ELSEVIER
Available online at www.sciencedirect.com
SCIENCE DIRECT®
Journal of Number Theory 109 (2004) 120–135
JOURNAL OF Number Theory
www.elsevier.com/locate/jnt

Quantum integers and cyclotomy

Alexander Borisov[a], Melvyn B. Nathanson[b,*], Yang Wang[c]

[a]*Department of Mathematics, Pennsylvania State University, University Park, PA 16802, USA*
[b]*Department of Computer Science and Mathematics, Lehman College (CUNY), Bronx, NY 10468, USA*
[c]*Department of Mathematics, Georgia Institute of Technology, Atlanta, GA 30332, USA*

Received 6 October 2003; revised 5 May 2004

Communicated by A. Granville

Abstract

A sequence of functions $\mathscr{F} = \{f_n(q)\}_{n=1}^{\infty}$ satisfies the functional equation for multiplication of quantum integers if $f_{mn}(q) = f_m(q)f_n(q^m)$ for all positive integers m and n. This paper describes the structure of all sequences of rational functions with coefficients in **Q** that satisfy this functional equation.

MSC: primary 39B05; 81R50; 11R18; 11T22; 11B13

Keywords: Quantum integers; Quantum polynomial; Polynomial functional equation; Cyclotomic polynomials

1. The functional equation for multiplication of quantum integers

Let $\mathbf{N} = \{1, 2, 3, \ldots\}$ denote the positive integers. For every $n \in \mathbf{N}$, we define the polynomial

$$[n]_q = 1 + q + q^2 + \cdots + q^{n-1}.$$

* Corresponding author. Fax: +1-973-921-9615.
E-mail addresses: borisov@math.psu.edu (A. Borisov), melvyn.nathanson@lehman.cuny.edu (M.B. Nathanson), wang@math.gatech.edu (Y. Wang).

0022-314X/$ - see front matter © 2004 Elsevier Inc. All rights reserved.
doi:10.1016/j.jnt.2004.06.015

This polynomial is called the *quantum integer n*. The sequence of polynomials $\{[n]_q\}_{n=1}^{\infty}$ satisfies the following functional equation:

$$f_{mn}(q) = f_m(q) f_n(q^m) \tag{1}$$

for all positive integers m and n. Nathanson [1] asked for a classification of all sequences $\mathcal{F} = \{f_n(q)\}_{n=1}^{\infty}$ of polynomials and of rational functions that satisfy the functional equation (1).

The following statements are simple consequences of the functional equation. Proofs can be found in Nathanson [1].

Let $\mathcal{F} = \{f_n(q)\}_{n=1}^{\infty}$ be any sequence of functions that satisfies (1). Then $f_1(q) = f_1(q)^2 = 0$ or 1. If $f_1(q) = 0$, then $f_n(q) = f_1(q) f_n(q) = 0$ for all $n \in \mathbf{N}$, and $\mathcal{F}$ is a trivial solution of (1). In this paper, we consider only nontrivial solutions of the functional equation, that is, sequences $\mathcal{F} = \{f_n(q)\}_{n=1}^{\infty}$ with $f_1(q) = 1$.

Let P be a set of prime numbers, and let $S(P)$ be the multiplicative semigroup of $\mathbf{N}$ generated by P. Then $S(P)$ consists of all integers that can be represented as a product of powers of prime numbers belonging to P. Let $\mathcal{F} = \{f_n(q)\}_{n=1}^{\infty}$ be a nontrivial solution of (1). We define the support

$$\text{supp}(\mathcal{F}) = \{n \in \mathbf{N} : f_n(q) \neq 0\}.$$

There exists a unique set P of prime numbers such that $\text{supp}(\mathcal{F}) = S(P)$. Moreover, the sequence $\mathcal{F}$ is completely determined by the set $\{f_p(q) : p \in P\}$. Conversely, if P is any set of prime numbers, and if $\{h_p(q) : p \in P\}$ is a set of functions such that

$$h_{p_1}(q) h_{p_2}(q^{p_1}) = h_{p_2}(q) h_{p_1}(q^{p_2}) \tag{2}$$

for all $p_1, p_2 \in P$, then there exists a unique solution $\mathcal{F} = \{f_n(q)\}_{n=1}^{\infty}$ of the functional equation (1) such that $\text{supp}(\mathcal{F}) = S(P)$ and $f_p(q) = h_p(q)$ for all $p \in P$.

