A q-analogue of the Euler totient function

Peter Bala, Jan 15 2024

We define a q-analogue of the arithmetical totient function $\phi(n)$ and prove q-versions of some elementary results about $\phi(n)$.

Euler's totient function $\phi(n)$ = A000010(n) is defined as the number of positive integers less than or equal to n that are coprime to n.

$$\phi(n) \;=\; \sum_{\substack{1 \le k \le n \\ \gcd(k,n)=1}} 1. \tag{1}$$

Two elementary properties of the totient function are Gauss' formula

$$\sum_{d|n} \phi(d) = n, \tag{2}$$

and the formula obtained from it by Möbius inversion

$$\sum_{d|n} \mu(d)\frac{n}{d} = \phi(n). \tag{3}$$

We define the *q-totient function* $\phi_n(q)$, a q-analogue of the totient function $\phi(n)$, to be the polynomial

$$\phi_n(q) \;=\; \sum_{\substack{1 \le k \le n \\ \gcd(k,n)=1}} q^k \tag{4}$$

so that $\phi_n(1) = \phi(n)$. The polynomial $\phi_n(q)$ is the n-th row polynomial of A300294. The first few values are tabled below

n	1	2	3	4	5	6
$\phi_n(q)$	q	q	$q+q^2$	$q+q^3$	$q+q^2+q^3+q^4$	$q+q^5$

The following q-analogue of (2) is stated in [Cam, equation 1.6]. Our proof follows one of the standard proofs of Gauss' formula.

Theorem 1.

$$\sum_{d|n} \phi_d(q^{n/d}) = q + q^2 + \cdots + q^n. \tag{5}$$

Proof.

Let $A_n = \{1, 2, ..., n\}$. For each positive integer d, a divisor of n, define

$$A_d = \{x : 1 \leq x \leq n, \gcd(x, n) = d\}. \tag{6}$$

Clearly, A_n is the disjoint union of A_d taken over all the divisors of n:

$$A_n = \sqcup_{d|n} A_d.$$

Hence

$$q + q^2 + \cdots + q^n = \sum_{d|n} \left(\sum_{x \in A_d} q^x \right). \tag{7}$$

Each element of $x \in A_d$ is divisible by d, say $x = dy$. Now $\gcd(dy, n) = d$ if and only if $\gcd(y, n/d) = 1$. Furthermore, $1 \leq dy \leq n$ if and only if $1 \leq y \leq n/d$.

Therefore from (6)

$$A_d = \{dy : 1 \leq y \leq n/d \text{ and } \gcd(y, n/d) = 1\}.$$

Hence, by the definition (4) of the q-totient function,

$$\sum_{x \in A_d} q^x = \phi_{n/d}\left(q^d\right).$$

It follows from (7) that

$$\begin{aligned} q + q^2 + \cdots + q^n &= \sum_{d|n} \left(\sum_{x \in A_d} q^x \right) \\ &= \sum_{d|n} \phi_{n/d}\left(q^d\right) \\ &= \sum_{d|n} \phi_d\left(q^{n/d}\right). \square \end{aligned}$$

A q-analogue of Cesáro's identity.

Theorem 1 is the particular case $f(n) = 1$ of the following more general result.

Theorem 2. Let f be an arithmetic function. For positive integer n we have

$$\sum_{k=1}^{n} f\left(\gcd(k, n)\right) q^k = \sum_{d|n} f(d)\, \phi_{n/d}\left(q^d\right). \tag{8}$$

Proof.

$$\sum_{k=1}^{n} f\left(\gcd(k,n)\right) q^k \quad = \quad \sum_{d|n} f(d) \sum_{\substack{y \leq n/d \\ \gcd(y, n/d)=1}} q^{dy} = \sum_{d|n} f(d)\phi_{n/d}\left(q^d\right). \square$$

Setting $q = 1$ in (8) we recover Cesáro's identity [Ces]

$$\sum_{k=1}^{n} f\left(\gcd(k,n)\right) = \sum_{d|n} f(d)\phi\left(\frac{n}{d}\right).$$

Next we give a q-analogue of (3).

Theorem 3. *For* $n \geq 2$,

$$\sum_{d|n} \mu(d)\frac{q^n-1}{q^d-1} = \phi_n(q). \tag{9}$$

Proof.

Let

$$\mathrm{P}(n,q) = \sum_{d|n} \mu(d)\frac{q^n-1}{q^d-1} \tag{10}$$

denote the left-hand side of (9).

If $d|n$ then

$$\frac{q^n-1}{q^d-1} = 1 + q^d + q^{2d} + \cdots + q^{(n/d-1)d}, \tag{11}$$

so $\mathrm{P}(n,q)$ is polynomial in q of degree less than n.

We calculate the coefficient of q^k in $\mathrm{P}(n,q)$ for $0 \leq k < n$. There are three cases to consider.

(i) $k = 0$. The constant term of $\mathrm{P}(n,q)$ is $\sum_{d|n} \mu(d) = 0$ for $n \geq 2$.

