INTEGERS: ELECTRONIC JOURNAL OF COMBINATORIAL NUMBER THEORY 7 (2007), #A43

THE NUMBER OF RELATIVELY PRIME SUBSETS AND PHI FUNCTIONS FOR $\{m, m+1, \dots, n\}$

Mohamed El Bachraoui[1]
School of Science and Engineering, Al Akhawayn University, Ifrane, Morocco
melbachraoui@gmail.com

Received: 4/10/07, Revised: 9/11/07, Accepted: 9/17/07, Published: 9/28/07

Abstract

The work in this paper is inspired and motivated by some work of Nathanson. We count the number of relatively prime subsets and the number of relatively prime subsets having some fixed cardinality that are in $\{m, m+1, \dots, n\}$. We also count the number of nonempty subsets of $\{m, m+1, \dots, n\}$ whose gcd is relatively prime to n and the number of nonempty subsets $\{m, m+1, \dots, n\}$ having some fixed cardinality and whose gcd is relatively prime to n. Our work generalizes the results on relatively prime subsets of $\{1, 2, \dots, n\}$ and on phi functions for sets $\{1, 2, \dots, n\}$. Our proofs use an extension of the Möbius inversion formula to functions of several variables.

1. Preliminaries

We say that a set of integers A is *relatively prime* if $\gcd(A) = 1$. Clearly, if $1 \in A$, then A is relatively prime. Moreover, if $\gcd(A) = d$, then the set $\frac{1}{d}A = \left\{\frac{a}{d} :\ a \in A\right\}$ is relatively prime. Throughout the paper, $[x]$, the floor of x, satisfies the following basic identity

$$\left[\frac{x}{d}\right] = \left[\frac{[x]}{d}\right] \text{ for all real } x \text{ and positive integer } d. \tag{1}$$

Let m, n, and k denote positive integers.

Definition 1. An *arithmetical function of k variables* is a complex-valued function with domain $\mathbb{N} \times (\{0\} \cup \mathbb{N})^{k-1}$. A *generalized arithmetical function of k variables* is a complex-valued

[1]Current address: Dept. of Mathematical Sciences, United Arab Emirates University, P.O.Box 17551, Al-Ain, United Arab Emirates.

function G with domain $(0,\infty)^k$ such that $G(y_1, y_2, \ldots, y_{k-1}, x) = 0$ whenever $0 < x < 1$. An arithmetical function of one variable is simply called *arithmetical* and a generalized arithmetical function of one variable is simply said to be *generalized arithmetical*.

For example, the *Möbius* function μ, the *unit* function $u(n) = 1$ for all $n \in \mathbb{N}$, and the *identity* function

$$I(n) = \left[\frac{1}{n}\right] = \begin{cases} 1 & \text{if } n = 1 \\ 0 & \text{if } n > 0 \end{cases}$$

are arithmetical. If α and β are two arithmetical functions, then their *Dirichlet product* is

$$(\alpha * \beta)(n) = \sum_{d|n} \alpha(d)\beta(\frac{n}{d}).$$

The Dirichlet product is commutative, associative, and has the function I as an identity, i.e.,

$$\alpha * I = \alpha \text{ for all arithmetical } \alpha.$$

An arithmetical function α is said to have an *inverse* α^{-1} if $\alpha * \alpha^{-1} = I$. For instance, we have

$$\mu^{-1} = u \tag{2}$$

since

$$(\mu * u)(n) = \sum_{d|n} \mu(d) u\left(\frac{n}{d}\right) = \sum_{d|n} \mu(d) = \begin{cases} 1, & \text{if } n = 1, \\ 0, & \text{if } n > 1 \end{cases} = I(n).$$

2. Möbius Inversion Formulas for Multivariable Functions

In this section we extend generalized convolutions and the Möbius inversion formula to functions of more than one variable. The inspiration for the results in this section came from the work of Apostol in [1] on convolutions and inversion formulas for arithmetical functions.

