Chamchuri Journal of Mathematics
Volume 6(2014), 47–55
http://www.math.sc.chula.ac.th/cjm

A Generalization of Euler's Totient Function

Pitchayatak Ponrod* and Ajchara Harnchoowong

Received 25 April 2014
Revised 8 July 2014
Accepted 10 July 2014

Abstract: J. Freed-Brown, M. Holder, M. E. Orrison and M. Vrable introduced a new generalization of Euler's totient function, $M_k(n)$, defined to be the number of sequences $(g_1, \ldots, g_k)$ of elements in $\mathbb{Z}_n$ such that if G_i is the subgroup of $\mathbb{Z}_n$ generated by $\{g_1, \ldots, g_i\}$, then

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

They also defined the function $M(n)$ to be $M_k(n)$ where k is the largest integer such that $M_k(n)$ is nonzero. They gave the formulas for $M_k(p^e)$ and $M(p^e q^f)$ where p and q are distinct primes and k, e and f are natural numbers. In this article, some more properties of $M_k(n)$ and $M(n)$ are investigated.

Keywords: Euler's Totient Function, Generalized Euler's Totient Function

2000 Mathematics Subject Classification: 11A25

1 Introduction

Euler's totient function, $\phi(n)$, is the number of natural numbers less than or equal to n which are relatively prime to n. Many generalizations of the Euler's totient function are given, see e.g. [1] and [3]. In [2], J. Freed-Brown, M. Holden, M. E. Orrison and M. Vrable introduced a new generalization of Euler's totient function,

*Corresponding author

$M_k(n)$, which is defined to be the number of sequences $(g_1, \ldots, g_k)$ of elements in $\mathbb{Z}_n$ such that if G_i is the subgroup generated by $\{g_1, \ldots, g_i\}$, then

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

Together with the convention that $M_1(1) = 1$, we have that $M_1(n) = \phi(n)$ for all natural numbers n.

Let $\Omega(n)$ be the number of prime factors of n with multiplicity. Note that for a fixed n, $M_k(n)$ will eventually become 0. In fact,

Remark 1.1. For $k, n \in \mathbb{N}$, $M_k(n) \neq 0$ if and only if $1 \leq k \leq \Omega(n)$.

Let $M(n) = M_k(n)$ where k is the largest integer such that $M_k(n)$ is nonzero. By the above remark, $M(n) = M_{\Omega(n)}(n)$. $M_k(n)$ has the following recursive identities:

Theorem 1.2. [2] If $n, k, l \in \mathbb{N}$, then

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

From this we have the following theorem.

Theorem 1.3. If $n \in \mathbb{N}$ with $n \geq 2$, then

$$M(n) = \sum_{p|n} p^{\Omega(n)-1}(p-1) M(\frac{n}{p}).$$

Proof. The theorem clearly holds when $\Omega(n) = 1$, so assume that $m = \Omega(n) \geq 2$. By Theorem 1.2,

$$M(n) = M_m(n) = \sum_{\substack{1<d<n \\ d|n}} d^{m-1}\phi(d) M_{m-1}(\frac{n}{d}).$$

By Remark 1.1, $M_{m-1}(\frac{n}{d})$ is nonzero only if d is a prime. Thus

$$M(n) = \sum_{\substack{1<d<n \\ d|n}} d^{m-1}\phi(d) M_{m-1}(\frac{n}{d}) = \sum_{\substack{p|n \\ p \text{ is a prime}}} p^{\Omega(n)-1}(p-1) M(\frac{n}{p}).$$

□

In case $n = p^e$ for some prime p and natural number e, it has been proved in [2] that

Theorem 1.4. [2] If p is a prime and $e, k \in \mathbb{N}$ with $e \geq k \geq 1$, then

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

Also in [2], the formulas for $M_k(p^e)$ and $M(p^e q^f)$ in terms of cyclotomic polynomials and symmetric polynomials, respectively, were given.

2 More Properties of $M_k(n)$

By using Theorem 1.2 recursively, we get a formula for $M_k(n)$ concerning the sequences of divisors instead of the sequences of subgroups and generators as in the definition of $M_k(n)$.