For example, for the set $P = \{2, 5, 7\}$, the reciprocal polynomials

$$\begin{aligned}
h_2(q) &= 1 - q + q^2, \\
h_5(q) &= 1 - q + q^3 - q^4 + q^5 - q^7 + q^8, \\
h_7(q) &= 1 - q + q^3 - q^4 + q^6 - q^8 + q^9 - q^{11} + q^{12}
\end{aligned}$$

satisfy the commutativity condition (2). Since

$$h_p(q) = \frac{[p]_{q^3}}{[p]_q} \quad \text{for } p \in P,$$

it follows that

$$f_n(q) = \frac{[n]_{q^3}}{[n]_q} \quad \text{for all } n \in S(P). \tag{3}$$

Moreover, $f_n(q)$ is a polynomial of degree $2(n-1)$ for all $n \in S(P)$.

Let $\mathcal{F} = \{f_n(q)\}_{n=1}^{\infty}$ be a solution of the functional equation (1) with $\text{supp}(\mathcal{F}) = S(P)$ If $P = \emptyset$, then $\text{supp}(\mathcal{F}) = \{1\}$. It follows that $f_1(q) = 1$ and $f_n(q) = 0$ for all $n \geqslant 2$. Also, for any prime p and any function $h(q)$, there is a unique solution of the functional equation (1) with $\text{supp}(\mathcal{F}) = S(\{p\})$ and $f_p(q) = h(q)$. Thus, we only need to investigate solutions of (1) for $\text{card}(P) \geqslant 2$.

If $\mathcal{F} = \{f_n(q)\}_{n=1}^{\infty}$ and $\mathcal{G} = \{g_n(q)\}_{n=1}^{\infty}$ are solutions of (1) with $\text{supp}(\mathcal{F})=\text{supp}(\mathcal{G})$, then, for any integers d, e, r, and s, the sequence of functions $\mathcal{H} = \{h_n(q)\}_{n=1}^{\infty}$, where

$$h_n(q) = f_n(q^r)^d g_n(q^s)^e,$$

is also a solution of the functional equation (1) with $\text{supp}(\mathcal{H}) = \text{supp}(\mathcal{F})$. In particular, if $\mathcal{F} = \{f_n(q)\}_{n=1}^{\infty}$ is a solution of (1), then $\mathcal{H} = \{h_n(q)\}_{n=1}^{\infty}$ is another solution of (1), where

$$h_n(q) = \begin{cases} 1/f_n(q) & \text{if } n \in \text{supp}(\mathcal{F}), \\ 0 & \text{if } n \notin \text{supp}(\mathcal{F}). \end{cases}$$

The functional equation also implies that

$$f_m(q) f_n(q^m) = f_n(q) f_m(q^n) \tag{4}$$

for all positive integers m and n, and

$$f_{m^k}(q) = \prod_{i=0}^{k-1} f_m(q^{m^i}). \tag{5}$$

Let $\mathcal{F} = \{f_n(q)\}_{n=1}^{\infty}$ be a solution in rational functions of the functional equation (1) with $\text{supp}(\mathcal{F}) = S(P)$. Then there exist a completely multiplicative arithmetic function $\lambda(n)$ with support $S(P)$ and rational numbers t_0 and t_1 with $t_0(n-1) \in \mathbf{Z}$ and $t_1(n-1) \in \mathbf{Z}$ for all $n \in S(P)$ such that, for every $n \in S(P)$, we can write the rational function $f_n(q)$ uniquely in the form

$$f_n(q) = \lambda(n) q^{t_0(n-1)} \frac{u_n(q)}{v_n(q)}, \tag{6}$$

where $u_n(q)$ and $v_n(q)$ are monic polynomials with nonzero constant terms, and

$$\deg(u_n(q)) - \deg(v_n(q)) = t_1(n-1) \quad \text{for all } n \in \mathrm{supp}(\mathcal{F}).$$

