INTEGERS: ELECTRONIC JOURNAL OF COMBINATORIAL NUMBER THEORY 8 (2008), #A05

Q-BINOMIALS AND THE GREATEST COMMON DIVISOR

Keith R. Slavin
8474 SW Chevy Place, Beaverton, Oregon 97008, USA
kslavin@dsl-only.net

Received: 7/21/07, Revised: 1/4/08, Accepted: 1/8/08, Published: 1/29/08

Abstract

A q-binomial theorem is proved for q at complex roots of unity. This theorem comprises the Greatest Common Divisor (GCD) function. This theorem is then used to derive other new product theorems, and to express the GCD function and the GCD-sum function as finite products.

1. Introduction

The well-known q-binomial or Gaussian coefficient for an integer $n \geq 0$ can be defined [1, Section 3.3] as

$$\left[\begin{array}{c} n \\ k \end{array} \right]_q = \frac{\displaystyle\prod_{j=1}^{k}(1 - q^{n-k+j})}{\displaystyle\prod_{j=1}^{k}(1 - q^j)} \tag{1}$$

for $0 \leq k \leq n$, and is defined to be zero outside this range. It is shown here (in the Appendix) that when $q = e^{-2i\pi m/n}$ (q at roots of unity), we can obtain a q-binomial rational root theorem:

Theorem (q-binomial rational root)

$$\left[\begin{array}{c} n \\ k \end{array} \right]_{e^{-2i\pi m/n}} = \left\{ \begin{array}{ll} \left(\begin{array}{c} (n,m) \\ (n,m)k/n \end{array} \right) & \text{if } n|km \\ 0 & \text{otherwise} \end{array} \right\} \qquad k,m,n \in Z, n > 0, 0 \leq k \leq n. \tag{2}$$

where (n, m) is the GCD of n, m, and $\left(\begin{array}{c} a \\ b \end{array} \right)$ is the normal binomial function.

The appearance of the GCD function is surprising, and has many ramifications in later results.

2. Finite Product Theorems using the GCD

The well known q-binomial analog of the Newton binomial formula [1, Eq. 3.3.6] is given by

$$\prod_{k=0}^{n-1}(1+q^k t) = \sum_{k=0}^{n} q^{k(k-1)/2} \left[\begin{array}{c} n \\ k \end{array} \right]_q t^k.$$

For $q = e^{-2i\pi m/n}$, this becomes

$$\prod_{k=0}^{n-1}(1+e^{-2i\pi mk/n} t) = \sum_{k=0}^{n} e^{-\frac{i\pi mk(k-1)}{n}} \left[\begin{array}{c} n \\ k \end{array} \right]_{e^{-2i\pi m/n}} t^k. \qquad (3)$$

From the q-binomial rational root theorem (2), the q-binomial terms in the above summation are non-zero when $n|km$, and the other terms are zero. If $n|km$ and trivially $n|kn$, then $n|k(n,m)$. Therefore an iterator r related to iterator k is always integer if

$$r = \frac{k(n,m)}{n} \qquad n|km. \qquad (4)$$

We can now change the k iterator to r in the right-hand side of (3), obtaining

$$\prod_{k=0}^{n-1}(1+e^{-2i\pi km/n} t) = \sum_{r=0}^{(n,m)} e^{-\frac{i\pi mr}{(n,m)}(\frac{nr}{(n,m)}-1)} \left[\begin{array}{c} n \\ nr/(n,m) \end{array} \right]_{e^{-2i\pi m/n}} t^{nr/(n,m)}. \qquad (5)$$

We have already constrained $n|km$, so that from (4), $n|rmn/(m,n)$ which is trivially true as $(m,n)|m$. Therefore the q-binomial rational root theorem (2) gives

$$\left[\begin{array}{c} n \\ nr/(n,m) \end{array} \right]_{e^{-2i\pi m/n}} = \left(\begin{array}{c} (n,m) \\ r \end{array} \right). \qquad (6)$$

