Notes on Number Theory and Discrete Mathematics
ISSN 1310–5132
Vol. 20, 2014, No. 3, 1–28

Solutions with infinite support bases of a functional equation arising from multiplication of quantum integers

Lan Nguyen

Mathematics Department, University of Michigan-Ann Arbor
Ann Arbor, MI 48109, United States
e-mail: ltng@umich.edu

Abstract: It follows from our previous works and those of Nathanson that if P is a set of primes, then the greater the cardinality of P, the less likely that there exists a sequence of polynomials, satisfying the functional equation arising from multiplication of quantum integers studied by Nathanson, which has P as its support base and which cannot be generated by quantum integers. In this paper we analyze the set of roots of the polynomials involved leading to a direct construction of a polynomial solution Γ which has infinite support base P and which cannot be generated by quantum integers. Our results demonstrate that there are more to these solutions than those provided by quantum integers. In addition, we also show that a result of Nathanson does not hold if the condition $t_\Gamma = 1$ is removed.
Keywords: Diophantine equation, Quantum integer, q-series, Sumset, Polynomial functional equation, Cyclotomic polynomial.
AMS Classification: 11P99, 11C08.

1 Introduction and Background

The aim of this paper is to study the the collections of primes P associated, in the sense which is described in more details subsequently, to the solutions Γ of the functional equation discussed in [2] arising from multiplication of quantum integers. We consider the case where the fields of coefficients of Γ are of characteristic zero. From [2–4], we have seen that quantum integers serve as a source of generators for the solutions Γ above. From [4], it is known that there is no nontrivial sequence of polynomials, satisfying Functional Equation (2) with support base P containing all primes, which cannot be generated by quantum integers in the sense of Theorem 2.1 of [4]. On

the other hand, it is known, also from [4], that there exist sequences of polynomials satisfying Functional Equation (2) with support base P of finite cardinality, which cannot be generated by quantum integers. This paper investigates whether this phenomenon extends to the collection of sequences of polynomials satisfying Functional Equation (2) with support bases P of infinite cardinality.

First, let us give some basic background and main results from [2] as well as [4] concerning quantum integers and the functional equation arising from multiplication of these integers, which are relevant to this paper.

Definition 1.1. A quantum integer is a polynomial in q of the form

$$[n]_q := q^{n-1} + \ldots + q + 1 = \frac{q^n - 1}{q - 1} \tag{1.1}$$

where n is any natural number.

From [1] and [2], multiplication operation for quantum integers, called quantum multiplication, is defined by the following rule:

$$[m]_q \star [n]_q := [mn]_q = [m]_q \cdot [n]_{q^m} = [n]_q \cdot [m]_{q^n} \tag{1.2}$$

where $\star$ denotes quantum multiplication, multiplication operation for quantum integers, and $.$ denotes the usual multiplication of polynomials. It can be verified that Equation (1.2) is just the q-series expansion of the sumset

$$\{0, 1, \ldots, m-1\} + \{0, m, \ldots, (n-1)m\} = \{0, 1, \ldots, mn-1\}.$$

That leads Nathanson to study sequences of polynomials in q, $\Gamma = \{f_n(q) \mid n = 1, \ldots, \infty\}$ with coefficients contained in some field, satisfying the functional equations:

$$f_m(q) f_n(q^m) \overset{(1)}{=} f_n(q) f_m(q^n) \overset{(2)}{=} f_{mn}(q) \tag{1.3}$$

for all $m, n \in \mathbb{N}$. As in [2], we refer to the first equality in the above functional equation as Functional Equation (1) and the second equality as Functional Equation (2).

Remark 1.2. A sequence of polynomials which satisfies Functional Equation (2) automatically satisfies Functional Equation (1) but not vice versa ([2]).

Let $\Gamma = \{f_n(q)\}$ be a sequence of polynomials satisfying Functional Equation (2). The set of integers n in $\mathbb{N}$ where $f_n(q) \neq 0$ is called the support of Γ and denoted by $supp\{\Gamma\}$. If P is a set of rational primes and A_P consists of 1 and all natural numbers such that all their prime factors come from P, then A_P is a multiplicative semigroup which is called a prime multiplicative semigroup associated to P. From [2], the support of Γ is a multiplicative prime sub-semigroup of $\mathbb{N}$.

Theorem 1.3. *([2]) Let $\Gamma = \{f_n(q)\}$ be a sequence of polynomials satisfying Functional Equation (2). Then $supp\{\Gamma\}$ is of the form A_P for some set of primes P, and Γ is completely deter-*

mined by the collection of polynomials:

$$\{f_p(q) \mid p \in P\}.$$

As a result, studying any sequence Γ satisfying Functional Equation (2) reduces to studying the sub-collection of polynomials with prime indexes p in its support base P.

Definition 1.4. Let P be the collection of primes associated to the support A_P, in the sense of Theorem 1.3, of a sequence of polynomials Γ satisfying Functional Equation (2). Then P is called the support base of Γ.

In the reverse direction, if P is a set of primes in $\mathbb{N}$ then there is at least one sequence Γ satisfying Functional Equation (2) with $supp\{\Gamma\} = A_P$. One such sequence can be defined as the set of polynomials:

$$f_m(q) = \begin{cases} [m]_q & \text{if } m \in A_P; \\ 0 & \text{otherwise.} \end{cases}$$

Note that the coefficients of $f_m(q)$ are properly contained in $\mathbb{Q}$.

We say that a sequence Γ is nonzero if $supp\{\Gamma\} \neq \emptyset$. If Γ satisfies Functional Equation (2), then Γ is nonzero if and only if $f_1(q) = 1$ ([2]).

The degree of each polynomial $f_n(q) \in \Gamma$ is denoted by $deg(f_n(q))$. From [1, 2], it is known that there exists a rational number t_Γ such that:

$$deg(f_n(q)) = t_\Gamma(n-1)$$

for all n in $supp\{\Gamma\}$. This number t_Γ is not necessarily an integer (see [2] or [4] for an example of such a sequence). We discussed in [4] that t_Γ can only be non integral when the support base P of Γ is of the form $P = \{p\}$ for some prime p.

Let P be a set of primes. The next result provides a general way to construct a solution to the Functional Equation (2) with support base P:

Theorem 1.5. *([2]) Let P be a set of primes. Let $\Gamma' = \{f'_p(q) \mid p \in P\}$ be a collection of polynomials such that:*

$$f'_{p_1}(q) \cdot f'_{p_2}(q^{p_1}) = f'_{p_2}(q) \cdot f'_{p_1}(q^{p_2})$$

for all $p_i \in P$(i.e, satisfying Functional Equation (1)). Then there exists a unique sequence $\Gamma = \{f_n(q) \mid n \in \mathbb{N}\}$ of polynomials satisfying Functional Equation (2) such that $f_p(q) = f'_p(q)$ for all primes $p \in P$.

Theorem 1.6. *([2]) Let $\Gamma = \{f_n(q) \mid n \in \mathbb{N}\}$ be a nonzero sequence of polynomials satisfying Functional Equation (2) with support A_P for some set of primes P. Then there exists a unique completely multiplicative arithmetic function $\psi(n)$, a rational number t, and a unique sequence $\Sigma = \{g_n(q)\}$ satisfying (2) with the same support A_P such that:*

$$f_n(q) = \psi(n) q^{t(n-1)} g_n(q)$$

where $g_n(q)$ is a monic polynomial with $g_n(0) \neq 0$ for all $n \in A_P$.

As a result, in the rest of this paper, unless otherwise stated, all sequences of polynomials which we consider are normalized so that each polynomial is monic and having nonzero constant terms.

For a sequence Γ of polynomials satisfying Functional Equation (2), the smallest field K which contains all the coefficients of all the polynomials in Γ is called the Field of Coefficients of Γ. We are only concerned with sequences of polynomials whose fields of coefficients K are of characteristic zero. Unless stated otherwise, we always view Γ as a sequence of polynomials with coefficients in a fixed separable closure $\overline{K}$ of K which is embedded in $\mathbb{C}$ via a fixed embedding $\iota : \overline{K} \hookrightarrow \mathbb{C}$. Thus every element $f(q)$ of Γ can be viewed as a polynomial in $\mathbb{C}[q]$. We frequently view polynomials $f(q)$'s in Γ as elements of the ring $\mathbb{C}[q]$ through out this paper. Thus whenever that is necessary, it is implicitly assumed.

Definition 1.7. Let $\Gamma = \{f_n(q) \mid n \in \mathbb{N}\}$ be a sequence of polynomials satisfying Functional Equation (2). Then Γ is said to be generated by quantum integers if there exist ordered pairs of integers $\{u_i, t_i\}_i$ with $i = 1, \ldots, s$ such that $t_\Gamma = \sum_{i=1,\ldots,s} u_i t_i$ and

$$f_n(q) = \prod_{i=1}^{s} ([n]_{q^{u_i}})^{t_i}$$

for all n in $\mathbb{N}$.

2 Main results

From part (2) of Theorem 1.9, we know that there is no sequence Γ of polynomials satisfying Functional Equation (2) with support base P consisting of all primes and field of coefficients of characteristic zero strictly containing $\mathbb{Q}$. Therefore, there is no sequence Γ of polynomials satisfying Functional Equation (2) with support base P consisting of all primes which cannot be generated by quantum integers by part (1) of Theorem 1.9. On the other hand, it can be deduced from Key Proposition 1 of [4] that there is a finite set of primes P, namely $P = \{p, r\}$ for certain primes p and r, such that there exists a sequence of polynomial Γ satisfying Functional equation (2) with field of coefficients of characteristic zero strictly containing $\mathbb{Q}$ and support base P.

In the opposite direction, suppose that a set of primes P is given. We are interested in the question whether or not there exists a sequence of polynomials satisfying Functional Equation (2) with field of coefficients of characteristic zero and support base P. In the case where the field of coefficients is $\mathbb{Q}$, there exists at least one sequence of polynomials satisfying Functional Equation (2) having P as its support base, namely

$$\Gamma := \{f_n(q) = [n]_q \mid n \in A_P\}.$$

This sequence is in fact the unique sequence of monic polynomials satisfying Functional Equation (2) with support base P such that $\deg\{f_n(q)\} = n - 1$, or equivalently $t_\Gamma = 1$, if $P \supseteq \{2, p\}$ for

some odd prime p. However, except in the case where $|P| = 1$ ([4]), there is no known criterion for determining whether there exists a sequence of polynomials satisfying Functional Equation (2) with fields of coefficients strictly containing $\mathbb{Q}$ with a given set of prime P as its support base. Moreover, in the case where P has infinite cardinality, it is not even known if there exists a sequence of polynomials satisfying Functional Equation (2) with support base P and field of coefficients strictly containing $\mathbb{Q}$. It can be seen from [2] and [4] that the cardinality of the set of primes P has a direct impact on the existence of sequences Γ of polynomials, with field of coefficients of characteristic zero strictly containing $\mathbb{Q}$, satisfying Functional Equation (2) with support base P. In particular, Theorems 2.1 and 2.2 of [7] show that if r is a prime and P is the support base of a sequence of polynomials

$$\Gamma = \{f_n(q) \mid n \in \mathbb{N}\}$$

satisfying Functional Equation (2) with field of coefficients strictly containing $\mathbb{Q}$, then there exists a sequence of polynomials

$$\Gamma_r = \{g_n(q) \mid n \in \mathbb{N}\}$$

satisfying Functional Equation (2) with support base $P \cup \{r\}$ such that

$$g_p(q) = f_p(q)$$

for all p in P if and only if r satisfies certain conditions imposed by the sequence Γ and P. As a result, the greater the cardinality of the set of primes P, the less likely that there is a sequence of polynomials satisfying Functional Equation (2) with support base P and field of coefficients strictly containing $\mathbb{Q}$. In other word, if a set of primes P has large cardinality and if Γ is a sequence of polynomial satisfying Functional Equation (2) with support base P, then it is more likely that Γ is generated by quantum integers. In this paper, we show that, in spite of the restriction described by Theorems 2.1 and 2.2 of [7], there exist sequences of polynomials satisfying Functional Equation (2) with field of coefficients strictly containing $\mathbb{Q}$ and having infinite support base P. The existence of these sequences of polynomials demonstrates the limitation of quantum integers as generators of the solution of these functional equations.