For example, let P be a set of prime numbers with $\mathrm{card}(P) \geqslant 2$. Let $\lambda(n)$ be a completely multiplicative arithmetic function with support $S(P)$, and let t_0 be a rational number such that $t_0(n-1) \in \mathbf{Z}$ for all $n \in S(P)$. Let R be a finite set of positive integers and $\{t_r\}_{r\in R}$ a set of integers. We construct a sequence $\mathcal{F} = \{f_n(q)\}_{n=1}^{\infty}$ of rational functions as follows: For $n \in S(P)$, we define

$$f_n(q) = \lambda(n) q^{t_0(n-1)} \prod_{r\in R} [n]_{q^r}^{t_r}. \tag{7}$$

For $n \notin S(P)$ we set $f_n(q) = 0$. Then $\prod_{r\in R}[n]_{q^r}^{t_r}$ is a quotient of monic polynomials with coefficients in $\mathbf{Q}$ and nonzero constant terms. The sequence $\mathcal{F} = \{f_n(q)\}_{n=1}^{\infty}$ satisfies the functional equation (1), and $\mathrm{supp}(\mathcal{F}) = S(P)$.

We shall prove that every solution of the functional equation (1) in rational functions with coefficients in $\mathbf{Q}$ is of the form (7). This provides an affirmative answer to Problem 6 in [1] in the case of the field $\mathbf{Q}$.

2. Roots of unity and solutions of the functional equation

Let K be an algebraically closed field, and let K^* denote the multiplicative group of nonzero elements of K. Let Γ denote the group of roots of unity in K^*, that is,

$$\Gamma = \{\zeta \in K^* : \zeta^n = 1 \text{ for some } n \in N\}.$$

Since Γ is the torsion subgroup of K^*, every element in $K^* \setminus \Gamma$ has infinite order. We define the *logarithm group*

$$L(K) = K^*/\Gamma$$

and the map

$$L : K^* \to L(K)$$

by

$$L(a) = a\Gamma \quad \text{for all } a \in K^*.$$

We write the group operation in $L(K)$ additively

$$L(a) + L(b) = a\Gamma + b\Gamma = ab\Gamma = L(ab).$$

Lemma 1. *Let K be an algebraically closed field, and $L(K)$ its logarithm group. Then $L(K)$ is a vector space over the field* $\mathbf{Q}$ *of rational numbers.*

Proof. Let $a \in K^*$ and $m/n \in \mathbf{Q}$. Since K is algebraically closed, there is an element $b \in K^*$ such that

$$b^n = a^m.$$

We define

$$\frac{m}{n} L(a) = L(b).$$

Suppose $m/n = r/s \in \mathbf{Q}$, and that

$$c^s = a^r$$

for some $c \in K^*$. Since $ms = nr$, it follows that

$$c^{ms} = a^{mr} = b^{nr} = b^{ms},$$

and so $c/b \in \Gamma$. Therefore,

$$\frac{m}{n} L(a) = L(b) = b\Gamma = c\Gamma = L(c) = \frac{r}{s} L(a)$$

and $(m/n)L(a)$ is well defined. It is straightforward to check that $L(K)$ is a $\mathbf{Q}$-vector space. $\square$

Lemma 2. *Let P be a set of primes, $\text{card}(P) \geqslant 2$, and let $S(P)$ be the multiplicative semigroup generated by P. For every integer $m \in S(P) \setminus \{1\}$ there is an integer $n \in S(P)$ such that* $\log m$ *and* $\log n$ *are linearly independent over* $\mathbf{Q}$. *Equivalently, for every integer $m \in S(P) \setminus \{1\}$ there is an integer $n \in S(P)$ such that there exist integers r and s with $m^r = n^s$ if and only if $r = s = 0$.*

Proof. If $m = p^k$ is a prime power, let n be any prime in $P \setminus \{p\}$. If m is divisible by more than one prime, let n be any prime in P. The result follows immediately from the fundamental theorem of arithmetic. $\square$

Let K be a field. A *function on* K is a map $f : K \to K \cup \{\infty\}$. For example, $f(q)$ could be a polynomial or a rational function with coefficients in K. We call $f^{-1}(0)$ the set of *zeros* of f and $f^{-1}(\infty)$ the set of *poles* of f.