Definition 2. Let α be an arithmetical function, F an arithmetical function of k variables, and G a generalized arithmetical function of k variables. Then we define two arithmetical functions in k variables $\alpha \bullet F$ and $\alpha \diamond F$ and a generalized arithmetical function $\alpha \circ G$ as follows:

$$(\alpha \bullet F)(m, n_1, n_2, \ldots, n_{k-1}) = \sum_{d|m} \alpha(d) F\left(\frac{m}{d}, \left[\frac{n_1}{d}\right], \left[\frac{n_2}{d}\right], \ldots, \left[\frac{n_{k-1}}{d}\right]\right).$$

$$(\alpha \diamond F)(n_1, n_2, \ldots, n_k) = \sum_{d|\gcd(n_1, n_2, \ldots, n_k)} \alpha(d) F\left(\frac{n_1}{d}, \frac{n_2}{d}, \ldots, \frac{n_k}{d}\right).$$

$$(\alpha \circ G)(y_1, y_2, \ldots, y_{k-1}, x) = \sum_{n \le x} \alpha(x) G\left(\frac{y_1}{n}, \frac{y_2}{n}, \ldots, \frac{y_{k-1}}{n}, \frac{x}{n}\right).$$

The following result states that the function I behaves as a left identity for the classes of arithmetical functions and generalized arithmetical functions.

Proposition 1. If F is an arithmetical function of k variables and G is a generalized arithmetical function of k variables, then the following identities hold.

$$(a) \qquad I \bullet F = I \diamond F = F.$$

$$(b) \qquad I \circ G = G.$$

Proof. (a) We have

$$(I \bullet F)(m, n_1, n_2 \ldots, n_{k-1}) = \sum_{d|m} I(d) F\left(\frac{m}{d}, \left[\frac{n_1}{d}\right], \left[\frac{n_2}{d}\right], \ldots, \left[\frac{n_{k-1}}{d}\right]\right) = F(m, n_1, n_2 \ldots, n_{k-1})$$

and

$$(I \diamond F)(n_1, n_2 \ldots, n_k) = \sum_{d|\gcd(n_1, n_2, \ldots, n_k)} I(d) F\left(\frac{n_1}{d}, \frac{n_2}{d}, \ldots, \frac{n_k}{d}\right) = F(n_1, n_2 \ldots, n_k).$$

(b) Similar to (a). □

Theorem 1. If α and β are arithmetical functions, F is an arithmetical function of k variables, and G is a generalized arithmetical function with k variables, then the following identities are true.

$$(a) \qquad \alpha \bullet (\beta \bullet F) = (\alpha * \beta) \bullet F.$$

$$(b) \qquad \alpha \circ (\beta \circ G) = (\alpha * \beta) \circ G.$$

$$(c) \qquad \alpha \diamond (\beta \diamond F) = (\alpha * \beta) \diamond F.$$

Proof. (a) We only prove the theorem for functions in two variables since the proof can be adapted easily for more variables. The following identities are true:

$$\begin{aligned}
(\alpha \bullet (\beta \bullet F))(m, n) &= \sum_{d|m} \alpha(d) (\beta \bullet F)\left(\frac{m}{d}, \left[\frac{n}{d}\right]\right) \\
&= \sum_{d|m} \alpha(d) \sum_{e|\frac{m}{d}} \beta(e) F\left(\frac{m}{de}, \left[\frac{\left[\frac{n}{d}\right]}{e}\right]\right) \\
&= \sum_{d|m} \alpha(d) \sum_{e|\frac{m}{d}} \beta(e) F\left(\frac{m}{de}, \left[\frac{n}{de}\right]\right) \\
&= \sum_{c|m} \left(\sum_{d|c} \alpha(d) \beta(\frac{c}{d})\right) F\left(\frac{m}{c}, \left[\frac{n}{c}\right]\right) \\
&= \sum_{c|m} (\alpha * \beta)(c) F\left(\frac{m}{c}, \left[\frac{n}{c}\right]\right) \\
&= ((\alpha * \beta) \bullet F)(m, n),
\end{aligned}$$