Our main results in this paper can be summarized as follows:

Theorem 2.1. *Let P be a set of primes. Suppose that one of the following conditions holds:*

1. *$P = \{p\}$ or $\{p, r\}$ for some primes p and r.*
2. *4 divides $p - 1$ for all odd primes p in P.*
3. *There exists an odd prime r such that r divides $p - 1$ for all p in P.*
4. *There exists an odd prime r such that r divides $p - 1$ for all odd primes p in $P - \{r\}$.*

Then there exists a sequence $\Gamma = \{f_n(q) \mid n \in \mathbb{N}\}$ of polynomials satisfying Functional Equation (2) with field of coefficients strictly containing $\mathbb{Q}$ and support base P.

Corollary 2.2. *There exists a sequence Γ of polynomials satisfying Functional Equation (2) with field of coefficients strictly containing $\mathbb{Q}$ and support base of infinite cardinality. In other word, there exists at least one sequence of polynomials satisfying Functional Equation (2) with infinite support base, which cannot be generated by quantum integers.*

Remark 2.3.

- Part (1) of Theorem 2.1 demonstrates in particular that there exists a sequence of polynomials, satisfying Functional Equation (2) with support base $P = \{2, p\}$ for some odd prime p, which cannot be generated by quantum integers in the sense defined earlier. This shows that the condition $t_\Gamma = 1$ in Theorem 9 of [2] is necessary for fields of coefficients of characteristic zero.

- Corollary 2.2 establishes the existence of a sequence of polynomials satisfying Functional Equation (2) with support base of infinite cardinality, which cannot be generated by quantum integers. This also proves the necessity of Proposition 3.10 of [2].

- Theorem 2.1 lays the foundation for [6] which provides the set of necessary and sufficient conditions for the existence of a sequence of polynomials satisfy Functional Equation (2) with support base P which cannot be generated by quantum integers.

3 Proofs of Main results

Proof. (Proof of Theorem 2.1)

(1) If $P = \{p\}$ for some prime p, then the existence of a sequence of polynomials Γ satisfying Functional Equation (2), with field of coefficients strictly containing $\mathbb{Q}$, is guaranteed by [1]. After a normalization using Theorem 1.6, such sequences have the form

$$\Gamma = \{f_{p^n}(q) \mid n \in \mathbb{N}\}$$

where:

- $f_{p^0}(q) = 1$.
- $f_{p^n}(q) = f_p(q) f_{p^{n-1}}(q^2)$ where $f_p(q)$ is a monic polynomial with nonzero constant term and coefficients not properly contained in $\mathbb{Q}$.

It follows immediately from the definition of $f_p(q)$ and Γ that the field of coefficients of Γ strictly contains $\mathbb{Q}$. As a result, Γ cannot be generated by quantum integers in the sense of Definition 1.7.

Suppose $P = \{p, r\}$ for some prime p and r. First let us give some terminology involved in the construction of our sequence.

Let u be any positive integer and p be any prime number. The polynomial denoted by $P_{u,p}(q)$ or $P_{up}(q)$ is the irreducible cyclotomic polynomial in $\mathbb{Q}[q]$ whose roots are all primitive up-roots of unity. $P_{u,p}(q)$ is sometimes denoted by $P_{up}(q)$ or $P_v(q)$ where $v = up$. For a primitive n-root

of unity α in $\mathbb{C}$, which can be written in the form $\alpha = e^{\frac{2\pi i w}{n}}$ for some primitive residue class w modulo n, we always identify α, via the Chinese Remainder Theorem, with the tuples $(u_i)_i$ where $\prod_i (p_i)^{m_i}$ is the prime factorization of n and $u_i \in (\mathbb{Z}/p_i^{m_i}\mathbb{Z})^*$ for each i such that

$$u_i \equiv w(p_i^{m_i}).$$

We also need to recall from [4, 5] the following definitions since they are used frequently in the subsequent part of our work.

Definition 3.1. 1) Let $P_{u,p}(q)$ and $P_{u,r}(q)$ be the cyclotomic polynomials with coefficients in $\mathbb{Q}$ of orders up and ur respectively. Let $F_{u,p}(q)$ and $F_{u,r}(q)$ be two polynomials dividing $P_{u,p}(q)$ and $P_{u,r}(q)$ respectively. If $F_{u,p}(q)$ and $F_{u,r}(q)$ satisfy the condition that for each primitive residue class w modulo u, all the roots of $P_{u,p}(q)$ represented by the collection of tuples $\{(\gamma_p, (w_{p_j})_j) \mid \gamma_p = 1, \ldots, p-1\}$ if p does not divide u (resp. by the collection $\{(w_p + t(p^l), (w_{p_j})_{j,p_j \neq p}) \mid t = 0, \ldots, p-1\}$ if $p^l | u$ for some positive integer $l \geq 1$) are roots $F_{u,p}(q)$ if and only if all the roots of $P_{u,r}(q)$ represented by the collection $\{\gamma_r, (w_{p_j})_j \mid \gamma_r = 1, \ldots, r-1\}$ if r does not divide u (resp. by the collection $\{w_r + s(r^h), (w_{p_j})_{j,p_j \neq r} \mid s = 0, \ldots, r-1\}$ if $r^h | u$ for some positive integer $h \geq 1$) are roots $F_{u,r}(q)$, then we will say that $F_{u,p}(q)$ and $F_{u,r}(q)$ are **compatible**. For example, $P_{u,p}(q)$ and $P_{u,r}(q)$ are compatible for any positive integer u, primes p and r, a fact which is proven in [3] for the case where pr does not divide u as well as when either p or r dividing u.

2) Two polynomials $f_{u,p}(q)$ and $f_{u,r}(q)$ are said to be **super-compatible** if $f_{u,p}(q) = = \prod_i (F_{u,p}^{(i)}(q))^{n_i}$ and $f_{u,r}(q) = \prod_i (F_{u,r}^{(i)}(q))^{n_i}$ where $F_{u,p}^{(i)}(q)$ and $F_{u,r}^{(i)}(q)$ are polynomials which are compatible for all i. In particular, $P_{u,p}(q)^n$ and $P_{u,r}(q)^n$ are super-compatible for any nonnegative integer n. Thus compatibility is a special case of super-compatibility.

Remark 3.2. To understand the rationality of this definition, the readers can consult [4, 5]. The polynomials $F_{u,\square}^{(i)}(q)$'s in the definition of super-compatible might not unique for any i, where $\square$ denotes either p or r.

Let p and r be any distinct primes in the support of Γ. Define $f_{u_p,p}(q)$ to be the factor of $f_p(q)$ such that its roots consist of all the roots of $f_p(q)$ with multiplicities which are primitive pu_p-roots of unity. Then $f_p(q) = \prod_{u_{p,j} > u_{p,j+1}} f_{u_{p,j},p}(q)$ in the ring $\mathbb{C}[q]$. Similarly, $f_r(q) = \prod_{u_{r,i} > u_{r,i+1}} f_{u_{r,i},r}(q)$. We call j (resp. i) or interchangeably $u_{p,j}$ (resp. $u_{r,i}$) the j-**level** (resp. i-**level**) or $u_{p,j}$-level (resp. $u_{r,i}$-level) of $f_p(q)$ (resp. $f_r(q)$) if $f_{u_{p,j}}(q)$ (resp. $f_{u_{r,i}}(q)$) is a nontrivial factor of $f_p(q)$ (resp. $f_r(q)$). Define $V := \{v_{p,r,k} \mid v_{p,r,k} > v_{p,r,k+1}\} := \{u_{p,j}\}_j \cup \{u_{r,i}\}_i$. We refer to k or $v_{p,r,k}$ as the k-**bi-level** with respect to p and r or the $v_{p,r,k}$-bi-level of $f_p(q)$ and $f_r(q)$. Note that level i of $f_p(q)$ or $f_r(q)$ is not necessarily equal to the bi-level i of $f_p(q)$ and $f_r(q)$. Using V and these product decompositions, we write Functional Equation (1) with respect to $f_p(q)$ and $f_r(q)$ as:

$$\begin{array}{ccc}
f_{v_{p,r,1},p}(q)^{s_{v_{p,1}}} f_{v_{p,r,1},r}(q^p)^{s_{v_{r,1}}} & \overset{(1)}{\longleftrightarrow} & f_{v_{p,r,1},r}(q)^{s_{v_{r,1}}} f_{v_{p,r,1},p}(q^r)^{s_{v_{p,1}}} \\
\cdots & \cdots & \cdots \\
f_{v_{p,r,k},p}(q)^{s_{v_{p,k}}} f_{v_{p,r,k},r}(q^p)^{s_{v_{r,k}}} & \overset{(k)}{\longleftrightarrow} & f_{v_{p,r,k},r}(q)^{s_{v_{r,k}}} f_{v_{p,r,k},p}(q^r)^{s_{v_{p,k}}} \\
\cdots & \cdots & \cdots \\
f_p(q) f_r(q^p) & = & f_r(q) f_p(q^r)
\end{array}$$

where:

- $s_{p,k} = 1$ if $f_{v_{p,r,k},p}(q)$ nontrivially divides $f_p(q)$ (i.e., $f_{v_{p,r,k},p}(q) = f_{u_i,p}(q)$ for some u_i) and 0 otherwise.
- $s_{r,k} = 1$ if $f_{v_{p,r,k},r}(q)$ nontrivially divides $f_r(q)$ (i.e., $f_{v_{p,r,k},r}(q) = f_{u_i,r}(q)$ for some u_i) and 0 otherwise.
- $\prod_k f_{v_{p,r,k},p}(q)^{s_{v_{p,k}}} f_{v_{p,r,k}}(q^p)^{s_{v_{r,k}}} = f_p(q) f_r(q^p)$.
- $\prod_j f_{v_{p,r,k},r}(q)^{s_{v_{r,k}}} f_{v_{p,r,k}}(q^r)^{s_{v_{p,j}}} = f_r(q) f_p(q^r)$.
- The symbol $\overset{(j)}{\longleftrightarrow}$ indicates the functional equation (1) at the bi-level j (note that the polynomial expressions on the left hand side and the right hand side of $\longleftrightarrow$ at each bi-level are not necessarily equal).

Note that for every bi-level k where $v_{p,r,k}$ appears in the equation above, either $s_{p,k} = 1$ or $s_{r,k} = 1$.

The above version of Functional Equation (1) is called the **Expanded Functional Equation** (1) with respect to p and r, denoted by EFE(1). The EFE(1) above is said to be in **reduced form** if at each bi-level k where pr does not divide $v_{p,r,k}$, the line

$$f_{v_{p,r,k},p}(q)^{s_{v_{p,k}}} f_{v_{p,r,k},r}(q^p)^{s_{v_{r,k}}} \overset{(k)}{\longleftrightarrow} f_{v_{p,r,k},r}(q)^{s_{v_{r,k}}} f_{v_{p,r,k},p}(q^r)^{s_{v_{p,k}}}$$

in EFE (1) is replaced by

(i) $f_{v_{p,r,k},r}(q^p)^{s_{v_{r,k}}} \overset{(k)}{\longleftrightarrow} f_{v_{p,r,k},r}(q)^{s_{v_{r,k}}} \frac{f_{v_{p,r,k},p}(q^r)^{s_{v_{p,k}}}}{f_{v_{p,r,k},p}(q)^{s_{v_{p,k}}}}$ if $(r, v_{p,r,k}) = 1$.

(ii) $f_{v_{p,r,k},p}(q)^{s_{v_{p,k}}} \frac{f_{v_{p,r,k},r}(q^p)^{s_{v_{r,k}}}}{f_{v_{p,r,k},r}(q)^{s_{v_{r,k}}}} \overset{(k)}{\longleftrightarrow} f_{v_{p,r,k},p}(q^r)^{s_{v_{p,k}}}$ if $(p, v_{p,r,k}) = 1$, or

(iii) $\frac{f_{v_{p,r,k},p}(q^r)^{s_{v_{p,k}}}}{f_{v_{p,r,k},p}(q)^{s_{v_{p,k}}}} \overset{(k)}{\longleftrightarrow} \frac{f_{v_{p,r,k},r}(q^p)^{s_{v_{r,k}}}}{f_{v_{p,r,k},r}(q)^{s_{v_{r,k}}}}$ if $(pr, v_{p,r,k}) = 1$.