Theorem 2.1. For $k, n \in \mathbb{N}$ with $k \geq 2$,

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

For $M(n)$, we can instead consider a multiset of prime divisors of n, which is denoted by P_n.

Theorem 2.2. If $n \in \mathbb{N}$ with $n \geq 2$ and $m = \Omega(n)$, then

$$M(n) = M_m(n) = \left(\prod_{p^k \| n} (p-1)^k \right) \sum_{\{q_1,q_2,\ldots,q_m\}=P_n} q_1 q_2^2 q_3^3 \cdots q_{m-1}^{m-1},$$

where the summation takes over all distinct permutations of elements in P_n.

Proof. Using Theorem 1.3 recursively, we get

$$\begin{aligned} M(n) &= \sum_{q_{m-1}|n} \sum_{q_{m-2}|\frac{n}{q_{m-1}}} \cdots \sum_{q_1|\frac{n}{q_2 q_3 \cdots q_{m-1}}} (q_1-1)\cdots(q_{m-1}-1) \\ &\qquad\qquad M(\frac{n}{q_1 q_2 \cdots q_{m-1}}) q_1 q_2^2 \cdots q_{m-1}^{m-1} \\ &= \sum_{\{q_1,q_2,\ldots,q_m\}=P_n} (q_1-1)(q_2-1)\cdots(q_{m-1}-1)M(q_m) q_1 q_2^2 \cdots q_{m-1}^{m-1} \\ &= \sum_{\{q_1,q_2,\ldots,q_m\}=P_n} (q_1-1)(q_2-1)\cdots(q_{m-1}-1)(q_m-1) q_1 q_2^2 \cdots q_{m-1}^{m-1}. \end{aligned}$$

For any permutation $q_1, q_2, \ldots, q_m$ of prime divisors (counting multiplicity) of n,

$$(q_1-1)(q_2-1)\cdots(q_{m-1}-1)(q_m-1) = \prod_{p^k \| n} (p-1)^k.$$

Hence

$$M(n) = \left(\prod_{p^k \| n} (p-1)^k\right) \sum_{\{q_1,q_2,\ldots,q_m\}=P_n} q_1 q_2^2 \cdots q_{m-1}^{m-1}.$$

□

Next, we will investigate the increasing of $M_k(n)$. Recall that if $m, n \in \mathbb{N}$ and $d = (m,n)$, then

$$\frac{\phi(mn)}{\phi(m)\phi(n)} = \frac{d}{\phi(d)} = \prod_{p|d} \frac{p}{p-1}.$$

We see that $M_1(4) = 2 = M_2(4)$. For $n > 4$, we have

Theorem 2.3. If $n \in \mathbb{N}$ such that $n > 4$ and $2 \leq \Omega(n)$, then $M_1(n) < M_2(n)$.

Proof. Assume that $2 \leq \Omega(n)$ and $n > 4$. Let p be the least prime dividing n. We see that $\frac{(p,\frac{n}{p})}{\phi((p,\frac{n}{p}))} < \frac{n}{p}$. Hence

$$M_1(n) = \phi(n) = \phi(p)\phi(\frac{n}{p})\frac{(p,\frac{n}{p})}{\phi((p,\frac{n}{p}))} < \frac{n}{p}\phi(p)\phi(\frac{n}{p}) \leq \sum_{\substack{d|n \\ 1<d<n}} d\phi(d)\phi(\frac{n}{d}) = M_2(n).$$

□

For $2 \leq k \leq \Omega(n) - 2$, the increasing of $M_k(n)$ requires these additional definitions and lemmas.

Definition 2.4. Let $k, n \in \mathbb{N}$ such that $k \leq \Omega(n) - 1$. We call a sequence $(d_1, d_2, \ldots, d_k)$ a d-sequence if $1 < d_1 < d_2 < \cdots < d_k < n$, $d_i | d_{i+1}$ and $d_k | n$. In this case, $(d_1, d_2, \ldots, d_k)$ is a d-sequence of length k.

Remark 2.5. For $k, n \in \mathbb{N}$, if $(d_1, d_2, \ldots, d_k)$ is a d-sequence, then $\Omega(d_i) \geq i$ for all $1 \leq i \leq k$.