where the third identity follows by Equation (1).
(b) This part is obtained similarly as part (a).
(c) We only prove the result for functions in two variables since the proof can be adapted easily for more variables. The following identities are true:

$$\begin{aligned}
(\alpha \diamond (\beta \diamond F))(m,n) &= \sum_{d \mid \gcd(m,n)} \alpha(d)(\beta \diamond F)\left(\frac{m}{d}, \frac{n}{d}\right) \\
&= \sum_{d \mid \gcd(m,n)} \alpha(d) \sum_{e \mid \gcd(\frac{m}{d}, \frac{n}{d})} \beta(e) F\left(\frac{m}{de}, \frac{n}{de}\right) \\
&= \sum_{c \mid \gcd(m,n)} \left(\sum_{d \mid c} \alpha(d) \beta\left(\frac{c}{d}\right) \right) F\left(\frac{m}{c}, \frac{n}{c}\right) \\
&= \sum_{c \mid \gcd(m,n)} (\alpha * \beta)(c) F\left(\frac{m}{c}, \frac{n}{c}\right) \\
&= \big((\alpha * \beta) \diamond F\big)(m,n).
\end{aligned}$$

□

We now give the following variants of the Möbius inversion formula and note that part (b) is a generalization for [1, Theorem 2.22]. For simplicity we let

$$(m, \bar{n}) = (m, n_1, n_2, \ldots, n_{k-1}), \ \left(\frac{m}{d}, \left[\frac{\bar{n}}{d}\right]\right) = \left(\frac{m}{d}, \left[\frac{n_1}{d}\right], \left[\frac{n_2}{d}\right], \ldots, \left[\frac{n_{k-1}}{d}\right]\right),$$

$$(\bar{y}, x) = (y_1, y_2, \ldots, y_{k-1}, x), \text{ and } \left(\frac{\bar{y}}{n}, \frac{x}{n}\right) = \left(\frac{y_1}{n}, \frac{y_2}{n}, \ldots, \frac{y_{k-1}}{n}, \frac{x}{n}\right).$$

Theorem 2. Let α be an arithmetical function that has an inverse α^{-1}.
(a) If F and G are arithmetical of k variables, then

$$G(m, \bar{n}) = \sum_{d \mid m} \alpha(d) F\left(\frac{m}{d}, \left[\frac{\bar{n}}{d}\right]\right) \text{ if and only if } F(m, \bar{n}) = \sum_{d \mid m} \alpha^{-1}(d) G\left(\frac{m}{d}, \left[\frac{\bar{n}}{d}\right]\right)$$

and

$$G(m, \bar{n}) = \sum_{d \mid m} F\left(\frac{m}{d}, \left[\frac{\bar{n}}{d}\right]\right) \text{ if and only if } F(m, \bar{n}) = \sum_{d \mid m} \mu(d) G\left(\frac{m}{d}, \left[\frac{\bar{n}}{d}\right]\right).$$

(b) If F and G are generalized arithmetical of k variables, then

$$G(\bar{y}, x) = \sum_{n \le x} \alpha(n) F\left(\frac{\bar{y}}{n}, \frac{x}{n}\right) \text{ if and only if } F(\bar{y}, x) = \sum_{n \le x} \alpha^{-1}(n) G\left(\frac{\bar{y}}{n}, \frac{x}{n}\right)$$

and

$$G(\bar{y}, x) = \sum_{n \le x} F\left(\frac{\bar{y}}{n}, \frac{x}{n}\right) \text{ if and only if } F(\bar{y}, x) = \sum_{n \le x} \mu(n) G\left(\frac{\bar{y}}{n}, \frac{x}{n}\right)$$