(iv) The line $f_p(q) f_r(q^p) = f_r(q) f_p(q^r)$ is replaced by $Q_{p,r}(q) = Q_{p,r}(q)$ where $Q_{p,r}(q)$ is the product of all expressions of the left hand columns (or the right hand column) after (i), (ii), (iii) have taken place, i.e.,

$$Q_{p,r}(q) = \frac{f_p(q) f_r(q^p)}{\prod_i f_{v_{p,r,i},r}(q)^{s_{r,i}(1-\delta_{p,i})} f_{v_{p,r,i},p}(q)^{s_{p,i}(1-\delta_{r,i})}}$$

$$= \frac{f_r(q) f_p(q^r)}{\prod_i f_{v_{p,r,i},r}(q)^{s_{r,i}(1-\delta_{p,i})} f_{v_{p,r,i},p}(q)^{s_{p,i}(1-\delta_{r,i})}}.$$

Remark 3.3. (1) An EFE(1) with respect to p and r can be transformed into its reduced form by dividing both polynomials $f_p(q) f_r(q^p)$ and $f_r(q) f_p(q^r)$ by $\prod_i f_{v_{p,r,i},r}(q)^{s_{r,i}(1-\delta_{p,i})} f_{v_{p,r,i},p}(q)^{s_{p,i}(1-\delta_{r,i})}$; (2) The product of all the rational expressions in the left hand column and the product of those in the right hand column of the reduced form of the EFE(1) are equal, and thus can be denoted by the same polynomial $Q_{p,r}(q)$; (3) For each line (i), the product of all expressions on both sides of $\longleftrightarrow$ remains equal after (i), (ii) or (iii) have taken place. It is shown in [4] that all the rational

expressions above are actually polynomials when they occur, and that for each of these rational expressions, its roots are primitive roots of unity of the same order.

Definition 3.4. Let $\square$ denote either p or r and $\triangle$ denote the other. The polynomial $f_{v_{p,r,m},\square}(q) \neq 1$ is said to be **directly related** to the polynomial $f_{v_{p,r,n},\triangle}(q) \neq 1$ for some $n \neq m$ if $f_{v_{p,r,m},\square}(q) = f_{v_{p,r,n},\triangle}(q)$ and

$$f_{v_{p,r,m},\square}(q)\frac{f_{v_{p,r,l},\triangle}(q^{\square})^{s_{\triangle,l}}}{f_{v_{p,r,l},\triangle}(q)^{s_{\triangle,l}(1-\delta_{\square,l})}} \neq f_{v_{p,r,n},\triangle}(q)\frac{f_{v_{p,r,l},\square}(q^{\triangle})^{s_{\square,l}}}{f_{v_{p,r,l},\square}(q^{\triangle})^{s_{\square,l}(1-\delta_{\triangle,l})}}$$

for for all $l > m, n$ such that $v_{p,r,m}\square = v_{p,r,l}\triangle\square$. The polynomial $f_{v_{p,r,m},\square}(q) \neq 1$ is said to **semi-directly related** to $f_{v_{p,r,n},\square}(q) \neq 1$ (or vice versa) if

$$f_{v_{p,r,m},\square}(q)\frac{f_{v_{p,r,n},\triangle}(q^{\square})^{s_{\triangle,n}}}{f_{v_{p,r,n},\triangle}(q)^{s_{\triangle,n}(1-\delta_{\square,n})}} = \frac{f_{v_{p,r,n},\square}(q^{\triangle})}{f_{v_{p,r,n},\square}(q^{\triangle})^{(1-\delta_{\triangle,n})}}.$$

Suppose either $f_{v_{p,r,m},\square}(q)$ or $f_{v_{p,r,n},\triangle}(q)$ is nontrivial such that $v_{p,r,m}\square = v_{p,r,n}\triangle$ and

$$f_{v_{p,r,m},\square}(q)\frac{f_{v_{p,r,l},\triangle}(q^{\square})^{s_{\triangle,l}}}{f_{v_{p,r,l},\triangle}(q)^{s_{\triangle,l}(1-\delta_{\square,l})}} = f_{v_{p,r,n},\triangle}(q)\frac{f_{v_{p,r,l},\square}(q^{\triangle})^{s_{\square,l}}}{f_{v_{p,r,l},\square}(q^{\triangle})^{s_{\square,l}(1-\delta_{\triangle,l})}}$$

for some bi-levels $l > n, m$. Then $f_{v_{p,r,m},\square}(q)$ is said to be **indirectly related** to the ordered pair of polynomials $(f_{v_{p,r,n},\triangle}(q), f_{v_{p,r,l},\square}(q))$ (or $f_{v_{p,r,n},\triangle}(q)$ is **indirectly related** to the ordered pair $(f_{v_{p,r,m},\square}(q), f_{v_{p,r,l},\square}(q))$).

If two (or three in the case of indirect relation) polynomials satisfy one of the related relations above, we refer to the levels, namely $v_{p,r,m}$ and $v_{p,r,n}$ (and $v_{p,r,l}$ if applicable), of the polynomials involved as the **related levels** or as being **related**. Similarly, we also refer to these polynomials or the lines of EFE(1) containing the polynomials involved in such relations as being related polynomials or related lines respectively.

Now, let us construct a sequence of polynomials satisfying Functional Equation (2) with field of coefficients strictly containing $\mathbb{Q}$ and with P as its support base. Let $P = \{p, r\}$ and suppose that $p < r$. Let us suppose that there exists a sequence of polynomials Γ satisfying Functional Equation (2) with support containing p and r and field of coefficients strictly containing $\mathbb{Q}$. Then elements of Γ cannot be generated by quantum integers by Theorem 1.9. Let $f_p(q)$ and $f_r(q)$ be the polynomials in Γ corresponding to p and r. Let us suppose further that 1 is the highest power of p and r dividing $v_{p,r,1}$ where $v_{p,r,1}$ is the integer appearing in line (1) of EFE(1) with respect to p and r.

Proposition 3.5. *(Key Proposition 1)*

The reduced form of EFE(1) with respect to p and r has the form

$$\begin{array}{ccc} f_{v_{p,r,1},p}(q)f_{v_{p,r,1},r}(q^p) & \overset{(1)}{\leftrightarrow} & f_{v_{p,r,1},r}(q)f_{v_{p,r,1},p}(q^r) \\ \cdots & \cdots & \cdots \end{array}$$

$$
\begin{array}{ccc}
f_{v_{p,r,d_1},p}(q)^{s_{p,d_1}\delta_{r,d_1}}\frac{f_{v_{p,r,d_1},r}(q^p)^{s_{r,d_1}}}{f_{v_{p,r,d_1},r}(q)^{s_{r,d_1}(1-\delta_{p,d_1})}} & \overset{(d_1)}{\leftrightarrow} & f_{v_{p,r,d_1},r}(q)^{s_{r,d_1}\delta_{p,d_1}}\frac{f_{v_{p,r,d_1},p}(q^r)^{s_{p,d_1}}}{f_{v_{p,r,d_1},p}(q)^{s_{p,d_1}(1-\delta_{r,d_1})}} \\
\cdots & \cdots & \cdots \\
f_{\frac{v_{p,r,1}}{p},p}(q)^{s_{p,k_1}}\frac{f_{\frac{v_{p,r,1}}{p},r}(q^p)}{f_{\frac{v_{p,r,1}}{p},r}(q)} & \overset{(k_1)}{\leftrightarrow} & f_{\frac{v_{p,r,1}}{p},p}(q^r)^{s_{p,k_1}} \\
\cdots & \cdots & \cdots \\
f_{v_{p,r,d_2},p}(q)^{s_{p,d_r}\delta_{r,d_2}}\frac{f_{v_{p,r,d_2},r}(q^p)^{s_{r,d_2}}}{f_{v_{p,r,d_2},r}(q)^{s_{r,d_2}(1-\delta_{p,d_2})}} & \overset{(d_2)}{\leftrightarrow} & f_{v_{p,r,d_2},r}(q)^{s_{r,d_2}\delta_{p,d_2}}\frac{f_{v_{p,r,d_2},p}(q^r)^{s_{p,d_2}}}{f_{v_{p,r,d_2},p}(q)^{s_{p,d_2}(1-\delta_{r,d_2})}} \\
\cdots & \cdots & \cdots \\
f_{\frac{v_{p,r,1}p}{r},r}(q^p)^{s_{r,k_2}} & \overset{(k_2)}{\leftrightarrow} & f_{\frac{v_{p,r,1}p}{r},r}(q)^{s_{r,k_2}}\frac{f_{\frac{v_{p,r,1}p}{r},p}(q^r)^{s_{p,k_2}}}{f_{\frac{v_{p,r,1}p}{r},p}(q)^{s_{p,k_2}}} \\
\cdots & \cdots & \cdots \\
f_{v_{p,r,d_3},p}(q)^{s_{p,d_3}\delta_{r,d_3}}\frac{f_{v_{p,r,d_3},r}(q^p)^{s_{r,d_3}}}{f_{v_{p,r,d_3},r}(q)^{s_{r,d_3}(1-\delta_{p,d_3})}} & \overset{(d_3)}{\leftrightarrow} & f_{v_{p,r,d_3},r}(q)^{s_{r,d_3}\delta_{p,d_3}}\frac{f_{v_{p,r,d_3},p}(q^r)^{s_{p,d_3}}}{f_{v_{p,r,d_3},p}(q)^{s_{p,d_3}(1-\delta_{r,d_3})}} \\
\cdots & \cdots & \cdots \\
f_{\frac{v_{p,r,1}}{r},r}(q^p)^{s_{r,k_3}} & \overset{(k_3)}{\leftrightarrow} & f_{\frac{v_{p,r,1}}{r},r}(q)^{s_{r,k_3}}\frac{f_{\frac{v_{p,r,1}}{r},p}(q^r)^{s_{p,k_3}}}{f_{\frac{v_{p,r,1}}{r},p}(q)^{s_{p,k_3}}} \\
\cdots & \cdots & \cdots \\
f_{v_{p,r,d_4},p}(q)^{s_{p,d_4}\delta_{r,d_4}}\frac{f_{v_{p,r,d_4},r}(q^p)^{s_{r,d_4}}}{f_{v_{p,r,d_4},r}(q)^{s_{r,d_4}(1-\delta_{p,d_4})}} & \overset{(d_4)}{\leftrightarrow} & f_{v_{p,r,d_4},r}(q)^{s_{r,d_4}\delta_{p,d_4}}\frac{f_{v_{p,r,d_4},p}(q^r)^{s_{p,d_4}}}{f_{v_{p,r,d_4},p}(q)^{s_{p,d_4}(1-\delta_{r,d_4})}} \\
\cdots & \cdots & \cdots \\
\frac{f_{\frac{v_{p,r,1}}{rp},r}(q^p)^{s_{r,k_4}}}{f_{\frac{v_{p,r,1}}{rp},r}(q)^{s_{r,k_4}}} & \overset{(k_4)}{\leftrightarrow} & \frac{f_{\frac{v_{p,r,1}}{rp},p}(q^r)^{s_{p,k_4}}}{f_{\frac{v_{p,r,1}}{rp},p}(q)^{s_{p,k_4}}} \\
\cdots & \cdots & \cdots \\
f_{v_{p,r,d_5},p}(q)^{s_{p,d_5}\delta_{r,d_5}}\frac{f_{v_{p,r,d_5},r}(q^p)^{s_{r,d_5}}}{f_{v_{p,r,d_5},r}(q)^{s_{r,d_5}(1-\delta_{p,d_5})}} & \overset{(d_5)}{\leftrightarrow} & f_{v_{p,r,d_5},r}(q)^{s_{r,d_5}\delta_{p,d_5}}\frac{f_{v_{p,r,d_5},p}(q^r)^{s_{p,d_5}}}{f_{v_{p,r,d_5},p}(q)^{s_{p,d_5}(1-\delta_{r,d_5})}} \\
\cdots & \cdots & \cdots \\
Q_{p,r}(q) & = & Q_{p,r}(q)
\end{array}
$$

where:

- d_1 *(resp.* k_1*) is any bi-level of EFE*(1) *with respect to* p *and* r *such that* $v_{p,r,1} > v_{p,r,d_i} > \frac{v_{p,r,1}}{p}$ *(resp.* $v_{p,r,k_1} = \frac{v_{p,r,1}}{p}$*).*
- d_2 *(resp.* k_2*) is any bi-level of EFE*(1) *with respect to* p *and* r *such that* $\frac{v_{p,r,1}}{p} > v_{p,r,d_2} > \frac{v_{p,r,1}p}{r}$ *(resp.* $v_{p,r,k_2} = \frac{v_{p,r,1}p}{r}$*).*
- d_3 *(resp.* k_3*) is any bi-level of EFE*(1) *with respect to* p *and* r *such that* $\frac{v_{p,r,1}p}{r} > v_{p,r,d_3} > \frac{v_{p,r,1}}{r}$ *(resp.* $v_{p,r,k_3} = \frac{v_{p,r,1}}{r}$*).*
- d_4 *(resp.* k_4*) is any bi-level of EFE*(1) *with respect to* p *and* r *such that* $\frac{v_{p,r,1}}{r} > v_{p,r,d_3} > \frac{v_{p,r,1}}{pr}$ *(resp.* $v_{p,r,k_4} = \frac{v_{p,r,1}}{pr}$*).*
- d_5 *is any bi-level of EFE*(1) *with respect to* p *and* r *such that* $\frac{v_{p,r,1}}{pr} > v_{p,r,d_5}$*.*
- *All the rational expressions above are polynomials.*

Proof. First of all, all the rational expressions appearing in EFE(1) with respect to p and r are polynomials by Key Proposition $1'$ of [4]. Secondly, there is nothing to prove about the forms of lines (d_1), (d_2), (d_3), (d_4) and (d_5) since they are just the general form of any line in EFE(1) with respect to any two primes, namely p and r in this case. We only need to prove that lines (1), (k_1), (k_2), (k_3) and (k_4) take the forms as above.

