Journal of Mathematical Research & Exposition
Vol. 17, No. 4, 519- 523, Nov. 1997

A Further Combinatorial Number-Theoretic Extension of Euler's Totient*

Pentti Haukkanen
(Dept. of Math. Scis., University of Tampere, P. O. Box 607, FIN- 33101 Tampere, Finland)

Abstract Recently, L. C. Hsu and Wang Jun generated new combinatorial number-theoretic functions serving as generalizations of Euler's totient. In this paper we form an extensive class of generalized Euler totients by translating the most general counting functions of Hsu and Wang on integers to the setting of Narkiewicz's regular convolution. This class casts in the same framework various famous generalizations of Euler's totient, such as Cohen's totient, Jordan's totient, Klee's totient, Schemmel's totient, Stevens's totient, the unitary analogue of Euler's totient and Euler's totient with respect to Narkiewicz's regular convolution.

Keywords Euler's totient, regular convolution, restricted sets of integers (mod n)

Classification AMS(1991) 11A25/CCL O156.1

1. Introduction

Euler's totient $\varnothing(n)$ counts the number of integers a (mod n) such that gcd $(a, n) = 1$. There is in the literature a large number of generalizations and analogues of Euler's totient, with most of them being combinatorial number-theoretic functions. For example, Jordan's totient $J_u(n)$ counts the number of u-vectors $\langle a_1, a_2, \cdots, a_u\rangle$ of integers (mod n) such that gcd $(a_1, a_2, \cdots, a_u, n) = 1$. General accounts on generalizations and analogues of Euler's totient can be found e.g. in [3, Chapter V], [5], [12, Chapter V] and [13].

Hsu and Wang adopt a new combinatorial number-theoretic approach to generate generalizations and analogues of Euler's totient in their recent papers [7] and [15] (see also [6]). Various famous generalizations and analogues of Euler's totient can be written in the language of this approach. Euler's totient $\varnothing(n)$ is, in the language of this approach, the number of integers a (mod n) such that $a \not\equiv 0$ (mod p) for all $p \mid n$.

The most extensive counting theorem of [7] on integers concerns certain restricted sets of integers (mod n), while the most extensive counting theorem of [15] concerns certain restricted sets of u-vectors of integers (mod n), see [7, Theorem 2.2] and [15, Theorem 3.3] or Remarks 3.1 and 3.2 of this paper. In this paper we combine the ideas of [7, Theorem 2.2] and [15, Theorem 3.3]. We present the combined result in the setting of Narkiewicz's regular convo-

* Received Dec. 11, 1995.

lution. Hsu and Wang [7, 15] deal with the Dirichlet convolution, which is an example of Narkiewicz's regular convolution.

We interpret in terms of the generalized Euler totient of this paper the following famous generalizations and analogues of Euler's totient: Cohen's totient, Jordan's totient, Klee's totient, Schemmel's totient, Stevens's totient, the unitary analogue of Euler's totient and Euler's totient with respect to Narkiewicz's regular convolution, see Examples 3.1-3.2. We also obtain, as a special case of the generalized Euler totient of this paper, the example of a rational arithmetical function of order $(1, r)$ with respect to Narkiewicz's regular convolution given in [6], see Remark 3.2.

2 Regular convolution

We assume that the reader is familiar with the concept of Narkiewicz's regular convolution. Background material on regular convolutions can be found e.g. in [6], [9, Chapter 4], [10] and [11]. We use the same notations as that in [6]. In addition, we use the following notations.

Let A be a regular convolution and k a positive integer. The convolution A_k is defined by $A_k(n) = \{d: d^k \in A(n^k)\}$. It is known [11] that the convolution A_k is regular whenever the convolution A is regular. The symbol $(m, n)_{\{A, k\}}$ denotes the greatest kth power divisor of m which belongs to $A(n)$. In particular, we denote $(m, n)_{A,1} = (m, n)_A$, $(m, n)_{D,k} = (m, n)_k$, $(m, n)_D = (m, n)$ and $(m, n)_U = (m, n)^*$. Note that (m, n) is the usual greatest common divisor of m and n.

3 The main counting theorem

Let A be an arbitrary but fixed regular convolution. Let Q be a set of integers (> 1) such that each A-primitive prime power (> 1) A-divides at most one of them. This means that for each A-primitive prime power $p^t (> 1)$ there is at most one $i = 1, 2, \cdots, o(p^t)$ such that $p^{\{it\}} \in Q$. Note that elements of Q are prime powers.

Definition *We say that a positive integer $n(> 1)$ is Q-ful if the following two conditions hold:*

a) If $p^t \in A(n)$, then $p^t \in A(q)$ for some $q \in Q$,

b) If $p^t \in A(n)$ and $p^t \in A(q)$ for some $q \in Q$, then $q \in A(n)$,

where p^t denotes an A-primitive prime power > 1.

