Yet Another Generalization of Euler's Totient Function

Matthew Holden, Michael Orrison, Michael Vrable

For every positive integer n, Euler's totient function, or ϕ-function, gives the number $\phi(n)$ of integers less than n that are relatively prime to n, with the convention that $\phi(1) = 1$. Students of abstract algebra also know $\phi(n)$ as the number of generators of the cyclic group $\mathbb{Z}/n\mathbb{Z}$. It therefore seems worthwhile to consider generalizations of Euler's totient function from a group theoretic perspective.

One such generalization is Jordan's totient function [2, pp. 147-155]. For positive integers n and k, $J_k(n)$ is defined to be the number of k-tuples $(a_1, \ldots, a_k)$ from $\{1, \ldots, n\}$ such that the greatest common divisor of $\{a_1, \ldots, a_k\}$ is relatively prime to n. Note that J_k is a generalization Euler's totient function since $J_1(n) = \phi(n)$.

To view Jordan's totient function from a group theoretic perspective, note that $J_k(n)$ also counts the number of sequences $(g_1, \ldots, g_k)$ of elements in $\mathbb{Z}/n\mathbb{Z}$ such that, if G_i is the subgroup generated by $\{g_1, \ldots, g_i\}$, then

$$\{0\} \leq G_1 \leq \cdots \leq G_{k-1} \leq G_k = \mathbb{Z}/n\mathbb{Z}.$$

Moreover, by using simple properties of subgroups and quotient groups of $\mathbb{Z}/n\mathbb{Z}$, identities concerning $J_k(n)$ may be obtained. For example, Gegenbauer (see [2, p. 151]) showed that

$$J_{k+l}(n) = \sum_{\substack{1 \leq d \leq n \\ d|n}} d^l J_k(d) J_l(n/d).$$

To see why Gegenbauer's result is true, recall that for each divisor d of n, there is a unique subgroup of order d in $\mathbb{Z}/n\mathbb{Z}$. Furthermore, the corresponding quotient group $(\mathbb{Z}/n\mathbb{Z})/(\mathbb{Z}/d\mathbb{Z})$ is isomorphic to $\mathbb{Z}/(n/d)\mathbb{Z}$. There are $J_k(d)$ sequences of length k for $\mathbb{Z}/d\mathbb{Z}$. Every extension of such a sequence to a sequence of length $k + l$ for $\mathbb{Z}/n\mathbb{Z}$ corresponds to a sequence of length l for the quotient group. Since every element of the quotient group has d representatives in $\mathbb{Z}/n\mathbb{Z}$, the number of sequences of length $k+l$ that pass through $\mathbb{Z}/d\mathbb{Z}$ is $d^l J_k(d) J_l(n/d)$. Summing over all divisors gives Gegenbauer's result. (See [2] or [4] for other identities involving $J_k(n)$.)

In this note, we consider a variation of Jordan's totient function defined as follows. For positive integers n and k, let $M_k(n)$ be the number of sequences

$(g_1, \ldots, g_k)$ of elements in $\mathbb{Z}/n\mathbb{Z}$ such that, if G_i is the subgroup generated by $\{g_1, \ldots, g_i\}$, then

$$\{0\} < G_1 < \cdots < G_{k-1} < G_k = \mathbb{Z}/n\mathbb{Z}.$$

In other words, $M_k(n)$ counts only those sequences $(g_1, \ldots, g_k)$ with the property that G_i is strictly contained in G_{i+1} for $i = 1, \ldots, k-1$. Together with the convention that $M_1(1) = 1$, we have that $M_1(n) = \phi(n)$. The function $M_k(n)$ is therefore another generalization of Euler's totient function.

One noteworthy feature of $M_k(n)$ is that, for a fixed n, $M_k(n)$ will eventually become 0. In fact, if $n = p_1^{e_1} \cdots p_r^{e_r}$ where the p_i are prime, then $M_k(n) = 0$ for all $k > e_1 + \cdots + e_r$. This of course follows from the fact that there are no appropriate sequences of subgroups of length more than $e_1 + \cdots + e_r$. Unlike J_k, however, M_k is not multiplicative, i.e., $J_k(m)J_k(n)$ need not equal $J_k(mn)$ when m and n are relatively prime. For example, $M_2(6) = 10$ while $M_2(2) = M_2(3) = 0$.

We conclude this note with some additional properties of M_k.