Definition 2.6. Let $k, n \in \mathbb{N}$ such that $2 \leq k < \Omega(n)$ and $(d_1, d_2, \ldots, d_k)$ be a d-sequence of length k. For each $i \in \mathbb{N}$ with $1 \leq i \leq k$, let $(d_{i,1}, d_{i,2}, \ldots, d_{i,k-1})$ be the sequence $(d_1, d_2, \ldots, d_k)$ excluding d_i.

Lemma 2.7. Let $k, n \in \mathbb{N}$ with $k \geq 2$ and $(d_1, d_2, \ldots, d_k)$ be a d-sequence. Then

$$\frac{\sum_{i=1}^{k} \phi(d_{i,1})\phi(\frac{d_{i,2}}{d_{i,1}}) \cdots \phi(\frac{d_{i,k-1}}{d_{i,k-2}})\phi(\frac{n}{d_{i,k-1}})d_{i,1}d_{i,2} \cdots d_{i,k-1}}{\phi(d_1)\phi(\frac{d_2}{d_1}) \cdots \phi(\frac{d_k}{d_{k-1}})\phi(\frac{n}{d_k})d_1 d_2 \cdots d_k} < 2.$$

Proof. Set $d_0 = 1$. For each $1 \leq i \leq k$, by Remark 2.5, it follows that $\Omega(d_i) \geq i$, so

$$\frac{\phi(d_{i,1})\phi(\frac{d_{i,2}}{d_{i,1}}) \cdots \phi(\frac{d_{i,k-1}}{d_{i,k-2}})\phi(\frac{n}{d_{i,k-1}})d_{i,1}d_{i,2} \cdots d_{i,k-1}}{\phi(d_1)\phi(\frac{d_2}{d_1}) \cdots \phi(\frac{d_k}{d_{k-1}})\phi(\frac{n}{d_k})d_1 d_2 \cdots d_k} = \frac{\phi(\frac{d_{i+1}}{d_{i-1}})}{\phi(\frac{d_i}{d_{i-1}})\phi(\frac{d_{i+1}}{d_i})d_i}$$

$$\leq \frac{\prod_{p|d_i} \frac{p}{p-1}}{d_i} \leq \frac{\prod_{p|2^i} \frac{p}{p-1}}{2^i} = \frac{1}{2^{i-1}}.$$

Hence

$$\frac{\sum_{i=1}^{k} \phi(d_{i,1})\phi(\frac{d_{i,2}}{d_{i,1}}) \cdots \phi(\frac{d_{i,k-1}}{d_{i,k-2}})\phi(\frac{n}{d_{i,k-1}})d_{i,1}d_{i,2} \cdots d_{i,k-1}}{\phi(d_1)\phi(\frac{d_2}{d_1}) \cdots \phi(\frac{d_k}{d_{k-1}})\phi(\frac{n}{d_k})d_1 d_2 \cdots d_k} \leq \sum_{i=1}^{k} \frac{\phi(\frac{d_{i+1}}{d_{i-1}})}{\phi(\frac{d_i}{d_{i-1}})\phi(\frac{d_{i+1}}{d_i})d_i}$$

$$\leq \sum_{i=1}^{k} \frac{1}{2^{i-1}} < 2.$$

□

Definition 2.8. Let $k, n \in \mathbb{N}$ with $k \leq \Omega(n) - 1$ and $(d_1, d_2, \ldots, d_k)$ be a d-sequence. For convenience, let $d_0 = 1$ and $d_{k+1} = n$ unless it is said otherwise. We say that the sequence $(d_1, d_2, \ldots, d_k)$ can be extended if there exist $a, i \in \mathbb{N}$ such that $d_{i-1} < a < d_i$ and $d_{i-1}|a|d_i$.

Remark 2.9. Let $k, n \in \mathbb{N}$. If $2 \leq k \leq \Omega(n) - 2$, then any d-sequence of length $k-1$ can be extended to at least two different d-sequences of length k.

Lemma 2.10. Let $k, n \in \mathbb{N}$ with $k \geq 2$. If any d-sequence of length $k-1$ can be extended to at least two different d-sequences, then $M_k(n) < M_{k+1}(n)$.