We denote u-vectors of integers as $\mathbf{a} = \langle a_1, a_2, \cdots, a_u \rangle$, and we write $\mathbf{a} \equiv \mathbf{b} \pmod n$ if $a_i = b_i$ for all $i = 1, 2, \cdots, u$. For each $q \in Q$, let $B(q)$ be a subset of $\mathbf{Z}_q^u$, where $\mathbf{Z}_q^u = \{\mathbf{a}: 0 \leq a_i < q, i = 1, 2, \cdots, u\}$.

Definition *We say that a u-vector $\mathbf{a}$ is B-prime to n if*

$$\forall q \in Q \text{ having a common } A\text{-divisor} > 1 \text{ with } n: \forall \mathbf{b} \in B(q): \mathbf{a} \not\equiv \mathbf{b} \pmod q.$$

If $\mathbf{a}$ is B-prime to n, we write $(\mathbf{a}, n)_B = 1$.

Now, we introduce the functions that we need in counting the number of u-vectors $\mathbf{a} \pmod n$ such that $(\mathbf{a}, n)_B = 1$. Let $f(q)$ denote the cardinality of $B(q)$, and let μ_B denote the arithmetical function defined by

$$\mu_B(n) = \begin{cases} 1 & \text{if } n = 1, \\ (-1)^s f(q_1)\cdots f(q_s) & \text{if } n = q_1\cdots q_s \text{ is a product of distinct elements of } Q, \\ 0 & \text{otherwise.} \end{cases}$$

If Q is the set of all A-primitive prime powers (>1) and if $B(q) = \{0\}$ for all $q \in Q$, then μ_B is the A-analogue of the Möbius function μ_A. In the case of Dirichlet convolution this becomes the classical function μ. Finally, we define the arithmetical function $\varnothing_B$ by

$$\varnothing_B(n) = (E^u *_A \mu_B)(n) = \sum_{d \in A(n)} (n/d)^u \mu_B(d), \tag{3.1}$$

where $E^u(n) = n^u$ for all n. It can be verified that if n is Q-ful, then

$$\varnothing_B(n) = n^u \prod_{\substack{q \in A(n) \\ q \in Q}} \left(1 - \frac{f(q)}{q^u}\right). \tag{3.2}$$

Theorem 1 *Let n be a Q-ful number. Then the number of u-vectors* $\mathbf{a}$ (mod n) such that $(\mathbf{a}, n)_B = 1$ is equal to $\varnothing_B(n)$.

Proof Let $n = n_1 n_2 \cdots n_s$ be the factorization of n into prime powers such that $q_i \in A(n_i)$, where $q_i \in Q$, $i = 1, 2, \cdots, s$. Let $N_B(n)$ denote the number of u-vectors $\mathbf{a}$ (mod n) such that $(\mathbf{a}, n)_B = 1$. Using the Chinese remainder theorem we can show that $N_B(n) = N_B(n_1) N_B(n_2) \cdots N_B(n_s)$, cf. the proofs of [6, Theorem 1], [7, Theorem 2.1] and [15, Theorem 3.3].

We next consider the value of $N_B(n_i)$. Let $\mathbf{a}_i \in \mathbf{Z}^u_{n_i}$. Then $\mathbf{a}_i$ can be written uniquely as $\mathbf{a}_i = \mathbf{m} q_i + \mathbf{r}$, where $0 \le m_j < n_i/q_i$, $j = 1, 2, \cdots, u$, and $\mathbf{r} \in \mathbf{Z}^u_{q_i}$. Clearly, $(\mathbf{a}_i, n_i)_B = 1$ if and only if $(\mathbf{r}, n_i)_B = 1$, and $(\mathbf{r}, n_i)_B = 1$ if and only if $\mathbf{r} \in \mathbf{Z}^u_{q_i} \setminus B(q_i)$. Therefore

$$N_B(n_i) = (n_i/q_i)^u (q_i^u - f(q_i)) = n_i^u (1 - f(q_i)/q_i^u).$$

Now, application of the formula $N_B(n) = N_B(n_1) N_B(n_2) \cdots N_B(n_s)$ proves that

$$N_B(n) = n^u \prod_{\substack{q \in A(n) \\ q \in Q}} \left(1 - \frac{f(q)}{q^u}\right).$$

Thus, by (3.2), we have $N_B(n) = \varnothing_B(n)$. This completes the proof.

Several famous totient functions may be presented in the language of the function $\varnothing_B(n)$ in Theorem 1.