We substitute (6) into right-hand side of (5) and, as $\frac{mr}{(n,m)}(\frac{nr}{(n,m)}-1)$ is an integer, we also substitute $e^{i\pi} = -1$, obtaining the following binomial GCD theorem:

$$\prod_{k=0}^{n-1}(1+e^{-2i\pi km/n} t) = \sum_{r=0}^{(n,m)} (-1)^{\frac{mr}{(n,m)}(\frac{nr}{(n,m)}-1)} \left(\begin{array}{c} (n,m) \\ r \end{array} \right) t^{nr/(n,m)}. \qquad (7)$$

The above result can give a very efficient expansion when $(n,m) \ll n$. In addition, if n is odd, then $n/(n,m)$ is odd, and therefore $r(nr/(n,m)-1)$ is always even, so we get the special case

$$\prod_{k=0}^{n-1}(1+e^{-2i\pi km/n} t) = \sum_{r=0}^{(n,m)} \left(\begin{array}{c} (n,m) \\ r \end{array} \right) t^{nr/(n,m)} = (1+t^{n/(n,m)})^{(n,m)} \qquad \text{odd}\, n \geq 1 \qquad (8)$$

where the last step is from the binomial theorem. If we set $t = 1$ we get

$$\prod_{k=0}^{n-1}(1+e^{-2i\pi km/n}) = 2^{(n,m)} \qquad \text{odd}\, n \geq 1.$$

Interestingly, this result gives an equation for the GCD for odd n as

$$(n,m) = \log_2 \prod_{k=0}^{n-1}(1+e^{-2i\pi km/n}) \qquad \text{odd}\, n \geq 1. \tag{9}$$

Note that the right-hand side can be evaluated for m in the complex domain, although its interpretation for non-integer values is unclear.

From (9), using $\cos(x) = (e^{ix} + e^{-ix})/2$, we get the real product

$$(n,m) = n + \log_2 \left(\left(\prod_{k=1}^{(n-1)/2} \cos \frac{km\pi}{n} \right)^2 \right) \qquad \text{odd}\, n \geq 1.$$

The GCD-sum $g(n)$ [2] can be found from (9) as

$$g(n) = \sum_{m=0}^{n-1}(n,m) = \log_2 \prod_{m=0}^{n-1}\prod_{k=0}^{n-1}(1+e^{-2i\pi km/n}) \qquad \text{odd}\, n \geq 1.$$

Note that $g(n) = 2n - 1$ is only true if n is prime, although the two-dimensional product comprises a very inefficient primality test.

Substituting $t = e^{-2ix}$ into (7) we can obtain the following trigonometric binomial theorem:

$$\prod_{k=0}^{n-1} \cos\left(x + \frac{km\pi}{n}\right) = \left\{ \begin{array}{ll} \frac{1}{2^n}(-1)^{\frac{nm}{4}} \left(\begin{array}{c} (n,m) \\ (n,m)/2 \end{array} \right) & \text{if}\, (n,m)\, \text{is even} \\ 0 & \text{otherwise} \end{array} \right\} +$$
$$\frac{1}{2^{n-1}} \sum_{r=0}^{\left\lfloor \frac{(n-2)(n,m)}{2n} \right\rfloor} (-1)^{\frac{nmr}{(n,m)^2}((n,m)-r)} \left(\begin{array}{c} (n,m) \\ r \end{array} \right) \cos\left(\left(1 - \frac{2r}{(n,m)}\right)\left(nx + \frac{(n-1)m\pi}{2}\right)\right), \tag{10}$$

for $n \geq 2$ and even. Similarly, substituting $t = e^{-2ix}$ into (8), we can also obtain:

$$\prod_{k=0}^{n-1} \cos\left(x + \frac{km\pi}{n}\right) = \frac{1}{2^{n-1}} \sum_{r=0}^{\left\lfloor \frac{(n-1)(n,m)}{2n} \right\rfloor} \left(\begin{array}{c} (n,m) \\ r \end{array} \right) \cos\left(\left(1 - \frac{2r}{(n,m)}\right)\left(nx + \frac{(n-1)m\pi}{2}\right)\right), \tag{11}$$

for $n \geq 1$ and odd. Similar results for sine products are obtained by substituting $x \to x - \pi/2$.