Since the field of coefficients of Γ strictly contains $\mathbb{Q}$ by assumption, it can be verified that $f_p(q)$ and $f_r(q)$ are nontrivial polynomials ([4]). As a result, $f_{v_{p,r,1},p}(q)$ and $f_{v_{p,r,1},r}(q)$ are nontrivial, or equivalently $s_{p,1} = s_{r,1} = 1$. In addition, $\delta_{r,1} = \delta_{p,1} = 1$ since both p and r divide $v_{p,r,1}$ by assumption. Therefore, line (1) takes on such form.

Since $p < r$ by assumption, it can be verified that $f_{v_{p,r,1},r}(q)$ must be semi-directly related to $f_{v_{p,r,i},r}(q)$ for some bi-level i, i.e.,

$$\frac{f_{v_{p,r,i},r}(q^p)^{s_{r,i}}}{f_{v_{p,r,i},r}(q)^{s_{r,i}(1-\delta_{p,i})}} = f_{v_{p,r,1},r}(q)\frac{f_{v_{p,r,i},p}(q^r)^{s_{p,i}}}{f_{v_{p,r,i},p}(q)^{s_{p,i}(1-\delta_{r,i})}}.$$

Hence $v_{p,r,i} = \frac{v_{p,r,1}}{p}$ and thus $\delta_{p,i} = 0$ since p is the highest power of p dividing $v_{p,r,1}$ by assumption. Moreover, $f_{v_{p,r,1},r}(q) \neq 1$ implies that $\frac{f_{v_{p,r,i},r}(q^p)^{s_{r,i}}}{f_{v_{p,r,i},r}(q)^{s_{r,i}(1-\delta_{p,i})}} \neq 1$. Hence $s_{r,i} = 1$. Therefore

$$\frac{f_{v_{p,r,i},r}(q^p)^{s_{r,i}}}{f_{v_{p,r,i},r}(q)^{s_{r,i}(1-\delta_{p,i})}} = \frac{f_{\frac{v_{p,r,1}}{p},r}(q^p)}{f_{\frac{v_{p,r,1}}{p},r}(q)}.$$

On the other hand, r divides $v_{p,r,1}$ and thus $\frac{v_{p,r,1}}{p}$. Hence $\delta_{r,i} = 1$. Therefore, line (k_1) takes the form above.

As $p < r$, it can be verified that there are three possibilities:

(a) $f_{v_{p,r,1},p}(q)$ is directly related to $f_{v_{p,r,i},r}(q)$ for some bi-level i, i.e.,

$$f_{v_{p,r,1},p}(q) = f_{v_{p,r,i},r}(q)^{s_{r,i}}$$

for some bi-level i.

(b) $f_{v_{p,r,1},p}(q)$ is semi-directly related to $f_{v_{p,r,j},p}(q)$, i.e.,

$$f_{v_{p,r,1},p}(q)\frac{f_{v_{p,r,j},r}(q^p)^{s_{r,j}}}{f_{v_{p,r,j},r}(q)^{s_{r,j}(1-\delta_{p,j})}} = \frac{f_{v_{p,r,j},p}(q^r)^{s_{p,j}}}{f_{v_{p,r,j},p}(q)^{s_{p,j}(1-\delta_{r,j})}}.$$

(c) $f_{v_{p,r,1},p}(q)$ is indirectly related to the ordered pair $(f_{v_{p,r,i},r}(q), f_{v_{p,r,j},p}(q))$ of polynomials, i.e.,

$$f_{v_{p,r,1},p}(q)\frac{f_{v_{p,r,j},r}(q^p)^{s_{r,j}}}{f_{v_{p,r,j},r}(q)^{s_{r,j}(1-\delta_{p,j})}} = f_{v_{p,r,i},r}(q)^{s_{r,l}}\frac{f_{v_{p,r,j},p}(q^r)^{s_{p,j}}}{f_{v_{p,r,j},p}(q)^{s_{p,j}(1-\delta_{r,j})}}.$$

It can be verified from (a), (b) and (c) that $v_{p,r,i} = \frac{v_{p,r,1}p}{r}$ and $v_{p,r,j} = \frac{v_{p,r,1}}{r}$. Moreover, it can be verified that r does not divide $\frac{v_{p,r,1}p}{r}$ and $\frac{v_{p,r,1}}{r}$ while p divide $\frac{v_{p,r,1}p}{r}$ and $\frac{v_{p,r,1}}{r}$. As a result,

$$\delta_{r,k_2} = 0 = \delta_{r,k_3},$$

$$\delta_{p,k_2} = 1 = \delta_{p,k_3}.$$

Therefore, lines (k_2) and (k_3) have such forms.

Again since $p < r$, it can be verified that there are three possibilities:
(a) $f_{\frac{v_{p,r,1}}{p},p}(q)^{s_{p,k_1}}$ is directly related to $f_{v_{p,r,i},r}(q)^{s_{r,i}}$ for some bi-level i, i.e.,

$$f_{\frac{v_{p,r,1}}{p},p}(q)^{s_{p,k_1}} = f_{v_{p,r,i},r}(q)^{s_{r,i}}.$$

(b) $f_{\frac{v_{p,r,1}}{p},p}(q)^{s_{p,k_1}}$ is semi-directly related to $f_{v_{p,r,j},p}(q)^{s_{p,j}}$, i.e.,

$$f_{\frac{v_{p,r,1}}{p},p}(q)^{s_{p,k_1}} \frac{f_{v_{p,r,j},r}(q^p)^{s_{r,j}}}{f_{v_{p,r,j},r}(q)^{s_{r,j}(1-\delta_{p,j})}} = \frac{f_{v_{p,r,j},p}(q^r)^{s_{p,j}}}{f_{v_{p,r,j},p}(q)^{s_{p,j}(1-\delta_{r,j})}}$$

(c) $f_{\frac{v_{p,r,1}}{p},p}(q)^{s_{p,k_1}}$ is indirectly related to the ordered pair $(f_{v_{p,r,i},r}(q)^{s_{r,i}}, f_{v_{p,r,j},p}(q)^{s_{p,j}})$, i.e.,

$$f_{\frac{v_{p,r,1}}{p},p}(q)^{s_{p,k_1}} \frac{f_{v_{p,r,j},r}(q^p)^{s_{r,j}}}{f_{v_{p,r,j},r}(q)^{s_{r,j}(1-\delta_{p,j})}} = f_{v_{p,r,i},r}(q)^{s_{p,l}} \frac{f_{v_{p,r,j},p}(q^r)^{s_{p,j}}}{f_{v_{p,r,j},p}(q)^{s_{p,j}(1-\delta_{r,j})}}.$$

It can be verified from (a), (b) and (c), $v_{p,r,i} = \frac{v_{p,r,1}}{r}$ and $v_{p,r,j} = \frac{v_{p,r,1}}{pr}$. Also, since p does not divide $\frac{v_{p,r,1}}{pr}$ while r does not divide $\frac{v_{p,r,1}}{pr}$,

$$\delta_{p,k_4} = 0 = \delta_{r,k_4}.$$

As a result, line (k_4) takes on such form. Therefore, the result follows. □

Let us construct a sequence, also denoted by Γ, satisfying Functional Equation (2) with field of coefficients strictly containing $\mathbb{Q}$ and $P = \{p, r \mid p < r\}$ as its support base, using the Key Proposition 1 above. This construction is partitioned into several steps.

Step 1: Define

$$v_{p,r,1} := u = pr.$$

Then $u > 2$ and 1 is the highest power of p and r dividing $v_{p,r,1}$ as required in the hypothesis of Key Proposition 1. Since $p < r$, r is an odd prime. Let $\mathcal{A}_p$ be a $(\mathbb{Z}/p\mathbb{Z})^*$ and $\mathcal{A}_r$ is a nonempty proper subset of $(\mathbb{Z}/r\mathbb{Z})^*$. Then

$$\mathcal{A}_p \times \mathcal{A}_r := \mathcal{A}_{pr} < (\mathbb{Z}/p\mathbb{Z})^* \times (\mathbb{Z}/r\mathbb{Z})^* \cong (\mathbb{Z}/pr\mathbb{Z})^*.$$

Step 2: Extract lines (1), (k_1), (k_2), (k_3) and (k_4), i.e., those lines which are known to take on some particular forms and which we call the **optimal lines**, from EFE(1) with respect to p and r in Key Proposition 1 above:

$$\begin{array}{ccc} f_{v_{p,r,1},p}(q) f_{v_{p,r,1},r}(q^p) & \overset{(1)}{\leftrightarrow} & f_{v_{p,r,1},r}(q) f_{v_{p,r,1},p}(q^r) \\ \cdots & \cdots & \cdots \\ f_{\frac{v_{p,r,1}}{p},p}(q)^{s_{p,k_1}} \frac{f_{\frac{v_{p,r,1}}{p},r}(q^p)}{f_{\frac{v_{p,r,1}}{p},r}(q)} & \overset{(k_1)}{\leftrightarrow} & f_{\frac{v_{p,r,1}}{p},p}(q^r)^{s_{p,k_1}} \\ \cdots & \cdots & \cdots \end{array}$$

$$
\begin{array}{ccc}
f_{\frac{v_{p,r,1}p}{r},r}(q^p)^{s_{r,k_2}} & \overset{(k_2)}{\leftrightarrow} & f_{\frac{v_{p,r,1}p}{r},r}(q)^{s_{r,k_2}} \frac{f_{\frac{v_{p,r,1}p}{r},p}(q^r)^{s_{p,k_2}}}{f_{\frac{v_{p,r,1}p}{r},p}(q)^{s_{p,k_2}}} \\
\cdots & \cdots & \cdots \\
f_{\frac{v_{p,r,1}}{r},r}(q^p)^{s_{r,k_3}} & \overset{(k_3)}{\leftrightarrow} & f_{\frac{v_{p,r,1}}{r},r}(q)^{s_{r,k_3}} \frac{f_{\frac{v_{p,r,1}}{r},p}(q^r)^{s_{p,k_3}}}{f_{\frac{v_{p,r,1}}{r},p}(q)^{s_{p,k_3}}} \\
\cdots & \cdots & \cdots \\
\frac{f_{\frac{v_{p,r,1}}{rp},r}(q^p)^{s_{r,k_4}}}{f_{\frac{v_{p,r,1}}{rp},r}(q)^{s_{r,k_4}}} & \overset{(k_4)}{\leftrightarrow} & \frac{f_{\frac{v_{p,r,1}}{rp},p}(q^r)^{s_{p,k_4}}}{f_{\frac{v_{p,r,1}}{rp},p}(q)^{s_{p,k_4}}} \\
\cdots & \cdots & \cdots
\end{array}
$$