(ii) Next suppose k is such that $\gcd(k,n) = D > 1$. We shall show that the coefficient of q^k in the polynomial $P(n,q)$ is zero.

From (11), we see that we get a contribution of $\mu(d)$ to the coefficient of q^k from each divisor d of n such that some multiple of d is equal to k, that is, from the divisors d of $\gcd(n,k) = D$.

Thus

$$\begin{aligned} \text{the coefficient of } q^k \text{in } \mathrm{P}(n,q) &= \sum_{d|D} \mu(d) \\ &= 0. \end{aligned}$$

(iii) Finally, suppose now k is such that $\gcd(k,n) = 1$. Then only the summand $(q^n-1)/(q-1) = 1+q+\cdots+q^{n-1}$ in (10), corresponding to the divisor $d=1$, includes the term q^k, and that with coefficient equal to 1. We conclude that

$$\begin{aligned} \mathrm{P}(n,q) &= \sum_{d|n} \mu(d) \frac{q^n-1}{q^d-1} \\ &= \sum_{\gcd(k,n)=1} q^k \\ &= \phi_n(q). \square \end{aligned}$$

An easy corollary of Theorem 3 is that the generating function of the q-totient polynomials takes the form

$$\begin{aligned} \sum_{n\geq 1} \mu(n) \frac{x^n}{(1-x^n)(1-q^n x^n)} &= qx + qx^2 + \left(q+q^2\right)x^3 + \left(q+q^3\right)x^4 + \\ & \left(q+q^2+q^3+q^4\right)x^5 + \left(q+q^5\right)x^6 + \cdots \end{aligned}$$

The Möbius function and Ramanujan's sum as values of the q-totient function

Setting $q = e^{2\pi i/n}$ in Theorem 3, we find that

$$\begin{aligned} \mu(n) &= \phi_n\left(e^{2\pi i/n}\right) \\ &= \sum_{\substack{1 \leq k \leq n \\ \gcd(k,n)=1}} e^{2\pi ik/n}, \end{aligned}$$

expressing the Möbius function $\mu(n)$ as the sum of the primitive n-th roots of unity. This is a well-known result. See, for example, [H&W, Theorem 271 with $m=1$].

More generally, Ramanujan's two parameter sum $c_n(m)$ (see A054533) defined by

$$c_n(m) \quad = \quad \sum_{\substack{1 \le k \le n \\ \gcd(k,n)=1}} e^{2\pi i k m/n}$$

can be expressed as a value of the q-totient function:

$$c_n(m) \quad = \quad \phi_n\left(e^{2\pi i m/n}\right). \tag{12}$$

It can be shown from the definition that $c_n(m)$ is multiplicative when considered as a function of n for a fixed value of m: that is, for n_1 and n_2 coprime we have

$$c_{n_1}(m)c_{n_2}(m) = c_{n_1 n_2}(m). \tag{13}$$

The q-totient function $\phi_n(q)$ is not multiplicative as a function of n. However, for n_1 and n_2 coprime, it follows from (12) and (13) that the polynomial $\phi_{n_1}(q^{n_2})\,\phi_{n_2}(q^{n_1}) - \phi_{n_1 n_2}(q)$ vanishes for $q = \exp\left(\dfrac{2\pi i m}{n_1 n_2}\right)$, $0 \le m < n_1 n_2$, the $n_1 n_2$-th roots of unity, and so factorises as

$$\phi_{n_1}(q^{n_2})\,\phi_{n_2}(q^{n_1}) - \phi_{n_1 n_2}(q) = p(q)\left(q^{n_1 n_2} - 1\right)$$

for some polynomial $p(q)$ (depending on n_1 and n_2). It appears that $p(q)$ has integer coefficients. If true, then

$$\phi_{n_1}(q^{n_2})\,\phi_{n_2}(q^{n_1}) - \phi_{n_1 n_2}(q) \equiv 0 \bmod \left(q^{n_1 n_2} - 1\right), \quad \gcd(n_1, n_2) = 1, \tag{14}$$

in the polynomial ring $\mathbb{Z}[q]$. The congruence (14) could then be regarded as the analogue of multiplicativity for the q-totient function. When $q = 1$, (14) is simply the statement that the totient function is multiplicative:

$$\phi(n_1)\,\phi(n_2) = \phi(n_1 n_2), \quad \gcd(n_1, n_2) = 1.$$

References

[Cam] Geoffrey B. Campbell, A new class of infinite products, and Euler's totient, Internat. J. of Math. & Math. Sci. Vol. 17 No. 3 (1994) 417-422.

[Ces] E. Cesáro, Etude moyenne du plus grand commun diviseur de deux nombres, Ann. Mat. Pura Appl. 13 (1885), 235–250.

[H and W] Hardy, G. H.; Wright, E. M. , An Introduction to the Theory of Numbers (5th ed.), Oxford University Press, (1980) [First edition published 1938], ISBN 978-0-19-853171-5.