3. Proof of Some Well-known Special Cases

Proof. If $(n, m) = 1$, then both (10) and (11) simplify to give the same special case for $n > 0$ as

$$\prod_{k=0}^{n-1} \cos\left(x + \frac{km\pi}{n}\right) = \frac{1}{2^{n-1}} \cos\left(nx + \frac{(n-1)m\pi}{2}\right) \qquad n > 0, (n, m) = 1. \tag{12}$$

By setting $m = 1$ and substituting $x \to x - \pi/2$, equation (12) gives

$$\sin nx = 2^{n-1} \prod_{k=0}^{n-1} \sin\left(x + \frac{k\pi}{n}\right).$$

By setting $m = 1$ and substituting $x \to x - \pi/2 - \pi/(2n)$, equation (12) gives

$$\cos nx = 2^{n-1} \prod_{k=0}^{n-1} \sin\left(x + \frac{(2k+1)\pi}{2n}\right).$$

Both results are also given in [3, Sec. 1.392].

If $(n, m) = 2$, then n is even, and (10) applies to give the special case

$$\prod_{k=0}^{n-1} \cos\left(x + \frac{km\pi}{n}\right) = \frac{1}{2^{n-1}} \left((-1)^{\frac{nm}{4}} + \cos\left(nx + \frac{(n-1)m\pi}{2}\right)\right) \qquad n > 0, (n, m) = 2.$$

Subcase $m = 2$ of this special case is given in [3, Sec. 1.393], where the result has simply been characterized as true for even n. None of these published special cases have even hinted at the more general connection with the GCD function.

Acknowledgments

Some of this work was done while I was working for Tektronix, Inc. Their support is gratefully acknowledged. Also I would like to thank Professor George E. Andrews for his insight and helpful comments.

References

[1] George E. Andrews, The Theory of Partitions. Cambridge University Press, (1984), Chapter 3.

[2] Kevin A. Broughan, The gcd-sum function. Journal of Integer Sequences, Vol. 4 (2001), Article 01.2.2.

[3] I.S.Gradshteyn and I.M.Ryzhik, Table of Integrals, Series, and Products. (6th edition) Academic Press, 2000.

Appendix: Proof of Q-Binomial GCD Coefficient Theorem

We prove the q-binomial root of unity theorem (2), restated below

$$\left[\begin{array}{c} n \\ k \end{array}\right]_{e^{-2i\pi m/n}} = \left\{ \begin{array}{ll} \left(\begin{array}{c} (n,m) \\ (n,m)k/n \end{array}\right) & \text{if } n|km \\ 0 & \text{otherwise} \end{array} \right\} \qquad k,m,n \in Z, n>0, 0 \le k \le n. \tag{13}$$

Proof. We start by using (1) with $q = e^{-2im\pi/n}$, and evaluating it as a limit as $x \to m\pi/n$:

$$\left[\begin{array}{c} n \\ k \end{array}\right]_{e^{-2i\pi m/n}} = \lim_{x\to\pi m/n} \prod_{j=1}^{k} \frac{(1-e^{-2i(n-k+j)x})}{(1-e^{-2ijx})} = \prod_{j=1}^{k} T_j \tag{14}$$

where the T_j are defined by

$$T_j = \lim_{x\to m\pi/n} \frac{(1-e^{-2i(n-k+j)x})}{(1-e^{-2ijx})}. \tag{15}$$

We now prove (13) for each of the two cases $n|km$ and $n \nmid km$ separately.

Case 1 : $n|km$

The proof of this case is split into two further subcases: the product terms T_j in (14) where $n \nmid jm$, and the other terms where $n|jm$. The two sets of products are later recombined to obtain the product for the case $n|km$.