For each $p_j \in P$, let $f_{u,p_j}(q)$ be a monic polynomial with nonzero constant term whose roots are primitive up_j-roots of unity represented, via the Chinese Remainder Theorem (see the proof of Key Proposition $1'$ of [4] for more details), by collection of tuples:

$$A(p_j) := \{(w_{p_j} + t(p_j), w_{p_i}) \mid 0 \leq t \leq p_j - 1, p_i \in P - \{p_j\}, w_{p_i} \in \mathcal{A}_{p_i}, w_{p_j} \in \mathcal{A}_{p_j}\}.$$

Remark 3.6. Recall from [2] and [4] that when we use the phrase *the collection of roots of a certain polynomial is represented by a collection of tuples, we mean there is a one to one correspondence between the collection of roots of that polynomial and the elements of such collection of tuples, via Chinese Remainder Theorem.*

Then $f_{u,p_n}(q)$ and $f_{u,p_m}(q)$ are super-compatible for any pair of primes p_n and p_m, and their coefficients are not properly contained in $\mathbb{Q}$. In particular, $f_{u,p}(q)$ and $f_{u,r}(q)$ are super-compatible and are not in $\mathbb{Q}[q]$. Moreover, it can be verified using super-compatibility (as in Key Proposition 1 and $1'$ of [4]) that

$$f_{u,r}(q^p) = f_{u,p}(q^r).$$

Step 3: (a) Let $f_{\frac{v_{p,r,1}}{p},r}(q) = P_{\frac{v_{p,r,1}}{p},r}(q)$ where $P_{\frac{v_{p,r,1}}{p},r}(q)$ is the cyclotomic polynomial with coefficients in $\mathbb{Q}$ and of order $\frac{v_{p,r,1}}{p}r$. Hence

$$\frac{f_{\frac{v_{p,r,1}}{p},r}(q^p)}{f_{\frac{v_{p,r,1}}{p},r}(q)} = P_{\frac{v_{p,r,1}}{p}p,r}(q) = P_{v_{p,r,1},r}(q)$$

where $P_{\frac{v_{p,r,1}}{p}p,r}(q)$ is the cyclotomic polynomial with coefficients in $\mathbb{Q}$ and of order $\frac{v_{p,r,1}}{p}pr = v_{p,r,1}r$.

Let $f_{\frac{v_{p,r,1}}{r},p}(q) = P_{\frac{v_{p,r,1}}{r},p}(q)$ where $P_{\frac{v_{p,r,1}}{r},p}(q)$ is the cyclotomic polynomial with coefficients in $\mathbb{Q}$ and of order $\frac{v_{p,r,1}}{r}p$. Thus

$$\frac{f_{\frac{v_{p,r,1}}{r},p}(q^r)}{f_{\frac{v_{p,r,1}}{r},p}(q)} = P_{\frac{v_{p,r,1}}{r}r,p}(q) = P_{v_{p,r,1},p}(q)$$

where $P_{\frac{v_{p,r,1}}{r}r,p}(q)$ is the cyclotomic polynomial with coefficients in $\mathbb{Q}$ and of order $\frac{v_{p,r,1}}{r}rp = v_{p,r,1}p$.

Let $f_{\frac{v_{p,r,1}}{rp},r}(q) = P_{\frac{v_{p,r,1}}{rp},r}(q)$ and $f_{\frac{v_{p,r,1}}{rp},p}(q) = P_{\frac{v_{p,r,1}}{rp},p}(q)$, where $P_{\frac{v_{p,r,1}}{rp},r}(q)$ (resp. $P_{\frac{v_{p,r,1}}{rp},p}(q)$)

is the cyclotomic polynomial with coefficients in $\mathbb{Q}$ of order $\frac{v_{p,r,1}}{rp}r = \frac{v_{p,r,1}}{p}$ (resp. $\frac{v_{p,r,1}}{rp}p = \frac{v_{p,r,1}}{r}$). Therefor

e

$$\frac{f_{\frac{v_{p,r,1}}{rp},r}(q^p)}{f_{\frac{v_{p,r,1}}{rp},r}(q)} = P_{\frac{v_{p,r,1}}{rp}p,r}(q) = P_{\frac{v_{p,r,1}}{r},r}(q) = P_{\frac{v_{p,r,1}}{p},p}(q) = P_{\frac{v_{p,r,1}}{rp}r,p}(q) = \frac{f_{\frac{v_{p,r,1}}{rp},p}(q^r)}{f_{\frac{v_{p,r,1}}{rp},p}(q)}$$

where

$$P_{\frac{v_{p,r,1}}{rp}p,r}(q) = P_{\frac{v_{p,r,1}}{r},r}(q) = P_{\frac{v_{p,r,1}}{p},p}(q) = P_{\frac{v_{p,r,1}}{rp}r,p}(q)$$

is the cyclotomic polynomial with coefficients in $\mathbb{Q}$ of order $v_{p,r,1}$.

(b) Choose $s_{p,i}$'s and $s_{r,i}$'s appearing in the optimal lines above.

As $\frac{f_{\frac{v_{p,r,1}}{p},r}(q^p)}{f_{\frac{v_{p,r,1}}{p},r}(q)} = P_{v_{p,r,1},r}(q) \in \mathbb{Q}[q]$ in (a), it follows that the only choice possible for s_{p,k_1} is $s_{p,k_1} = 1$ since

$$P_{v_{p,r,1},r}(q) = \frac{f_{\frac{v_{p,r,1}}{p},r}(q^p)}{f_{\frac{v_{p,r,1}}{p},r}(q)} = f_{v_{p,r,1},r}(q) f_{\frac{v_{p,r,1}}{p},p}(q^r)^{s_{p,k_1}},$$

and $f_{v_{p,r,1},r}(q)$ is not in $\mathbb{Q}[q]$ by construction.

Let $s_{r,k_2} = 0 = s_{p,k_2}$ and $s_{r,k_3} = 1 = s_{p,k_3}$. Then

$$f_{v_{p,r,1},p}(q) f_{\frac{v_{p,r,1}}{r},r}(q^p) = \frac{f_{\frac{v_{p,r,1}}{r},p}(q^r)}{f_{\frac{v_{p,r,1}}{r},p}(q)} = P_{v_{p,r,1},p}(q).$$

Let $s_{r,k_4} = 0 = s_{p,k_4}$. Then with $s_{p,i}$ and $s_{r,i}$ for $i = 1, 2, 3$ chosen as above, the following must hold

$$f_{\frac{v_{p,r,1}}{p},p}(q) = f_{\frac{v_{p,r,1}}{r},r}(q).$$

Step 4: Let $1 := k_0$ and $K := \{k_0, k_1, k_2, k_3, k_4\}$. Define

$$f_p(q) = \prod_{i \in K} f_{v_{p,r,i},p}(q)^{s_{p,i}}$$

and

$$f_r(q) = \prod_{i \in K} f_{v_{p,r,i},r}(q)^{s_{r,i}}$$

where $s_{p,i}$ and $s_{r,i}$ for $i = 1, \ldots, 4$ are chosen as in Step 3.

Proposition 3.7. *(Key Proposition 2) The choices made in Step 3 are possible and the polynomials $f_p(q)$ and $f_r(q)$, constructed in Step 4 above, satisfy Functional Equation* (1).

Proof. To prove that the choice

$$f_{\frac{v_{p,r,1}}{p},r}(q) := P_{\frac{v_{p,r,1}}{p},r}(q)$$

is possible, it is sufficient for us to verify that

$$\frac{f_{\frac{v_{p,r,1}}{p},r}(q^p)}{f_{\frac{v_{p,r,1}}{p},r}(q)f_{v_{p,r,1},r}(q)} = g(q^r)$$

for some monic polynomial $g(q)$ with nonzero constant term since

$$\frac{f_{\frac{v_{p,r,1}}{p},r}(q^p)}{f_{\frac{v_{p,r,1}}{p},r}(q)} = f_{v_{p,r,1},r}(q)f_{\frac{v_{p,r,1}}{p},p}(q^r)^{s_{p,k_1}}.$$

With our choice of $f_{\frac{v_{p,r,1}}{p},r}(q)$,

$$P_{v_{p,r,1},r}(q) = \frac{f_{\frac{v_{p,r,1}}{p},r}(q^p)}{f_{\frac{v_{p,r,1}}{p},r}(q)}.$$

Therefore, the set of roots of $\frac{f_{\frac{v_{p,r,1}}{p},r}(q^p)}{f_{\frac{v_{p,r,1}}{p},r}(q)}$ can be represented the collection of tuples

$$A_r := \{(w_r + t(r), w_p) \mid 0 \leq t \leq r-1, w_r \in (\mathbb{Z}/r\mathbb{Z})^*, w_p \in (\mathbb{Z}/p\mathbb{Z})^*\}.$$

As the collection of roots of $f_{v_{p,r,1},r}(q)$ is presented by $A(r)$ (see definition in Step 2), the collection of root of

$$\frac{f_{\frac{v_{p,r,1}}{p},r}(q^p)}{f_{\frac{v_{p,r,1}}{p},r}(q)f_{v_{p,r,1},r}(q)}$$

can be represented by the collection of tuples

$$B(r) := \{(w_r + t(r), w_p) \mid 0 \leq t \leq r-1, w_p \in \mathcal{B}_p, w_r \in \mathcal{B}_r\}$$

where $\mathcal{B}_p = (\mathbb{Z}/p\mathbb{Z})^*$ and $\mathcal{B}_r = (\mathbb{Z}/r\mathbb{Z})^* - \mathcal{A}_r$. Let $g(q)$ be a monic polynomial who roots are primitive $v_{p,r,1}$-roots of unity represented by the collection of tuples

$$\{(w_r, w_p) \mid w_p \in \mathcal{B}_p, w_r \in \mathcal{B}_r\}.$$

Then it can be verified ([2], [4]) that $B(r)$ represents the collection of roots of $g(q^r)$. As a result, we may define

$$f_{\frac{v_{p,r,1}}{p},p}(q) := g(q).$$

Next, let us prove that if

$$f_{\frac{v_{p,r,1}}{r},p}(q) = P_{\frac{v_{p,r,1}}{r},p}(q),$$

then the choices $s_{r,k_2} = 0$ and $s_{p,k_3} = 1 = s_{r,k_3}$ make sense. As

$$f_{v_{p,r,1},p}(q)f_{\frac{v_{p,r,1}}{r},r}(q^p) = \frac{f_{\frac{v_{p,r,1}}{r},p}(q^r)}{f_{\frac{v_{p,r,1}}{r},p}(q)} = P_{v_{p,r,1},p}(q),$$

it is sufficient if we show that

$$\frac{f_{\frac{v_{p,r,1}}{r},p}(q^r)}{f_{\frac{v_{p,r,1}}{r},p}(q)f_{v_{p,r,1},p}(q)} = \frac{P_{v_{p,r,1},p}(q)}{f_{v_{p,r,1},p}(q)} = g(q^p)$$

for some polynomial $g(q)$. It can be verified that the collection of all roots of $P_{v_{p,r,1},p}(q)$ can be represented by the collection of tuples

$$A_p := \{(w_p + t(p), w_r) \mid 0 \leq t \leq p-1, w_p \in (\mathbb{Z}/p\mathbb{Z})^*, w_r \in (\mathbb{Z}/r\mathbb{Z})^*\}.$$

Hence the collection of roots of $\frac{P_{v_{p,r,1},p}(q)}{f_{v_{p,r,1},p}(q)}$ can be represented by the collection $A_p - A(p) = B(p)$ where

$$B(p) := \{(w_p + t(p), w_r) \mid 0 \leq t \leq p-1, w_r \in \mathcal{B}_r, w_p \in \mathcal{B}_p\}$$

where $\mathcal{B}_r = (\mathbb{Z}/r\mathbb{Z})^* - \mathcal{A}_r$ and $\mathcal{B}_p = (\mathbb{Z}/p\mathbb{Z})^*$. Let $g(q)$ be the monic polynomial whose roots can be represented by the collection of tuples

$$\{(w_p, w_r) \mid w_r \in \mathcal{B}_r, w_p \in \mathcal{B}_p\}.$$

As above, it can be verified that the collection of tuples $B(p)$ represents the collection of all roots of the polynomial $g(q^p)$. Therefore, we may define

$$f_{\frac{v_{p,r,1}}{r},r}(q) := g(q),$$

and the result follows.