Theorem 1. *Let K be an algebraically closed field. Let $\mathcal{F} = \{f_n(q)\}_{n=1}^{\infty}$ be a sequence of functions on K that satisfies the functional equation* (1). *Let P be the set of primes such that $\operatorname{supp}(\mathcal{F}) = S(P)$. If $\operatorname{card}(P) \geqslant 2$ and if, for every $n \in \operatorname{supp}(\mathcal{F})$, the function $f_n(q)$ has only finitely many zeros and only finitely many poles, then every zero and pole of $f_n(q)$ is either 0 or a root of unity.*

Proof. The proof is by contradiction. Let Γ be the group of roots of unity in K. Suppose that

$$f_n(a) = 0 \quad \text{for some } n \in \operatorname{supp}(\mathcal{F}) \text{ and } a \in K^* \setminus \Gamma.$$

By Lemma 2, there is an integer $m \in S(P)$ such that $\log m$ and $\log n$ are linearly independent over $\mathbf{Q}$. Since a has infinite order in the multiplicative group K^* and $f_n^{-1}(0)$ is finite, there are positive integers k and $M = m^k$ such that a^M is not a zero of the function $f_n(q)$. By (4), we have

$$f_M(q) f_n(q^M) = f_n(q) f_M(q^n).$$

Therefore,

$$f_M(a) f_n(a^M) = f_n(a) f_M(a^n) = 0.$$

Since $f_n(a^M) \neq 0$, it follows from (5) that

$$0 = f_M(a) = f_{m^k}(a) = \prod_{i=0}^{k-1} f_m(a^{m^i})$$

and so

$$f_m(a^{m^i}) = 0 \quad \text{for some } i \text{ such that } 0 \leqslant i \leqslant k-1.$$

Let

$$b = a^{m^i}.$$

Then

$$f_m(b) = 0,$$

$$b \in K^* \setminus \Gamma,$$

and

$$L(b) = m^i L(a) \tag{8}$$

Since $f_m^{-1}(0)$ is finite, there are positive integers ℓ and $N = n^\ell$ such that z^N is not a zero of $f_m(q)$ for every $z \in f_m^{-1}(0)$ with $z \in K^* \setminus \Gamma$. Since K is algebraically closed, we can choose $c \in K$ such that

$$c^N = b.$$

Then

$$f_m(c) \neq 0,$$

$$c \in K^* \setminus \Gamma$$

and

$$NL(c) = L(b). \tag{9}$$

Again applying (4), we have

$$f_m(q) f_N(q^m) = f_N(q) f_m(q^N)$$

and so

$$f_m(c) f_N(c^m) = f_N(c) f_m(c^N) = f_N(c) f_m(b) = 0.$$

It follows that

$$0 = f_N(c^m) = f_{n^\ell}(c^m) = \prod_{j=0}^{\ell-1} f_n(c^{mn^j})$$

and so

$$f_n(c^{mn^j}) = 0 \quad \text{for some } j \text{ such that } 0 \leqslant j \leqslant \ell - 1.$$

Let

$$a' = c^{mn^j}.$$

Then

$$f_n(a') = 0,$$

$$a' \in K^* \setminus \Gamma,$$

and

$$L(a') = mn^j L(c) \tag{10}$$

Combining (8)–(10), we obtain

$$L(a') = \frac{mn^j}{N} L(b) = \frac{m^{i+1}}{n^{\ell-j}} L(a)$$

that is,

$$L(a') = \frac{m^{i'}}{n^{j'}} L(a), \text{ where } 1 \leqslant i' \leqslant k \text{ and } 1 \leqslant j' \leqslant \ell. \tag{11}$$

What we have accomplished is the following: Given an element $a \in f_n^{-1}(0)$ that is neither 0 nor a root of unity, we have constructed another element $a' \in f_n^{-1}(0)$ that is also neither 0 nor a root of unity, and that satisfies (11). Iterating this process, we obtain an infinite sequence of such elements. However, the number of zeros of $f_n(q)$ is finite, and so the elements in this sequence cannot be pairwise distinct. It follows that there is an element

$$a \in f_n^{-1}(0) \setminus (\Gamma \cup \{0\})$$

such that

$$L(a) = \frac{m^r}{n^s} L(a),$$

where r and s are positive integers. Then

$$a^{n^s}\Gamma = L\left(a^{n^s}\right) = n^s L(a) = m^r L(a) = L\left(a^{m^r}\right) = a^{m^r}\Gamma.$$

Since a is not a root of unity, it follows that

$$m^r = n^s,$$

which contradicts the linear independence of $\log m$ and $\log n$ over $\mathbf{Q}$. Therefore, the zeros of the functions $f_n(q)$ belong to $\Gamma \cup \{0\}$ for all $n \in \text{supp}(\mathcal{F})$.