Subcase 1.1: $n|km$, $n \nmid jm$

We first consider the value of T_j for all m in the product (14) where $n \nmid jm$. In this case, at the limit, the denominator of T_j in (15) is never zero, so we evaluate at the limit and separate out the j term in the numerator to get

$$T_j = \frac{1-e^{-2i\pi(n-k)m/n}e^{-2i\pi jm/n}}{1-e^{-2i\pi jm/n}} \qquad n|km, n \nmid jm. \tag{16}$$

Now $n|km$ so therefore $(n-k)m/n$ is an integer and therefore $e^{-2i\pi(n-k)m/n} = 1$. As $n \nmid jm$, none of the terms are zero and (16) simplifies to

$$T_j = 1 \qquad n|km, n \nmid jm. \tag{17}$$

Subcase 1.2: $n|km, n|jm$

We next consider the value of T_j for all j in the product (13) where $n|km$ and $n|jm$. In this case, jm/n and $(n-k+j)m/n$ are both integers so the numerator and denominator of (15) both tend to zero at the limit. We use L'Hospital's rule, taking the ratio of the partial derivatives of the numerator and denominator with respect to x to give

$$T_j = \lim_{x\to\pi m/n} \frac{-2i(n-k+j)e^{-2i(n-k+j)x}}{-2ije^{-2ijx}} = \frac{n-k+j}{j} \qquad n|km, n|jm. \tag{18}$$

Now we combine subcases 1.1 and 1.2 to obtain $\prod_{j=1}^{k} T_j$ when $n|km$. We first split the product of (14) into two separate products, one where $n \nmid jm$, and the other where $n|jm$. Using results (17) and (18), we obtain a single product over the range $1 \le j \le k$ as

$$\begin{bmatrix} n \\ k \end{bmatrix}_{e^{-2i\pi m/n}} = \prod_{\substack{j=1 \\ n|jm}}^{k} \frac{n-k+j}{j}. \qquad (19)$$

Comparing (19) with (13), it remains to prove only that

$$\begin{pmatrix} (n,m) \\ (n,m)k/n \end{pmatrix} = \prod_{\substack{j=1 \\ n|jm}}^{k} \frac{n-k+j}{j} \qquad n|km, 0 \le k \le n. \qquad (20)$$

Note that this product only contains those terms for which $n|jm$.

As $0 \le k \le n$, we can apply a change of variable $j \to n-k+j$ to the right-hand side of (20):

$$\prod_{\substack{j=1 \\ n|jm}}^{k} \frac{n-k+j}{j} = \frac{\displaystyle\prod_{\substack{j=1 \\ n|jm}}^{k} (n-k+j)}{\displaystyle\prod_{\substack{j=1 \\ n|jm}}^{k} j} = \frac{\displaystyle\prod_{\substack{j=n-k+1 \\ n|(j-n+k)m}}^{n} j}{\displaystyle\prod_{\substack{j=1 \\ n|jm}}^{k} j}.$$

For the case $n|km$, the above condition $n|(j-k+n)m$ is equivalent to $n|jm$. Therefore

$$\prod_{\substack{j=1 \\ n|jm}}^{k} \frac{n-k+j}{j} = \frac{\displaystyle\prod_{\substack{j=n-k+1 \\ n|jm}}^{n} j}{\displaystyle\prod_{\substack{j=1 \\ n|jm}}^{k} j} = \frac{\displaystyle\prod_{\substack{j=1 \\ n|jm}}^{n} j}{\left(\displaystyle\prod_{\substack{j=1 \\ n|jm}}^{k} j\right) \displaystyle\prod_{\substack{j=1 \\ n|jm}}^{n-k} j} = \frac{f(n)}{f(k)\, f(n-k)}. \qquad (21)$$

where the function $f(p) = \prod_{\substack{j=1 \\ n|jm}}^{p} j$. We now have need of the following.

Lemma 1 Let r be a positive integer such that

$$r = \frac{n}{(n,m)}. \qquad (22)$$

If p is an integer such that

$$n|pm \tag{23}$$

then $r|p$ and

$$\prod_{\substack{j=1\\n|jm}}^{p} j = \prod_{q=1}^{p/r} qr. \tag{24}$$

Proof. We first assume that $j = qr$, and then show that the set of terms in each product are the same. From (22) we get

$$j = qn/(n,m). \tag{25}$$

For any integer iterator value q in the range given in the right-hand product, we need to show that $n|jm$ is true for each corresponding term in the left-hand product. From (25), $n|j(n,m)$, so $n|jm$ is also true.