(c) If F and G are arithmetical of k variables, then we have the following two equivalences:

$$G(n_1, n_2, \ldots, n_k) = \sum_{d|\gcd(n_1,n_2,\ldots,n_k)} \alpha(d) F\left(\frac{n_1}{d}, \frac{n_2}{d}, \ldots, \frac{n_k}{d}\right) \text{ if and only if}$$

$$F(n_1, n_2, \ldots, n_k) = \sum_{d|\gcd(n_1,n_2,\ldots,n_k)} \alpha^{-1}(d) G\left(\frac{n_1}{d}, \frac{n_2}{d}, \ldots, \frac{n_k}{d}\right)$$

and

$$G(n_1, n_2, \ldots, n_k) = \sum_{d|\gcd(n_1,n_2,\ldots,n_k)} F\left(\frac{n_1}{d}, \frac{n_2}{d}, \ldots, \frac{n_k}{d}\right) \text{ if and only if}$$

$$F(n_1, n_2, \ldots, n_k) = \sum_{d|\gcd(n_1,n_2,\ldots,n_k)} \mu(d) G\left(\frac{n_1}{d}, \frac{n_2}{d}, \ldots, \frac{n_k}{d}\right).$$

Proof. (a) Assume that $G = \alpha \bullet F$. Then by virtue of Theorem 1 and Proposition 1 we find that

$$\alpha^{-1} \bullet G = \alpha^{-1} \bullet (\alpha \bullet F) = (\alpha^{-1} * \alpha) \bullet F = I \bullet F = F.$$

The implication from right to left follows similarly. The second equivalence of part (a) is a special case of the first one since $\mu^{-1} = u$ by Equation (2).
Parts (b) and (c) are obtained similarly. □

3. Relatively Prime Subsets

Definition 3. Let

$$g(m, n) = \#\{A \subseteq \{m, \ldots, n\} : \ m \in A \text{ and } \gcd(A) = 1\},$$

$$g_k(m, n) = \#\{A \subseteq \{m, \ldots, n\} : \ m \in A, \ \#A = k, \text{ and } \gcd(A) = 1\},$$

$$f(m, n) = \#\{A \subseteq \{m, \ldots, n\} : \ A \neq \emptyset \text{ and } \gcd(A) = 1\}, \text{ and}$$

$$f_k(m, n) = \#\{A \subseteq \{m, \ldots, n\} : \ \#A = k \text{ and } \gcd(A) = 1\}.$$

Note that the functions g, g_k, and f_k count sets $A \subseteq \{m, \ldots, n\}$ that are nonempty because of the condition $m \in A$ in the definitions of g and g_k and the condition $\#A = k$ in the definition of f_k.
In [2], $f(n) = f(1, n)$ and $f_k(n) = f_k(1, n)$ and by [2, Theorem 1] we have

$$f(1, n) = \sum_{d=1}^{n} \mu(d)(2^{[\frac{n}{d}]} - 1) \text{ and } f_k(1, n) = \sum_{d=1}^{n} \mu(d) \binom{[\frac{n}{d}]}{k}. \tag{3}$$

Lemma 1. If $n \geq m$, then we have the following two identities.

$$(a) \ g(m, n) = \sum_{d|m} \mu(d) 2^{[\frac{n}{d}] - \frac{m}{d}}.$$

$$(b)\ g_k(m,n) = \sum_{d|m} \mu(d) \binom{[\frac{n}{d}] - \frac{m}{d}}{k-1}.$$

Proof. (a) Let $\mathcal{P}(m,n)$ denote the set of subsets of $\{m,\ldots,n\}$ containing m. Clearly, $\#\mathcal{P}(m,n) = 2^{n-m}$. It is also clear that the set $\mathcal{P}(m,n)$ can be partitioned using the relation of having the same gcd. Moreover, the mapping $A \mapsto \frac{1}{d}A$ is a one-to-one correspondence between the subsets of $\mathcal{P}(m,n)$ having gcd $= d$ (dividing m) and the relatively prime subsets of $\{\frac{m}{d},\ldots,[\frac{n}{d}]\}$ which contain $\frac{m}{d}$. Then we find the following identity

