Additive Number Theory and the Ring of Quantum Integers[*]

M.B. Nathanson[**]

In memoriam Levon Khachatrian

Abstract. Let m and n be positive integers. For the quantum integer $[n]_q = 1 + q + q^2 + \cdots + q^{n-1}$ there is a natural polynomial addition such that $[m]_q \oplus_q [n]_q = [m+n]_q$ and a natural polynomial multiplication such that $[m]_q \otimes_q [n]_q = [mn]_q$. These definitions are motivated by elementary decompositions of intervals of integers in combinatorics and additive number theory. This leads to the construction of the ring of quantum integers and the field of quantum rational numbers.

1 The Quantum Arithmetic Problem

For every positive integer n we have the *quantum integer*

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

Then

$$\mathcal{F} = \{[n]_q\}_{n=1}^{\infty}$$

is a sequence of polynomials in the variable q. This sequence arises frequently in the study of q-series and of quantum groups (cf. Kassel [1, Chapter IV]). Adding and multiplying polynomials in the usual way, we observe that

$$[m]_q + [n]_q \neq [m+n]_q$$

and

$$[m]_q \cdot [n]_q \neq [mn]_q.$$

This suggests the problem of introducing new operations of addition and multiplication of the polynomials in a sequence so that addition and multiplication of quantum integers behave properly. We can state the problem more precisely as follows. Define "natural" operations of *quantum addition*, denoted $\oplus_q$, and *quantum multiplication*, denoted $\otimes_q$, on the polynomials in an arbitrary sequence $\mathcal{F} = \{f_n(q)\}_{n=1}^{\infty}$ of polynomials such that $f_m(q) \oplus_q f_n(q)$ and $f_m(q) \otimes_q f_n(q)$

[*] 2000 Mathematics Subject Classification: Primary 11B75, 11N80, 05A30, 16W35, 81R50. Secondary 11B13. Key words and phrases. Quantum integers, quantum addition and multiplication, polynomial functional equations, additive bases.

[**] This work was supported in part by grants from the NSA Mathematical Sciences Program and the PSC-CUNY Research Award Program.

R. Ahlswede et al. (Eds.): Information Transfer and Combinatorics, LNCS 4123, pp. 505–511, 2006.

are polynomials, not necessarily in $\mathcal{F}$. We want to construct these operations so that, when applied to the polynomial sequence $\mathcal{F} = \{[n]_q\}_{n=1}^{\infty}$ of quantum integers, we have

$$[m]_q \oplus_q [n]_q = [m+n]_q \tag{1}$$

and

$$[m]_q \otimes_q [n]_q = [mn]_q \tag{2}$$

for all positive integers m and n. We would like these operations to determine the quantum integers uniquely.

2 Combinatorial Operations on Intervals of Integers

Let A and B be sets of integers, and let m be an integer. We define the *sumset*

$$A + B = \{a + b : a \in A \text{ and } b \in B\},$$

the *translation*

$$m + A = \{m + a : a \in A\},$$

and the *dilation*

$$m * A = \{ma : a \in A\}.$$

We write $A \oplus B = C$ if $A + B = C$ and every element of C has a unique representation as the sum of an element of A and an element of B.

Let $[n] = \{0, 1, 2, \ldots, n-1\}$ denote the set of the first $n-1$ nonnegative integers. Then

$$\begin{aligned}[m+n] &= \{0, 1, 2, \ldots, m+n-1\} \\ &= \{0, 1, 2, \ldots, m-1\} \cup \{m, m+1, m+2, \ldots, m+n-1\} \\ &= \{0, 1, 2, \ldots, m-1\} \cup m + \{0, 1, 2, \ldots, n-1\} \\ &= [m] \cup (m + [n]),\end{aligned}$$

and

$$[m] \cap (m + [n]) = \varnothing.$$

Moreover,

$$\begin{aligned}[mn] &= \{0, 1, 2, \ldots, mn-1\} \\ &= \{0, 1, 2, \ldots, m-1\} \oplus \{0, m, 2m, \ldots, m(n-1)\} \\ &= \{0, 1, 2, \ldots, m-1\} \oplus m * \{0, 1, 2, \ldots, n-1\} \\ &= [m] \oplus (m * [n]).\end{aligned}$$

If $m_1, \ldots, m_r$ are positive integers, then, by induction, we have the partition

$$[m_1 + m_2 + \cdots + m_r] = \bigcup_{j=1}^{r} \left(\sum_{i=1}^{j-1} m_i + [m_j] \right)$$

into pairwise disjoint sets, and the direct sum decomposition

$$[m_1 m_2 \cdots m_r] = \bigoplus_{j=1}^{r} \left(\prod_{i=1}^{j-1} m_i * [m_j] \right).$$

