z_2 (let us denote it D_1 resp. D_2) onto an open neighbourhood of 0, which we denote D. That is $g_1(z_1) = g_2(z_2) = 0$, but $g_1'(z_1), g_2'(z_2) \neq 0$. Let $\alpha(z) = g_2^{-1} \circ g_1(z)$. Then α is obviously an analytic bijection of D_1 onto D_2. Finally, the following calculation shows that α preserves f:

$$f(\alpha z) = c + g_2(\alpha z)^{k+1} = c + g_2\big(g_2^{-1} \circ g_1(z)\big)^{k+1} = c + g_1(z)^{k+1} = f(z). \qquad ■$$

References

[1] D. Alexander, C. Cummins, J. McKay and C. Simons, *Completely replicable functions.* In: Groups, combinatorics and geometry (Durham, 1990), Cambridge Univ. Press, Cambridge, 1992, 87–98.
[2] R. E. Borcherds, *Monstrous moonshine and monstrous Lie superalgebras.* Invent. Math. **109**(1992), 405–444.
[3] R. E. Borcherds and A. J. E. Ryba, *Modular Moonshine II.* Duke Math. J. **83**(1996), 435–459.
[4] H. Cohn and J. McKay, *Spontaneous generation of modular invariants.* Math. Comp. **65**(1996), 1295–1309.
[5] ———, *Modular functions from nothing.* Preprint, 1994.
[6] J. H. Conway and S. P. Norton, *Monstrous moonshine.* Bull. London Math. Soc. **11**(1979), 308–339.
[7] C. J. Cummins and T. Gannon, *Modular equations and the genus zero property of moonshine functions.* Invent. Math. (3) **129**(1998), 413–443.
[8] I. B. Frenkel, J. Lepowsky and A. Meurman, *Vertex operators and the Monster.* Academic Press, Boston, 1988.
[9] K. Mahler, *On a class of non-linear functional equations connected with modular functions.* J. Austral. Math. Soc. **22(A)**(1976), 65–118.
[10] Y. Martin, *On modular invariance of completely replicable functions.* In: Moonshine, the Monster, and related topics (South Hadley, MA, 1994), Contemp. Math. **193**(1996), 263–286.
[11] J. McKay and H. Strauss, *The q-series of monstrous moonshine and the decomposition of the head characters.* Comm. Algebra **18**(1990), 253–278.
[12] S. P. Norton, *More on moonshine.* In: Computational Group Theory (ed. M. D. Atkinson), Academic Press, 1984, 185–193.
[13] ———, *Non-monstrous Moonshine.* In: "Groups, Difference Sets, and the Monster" (eds. K.T. Arasu *et al.*), de Gruyter, 1996, 433–441.

Department of Mathematics
Massachusetts Institute of Technology
Cambridge, MA 02139
USA
email: kozlov@math.ias.edu, kozlov@math.mit.edu, kozlov@math.kth.se

Current address:
School of Mathematics
Institute for Advanced Study
Olden Lane
Princeton, NJ 08540
USA

https://doi.org/10.4153/CJM-1999-045-x Published online by Cambridge University Press