Proof. By Theorem 2.1 and Lemma 2.7,

$$\begin{aligned}
&M_{k+1}(n)\\
&\quad= \sum_{\substack{1<d_1<\cdots<d_k<d_{k+1}=n\\ d_i\mid d_{i+1}}} \phi(d_1)\phi(\frac{d_2}{d_1})\cdots\phi(\frac{d_k}{d_{k-1}})\phi(\frac{n}{d_k})d_1\cdots d_k\\
&\quad= \sum_{\substack{(d_1,d_2,\cdots,d_k)\\ \text{is a } d\text{-sequence}}} \phi(d_1)\phi(\frac{d_2}{d_1})\cdots\phi(\frac{d_k}{d_{k-1}})\phi(\frac{n}{d_k})d_1\cdots d_k\\
&\quad> \frac{1}{2}\sum_{\substack{(d_1,d_2,\cdots,d_k)\\ \text{is a } d\text{-sequence}}} \sum_{i=1}^{k} \phi(d_{i,1})\phi(\frac{d_{i,2}}{d_{i,1}})\cdots\phi(\frac{d_{i,k-1}}{d_{i,k-2}})\phi(\frac{n}{d_{i,k-1}})d_{i,1}d_{i,2}\cdots d_{i,k-1}.
\end{aligned}$$

By the assumption that any d-sequence of length $k-1$ can be extended to at least two different sequences, that is, there are at least two different d-sequences of length k which are extensions of a d-sequence of length $k-1$, then

$$\begin{aligned}
M_{k+1}(n) &> \frac{1}{2}\left(2\sum_{\substack{(d_1,d_2,\cdots,d_{k-1})\\ \text{is a } d\text{-sequence}}} \phi(d_1)\phi(\frac{d_2}{d_1})\cdots\phi(\frac{d_{k-1}}{d_{k-2}})\phi(\frac{n}{d_{k-1}})d_1d_2\cdots d_{k-1}\right)\\
&= M_k(n).
\end{aligned}$$

□

Using the above lemmas, we can easily prove

Theorem 2.11. Let $k,n\in\mathbb{N}$. If $2\le k\le\Omega(n)-2$, then $M_k(n)<M_{k+1}(n)$.

If $k=\Omega(n)-1$, then $M_k(n)<M_{k+1}(n)$ does not necessarily hold. For example, $M_2(12)=44<76=M_3(12)$, while $M_2(8)=12>8=M_3(8)$.

Recall the definition of $M_k(n)$. We can view the definition of $M_k(n)$ in number theoretically perspective as the number of sequences $(g_1,g_2,\ldots,g_k)$ from $\{1,2,\ldots,n\}$ such that

$$n>(n,g_1)>(n,g_1,g_2)>\cdots>(n,g_1,g_2,\ldots,g_k)=1.$$

It is well-known that $M_1=\phi$ is multiplicative, however this is not true for other $M_k(n)$ with $k\ge 2$.

Theorem 2.12. Let $m,n,k\in\mathbb{N}$ such that $(m,n)=1$. If $2\le k\le\Omega(mn)$, then $M_k(mn)>M_k(m)M_k(n)$.

Proof. Let $m, n \in \mathbb{N}$ such that $(m, n) = 1$. For each sequence $(m_1, m_2, \ldots, m_k)$ for $M_k(m)$ and $(n_1, n_2, \ldots, n_k)$ for $M_k(n)$, we can form a distinct sequence $(a_1, a_2, \ldots, a_k)$ for $M_k(mn)$ from $\{1, 2, \ldots, mn\}$ such that $a_i \equiv m_i \pmod{m}$ and $a_i \equiv n_i \pmod{n}$. So $M_k(mn) \geq M_k(m)M_k(n)$. Next, for a sequence $(m_1, m_2, \ldots, m_k)$ for $M_k(m)$, we can form a sequence for $M_k(mn)$ by

$$(a_1, a_2, \ldots, a_k) = (m_1 n, m_2 n, \ldots, m_{k-1} n, 1).$$

Since $a_1 = m_1 n \equiv 0 \pmod{n}$, so $n \not> (n, a_1)$. Thus there exists a sequence for $M_k(mn)$ that is not formed from any pair of $(m_1, m_2, \ldots, m_k)$ and $(n_1, n_2, \ldots, n_k)$. Hence

$$M_k(mn) > M_k(m)M_k(n).$$

□

Theorem 2.13. For $n \in \mathbb{N}$, $\phi(n)|M(n)$.