Replacing the sequence $\mathcal{F} = \{f_n(q)\}_{n\in\text{supp}(\mathcal{F})}$ with $\mathcal{F}' = \{1/f_n(q)\}_{n\in\text{supp}(\mathcal{F})}$, we conclude that the poles of the functions $f_n(q)$ also belong to $\Gamma \cup \{0\}$ for all $n \in \text{supp}(\mathcal{F})$. This completes the proof. $\square$

3. Rational solutions of the functional equation

In this section, we shall completely classify sequences of rational functions with rational coefficients that satisfy the functional equation for quantum multiplication.

For $k \geqslant 1$, let $\Phi_k(q)$ denote the kth cyclotomic polynomial. Then

$$F_k(q) = q^k - 1 = \prod_{d|k} \Phi_d(q)$$

and

$$\Phi_k(q) = \prod_{d|k} F_d(q)^{\mu(k/d)}, \tag{12}$$

where $\mu(k)$ is the Möbius function. Let ζ be a primitive dth root of unity. Then $F_k(\zeta) = 0$ if and only if d is a divisor of k. We define

$$F_0(q) = \Phi_0(q) = 1.$$

Note that

$$F_k(q) = q^k - 1 = (q-1)(1 + q + \cdots + q^{k-1}) = F_1(q)[k]_q \tag{13}$$

for all $k \geqslant 1$.

A *multiset* $U = (U_0, \delta)$ consists of a finite set U_0 of positive integers and a function $\delta : U_0 \to \mathbf{N}$. The positive integer $\delta(u)$ is called the *multiplicity* of u. Multisets $U = (U_0, \delta)$ and $U' = (U_0', \delta')$ are equal if $U_0 = U_0'$ and $\delta(u) = \delta'(u)$ for all $u \in U_0$. Similarly, $U \subseteq U'$ if $U_0 \subseteq U_0'$ and $\delta(u) \leqslant \delta'(u)$ for all $u \in U_0$. The multisets U and U' are *disjoint* if $U_0 \cap U_0' = \emptyset$. We define

$$\prod_{u\in U} f_u(q) = \prod_{u\in U_0} f_u(q)^{\delta(u)}$$

and

$$\max(U) = \max(U_0).$$

If $U_0 = \emptyset$, then we set $\max(U) = 0$ and $\prod_{u\in U} f_u(q) = 1$.

Lemma 3. *Let U and U' be multisets of positive integers. Then*

$$\prod_{u \in U} F_u(q) = \prod_{u' \in U'} F_{u'}(q), \tag{14}$$

if and only if $U = U'$.

Proof. Let $k = \max(U \cup U')$. Let ζ be a primitive kth root of unity. If $k \in U'$, then

$$\prod_{u \in U} F_u(\zeta) = \prod_{u' \in U'} F_{u'}(\zeta) = 0,$$

and so $k \in U$. Dividing (14) by $F_k(q)$, reducing the multiplicity of k in the multisets U and U' by 1, and continuing inductively, we obtain $U = U'$. □

Let $\mathcal{F} = \{f_n(q)\}_{n=1}^{\infty}$ be a nontrivial solution of the functional equation (1), where $f_n(q)$ is a rational function with rational coefficients for all $n \in \mathrm{supp}(\mathcal{F})$. Because of the standard representation (6), we can assume that

$$f_n(q) = \frac{u_n(q)}{v_n(q)},$$

where $u_n(q)$ and $v_n(q)$ are monic polynomials with nonzero constant terms. By Theorem 1, the zeros of the polynomials $u_n(q)$ and $v_n(q)$ are roots of unity, and so we can write

$$f_n(q) = \frac{\prod_{u \in U_n'} \Phi_u(q)}{\prod_{v \in V_n'} \Phi_v(q)},$$

where U_n' and V_n' are disjoint multisets of positive integers. Applying (12), we replace each cyclotomic polynomial in this expression with a quotient of polynomials of the form $F_k(q)$. Then

$$f_n(q) = \frac{\prod_{u \in U_n} F_u(q)}{\prod_{v \in V_n} F_u(q)}, \tag{15}$$

where U_n and V_n are disjoint multisets of positive integers. Let

$$f_n(q) = \frac{\prod_{u \in U_n} F_u(q)}{\prod_{v \in V_n} F_v(q)} = \frac{\prod_{u' \in U_n'} F_{u'}(q)}{\prod_{v' \in V_n'} F_{v'}(q)},$$

where U_n and V_n are disjoint multisets of positive integers and U'_n and V'_n are disjoint multisets of positive integers. Then

$$\prod_{u \in U_n \cup V'_n} F_u(q) = \prod_{v \in U'_n \cup V_n} F_v(q).$$

By Lemma 3, we have the multiset identity

$$U_n \cup V'_n = U'_n \cup V_n.$$

Since $U_n \cap V_n = \emptyset$, it follows that $U_n \subseteq U'_n$ and so $U_n = U'_n$. Similarly, $V_n = V'_n$. Thus, the representation (15) is unique.