Associated to every set A of integers is the *generating function*

$$f_A(q) = \sum_{a \in A} q^a.$$

This is a formal Laurent series in the variable q. If A and B are finite sets of nonnegative integers and if m is a nonnegative integer, then $f_A(q)$ is a polynomial, and

$$f_{m+A} = q^m f_A(q)$$

and

$$f_{m*A}(q) = f_A(q^m).$$

If A and B are disjoint, then

$$f_{A \cup B}(q) = f_A(q) + f_B(q).$$

If $A + B = A \oplus B$, then

$$f_{A \oplus B}(q) = f_A(q) f_B(q).$$

The generating function of the interval $[n]_q$ is the quantum integer $[n]_q$. Since $[m] \cap (m + [n]) = \varnothing$, we have

$$\begin{aligned} [m+n]_q &= f_{[m+n]}(q) \\ &= f_{[m] \cup (m+[n])}(q) \\ &= f_{[m]}(q) + f_{m+[n]}(q) \\ &= f_{[m]}(q) + q^m f_{[n]}(q) \\ &= [m]_q + q^m [n_q]. \end{aligned}$$

Similarly,

$$\begin{aligned} [mn]_q &= f_{[mn]}(q) \\ &= f_{[m] \oplus (m*[n])}(q) \\ &= f_{[m]}(q) f_{m*[n]}(q) \\ &= f_{[m]}(q) f_{[n]}(q^m) \\ &= [m]_q [n]_{q^m}. \end{aligned}$$

These identities suggest natural definitions of quantum addition and multiplication. If $\mathcal{F} = \{f_n(q)\}_{n=1}^{\infty}$ is a sequence of polynomials, we define

$$f_m(q) \oplus_q f_n(q) = f_m(q) + q^m f_n(q) \tag{3}$$

and

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

Then

$$[m]_q \oplus_q [n]_q = [m+n]_q$$

and

$$[m]_q \otimes_q [n]_q = [mn]_q.$$

More generally, if $\mathcal{F} = \{f_n(q)\}_{n=1}^{\infty}$ is any sequence of functions, not necessarily polynomials, then we can define quantum addition and multiplication by (3) and (4). We shall prove that the only nonzero sequence $\mathcal{F} = \{f_n(q)\}_{n=1}^{\infty}$ of functions such that

$$f_m(q) \oplus_q f_n(q) = f_{m+n}(q)$$

and

$$f_m(q) \otimes_q f_n(q) = f_{mn}(q)$$

is the sequence of quantum integers.

3 Uniqueness of Quantum Arithmetic

Let $\mathcal{F} = \{f_n(q)\}_{n=1}^{\infty}$ be a sequence of polynomials in the variable q that satisfies the addition and multiplication rules for quantum integers, that is, $\mathcal{F}$ satisfies the *additive functional equation*

$$f_{m+n}(q) = f_m(q) + q^m f_n(q) \tag{5}$$

and the *multiplicative functional equation*

$$f_{mn}(q) = f_m(q) f_n(q^m) \tag{6}$$

for all positive integers m and n. Nathanson [2] showed that there is a rich variety of sequences of polynomials that satisfy the multiplicative functional equation (6), but there is not yet a classification of all solutions of (6). There is, however, a very simple description of all solutions of the additive functional equation (5).

Theorem 1. *Let $\mathcal{F} = \{f_n(q)\}_{n=1}^{\infty}$ be a sequence of functions that satisfies the additive functional equation (5). Let $h(q) = f_1(q)$. Then*

$$f_n(q) = h(q)[n]_q \qquad \text{for all } n \in \mathbb{N}. \tag{7}$$

Conversely, for any function $h(q)$ the sequence of functions $\mathcal{F} = \{f_n(q)\}_{n=1}^{\infty}$ defined by (7) is a solution of (5). In particular, if $h(q)$ is a polynomial in q, then $h(q)[n]_q$ is a polynomial in q for all positive integers n, and all polynomial solutions of (5) are of this form.

Proof. Suppose that $\mathcal{F} = \{f_n(q)\}_{n=1}^{\infty}$ is a solution of the additive functional equation (5). Define $h(q) = f_1(q)$. Since $[1]_q = 1$ we have

$$f_1(q) = h(q)[1]_q.$$

Let $n \geq 2$ and suppose that $f_{n-1}(q) = h(q)[n-1]_q$. From (5) we have

$$\begin{aligned} f_n(q) &= f_1(q) + qf_{n-1}(q) \\ &= h(q)[1]_q + qh(q)[n-1]_q \\ &= h(q)([1]_q + q[n-1]_q) \\ &= h(q)[n]_q. \end{aligned}$$

It follows by induction that $f_n(q) = h(q)[n]_q$ for all $n \in \mathbb{N}$.

Conversely, multiplying (5) by $h(q)$, we obtain

$$h(q)[m+n]_q = h(q)[m]_q + q^m h(q)[n]_q,$$

and so the sequence $\{h(q)[n]_q\}_{n=1}^{\infty}$ is a solution of the additive functional equation (5) for any function $h(q)$. This completes the proof.