Finally, with the choices of $s_{\square,k_i}$ for $i = 1, 2, 3$ made in Step 3, where $\square$ denotes either p or r, it follows that

$$f_{\frac{v_{p,r,1}}{p},p}(q)\frac{f_{\frac{v_{p,r,1}}{rp},r}(q^p)^{s_{r,k_4}}}{f_{\frac{v_{p,r,1}}{rp},r}(q)^{s_{r,k_4}}} = f_{\frac{v_{p,r,1}}{r},r}(q)\frac{f_{\frac{v_{p,r,1}}{rp},p}(q^r)^{s_{p,k_4}}}{f_{\frac{v_{p,r,1}}{rp},p}(q)^{s_{p,k_4}}}$$

Therefore, to show that the choices $s_{r,k_4} = 0 = s_{p,k_4}$ is possible, we must show that

$$f_{\frac{v_{p,r,1}}{p},p}(q) = f_{\frac{v_{p,r,1}}{r},r}(q).$$

This follows immediately from above since $f_{\frac{v_{p,r,1}}{p},p}(q)$ and $f_{\frac{v_{p,r,1}}{r},r}(q)$ are defined as monic polynomials whose roots are primitive $v_{p,r,1}$-roots of unity represented by the collection of tuples

$$\{(w_p, w_r) \mid w_r \in \mathcal{B}_r, w_p \in \mathcal{B}_p\}$$

and

$$\{(w_r, w_p) \mid w_p \in \mathcal{B}_p, w_r \in \mathcal{B}_r\}$$

respectively. The result follows since these two collections of tuples coincide.

By construction,

$$f_p(q) = f_{v_{p,r,1},p}(q) f_{v_{p,r,k_1},p}(q) f_{v_{p,r,k_3},p}(q)$$

and

$$f_r(q) = f_{v_{p,r,1},r}(q) f_{v_{p,r,k_1},r}(q) f_{v_{p,r,k_3},r}(q)$$

where

1. $f_{v_{p,r,1},r}(q^p) = f_{v_{p,r,1},p}(q^r)$.

2. $f_{v_{p,r,1},p}(q)f_{v_{p,r,k_3},p}(q)f_{v_{p,r,k_3},r}(q^p) = f_{v_{p,r,k_3},p}(q^r)$

3. $f_{v_{p,r,k_1},r}(q^p) = f_{v_{p,r,1},r}(q)f_{v_{p,r,k_1},r}(q)f_{v_{p,r,k_1},p}(q^r)$.

4. $f_{v_{p,r,k_1},p}(q) = f_{v_{p,r,k_3},r}(q)$.

It can be verified that the product of the polynomials on the left hand side of (1), (2), (3) and (4) (resp. the product of the polynomials on the right hand side of (1), (2), (3) and (4)) is equal to $f_p(q)f_r(q^p)$ (resp. $f_r(q)f_p(q^r)$). Therefore, the result follows.

□

As a result, the polynomials $f_p(q)$ and $f_r(q)$ induce a unique sequence Γ of polynomials satisfying Equation (2) with support base $\{p, r\}$ and with coefficients not properly contains in $\mathbb{Q}$. Therefore, Γ cannot be generated by quantum integers by Theorem 1.9.

(2) Now let us suppose that there exists an odd prime r such that r divides $p_j - 1$ for all p_j in P. There are two cases to consider:

(i) P contains 2: Let $u = 2r$. Then $u > 2$. Hence $|(\mathbb{Z}/u\mathbb{Z})^*| = |(\mathbb{Z}/2r\mathbb{Z})^*| > 1$. Therefore, there exists at least one nonempty proper subset, denoted by $\mathcal{A}_u$, of $(\mathbb{Z}/u\mathbb{Z})^* \cong (\mathbb{Z}/2\mathbb{Z})^* \times (\mathbb{Z}/r\mathbb{Z})^* \cong (\mathbb{Z}/r\mathbb{Z})^*$. Let $\mathcal{A}_r$ be the subset of $(\mathbb{Z}/r\mathbb{Z})^*$ such that

$$\mathcal{A}_u \cong \mathcal{A}_r.$$

Then $\mathcal{A}_r$ is a nonempty proper subset of $(\mathbb{Z}/r\mathbb{Z})^*$.

For each p_j in $P - \{2\}$, define

$$f_{p_j}(q) := f_{u,p_j}(q)f_{r,p_j}(q)$$

where:

1. $f_{u,p_j}(q)$ is a monic polynomial whose roots are primitive up_j-roots of unity represented by the collection of tuples

   $$\{(w_u, w_{p_j}) \mid w_u \in \mathcal{A}_u, w_{p_j} \in (\mathbb{Z}/p_j\mathbb{Z})^*\}.$$

   Hence $f_{u,p_j}(q)$ is a nontrivial monic polynomial whose coefficients are not properly contained in $\mathbb{Q}$.

2. $f_{r,p_j}(q) = P_{r,p_j}(q)$ is the cyclotomic polynomial of order rp_j, i.e., the irreducible (in $\mathbb{Q}[q]$) monic polynomial with coefficient in $\mathbb{Q}$ whose roots are all primitive rp_j-roots of unity. Hence roots of $f_{r,p_j}(q)$ are represented by the collection of tuples

   $$\{(w_r, w_{p_j}) \mid w_r \in (\mathbb{Z}/r\mathbb{Z})^*, w_{p_j} \in (\mathbb{Z}/p_j\mathbb{Z})^*\}.$$

Define

$$f_2(q) := f_{u,2}(q) f_{r,2}(q)$$

where:

1. $f_{u,2}(q)$ is a monic polynomial whose roots are primitive $u2$-roots of unity represented by the collection of tuples

   $$\{(1 + t(2), w_r) \mid 0 \leq t \leq 1, w_r \in \mathcal{A}_r\}.$$

   Hence $f_{u,2}(q)$ is a nontrivial monic polynomial whose coefficients are not properly contained in $\mathbb{Q}$.

2. $f_{r,2}(q)$ is a monic polynomial whose roots are primitive $r2$-roots of unity represented by the collection

   $$\{w_u \mid w_u \in (\mathbb{Z}/u\mathbb{Z})^* - \mathcal{A}_u\} \cong \{w_r \mid w_r \in (\mathbb{Z}/r\mathbb{Z})^* - \mathcal{A}_r\}.$$

For each $p_j \in P$, $f_{p_j(q)}$ is a nontrivial polynomial whose coefficients are not properly contained in $\mathbb{Q}$ since $f_{u,p_j}(q)$ is a nontrivial monic polynomial whose coefficients are not properly contained in $\mathbb{Q}$. (see [4] for details). Let p_n and p_m be two primes in $P - \{r\}$. Since $p_n \equiv p_m \equiv 1 (\text{mod } r)$ by assumption, it follows that $p_n \equiv p_m \equiv 1 (\text{mod } 2r)$. Therefore

$$\frac{f_{u,p_n}(q^{p_m})}{f_{u,p_n}(q)}$$

and

$$\frac{f_{u,p_m}(q^{p_n})}{f_{u,p_m}(q)}$$

are monic polynomials as a result of Key Proposition 1 and $1'$ of [4], whose roots are represented by the collection of tuples

$$\{(w_u, w_{p_n}, w_{p_m}) \mid w_u \in \mathcal{A}_u, w_{p_n} \in (\mathbb{Z}/p_n\mathbb{Z})^*, w_{p_m} \in (\mathbb{Z}/p_m\mathbb{Z})^*\}$$

and

$$\{(w_u, w_{p_m}, w_{p_n}) \mid w_u \in \mathcal{A}_u, w_{p_m} \in (\mathbb{Z}/p_m\mathbb{Z})^*, w_{p_n} \in (\mathbb{Z}/p_n\mathbb{Z})^*\}$$

respectively. These collections of tuples coincide. As a result,

$$\frac{f_{u,p_n}(q^{p_m})}{f_{u,p_n}(q)} = \frac{f_{u,p_m}(q^{p_n})}{f_{u,p_m}(q)},$$

or equivalently,

$$f_{u,p_m}(q) f_{u,p_n}(q^{p_m}) = f_{u,p_n}(q) f_{u,p_m}(q^{p_n}).$$

Since $f_{r,p_n}(q) = P_{r,p_n}(q)$ and $f_{r,p_m}(q) = P_{r,p_m}(q)$ respectively, it is straightforward to verify that

$$\frac{f_{r,p_n}(q^{p_m})}{f_{r,p_n}(q)} = \frac{P_{r,p_n}(q^{p_m})}{P_{r,p_n}(q)} = P_{rp_np_m}(q) = \frac{P_{r,p_m}(q^{p_n})}{P_{r,p_m}(q)} = \frac{f_{r,p_m}(q^{p_n})}{f_{r,p_m}(q)},$$

where $P_{rp_np_m}(q)$ is the cyclotomic polynomial with coefficients in $\mathbb{Q}$ and order rp_np_m. Therefore,

$$f_{r,p_m}(q)f_{r,p_n}(q^{p_m}) = f_{r,p_n}(q)f_{r,p_m}(q^{p_n}).$$

As a result,

$$f_{p_n}(q)f_{p_m}(q^{p_n}) = f_{p_m}(q)f_{p_n}(q^{p_m}),$$

i.e., $f_{p_n}(q)$ and $f_{p_m}(q)$ satisfy Functional Equation (1).

Next, let p be any odd prime in P. Let $f_p(q)$ be defined as above. Since $p \equiv 1(\text{mod } r)$ by assumption, $p \equiv 1(\text{mod } u)$. Hence

$$\frac{f_{u,2}(q^p)}{f_{u,2}(q)}$$

is a monic polynomial whose roots are primitive $u2p$-roots of unity. It can be verified from the collection of tuples of integers representing the roots of $f_{u,2}(q)$ stated earlier that the set of roots of $\frac{f_{u,2}(q^p)}{f_{u,2}(q)}$ consists of primitive $u2p$-roots of unity represented by the collection of tuples

$$\{(1 + t(2), w_r, w_p) \mid 0 \leq t \leq 1, w_r \in \mathcal{A}_r, w_p \in (\mathbb{Z}/p\mathbb{Z})^*\}.$$

By replacing either p_n (or p_m) by p in $f_{p_n}(q)$ (or $f_{p_m}(q)$) above, the collection of roots of $f_{u,p}(q)$ can be represented by the collection

$$\{(w_u, w_p) \mid w_u \in \mathcal{A}_u, w_p \in (\mathbb{Z}/p\mathbb{Z})^*\}.$$

It can be verified that roots of $f_{u,p}(q^2)$ are primitive $up2$-roots of unity represented by the collection of tuples

$$\{(1 + t(2), w_r, w_p) \mid 0 \leq t \leq 1, w_r \in \mathcal{A}_r, w_p \in (\mathbb{Z}/p\mathbb{Z})^*.$$

Hence,

$$f_{u,p}(q^2) = \frac{f_{u,2}(q^p)}{f_{u,2}(q)}$$

or equivalently,

$$f_{u,2}(q)f_{u,p}(q^2) = f_{u,2}(q^p).$$

As $\mathcal{A}_r$ is a nonempty proper subset of $(\mathbb{Z}/r\mathbb{Z})^*$ by construction, the coefficients of $f_{r,2}(q)$ are not properly contained in $\mathbb{Q}$. Then

$$\frac{f_{r,2}(q^p)}{f_{r,2}(q)}$$

is a monic polynomial, since $p \equiv 1(\text{mod } r)$ by assumption, whose roots are primitive $r2p$-roots

of unity. Its roots can be represented by the collection of tuples

$$\{(w_u, w_p) \mid w_u \in (\mathbb{Z}/u\mathbb{Z})^* - \mathcal{A}_u, w_p \in (\mathbb{Z}/p\mathbb{Z})^*\}.$$

Therefore, the collection of roots of the product of monic polynomials

$$f_{u,p}(q)\frac{f_{r,2}(q^p)}{f_{r,2}(q)}$$

is represented by

$$\{(w_u, w_p) \mid w_u \in (\mathbb{Z}/u\mathbb{Z})^* - \mathcal{A}_u, w_p \in (\mathbb{Z}/p\mathbb{Z})^*\}$$

$$\cup\{(w_u, w_p) \mid w_u \in \mathcal{A}_u, w_p \in (\mathbb{Z}/p\mathbb{Z})^*\} = \{(w_u, w_p) \mid w_u \in (\mathbb{Z}/u\mathbb{Z})^*, w_p \in (\mathbb{Z}/p\mathbb{Z})^*\}.$$

As $f_{r,p}(q) := P_{r,p}(q)$ by construction,

$$\frac{f_{r,p}(q^2)}{f_{r,p}(q)} = \frac{P_{r,p}(q^2)}{P_{r,p}(q)} = P_{rp2}(q)$$

where $P_{rp2}(q)$ is the cyclotomic polynomial in $\mathbb{Q}[q]$ of order $rp2$. Hence its roots are primitive $rp2 = up$-roots of unity represented by the collection of tuples

$$\{(w_u, w_p) \mid w_u \in (\mathbb{Z}/u\mathbb{Z})^*, w_p \in (\mathbb{Z}/p\mathbb{Z})^*\}.$$

As a result,

$$\frac{f_{r,p}(q^2)}{f_{r,p}(q)} = f_{u,p}(q)\frac{f_{r,2}(q^p)}{f_{r,2}(q)}.$$

Therefore,

$$f_{u,2}(q)f_{u,p}(q^2)\frac{f_{r,p}(q^2)}{f_{r,p}(q)} = f_{u,2}(q^p)f_{u,p}(q)\frac{f_{r,2}(q^p)}{f_{r,2}(q)},$$

or equivalently,

$$(f_{u,2}(q)f_{r,2}(q))(f_{u,p}(q^2)f_{r,p}(q^2)) = (f_{u,p}(q)f_{r,p}(q))(f_{u,2}(q^p)f_{r,2}(q^p)).$$

The last equality can be rewritten as

$$f_{u,2}(q)f_p(q^2) = f_p(q)f_2(q^p).$$

Therefore $f_{u,2}(q)$ and $f_{u,p}(q)$ satisfy Functional Equation (1) for any odd prime p in P. The collection of polynomials $\{f_s(q) \mid s \in P\}$, where $f_s(q)$ is defined above, induces a unique sequence Γ of polynomials satisfying Functional Equation (2) with support base P and field of coefficients strictly containing $\mathbb{Q}$ as desired.