$$2^{n-m} = \sum_{d|m} g\left(\frac{m}{d}, \left[\frac{n}{d}\right]\right),$$

which by Theorem 2(a) is equivalent to

$$g(m,n) = \sum_{d|m} \mu(d) 2^{[\frac{n}{d}] - \frac{m}{d}}.$$

(b) Noting that the correspondence $A \mapsto \frac{1}{d}A$ defined above preserves the cardinality and using a similar argument as in part (a), we find the following identity

$$\binom{n-m}{k-1} = \sum_{d|m} g_k\left(\frac{m}{d}, \left[\frac{n}{d}\right]\right)$$

which by Theorem 2(a) is equivalent to $g_k(m,n) = \sum_{d|m} \mu(d) \binom{[\frac{n}{d}] - \frac{m}{d}}{k-1}$. $\square$

Theorem 3. If $n \geq m$, then the following two identities are true.

$$(a)\ f(m,n) = \sum_{d=1}^{n} \mu(d)(2^{[\frac{n}{d}]} - 1) - \sum_{i=1}^{m-1} \sum_{d|i} \mu(d) 2^{[\frac{n}{d}] - \frac{i}{d}}.$$

$$(b)\ f_k(m,n) = \sum_{d=1}^{n} \mu(d) \binom{[\frac{n}{d}]}{k} - \sum_{i=1}^{m-1} \sum_{d|i} \mu(d) \binom{[\frac{n}{d}] - \frac{i}{d}}{k-1}.$$

Proof. (a) Repeatedly applying Lemma 1 together with Equation (3) yield the following identities:

$$\begin{aligned} f(m,n) &= f(m-1,n) - g(m-1,n) \\ &= f(m-2,n) - (g(m-2,n) + g(m-1,n)) \\ &= f(1,n) - \sum_{i=1}^{m-1} g(i,n) \\ &= \sum_{d=1}^{n} \mu(d)(2^{[\frac{n}{d}]} - 1) - \sum_{i=1}^{m-1} \sum_{d|i} \mu(d) 2^{[\frac{n}{d}] - \frac{i}{d}}. \end{aligned}$$

(b) Similar to (a). $\square$

4. Phi Functions

Definition 4. Let

$$\Psi(m,n) = \#\{A \subseteq \{m,\dots,n\} : \ m \in A \text{ and } \gcd(A \cup \{n\}) = 1\},$$

$$\Psi_k(m,n) = \#\{A \subseteq \{m,\dots,n\} : \ m \in A,\ \#A = k, \text{ and } \gcd(A \cup \{n\}) = 1\},$$

$$\Phi(m,n) = \#\{A \subseteq \{m,\dots,n\} : \ A \neq \emptyset \text{ and } \gcd(A \cup \{n\}) = 1\}, \text{ and}$$

$$\Phi_k(m,n) = \#\{A \subseteq \{m,\dots,n\} : \ \#A = k \text{ and } \gcd(A \cup \{n\}) = 1\}.$$

Note that the four functions in this definition count sets that are nonempty.
In [2], $\Phi(n) = \Phi(1,n)$ and $\Phi_k(n) = \Phi_k(1,n)$ and by [2, Theorem 3] we have

$$\Phi(1,n) = \sum_{d|n} \mu(d) 2^{n/d} \text{ and } \Phi_k(1,n) = \sum_{d|n} \mu(d) \binom{n/d}{k}. \tag{4}$$

Lemma 2. If $n \geq m$, then we have the following two identities.