We introduce the following notation for the *dilation* of a set: For any integer d and any set S of integers,

$$d * S = \{ds : s \in S\}.$$

Lemma 4. *Let $\mathcal{F} = \{f_n(q)\}_{n=1}^{\infty}$ be a nontrivial solution of the functional equation* (1) *with supp$(\mathcal{F}) = S(P)$, where card$(P) \geqslant 2$. Let*

$$f_n(q) = \frac{\prod_{u \in U_n} F_u(q)}{\prod_{v \in V_n} F_v(q)}$$

and U_n and V_n are disjoint multisets of positive integers. For every prime $p \in P$, let

$$m_p = \max(U_p \cup V_p).$$

There exists an integer r such that $m_p = rp$ for every $p \in P$. Moreover, either $m_p \in U_p$ for all $p \in P$ or $m_p \in V_p$ for all $p \in P$.

Proof. Let p_1 and p_2 be prime numbers in P, and let

$$\frac{m_{p_1}}{p_1} \geqslant \frac{m_{p_2}}{p_2}.$$

Equivalently,

$$p_2 m_{p_1} \geqslant p_1 m_{p_2}.$$

Applying functional equation (4) with $m = p_1$ and $n = p_2$, we obtain

$$\frac{\prod_{u\in U_{p_1}} F_u(q)}{\prod_{v\in V_{p_1}} F_v(q)} \frac{\prod_{u\in U_{p_2}} F_u(q^{p_1})}{\prod_{v\in V_{p_2}} F_v(q^{p_1})} = \frac{\prod_{u\in U_{p_2}} F_u(q)}{\prod_{v\in V_{p_2}} F_v(q)} \frac{\prod_{u\in U_{p_1}} F_u(q^{p_2})}{\prod_{v\in V_{p_1}} F_v(q^{p_2})},$$

where

$$U_{p_1} \cap V_{p_1} = U_{p_2} \cap V_{p_2} = \emptyset.$$

The identity

$$F_n(q^m) = \left(q^m\right)^n - 1 = q^{mn} - 1 = F_{mn}(q),$$

implies that

$$\begin{aligned}\frac{\prod_{u\in U_{p_1}\cup p_1 * U_{p_2}} F_u(q)}{\prod_{v\in V_{p_1}\cup p_1 * V_{p_2}} F_v(q)} &= \frac{\prod_{u\in U_{p_1}} F_u(q)}{\prod_{v\in V_{p_1}} F_v(q)} \frac{\prod_{u\in p_1 * U_{p_2}} F_u(q)}{\prod_{v\in p_1 * V_{p_2}} F_v(q)} \\ &= \frac{\prod_{u\in U_{p_2}} F_u(q)}{\prod_{v\in V_{p_2}} F_v(q)} \frac{\prod_{s\in p_2 * U_{p_1}} F_u(q)}{\prod_{t\in p_2 * V_{p_1}} F_v(q)} \\ &= \frac{\prod_{u\in U_{p_2}\cup p_2 * U_{p_1}} F_u(q)}{\prod_{v\in V_{p_2}\cup p_2 * V_{p_1}} F_v(q)}.\end{aligned}$$

By the uniqueness of the representation (15), it follows that

$$U_{p_1} \cup (p_1 * U_{p_2}) \cup V_{p_2} \cup (p_2 * V_{p_1}) = U_{p_2} \cup (p_2 * U_{p_1}) \cup V_{p_1} \cup (p_1 * V_{p_2}).$$

Recall that

$$m_{p_1} = \max\left(U_{p_1} \cup V_{p_1}\right).$$

If

$$m_{p_1} \in U_{p_1},$$

then

$$p_2 m_{p_1} \in p_2 * U_{p_1}$$

and so

$$p_2 m_{p_1} \in U_{p_1} \cup (p_1 * U_{p_2}) \cup V_{p_2} \cup (p_2 * V_{p_1}).$$

However,

(i) $p_2 m_{p_1} \notin U_{p_1}$ since $p_2 m_{p_1} > m_{p_1} = \max\left(U_{p_1} \cup V_{p_1}\right)$,
(ii) $p_2 m_{p_1} \notin p_2 * V_{p_1}$ since $m_{p_1} \in U_{p_1}$ and $U_{p_1} \cap V_{p_1} = \emptyset$,
(iii) $p_2 m_{p_1} \notin V_{p_2}$ since $p_2 m_{p_1} \geqslant p_1 m_{p_2} > m_{p_2} = \max\left(U_{p_2} \cup V_{p_2}\right)$.