Now we only need to show that the iterator limits in the two products are also the same. The first term of the left-hand product is the smallest multiple of m that is also a multiple of n, which is $nm/(n,m)$. This term occurs when the iterator j in (24) is at $n/(n,m) = r$ from (22). This agrees with the value of the first term at $q = 1$ for the right-hand product. The final value for the iterator q in the product of (24) is

$$p/r = p(n,m)/n. \tag{26}$$

From (23), $n|pm$, and $n|pn$, so that from the GCD definition

$$n|p(n,m).$$

Therefore from (22), $r|p$. The final term in the right-hand product is therefore $(p/r)r = p$, which, given (23), is also the final term in the left-hand product of (24). Therefore, with the same set of terms in both products of (24), the two sides are equal, and the proof of Lemma 1 is complete.

We continue the proof of (13) by showing that condition (23) in Lemma 1 is satisfied for all upper limits of the three product iterators j in the right-hand side of (21). This is trivially true for $f(n)$, and is true for $f(k)$ given that $n|km$, and therefore it is also true for $f(n-k)$. Therefore we can use (24) from Lemma 1 to replace each product in the right-hand side of (21) to give

$$\prod_{\substack{j=1\\n|jm}}^{k} \frac{n-k+j}{j} = \frac{\displaystyle\prod_{q=1}^{n/r} qr}{\left(\displaystyle\prod_{q=1}^{k/r} qr\right)\displaystyle\prod_{q=1}^{(n-k)/r} qr} = \frac{r^{n/r}\displaystyle\prod_{q=1}^{n/r} q}{\left(r^{k/r}\displaystyle\prod_{q=1}^{k/r} q\right) r^{(n-k)/r}\displaystyle\prod_{q=1}^{(n-k)/r} q}. \tag{27}$$

The powers of r in (27) cancel. Eliminating the remaining terms in r from Lemma 1 using (22), we get

$$\prod_{\substack{j=1\\ n|jm}}^{k} \frac{n-k+j}{j} = \frac{\displaystyle\prod_{q=1}^{(n,m)} q}{\left(\displaystyle\prod_{q=1}^{(n,m)k/n} q\right) \displaystyle\prod_{q=1}^{(n,m)(n-k)/n} q}. \tag{28}$$

From Lemma 1, all the limits on the product iterators of (28) are integers. Therefore we can define each product as a factorial to get

$$\prod_{\substack{j=1\\ n|jm}}^{k} \frac{n-k+j}{j} = \frac{(n,m)!}{((n,m)k/n)!\,((n,m)(n-k)/n)!}.$$

The $(n,m)(n-k)/n$ term is expanded to give

$$\prod_{\substack{j=1\\ n|jm}}^{k} \frac{n-k+j}{j} = \frac{(n,m)!}{((n,m)k/n)!\,((n,m)-(n,m)k/n)!} = \left(\begin{array}{c}(n,m)\\ (n,m)k/n\end{array}\right).$$

The last step is true from the definition of the binomial coefficient. This proves (20) and completes the proof of the q-binomial root of unity theorem (13) for the case when $n|km$.

Case 2: $n \nmid km$

In this case, if there is one more zero term in the product numerator of (14) than in its denominator, then the q-binomial is zero. This follows because all terms are of a similar form, so that the ratio of any pair of terms in the numerator and denominator, if the latter both tend to zero, is finite. All other terms in the product are finite. Therefore any extra zero term in the numerator product implies an overall result of zero. We first find the number of zero terms in the numerator, and then the number in the denominator. Finally, we show that the former exceeds the latter.