$$(a)\ \Psi(m,n) = \sum_{d|\gcd(m,n)} \mu(d) 2^{\frac{n-m}{d}}.$$

$$(b)\ \Psi_k(m,n) = \sum_{d|\gcd(m,n)} \mu(d) \binom{\frac{n-m}{d}}{k-1}.$$

Proof. (a) Let $\mathcal{P}(m,n)$ be as in the proof of Lemma and let

$$\mathcal{P}(m,n,d) = \{A \subseteq \{m,\dots,n\} : \ m \in A \text{ and } \gcd(A \cup \{n\}) = d\}.$$

We know that the set $\mathcal{P}(m,n)$, with 2^{n-m} elements, can be partitioned using the equivalence relation "$\equiv$" for having the same gcd, that is:

$$A \equiv B \text{ if and only if } A, B \in \mathcal{P}(m,n,d) \text{ for some } d|\gcd(m,n).$$

Furthermore, the mapping $A \mapsto \frac{1}{d}A$ is a one-to-one correspondence between $\mathcal{P}(m,n,d)$ and the set of subsets B of $\{m/d,\dots,n/d\}$ such that $m/d \in B$ and $\gcd(B \cup \{n/d\}) = 1$. Then we have that $\#\mathcal{P}(m,n,d) = \Psi\left(\frac{m}{d}, \frac{n}{d}\right)$. Thus, we find the following identity:

$$2^{n-m} = \sum_{d|\gcd(m,n)} \#\mathcal{P}(m,n,d) = \sum_{d|\gcd(m,n)} \Psi\left(\frac{m}{d}, \frac{n}{d}\right),$$

which by Theorem 2(c) is equivalent to

$$\Psi(m,n) = \sum_{d|\gcd(m,n)} \mu(d) 2^{\frac{n-m}{d}}.$$

(b) Noting that the correspondence $A \mapsto \frac{1}{d}A$ defined above preserves the cardinality and using an argument similar to the one in part (a), we obtain the following identity

$$\binom{n-m}{k-1} = \sum_{d|\gcd(m,n)} \Psi_k\left(\frac{m}{d}, \frac{n}{d}\right)$$

which by Theorem 2(c) is equivalent to

$$\Psi_k(m,n) = \sum_{d|\gcd(m,n)} \mu(d)\binom{\frac{n-m}{d}}{k-1}.$$

□

Theorem 4. If $n \geq m$, then the following two identities are true.

$$(a)\ \Phi(m,n) = \sum_{d|n} \mu(d)2^{\frac{n}{d}} - \sum_{i=1}^{m-1} \sum_{d|\gcd(i,n)} \mu(d)2^{\frac{n-i}{d}}.$$

$$(b)\ \Phi_k(m,n) = \sum_{d|n} \mu(d)\binom{n/d}{k} - \sum_{i=1}^{m-1} \sum_{d|\gcd(i,n)} \mu(d)\binom{\frac{n-i}{d}}{k-1}.$$

Proof. (a) Repeatedly applying Lemma 2(a) together with Equation (4) yield the following identities:

$$\begin{aligned}\Phi(m,n) &= \Phi(m-1,n) - \Psi(m-1,n)\\ &= \Phi(m-2,n) - (\Psi(m-2,n) + \Psi(m-1,n))\\ &= \Phi(1,n) - \sum_{i=1}^{m-1} \Psi(i,n)\\ &= \sum_{d|n} \mu(d)2^{\frac{n}{d}} - \sum_{i=1}^{m-1} \sum_{d|\gcd(i,n)} \mu(d)2^{\frac{n-i}{d}}.\end{aligned}$$

(b) Similar to (a). □

Acknowledgment The author is grateful to the referee for valuable comments and interesting suggestions.

References

[1] T. M. Apostol, *Introduction to Analytic Number Theory*, Undergraduate Texts in Mathematics, Springer, 1 edition, 1976.

[2] M. B. Nathanson, *Affine invariants, relatively prime sets, and a phi function for subsets of* $\{1, 2, \ldots, n\}$, Integers: Electronic Journal of Combinatorial Number Theory 7 (2007), #A01.