If $p_2 m_{p_1} > p_1 m_{p_2} = \max\left(p_1 * U_{p_2}\right)$, then $p_2 m_{p_1} \notin p_1 * U_{p_2}$. This is impossible, and so

$$p_2 m_{p_1} = p_1 m_{p_2} \in p_1 * U_{p_2},$$

$$m_{p_2} \in U_{p_2},$$

and

$$\frac{m_{p_1}}{p_1} = \frac{m_{p_2}}{p_2} = r \qquad \text{for all } p_1, p_2 \in P.$$

Similarly, if $m_{p_1} \in V_{p_1}$ for some $p_1 \in P$, then $m_{p_2} \in V_{p_2}$ for all $p_2 \in P$. This completes the proof. □

Theorem 2. *Let $\mathcal{F} = \{f_n(q)\}_{n=1}^{\infty}$ be a sequence of rational functions with coefficients in* **Q** *that satisfies the functional equation* (1). *If supp$(\mathcal{F}) = S(P)$, where P is a set of prime numbers and card$(P) \geqslant 2$, then there are*

(i) *a completely multiplicative arithmetic function $\lambda(n)$ with support $S(P)$,*
(ii) *a rational number t_0 such that $t_0(n-1)$ is an integer for all $n \in S(P)$,*
(iii) *a finite set R of positive integers and a set $\{t_r\}_{r \in R}$ of integers*

such that

$$f_n(q) = \lambda(n) q^{t_0(n-1)} \prod_{r \in R} [n]_{q^r}^{t_r} \quad \textit{for all } n \in \textit{supp}(\mathcal{F}). \tag{16}$$

Proof. It suffices to prove (16) for all $p \in P$. Recalling the representation (6), we only need to investigate the case

$$f_p(q) = \frac{\prod_{u \in U_p} F_u(q)}{\prod_{v \in V_p} F_v(q)},$$

where U_p and V_p are disjoint multisets of positive integers. Let $m_p = \max(U_p \cup V_p)$. By Lemma 4, there is a nonnegative integer m such that $m_p = mp$ for all $p \in P$. We can assume that $m_p \in U_p$ for all $p \in P$.

The proof is by induction on m. If $m = 0$, then $U_p = V_p = \emptyset$ and $f_p(q) = 1$ for all $p \in P$, hence (16) holds with $R = \emptyset$.

Let $m = 1$, and suppose that $m_p = p \in U_p$ for all $p \in P$. Then

$$f_p(q) = \frac{\prod_{u \in U_p} F_u(q)}{\prod_{v \in V_p} F_v(q)} = \frac{(q^p - 1)\prod_{u \in U'_p} F_u(q)}{\prod_{v \in V_p} F_v(q)}.$$

Since $q^p - 1 = F_1(q)[p]_q$, we have

$$\begin{aligned} g_p(q) &= \frac{f_p(q)}{[p]_q} \\ &= \frac{(q^p - 1)\prod_{u \in U_p \setminus \{p\}} F_u(q)}{[p]_q \prod_{v \in V_p} F_v(q)} \\ &= \frac{F_1(q)\prod_{u \in U_p \setminus \{p\}} F_u(q)}{\prod_{v \in V_p} F_v(q)} \\ &= \frac{\prod_{u \in U'_p} F_u(q)}{\prod_{v \in V'_p} F_v(q)}, \end{aligned}$$

where $U'_p \cap V'_p = \emptyset$. The sequence of rational functions $\mathcal{G} = \{g_n(q)\}_{n=1}^{\infty}$ is also a solution of the functional equation (1), and either $\max(U'_p \cup V'_p) = 0$ for all $p \in P$ or $\max(U'_p \cup V'_p) = p$ for all $p \in P$.