Proof. It is clear if $n = 1$ or n is a prime. Now let $n > 1$ be a composite number such that for every natural number $m < n$, $\phi(m)|M(m)$. By Theorem 1.3,

$$M(n) = \sum_{p|n} p^{\Omega(n)-1}(p-1)M(\frac{n}{p}).$$

For each prime p dividing n, $\phi(\frac{n}{p})$ is either $\frac{\phi(n)}{p}$ or $\frac{\phi(n)}{p-1}$. Since $\Omega(n) \geq 2$, in either case, $\phi(n)|p^{\Omega(n)-1}(p-1)\phi(\frac{n}{p})$ for any $p|n$. By induction hypothesis, $\phi(\frac{n}{p})|M(\frac{n}{p})$, so $\phi(n)|p^{\Omega(n)-1}(p-1)M(\frac{n}{p})$. Thus

$$\phi(n)|\sum_{p|n} p^{\Omega(n)-1}(p-1)M(\frac{n}{p}) = M(n).$$

□

Definition 2.14. For $n \in \mathbb{N}$, let

$$m(n) = \sum_{\{q_1, q_2, \ldots, q_m\} = P_n} q_1 q_2^2 \ldots q_{m-1}^{m-1}.$$

Theorem 2.15. Let $e \in \mathbb{N}$ and p, q, r be distinct primes. Then

$$m(p^e qr) = \sum_{k=\frac{(e-1)e}{2}}^{\frac{(e+1)(e+2)}{2}-1} \left(p^k \sum_{\substack{a+b=\frac{(e+1)(e+2)}{2}-k \\ a \neq b \\ 0 \leq a,b \leq e+1}} q^a r^b \right).$$

Proof. By the definition of $m(n)$,

$$m(p^e qr) = \sum_{\{q_1,\ldots,q_{e+2}\}=\{\underbrace{p,p,\ldots,p}_{e\ terms},q,r\}} q_1 q_2^2 \cdots q_{e+1}^{e+1}.$$

Since there are e copies of p's, so the least and the greatest powers of p are $0+1+2+\cdots+(e-1)=\frac{(e-1)e}{2}$ and $2+3+4+\cdots+(e+1)=\frac{(e+1)(e+2)}{2}-1$, respectively. If the power of p is k, then what is left for q and r is $\frac{(e+1)(e+2)}{2}-k$. And we see that q and r occupy different positions so they have the different powers, both of which are between 0 and $e+1$. □

In fact, the proof works for the following generalization.

Theorem 2.16. Let $e, f \in \mathbb{N}$ and $p, p_1, p_2, \ldots, p_f$ be distinct primes. Then

$$m(p^e p_1 p_2 \ldots p_f) = \sum_{k=\frac{(e-1)e}{2}}^{\frac{(e+f-1)(e+f)}{2}-\frac{(f-1)f}{2}} \left(p^k \sum_{\substack{a_1+a_2+\cdots+a_f=\frac{(e+f-1)(e+f)}{2}-k \\ a_i\neq a_j \\ 0\leq a_i\leq e+f-1}} p_1^{a_1}\cdots p_f^{a_f} \right).$$

References

[1] L. Dickson, History of the Theory of Numbers, Vol. I: Divisibility and Primality, Chelsea, New York, 1966.

[2] J. Freed-Brown, M. Holder, M. E. Orrison and M. Vrable, Cyclotomic Polynomials, Symmetric Polynomials, and a Generalization of Euler's Totient Function, Math. Magazine, 85(2012), 44-50.

[3] J. Sándor and B. Crstici, Handbook of Number Theory, II, Kluwer, Dordrecht, 2004.

Pitchayatak Ponrod
Department of Mathematics and Computer Science,
Faculty of Science,
Chulalongkorn University,
Bangkok 10330, Thailand
Email: final-song@hotmail.com

Ajchara Harnchoowong
Department of Mathematics and Computer Science,
Faculty of Science,
Chulalongkorn University,
Bangkok 10330, Thailand
Email: Ajchara.h@chula.ac.th