We can now show that the sequence of quantum integers is the only nonzero simultaneous solution of the additive and multiplicative functional equations (5) and (6).

Theorem 2. *Let $\mathcal{F} = \{f_n(q)\}_{n=1}^{\infty}$ be a sequence of functions that satisfies both functional equations (5) and (6). Then either $f_n(q) = 0$ for all positive integers n, or $f_n(q) = [n]_q$ for all n.*

Proof. The multiplicative functional equation implies that $f_1(q) = f_1(q)^2$, and so $f_1(q) = 0$ or 1. Since $\mathcal{F} = \{f_n(q)\}_{n=1}^{\infty}$ also satisfies the additive functional equation, it follows from Theorem 1 that there exists a function $h(q)$ such that $f_n(q) = h(q)[n]_q$ for all positive integers n, and so $h(q) = 0$ or 1. It follows that either $f_n(q) = 0$ for all n or $f_n(q) = [n]_q$ for all n. This completes the proof.

4 The Ring of Quantum Integers

We can now construct the ring of quantum integers and the field of quantum rational numbers. We define the function

$$[x]_q = \frac{1-q^x}{1-q}$$

of two variables x and q. This is called the *quantum number* $[x]_q$. Then

$$[0]_q = 0,$$

and for every positive integer n we have

$$[n]_q = \frac{1-q^n}{1-q} = 1 + q + \cdots + q^{n-1},$$

which is the usual quantum integer. The negative quantum integers are

$$[-n]_q = \frac{1-q^{-n}}{1-q} = -\frac{1}{q^n}[n]_q = -\left(\frac{1}{q} + \frac{1}{q^2} + \cdots + \frac{1}{q^n}\right).$$

Then

$$\begin{aligned} [x]_q \oplus_q [y]_q &= [x]_q + q^x [y]_q \\ &= \frac{1-q^x}{1-q} + q^x \frac{1-q^y}{1-q} \\ &= \frac{1-q^{x+y}}{1-q} \\ &= [x+y]_q \end{aligned}$$

and

$$\begin{aligned} [x]_q \otimes_q [y]_q &= [x]_q [y]_{q^x} \\ &= \frac{1-q^x}{1-q} \frac{1-q^{xy}}{1-q^x} \\ &= \frac{1-q^{xy}}{1-q} \\ &= [xy]_q. \end{aligned}$$

The identities

$$[x]_q \oplus_q [y]_q = [x+y]_q \qquad \text{and} \qquad [x]_q \otimes_q [y]_q = [xy]_q \tag{8}$$

immediately imply that the set

$$[\mathbf{Z}]_q = \{[n]_q : n \in \mathbf{Z}\}$$

is a commutative ring with the operations of quantum addition $\oplus_q$ and quantum multiplication $\otimes_q$. The ring $[\mathbf{Z}]_q$ is called the *ring of quantum integers.* The map $n \mapsto [n]_q$ from $\mathbf{Z}$ to $[\mathbf{Z}]_q$ is a ring isomorphism.

For any rational number m/n, the quantum rational number $[m/n]_q$ is

$$[m/n]_q = \frac{1-q^{m/n}}{1-q} = \frac{\frac{1-\left(q^{1/n}\right)^m}{1-q^{1/n}}}{\frac{1-\left(q^{1/n}\right)^n}{1-q^{1/n}}} = \frac{[m]_{q^{1/n}}}{[n]_{q^{1/n}}}.$$

Identities (8) imply that addition and multiplication of quantum rational numbers are well-defined. We call

$$[\mathcal{Q}]_q = \{[m/n]_q : m/n \in \mathcal{Q}\}$$

the *field of quantum rational numbers.*

If we consider $[x]_q$ as a function of real variables x and q, then

$$\lim_{q \to 1} [x]_q = x$$

for every real number x.

We can generalize the results in this section as follows:

Theorem 3. *Consider the function*

$$[x]_q = \frac{1-q^x}{1-q}$$

in the variables x and q. For any ring R, not necessarily commutative, the set

$$[R]_q = \{[x]_q : x \in R\}$$

is a ring with addition defined by

$$[x]_q \oplus_q [y]_q = [x]_q + q^x [y]_q.$$

and multiplication by

$$[x]_q \otimes_q [y]_q = [x]_q [y]_{q^x}$$

The map from R to $[R]_q$ defined by $x \mapsto [x]_q$ is a ring isomorphism.

Proof. This is true for an arbitrary ring R because the two identities in (8) are formal.

References

1. C. Kassel, Quantum Groups, Graduate Texts in Mathematics, Vol. 155, Springer-Verlag, New York, 1995.
2. M. B. Nathanson, A functional equation arising from multiplication of quantum integers, J. Number Theory 103, No. 2, 214–233, 2003.