Theorem 1. *If n, k and l are positive integers, then*

$$M_{k+l}(n) = \sum_{\substack{1<d<n \\ d|n}} d^l M_k(d) M_l(n/d).$$

Proof. The argument is similar to that for Gegenbauer's result, the only change being that the sum is now over the nontrivial divisors of n due to the strict containment of the corresponding subgroups. □

Corollary 2. *If n and k are positve integers, and p is prime, then*

$$M_{k+1}(p^n) = (p-1)p^{n-1} \sum_{j=k}^{n-1} M_k(p^j).$$

Proof. By Theorem 1,

$$\begin{aligned} M_{k+1}(p^n) &= \sum_{\substack{1<d<p^n \\ d|p^n}} d M_k(d) M_1(n/d) \\ &= \sum_{j=k}^{n-1} p^j M_k(p^j) \phi(p^{n-j}) \\ &= \sum_{j=k}^{n-1} (p-1)p^{n-1} M_k(p^j) \\ &= (p-1)p^{n-1} \sum_{j=k}^{n-1} M_k(p^j). \end{aligned}$$

□

Corollary 3. *If n and k are positive integers, then*

$$M_k(n) = \sum_{\substack{1<d_1<\cdots<d_{k-1}<n \\ d_i|d_{i+1}}} \phi(d_1)\phi(d_2/d_1)\cdots\phi(d_{k-1}/d_{k-2})\phi(n/d_{k-1})d_1\cdots d_{k-1}.$$

Proof. This follows from the fact that $M_1(n) = \phi(n)$ and from Theorem 1 by setting $l = 1$ and proceeding recursively. □

Theorem 4. *If p is prime and $n \geq k \geq 1$, then*

$$M_k(p^n) = (p-1)^k p^{n+\frac{k(k-3)}{2}} \prod_{i=1}^{k-1} \frac{p^{n-i}-1}{p^i-1}.$$

Proof. We use induction on k. First, note that if $k = 1$, then

$$M_1(p^n) = \phi(p^n) = (p-1)p^{n-1}.$$

This agrees with the formula. Next, let $k \geq 2$ and assume that the formula holds for postive integers less than k. By Corollary 2 and induction, we have

$$\begin{aligned}
M_k(p^n) &= (p-1)p^{n-1} \sum_{j=k-1}^{n-1} M_{k-1}(p^j) \\
&= (p-1)p^{n-1} \sum_{j=k-1}^{n-1} \left((p-1)^{k-1} p^{j+\frac{(k-1)(k-4)}{2}} \prod_{i=1}^{k-2} \frac{p^{j-i}-1}{p^i-1} \right) \\
&= (p-1)^k p^{n+\frac{k(k-3)}{2}} \sum_{j=k-1}^{n-1} \left(p^{j-(k-1)} \prod_{i=1}^{k-2} \frac{p^{j-i}-1}{p^i-1} \right) \\
&= (p-1)^k p^{n+\frac{k(k-3)}{2}} \prod_{i=1}^{k-1} \frac{p^{n-i}-1}{p^i-1}.
\end{aligned}$$

□

Theorem 5. *If p is prime and n is positive, then*

$$\sum_{k=1}^{n} M_k(p^n) = p^{n-1}(p-1) \prod_{k=2}^{n} \left(p^{k-2}(p-1)+1 \right).$$

Proof. We use induction on n. First note that the formula holds trivially when $n = 1$. Let $n \geq 2$ and assume that the formula holds for positive integers less

than n. Define $L(p^n) = \sum_{k=1}^{n} M_k(p^n)$. By Corollary 2 we have

$$\begin{aligned}
\sum_{k=1}^{n} M_k(p^n) &= M_1(p^n) + \sum_{k=2}^{n} M_k(p^n) \\
&= p^{n-1}(p-1) + \sum_{k=2}^{n} \left(p^{n-1}(p-1) \sum_{j=k-1}^{n-1} M_{k-1}(p^j) \right) \\
&= p^{n-1}(p-1) + p^{n-1}(p-1) \sum_{i=1}^{n-1} L(p^i) \\
&= p^{n-1}(p-1) \left(1 + \sum_{i=1}^{n-1} L(p^i) \right).
\end{aligned}$$

By induction we have

$$\begin{aligned}
1 + \sum_{i=1}^{n-1} L(p^i) &= \left(1 + \sum_{i=1}^{n-2} L(p^i) \right) + L(p^{n-1}) \\
&= \prod_{k=2}^{n-1} \left(p^{k-2}(p-1) + 1 \right) + p^{n-2}(p-1) \prod_{k=2}^{n-1} \left(p^{k-2}(p-1) + 1 \right) \\
&= \left(1 + p^{n-2}(p-1) \right) \prod_{k=2}^{n-1} \left(p^{k-2}(p-1) + 1 \right) \\
&= \prod_{k=2}^{n} \left(p^{k-2}(p-1) + 1 \right).
\end{aligned}$$

The theorem follows immediately. □

References

[1] L. Comtet, *Advanced combinatorics*, D. Reidel Publishing Co., Dordrecht, 1974.

[2] L. Dickson, *History of the theory of numbers. Vol. I: Divisibility and primality*, Chelsea Publishing Co., New York, 1966.

[3] P. Hall, *The Eulerian functions of a group*, Quart. J. Math. Oxford Ser. 7 (1936), 134–151.

[4] R. Sivaramakrishnan, *The many facets of Euler's totient. II. Generalizations and analogues*, Nieuw Arch. Wisk. (4) **8** (1990), no. 2, 169–187.