(ii) P does not contain 2: Let $u = r$. Then $u > 2$ and thus $|(\mathbb{Z}/u\mathbb{Z})^*| = |(\mathbb{Z}/r\mathbb{Z})^*| > 1$. Let p_j be any prime in P and let $\mathcal{A}_r$ is a nonempty proper subset of $(\mathbb{Z}/r\mathbb{Z})^*$. Define

$$f_{p_j}(q) = f_{u,p_j}(q)$$

where $f_{u,p_j}(q)$ is a monic polynomial whose roots are primitive up_j-root of unity and are represented by the collection of ordered pairs

$$\{(w_r, w_{p_j}) \mid w_r \in \mathcal{A}_r, w_{p_j} \in (\mathbb{Z}/p_j\mathbb{Z})^*\}.$$

Let p_n and p_m be two arbitrary primes in P. Hence the coefficients of $f_{u,p_j}(q)$ are not properly contained in $\mathbb{Q}$ since $\mathcal{A}_r$ is a nonempty proper subset of $(\mathbb{Z}/r\mathbb{Z})^*$. As $p_n \equiv p_m \equiv 1(\text{mod } r)$ by assumption, it follows from Key Proposition 1 and $1'$ of [4] that

$$\frac{f_{u,p_m}(q^{p_n})}{f_{u,p_m}(q)}$$

and

$$\frac{f_{u,p_n}(q^{p_m})}{f_{u,p_n}(q)}$$

are monic polynomials whose roots are primitive up_np_m-roots of unity represented by the collection of tuples

$$\{(w_r, w_{p_m}, w_{p_n}) \mid w_r \in \mathcal{A}_r, w_{p_m} \in (\mathbb{Z}/p_m\mathbb{Z})^*, w_{p_n} \in (\mathbb{Z}/p_n\mathbb{Z})^*\}$$

and

$$\{(w_r, w_{p_n}, w_{p_m}) \mid w_r \in \mathcal{A}_r, w_{p_n} \in (\mathbb{Z}/p_n\mathbb{Z})^*, w_{p_m} \in (\mathbb{Z}/p_m\mathbb{Z})^*\},$$

respectively. These two collection are identical. As as result,

$$\frac{f_{u,p_m}(q^{p_n})}{f_{u,p_m}(q)} = \frac{f_{u,p_n}(q^{p_m})}{f_{u,p_n}(q)}$$

or equivalently,

$$f_{u,p_n}(q)f_{u,p_m}(q^{p_n}) = f_{u,p_m}(q)f_{u,p_n}(q^{p_m}).$$

Therefore,

$$f_{p_n}(q)f_{p_m}(q^{p_n}) = f_{p_m}(q)f_{p_n}(q^{p_m}),$$

i.e., $f_{p_n}(q)$ and $f_{p_m}(q)$ satisfy Functional Equation (1). From this point, the result follows as in part (i) above.

(3) Next, suppose that 4 divide $p-1$ for all odd prime $p \in P$. There are two cases:
(i) P contains 2: Let $u = 4$. Then

$$|(\mathbb{Z}/u\mathbb{Z})^*| > 1.$$

Hence we can choose a nonempty proper subset, denoted by $\mathcal{A}_u$, of $(\mathbb{Z}/u\mathbb{Z})^*$. Let p be an odd prime of P. Let $f_{u,p}(q)$ be a monic polynomial whose roots are primitive up-roots of unity represented by the collection of tuples

$$\{(w_u, w_p) \mid w_u \in \mathcal{A}_u, w_p \in (\mathbb{Z}/p\mathbb{Z})^*\}.$$

Hence the coefficients of $f_{u,p}(q)$ are not properly contained in $\mathbb{Q}$. Let $f_{2,p}(q)$ be the cyclotomic polynomial in $\mathbb{Q}[q]$ of order $2p$. Hence its roots are primitive $2p$-root of unity represented by the collection of tuples

$$\{(w_2, w_p) \mid w_2 \in (\mathbb{Z}/2\mathbb{Z})^*, w_p \in (\mathbb{Z}/p\mathbb{Z})^*\}.$$

Let $f_{1,p}(q) = P_p(q)^2$ where $P_p(q)$ is the cyclotomic polynomial in $\mathbb{Q}[q]$ of order p. Since roots of $P_p(q)$ are primitive p-roots of unity represented by the collection of tuples

$$\{w_p \mid w_p \in (\mathbb{Z}/p\mathbb{Z})^*\},$$

the collection of roots of $f_{1,p}(q)$ is represented by the collection

$$\{w_p \mid w_p \in (\mathbb{Z}/p\mathbb{Z})^*\} \sqcup \{w_p \mid w_p \in (\mathbb{Z}/p\mathbb{Z})^*\}$$

with $\sqcup$ denoting the union where multiplicity is counted. Define

$$f_p(q) := f_{u,p}(q) f_{2,p}(q) f_{1,p}(q).$$

Let $f_{u,2}(q)$ be the monic polynomial whose roots are primitive $2u$-roots of unity represented by the collection of tuples

$$\{(w_u + t(u)) \mid 0 \leq t \leq 1, w_u \in \mathcal{A}_u\}.$$

Thus its coefficients are also not contained in $\mathbb{Q}$. Let $f_{2,2}(q)$ be the monic polynomial whose roots are primitive u-roots of unity represented by the collection of tuples

$$\{w_u \mid w_u \in (\mathbb{Z}/u\mathbb{Z})^* - \mathcal{A}_u\}.$$

It can be verified, using the fact that $(\mathbb{Z}/u\mathbb{Z})^* - \mathcal{A}_u$ is a nonempty proper subset of $(\mathbb{Z}/u\mathbb{Z})^*$, that the coefficients of $f_{2,2}(q)$ are not properly contained in $\mathbb{Q}$. Let $f_{1,2}(q)$ be the cyclotomic polynomial in $\mathbb{Q}[q]$ of order 2. Hence its root is represented by

$$\{w_2 \in (\mathbb{Z}/2\mathbb{Z})^*\}.$$

Define

$$f_2(q) = f_{u,2}(q) f_{2,2}(q) f_{1,2}(q).$$

Since $p \equiv 1 (\text{mod } u)$ by assumption, it can be verified that

$$\frac{f_{u,2}(q^p)}{f_{u,2}(q)}$$

and

$$f_{u,p}(q^2)$$

are a monic polynomials whose roots are primitive $up2$-roots of unity represented by the same

collection of tuples

$$\{(w_u + t(u), w_p) \mid 0 \leq t \leq 1, w_u \in \mathcal{A}_u, w_p \in (\mathbb{Z}/p\mathbb{Z})^*\}.$$

Therefore,

$$f_{u,p}(q^2) = \frac{f_{u,2}(q^p)}{f_{u,2}(q)}.$$

Since $p \equiv 1 (\text{mod } u)$, $p \equiv 1 (\text{mod } 2)$. It follows that

$$\frac{f_{2,2}(q^p)}{f_{2,2}(q)}$$

is a monic polynomial whose roots are primitive up-roots of unity represented by the collection of tuples

$$\{(w_u, w_p) \mid w_u \in (\mathbb{Z}/u\mathbb{Z})^* - \mathcal{A}_u, w_p \in (\mathbb{Z}/p\mathbb{Z})^*\}.$$

Hence the roots of the product of monic polynomials

$$f_{u,p}(q)\frac{f_{2,2}(q^p)}{f_{2,2}(q)}$$

are represented by the collection of tuples

$$\{(w_u, w_p) \mid w_u \in \mathcal{A}_u, w_p \in (\mathbb{Z}/p\mathbb{Z})^*\}$$

$$\cup\{(w_u, w_p) \mid w_u \in (\mathbb{Z}/u\mathbb{Z})^* - \mathcal{A}_u, w_p \in (\mathbb{Z}/p\mathbb{Z})^*\} = \{(w_u, w_p) \mid w_u \in (\mathbb{Z}/u\mathbb{Z})^*, w_p \in (\mathbb{Z}/p\mathbb{Z})^*\}.$$

It can be verified that $f_{2,p}(q^2)$ is a monic polynomial whose roots are primitive up-roots of unity represented by the collection of tuples

$$\{((w_2 + t(2)), w_p) \mid 0 \leq t \leq 1, w_2 \in (\mathbb{Z}/2\mathbb{Z})^*, w_p \in (\mathbb{Z}/p\mathbb{Z})^*\}$$

$$\cong \{((w_u, w_p) \mid w_u \in (\mathbb{Z}/u\mathbb{Z})^*, w_p \in (\mathbb{Z}/p\mathbb{Z})^*\}.$$

As a result,

$$f_{2,p}(q^2) = f_{u,p}(q)\frac{f_{2,2}(q^p)}{f_{2,2}(q)}.$$

Since $f_{1,2}(q) = P_2(q)$, the cylotomic polynomial in $\mathbb{Q}[q]$ of order 2,

$$\frac{f_{1,2}(q^p)}{f_{1,2}(q)} = \frac{P_2(q^p)}{P_2(q)} = P_{2p}(q),$$

the cyclotomic polynomial in $\mathbb{Q}[q]$ of order $2p$. Hence its roots can be represented by the collection of tuples

$$\{((w_2, w_p) \mid w_2 \in (\mathbb{Z}/2\mathbb{Z})^*, w_p \in (\mathbb{Z}/p\mathbb{Z})^*\}.$$

Thus the product of monic polynomials

$$f_{2,p}(q)\frac{f_{1,2}(q^p)}{f_{1,2}(q)}$$

is a monic polynomial whose roots are primitive $2p$-roots of unity represented by the collection of tuples

$$\{(w_2, w_p) \mid w_2 \in (\mathbb{Z}/2\mathbb{Z})^*, w_p \in (\mathbb{Z}/p\mathbb{Z})^*\} \sqcup \{(w_2, w_p) \mid w_2 \in (\mathbb{Z}/2\mathbb{Z})^*, w_p \in (\mathbb{Z}/p\mathbb{Z})^*\}$$

with $\sqcup$ denoting the union where multiplicity is counted. Since roots of $P_p(q)$ are presented by the collection

$$\{w_p \mid w_p \in (\mathbb{Z}/p\mathbb{Z})^*\},$$

it can be verified that the union of sets above represents exactly the collection of roots of

$$\frac{f_{1,p}(q^2)}{f_{1,p}(q)} = \frac{(P_p(q^2))^2}{(P_p(q))^2} = (P_{2p}(q))^2,$$

where $P_{2p}(q))$ denotes the cyclotomic polynomial in $\mathbb{Q}[q]$ of order $2p$. Therefore,

$$\frac{f_{1,p}(q^2)}{f_{1,p}(q)} = f_{2,p}(q)\frac{f_{1,2}(q^p)}{f_{1,2}(q)}.$$

As a result,

$$f_{u,p}(q^2)f_{2,p}(q^2)\frac{f_{1,p}(q^2)}{f_{1,p}(q)} = \frac{f_{u,2}(q^p)}{f_{u,2}(q)}f_{u,p}(q)\frac{f_{2,2}(q^p)}{f_{2,2}(q)}f_{2,p}(q)\frac{f_{1,2}(q^p)}{f_{1,2}(q)},$$

or equivalently

$$\begin{aligned}&(f_{u,2}(q)f_{2,2}(q)f_{1,2}(q))(f_{u,p}(q^2)f_{2,p}(q^2)f_{1,p}(q^2))\\ &= (f_{u,p}(q)f_{2,p}(q)f_{1,p}(q))(f_{u,2}(q^p)f_{2,2}(q^p)f_{1,2}(q^p)).\end{aligned}$$

The last equality can be rewritten as

$$f_2(q)f_p(q^2) = f_p(q)f_2(q^p).$$

Thus $f_2(q)$ and $f_p(q)$ satisfy Functional Equation (1). They induce, by Theorem 1.5, a unique sequence of polynomials

$$\Gamma = \{f_n(q) \mid n \in \mathbb{N}\}$$

whose elements satisfy Functional Equation (2) with support base P and with field of coefficients strictly containing $\mathbb{Q}$.