We now find the number of zeros in the product of the numerator terms in (14), where each numerator term is

$$N_m = 1 - e^{-2i\pi(n-k+j)m/n}.$$

This function is zero when

$$n|m(k-j). \tag{29}$$

For all $m, n, b \in Z$ where $n > 0$, it is trivially true that

$$n|\frac{mnb}{(n,m)}. \tag{30}$$

Note that the right-hand side is also chosen to be an integer multiple of m. Comparing (29) with (30), a zero in the numerator of (14) occurs when

$$k - j = \frac{nb}{(n,m)}. \tag{31}$$

From the product (14), $1 \le j \le k$, so that (31) implies that

$$0 \le b \le \frac{(k-1)(n,m)}{n}. \tag{32}$$

For some cases the fraction in (32) is not integer, so we find the next smaller integer using the floor operator:

$$0 \le b \le \left\lfloor \frac{(k-1)(n,m)}{n} \right\rfloor. \tag{33}$$

The number of integer values of b in the range of (33) gives the number of zeros in the numerator of (14) as

$$Z_{\mathrm{num}} = 1 + \left\lfloor \frac{(k-1)(n,m)}{n} \right\rfloor. \tag{34}$$

We now find the number of zeros in the product of the denominator terms in (14), where each denominator term is

$$D_m = 1 - e^{-2i\pi jm/n}.$$

This function is zero when $n|jm$. Hence from (30), $D_m = 0$ when

$$j = \frac{nb}{(n,m)}. \tag{35}$$

From the product (14), $1 \le j \le k$, so that for iterator values $j \ge 1$, (35) gives

$$b \ge \frac{(n,m)}{n}. \tag{36}$$

From the definition of the GCD function itself, $1 \le (n,m) \le n$, so that

$$0 < \frac{(n,m)}{n} \le 1. \tag{37}$$

Therefore from (36) and (37), as b is an integer, we have $b \ge 1$. At the other end of the range, $j \le k$, so from (35),

$$b \le \frac{k(n,m)}{n}. \tag{38}$$

As $n \nmid km$, then $n \ge 2$, and any prime factors of n that do not divide m also do not divide (n,m), so that

$$n \nmid k(n,m). \tag{39}$$

From (39), the right-hand side of (38) is not an integer, so for an integer b,

$$b \leq \left\lfloor \frac{k(n,m)}{n} \right\rfloor . \tag{40}$$

Earlier we found $b \geq 1$. From (40), we now have an inclusive range for b:

$$1 \leq b \leq \left\lfloor \frac{k(n,m)}{n} \right\rfloor .$$

The number of zeros in the denominator of (14) is the number of integer values taken by b which is

$$Z_{\text{denom}} = \left\lfloor \frac{k(n,m)}{n} \right\rfloor . \tag{41}$$

To complete the proof, we now show that $Z_{\text{num}} > Z_{\text{denom}}$. Let

$$r = \frac{n}{(n,m)}. \tag{42}$$

For Case 2, $n \nmid km$, so that $n \nmid k(n,m)$, which implies that $r \nmid k$. Furthermore, $n \nmid m$, and therefore $n \nmid (n,m)$ so that $(n,m) < n$ and $r \geq 2$. For $r, k \in Z$ and $r \geq 2$, it is readily apparent that

$$\left\lfloor \frac{k}{r} \right\rfloor = \left\lfloor \frac{k-1}{r} \right\rfloor \qquad r \nmid k \ . \tag{43}$$

These constraints allow substitution of (42) into (43) to get

$$\left\lfloor \frac{k(n,m)}{n} \right\rfloor = \left\lfloor \frac{(k-1)(n,m)}{n} \right\rfloor \qquad n \nmid km. \tag{44}$$

Therefore, from (41) and (44),

$$Z_{\text{denom}} = \left\lfloor \frac{(k-1)(n,m)}{n} \right\rfloor \qquad n \nmid km. \tag{45}$$

From (34) and (45), we finally get

$$Z_{\text{denom}} = Z_{\text{num}} - 1 \qquad n \nmid km.$$

So there is one fewer zero term in the denominator of (14) than the numerator, and the case for (13) where $n \nmid km$ is also proved. This completes the proof.