If $\max(U'_p \cup V'_p) = p$ for all $p \in P$, then we construct the sequence $\mathcal{H} = \{h_n(q)\}_{n=1}^{\infty}$ of rational functions

$$h_n(q) = \frac{g_n(q)}{[n]_q} = \frac{f_n(q)}{[n]_q^2}.$$

Continuing inductively, we obtain a positive integer t such that

$$f_n(q) = [n]_q^t \qquad \text{for all } n \in \mathrm{supp}(\mathcal{F}).$$

Thus, (16) holds in the case $m = 1$.

Let m be an integer such that the Theorem holds whenever $m_p < mp$ for all $p \in P$, and let $\mathcal{F} = \{f_n(q)\}_{n=1}^{\infty}$ be a solution of the functional equation (1) with $\mathrm{supp}(\mathcal{F}) = S(P)$

and $m_p = mp$ and $m_p \in U_p$ for all $p \in P$. The sequence $\mathcal{G} = \{g_n(q)\}_{n=1}^{\infty}$ with

$$g_n(q) = \frac{f_n(q)}{[n]_{q^r}}$$

is a solution of the functional equation (1). Since

$$F_{rp}(q) = q^{rp} - 1 = \left(q^r - 1\right)\left(1 + q^r + \cdots + q^{r(p-1)}\right) = F_r(q)[p]_{q^r},$$

it follows that

$$\begin{aligned} g_p(q) &= \frac{(q^{m_p} - 1)\prod_{u\in U_p\setminus\{m_p\}} F_u(q)}{[p]_{q^r}\prod_{v\in V_p} F_v(q)} \\ &= \frac{(q^{mp} - 1)\prod_{u\in U_p\setminus\{mp\}} F_u(q)}{[p]_{q^r}\prod_{v\in V_p} F_v(q)} \\ &= \frac{F_r(q)\prod_{u\in U_p\setminus\{mp\}} F_u(q)}{\prod_{v\in V_p} F_v(q)} \\ &= \frac{\prod_{u\in U'_p} F_u(q)}{\prod_{v\in V'_p} F_v(q)}, \end{aligned}$$

where $U'_p \cap V'_p = \emptyset$, and $\max(U_{p'} \cup V_{p'}) \leqslant mp$.

If $\max(U_{p'} \cup V_{p'}) = mp$, then $mp \in U'_p$. We repeat the construction with

$$h_n(q) = \frac{g_n(q)}{[n]_{q^r}} = \frac{f_n(q)}{[n]^2_{q^r}}.$$

Continuing this process, we eventually obtain a positive integer t_r such that the sequence of rational functions

$$\left\{\frac{f_n(q)}{[n]^{t_r}_{q^r}}\right\}_{n=1}^{\infty}$$

satisfies the functional equation (1), and

$$\frac{f_p(q)}{[p]^{t_r}_{q^r}} = \frac{\prod_{u\in U'_p} F_u(q)}{\prod_{v\in V'_p} F_v(q)},$$

where $U'_p \cap V'_p = \emptyset$ and $\max(U'_p \cup V'_p) < mp$. It follows from the induction hypothesis there is a finite set R of positive integers and a set $\{t_r\}_{r\in R}$ of integers such that

$$f_n(q) = \prod_{r\in R} [n]_{q^r}^{t_r} \qquad \text{for all } n \in \operatorname{supp}(\mathcal{F}).$$

This completes the proof. □

There remain two related open problems. First, we would like to have a simple criterion to determine when a sequence of rational functions satisfying the functional equation (1) is actually a sequence of polynomials. It is sufficient that all of the integers t_r in the representation (16) be nonnegative, but the example in (3) shows that this condition is not necessary.

Second, we would like to have a structure theorem for rational function solutions and polynomial solutions to the functional equation (1) with coefficients in an arbitrary field, not just the field of rational numbers.

Acknowledgments

Nathanson's work was supported in part by Grants from the NSA Mathematical Sciences Program and the PSC-CUNY Research Award Program. Yang's work was supported in part by National Science Foundation Grants DMS-0070586 and DMS-0139261. Nathanson and Wang began their collaboration at a conference on Combinatorial and Number Theoretic Methods in Harmonic Analysis at the Schrödinger Institute in Vienna in February, 2003.

References

[1] M.B. Nathanson, A functional equation arising from multiplication of quantum integers, J. Number Theory 103 (2003) 214–233.