Example 3.1 Jordan's totient $J_u(n)$ is defined as the number of u-vectors $\mathbf{a}$ of integers (mod n) such that $(a_1, a_2, \cdots, a_u, n) = 1$ (see [3, Chapter V]). If $A = D$, Q is the set of all primes and $B(p) = \{0\}$ for all primes p, then $\varnothing_B$ reduces to Jordan's totient. The expressions (3.1) and (3.2) reduce to the known expressions (see e.g. [12, Section V.3])

$$J_u(n) = \sum_{d | n} (n/d)^u \mu(d) = n^u \prod_{p | n} \left(1 - \frac{1}{p^u}\right).$$

Example 3. 2 Cohen's[1] totient $\varnothing_k(n)$ is defined as the number of integers $a \pmod{n^k}$ such that $(a, n^k)_k = 1$. If $A = D$, $u = 1$, Q is the set of the kth powers of primes, $B(p^k) = \{0\}$ for all primes p and n is replaced with n^k, then $\varnothing_B$ reduces to Cohen's totient. The expressions (3. 1) and (3. 2) reduce to the known expressions (see e. g. [12, Section V. 5])

$$\varnothing_k(n) = \sum_{d|n} (n/d)^k \mu(d) = n^k \prod_{p|n}\left(1 - \frac{1}{p^k}\right).$$

Further examples include Klee's totient[8], Schemmel's totient[13], Stevens's totient[14] and the unitary analogue of Euler's totient.[2]

Remark 3. 1 If $A = D$, $u = 1$ and Q is a set of positive integers such that each prime number divides one and only one of them, then Theorem 1 of this paper reduces to Theorem 2. 2 of [7].

Remark 3. 2 Let r be a positive integer. Let Q be the set of prime powers of the form p^{rt}, where $p^t(> 1)$ runs through the A-primitive prime powers such that $o(p^t) \geq r$. Then Q-ful numbers are the (A, r)-powerful numbers (see [6]). We form the sets $B(q)$, $q \in Q$, as follows. For each A-primitive prime power $p^t(> 1)$ and $i = 1, 2, \cdots, r$, let $S_i(p^t)$ be a subset of $\mathbf{Z}_{p^t}^u$. Let $\mathbf{M}(p^t)$ denote the set of $r \times u$ matrices over $\mathbf{Z}_{p^t}$ having the property that for every $M \in \mathbf{M}(p^t)$ there exists $i = 1, 2, \cdots, r$ such that the ith row of M belongs to $S_i(p^t)$. Now, we define

$$B(q) = B(p^{rt}) = \{\mathbf{a} \in \mathbf{Z}_{p^{rt}}^u : \mathbf{a} = (1, p^t, \cdots, p^{(r-1)t})M,\ M \in \mathbf{M}(p^t)\}$$

for each $q \in Q$. Then $(\mathbf{a}, n)_B = 1$ if and only if $(\mathbf{a}, n)_{S,r} = 1$, where $(\mathbf{a}, n)_{S,r}$ is as defined in [6]. Thus, in this case Theorem 1 of this paper reduces to Theorem 1 of [6]. The function $\varnothing_B$ becomes the function $\varnothing_{S,r}$ of [6] and is thus an A-rational arithmetical function of order $(1, r)$. If $A = D$ and $S_1 = S_2 = \cdots = S_r$, then we obtain Theorem 3. 3 of [15].

References

[1] E. Cohen, *An extension of Ramanujan's sum*, Duke Math. J., **16**(1949), 85-90.

[2] E. Cohen, *Arithmetical functions associated with the unitary divisors of an integer*, Math. Z., **74**(1960), 66-80.

[3] L. E. Dickson, *History of the Theory of Numbers*, Vol I, Chelsea, New York, 1971.

[4] P. Haukkanen, *Classical arithmetical identities involving a generalization of Ramanujan's sum*, Ann. Acad. Sci. Fenn. Ser. A. I Math. Dissertationes, **68**(1988), 1-69.

[5] P. Haukkanen, *Some generalized totient functions*, Math. Stud., **56**(1988), 65-74.

[6] P. Haukkanen, *A class of rational arithmetical functions with combinatorial meanings*, J. Math. Res. Exp., **17**: **2**(1997), 179-184.

[7] L. C. Hsu and Wang Jun, *Some combinatorial number-theoretic extensions of Euler's totient*, in Combinatorics and Graph Theory '95, Vol 2, Proceedings of the Summer School and International Conference on Combinatorics, World Scientific, Singapore-New Jersey-London-Hong Kong, 1995.

[8] V. L. Klee, *A generalization of Euler's function*, *Amer. Math. Monthly*, **55**(1948), 358-359.

[9] P. J. McCarthy, *Introduction to Arithmetical Functions*, Springer-Verlag, New York, 1986.

[10] W. Narkiewicz, *On a class of arithmetical convolutions*, Colloq. Math., **10**(1963), 81-94.

[11] V. Sita Ramaiah, *Arithmetical sums in regular convolutions*, J. Reine Angew. Math., **303**: **304**(1978), 265-283.

[12] R. Sivaramakrishnan, *Classical Theory of Arithmetic Functions*, in Monographs and Textbooks in Pure and Applied Mathematics, Vol. 126, Marcel Dekker, Inc., New York, 1989.

[13] R. Sivaramakrishnan, *The many facets of Euler's totient (II): Generalizations and analogues*, Nieuw Arch. Wiskd., **8**(1990), 169-187.

[14] H. Stevens, *Generalizations of the Euler φ-function*, Duke Math. J., **38**(1971), 181-186.

[15] Wang Jun and L. C. Hsu, *On certain generalized Euler-type totients and Möbius-type functions*, Preprint (Dalian University of Technology, China).