(ii) P does not contain 2: Let $u = 4$. Let p_n and p_m be two primes in P. Let $\mathcal{A}_u$ be a nonempty proper subset of $(\mathbb{Z}/u\mathbb{Z})^*$. Let $f_{u,p_n}(q)$ and $f_{u,p_n}(q)$ be the monic polynomials whose roots are primitive up_n-roots of unity and up_m-roots of unity respectively and represented by the collection

of tuples

$$\{(w_u, w_{p_n}) \mid w_u \in \mathcal{A}_u, w_{p_n} \in (\mathbb{Z}/p_n\mathbb{Z})^*\}$$

and

$$\{(w_u, w_{p_m}) \mid w_u \in \mathcal{A}_u, w_{p_m} \in (\mathbb{Z}/p_m\mathbb{Z})^*\}$$

respectively. It can be verified that the coefficients of $f_{u,p_n}(q)$ and $f_{p_n}(q)$ are not properly contained in $\mathbb{Q}$. Since $p_n \equiv p_m \equiv 1 (\text{mod } u)$ by assumption,

$$\frac{f_{u,p_n}(q^{p_m})}{f_{u,p_n}(q)}$$

and

$$\frac{f_{u,p_m}(q^{p_n})}{f_{u,p_m}(q)}$$

are monic polynomials whose roots are primitive up_np_m-roots of unity represented by the collections of tuples

$$\{(w_u, w_{p_n}, w_{p_m}) \mid w_u \in \mathcal{A}_u, w_{p_n} \in (\mathbb{Z}/p_n\mathbb{Z})^*, w_{p_m} \in (\mathbb{Z}/p_n\mathbb{Z})^*\}$$

and

$$\{(w_u, w_{p_m}, w_{p_n}) \mid w_u \in \mathcal{A}_u, w_{p_m} \in (\mathbb{Z}/p_m\mathbb{Z})^*, w_{p_n} \in (\mathbb{Z}/p_n\mathbb{Z})^*\}.$$

Since these two collections of tuples are equal,

$$\frac{f_{u,p_n}(q^{p_m})}{f_{u,p_n}(q)} = \frac{f_{u,p_m}(q^{p_n})}{f_{u,p_m}(q)},$$

or equivalently,

$$f_{u,p_m}(q) f_{u,p_n}(q^{p_m}) = f_{u,p_n}(q) f_{u,p_m}(q^{p_n}).$$

Define $f_{p_n}(q) := f_{u,p_n}(q)$ and $f_{p_m}(q) := f_{u,p_m}(q)$. Then $f_{p_n}(q)$ and $f_{p_n}(q)$ satisfy Functional Equation (1). The rest of the argument follows as in (i) above.

(4) Finally, suppose that there exists an odd prime r in P such that r divides $p-1$ for all primes p in $P - \{r\}$. Since $r > 2$,

$$|(\mathbb{Z}/r\mathbb{Z})^*| > 1.$$

Hence there exists at least one nonempty proper subset, denoted by $\mathcal{A}_r$, of $(\mathbb{Z}/r\mathbb{Z})^*$. Let p be any prime in $P - \{r\}$. Let $f_{r,p}(q)$ be the monic polynomial whose roots are primitive rp-roots of unity represented by the collection of tuples

$$\{(w_r, w_p) \mid w_r \in \mathcal{A}_r, w_p \in (\mathbb{Z}/p\mathbb{Z})^*\}.$$

Hence the coefficients of $f_{r,p}(q)$ are not properly contained in $\mathbb{Q}$. Let $f_{1,p}(q) := P_p(q)$, the cyclotomic polynomial in $\mathbb{Q}[q]$ of order p. Hence roots of $f_{1,p}(q)$ are represented by the collection of tuples

$$\{w_p \mid w_p \in (\mathbb{Z}/p\mathbb{Z})^*\}.$$

Define

$$f_p(q) := f_{r,p}(q) f_{1,p}(q).$$

On the other hand, let $f_{r,r}(q)$ be the monic polynomial whose roots are primitive r^2-roots of unity represented by the collection of tuple

$$\{(w_r + t(r)) \mid 0 \leq t \leq r-1, w_r \in \mathcal{A}_r\}.$$

It can be verified that the coefficients of $f_{r,r}(q)$ are not properly contained in $\mathbb{Q}$. Let $f_{1,r}(q)$ be the monic polynomial whose roots are primitive r-roots of unity represented by the collection of tuples

$$\{w_r \mid w_r \in (\mathbb{Z}/r\mathbb{Z})^* - \mathcal{A}_r\}.$$

Define

$$f_r(q) = f_{r,r}(q) f_{1,r}(q).$$

Since $p \equiv 1 (\text{mod } r)$ by hypothesis,

$$\frac{f_{r,r}(q^p)}{f_{r,r}(q)}$$

is a monic polynomial, by Key Proposition 1 of [4], whose roots are primitive r^2p-roots of unity represented by the collection of tuples

$$\{(w_r + t(r), w_p) \mid 0 \leq t \leq r-1, w_r \in \mathcal{A}_r, w_p \in (\mathbb{Z}/p\mathbb{Z})^*\}.$$

It can be verified also that $f_{r,p}(q^r)$ is a monic polynomial whose roots are primitive pr^2-roots of unity presented by the collection of tuples

$$\{(w_r + t(r), w_p) \mid 0 \leq t \leq r-1, w_r \in \mathcal{A}_r, w_p \in (\mathbb{Z}/p\mathbb{Z})^*\}.$$

Therefore,

$$f_{r,p}(q^r) = \frac{f_{r,r}(q^p)}{f_{r,r}(q)}.$$

It can be verified that

$$\frac{f_{1,p}(q^r)}{f_{1,p}(q)} = \frac{P_p(q^r)}{P_p(q)} = P_{pr}(q)$$

where $P_{pr}(q)$ is the cyclotomic polynomial in $\mathbb{Q}[q]$ of order pr. Hence its roots are primitive pr-roots of unity represented by the collection of tuples

$$\{(w_p, w_r) \mid w_r \in (\mathbb{Z}/r\mathbb{Z})^*, w_p \in (\mathbb{Z}/p\mathbb{Z})^*\}.$$

It can be verified that

$$\frac{f_{1,r}(q^p)}{f_{1,r}(q)}$$

is a monic polynomial whose roots are primitive rp-roots of unity represented by the collection of tuples

$$\{(w_r, w_p) \mid w_r \in (\mathbb{Z}/r\mathbb{Z})^* - \mathcal{A}_r, w_p \in (\mathbb{Z}/p\mathbb{Z})^*\}.$$

Therefore,

$$f_{r,p}(q)\frac{f_{1,r}(q^p)}{f_{1,r}(q)}$$

is a monic polynomial whose roots are primitive rp-roots of unity represented by the collection of tuples

$$\{(w_r, w_p) \mid w_r \in \mathcal{A}_r, w_p \in (\mathbb{Z}/p\mathbb{Z})^*\} \cup \{(w_r, w_p) \mid w_r \in (\mathbb{Z}/r\mathbb{Z})^* - \mathcal{A}_r, w_p \in (\mathbb{Z}/p\mathbb{Z})^*\}$$

$$= \{(w_r, w_p) \mid w_r \in (\mathbb{Z}/r\mathbb{Z})^*, w_p \in (\mathbb{Z}/p\mathbb{Z})^*\}.$$

As a result,

$$\frac{f_{1,p}(q^r)}{f_{1,p}(q)} = f_{r,p}(q)\frac{f_{1,r}(q^p)}{f_{1,r}(q)}.$$

Therefore,

$$f_{r,p}(q^r)\frac{f_{1,p}(q^r)}{f_{1,p}(q)} = f_{r,p}(q)\frac{f_{1,r}(q^p)}{f_{1,r}(q)}\frac{f_{r,r}(q^p)}{f_{r,r}(q)},$$

or equivalently,

$$(f_{r,r}(q)f_{1,r}(q))f_{r,p}(q^r)f_{1,p}(q^r) = (f_{r,p}(q)f_{1,p}(q))f_{1,r}(q^p)f_{r,r}(q^p).$$

The last equality can also be written as

$$f_r(q)f_p(q^r) = f_p(q)f_r(q^p),$$

i.e., $f_p(q)$ and $f_r(q)$ satisfy Functional Equation (1).

The collection of polynomials

$$\{f_p(q) \mid p \in P\}$$

induces, by Theorem 1.5, a unique sequence of polynomials $\Gamma = \{f_n(q) \mid n \in A_P\}$ satisfying Functional Equation (2) with field of coefficients strictly containing $\mathbb{Q}$. □

Proof. (proof of Corollary 2.2) It is known that the collection of natural numbers

$$\{4k + 1 \mid k = 1, \ldots, \infty\},$$

or more generally, the collection of natural numbers

$$\{rk + 1 \mid k \in 1, \ldots, \infty\},$$

where r is any fixed natural number, contains infinitely many primes (see Dirichlet's primes in arithmetic progression theorem). Let P be a collection of all primes of the form

$$P_1 = \{p_i \mid p_i = 4k_i + 1, k_i \in \mathbb{N}\},$$

or

$$P_2 = \{p_i \mid p_i = rk_i + 1, k_i \in \mathbb{N}\}$$

for some odd prime r. Then P_1 and P_2 are of infinite cardinality. Let P be any infinite subset of P_1 or P_2. Condition (2) or (3) of Theorem 2.1 says that if 4 divide $p-1$ for all p in a set of primes P or if there exists an odd prime r dividing $p-1$ for all primes p in P, then there exist sequences of polynomials Γ satisfying Functional Equation (2) with field of coefficients of characteristic zero strictly containing $\mathbb{Q}$ and support base P. Therefore, the result follows from Theorem 1.9. □

References

[1] Borisov, A., M. Nathanson, Y. Wang, Quantum Integers and Cyclotomy, *Journal of Number Theory*, Vol. 109, 2004, No. 1, 120–135.

[2] Nathanson, M., A Functional Equation Arising From Multiplication of Quantum Integers, *Journal of Number Theory*, Vol. 103, 2003, No. 2, 214–233.

[3] Nguyen, L., The Grothendieck Group associated to the Collection of all Solutions of a Functional Equation Arising from Multiplication of Quantum Integers with a given Support. *Proceeding of Combinatorics and Additive Number Theory*, 2011 (to appear).

[4] Nguyen, L., On the Solutions of a Functional Equation Arising from Multiplication of Quantum Integers, *Journal of Number Theory* Vol. 130, 2010, No. 6, 1292–1347.

[5] Nguyen, L., On the Classification of Solutions of a Functional Equation Arising from Multiplication of Quantum Integers. *Uniform Distribution Theory Journal*, 2012 (to appear).

[6] Nguyen, L., On the Support Base of a Functional Equation Arising from Multiplication of Quantum Integers, *Journal of Number Theory*, Vol. 130, 2010, Issue 6, 1348–1373.

[7] Nguyen, L., Extension of Supports of Solutions of a Functional Equation Arising from Multiplication of Quantum Integers. (in preparation)