ON THE NUMBER OF SUBSETS OF $[1, M]$ RELATIVELY PRIME TO $N$ AND ASYMPTOTIC ESTIMATES

Mohamed El Bachraoui
Department of Mathematical Sciences, United Arab Emirates University, P.O. Box 17551, Al-Ain, UAE
melbachraoui@uaeu.ac.ae

Received: 2/27/08, Accepted: 9/1/08, Published: 9/23/08

Abstract

A set $A$ of positive integers is relatively prime to $n$ if $\gcd(A \cup \{n\}) = 1$. Given positive integers $l \leq m \leq n$, let $\Phi([l, m], n)$ denote the number of nonempty subsets of $\{l, l+1, \ldots, m\}$ which are relatively prime to $n$ and let $\Phi_k([l, m], n)$ denote the number of such subsets of cardinality $k$. In this paper we give formulas for these functions for the case $l = 1$. Intermediate consequences include identities for the number of subsets of $\{1, 2, \ldots, n\}$ with elements in both $\{1, 2, \ldots, m\}$ and $\{m, m+1, \ldots, n\}$ which are relatively prime to $n$ and the number of such subsets having cardinality $k$. Some of our proofs use the Möbius inversion formula extended to functions of several variables.

1. Introduction

Let $k$ and $l \leq m \leq n$ denote positive integers, let $[l, m] = \{l, l+1, \ldots, m\}$, and let $\lfloor x \rfloor$ be the floor of $x$. For nonnegative integers $0 \leq M \leq N$ we have the following basic identity for binomial coefficients:

$$\sum_{j=k}^{N} \binom{j}{k} = \binom{N+1}{k+1}. \quad (1)$$

**Definition 1.** Let $\Phi([l, m], n) = \#\{A \subseteq [l, m] : A \neq \emptyset, \text{ and } \gcd(A \cup \{n\}) = 1\}$ and $\Phi_k([l, m], n) = \#\{A \subseteq [l, m] : \#A = k, \text{ and } \gcd(A \cup \{n\}) = 1\}$.

Nathanson [2] found

$$\Phi([1, n], n) = \sum_{d|n} \mu(d)2^{n/d},$$

$$\Phi_k([1, n], n) = \sum_{d|n} \mu(d) \binom{n/d}{k}. \quad (2)$$
El Bachraoui [1] obtained

\[ \Phi([m, n], n) = \sum_{d|n} \mu(d)2^{n/d} - \sum_{i=1}^{m-1} \sum_{d|(i,n)} \mu(d)2^{(n-i)/d}, \]

\[ \Phi_k([m, n], n) = \sum_{d|n} \mu(d) \binom{n/d}{k} - \sum_{i=1}^{m-1} \sum_{d|(i,n)} \mu(d) \binom{(n-i)/d}{k-1}. \]

Nathanson-Orosz [3] simplified the latter two identities and found

\[ \Phi([m, n], n) = \sum_{d|n} \mu(d)2^{(n/d) - [(m-1)/d]}, \]

\[ \Phi_k([m, n], n) = \sum_{d|n} \mu(d) \binom{n/d - [(m-1)/d]}{k}. \] (3)

2. Phi Functions for \([1, m]\)

Our main goal is to give identities for the functions \(\Phi([1, m], n)\) and \(\Phi_k([1, m], n)\). We need the following lemma.

**Lemma 2.** Let \(\Psi([1, m], n) = \#\{A \subseteq [1, m] : m \in A \text{ and } \gcd(A \cup \{n\}) = 1\}\) and \(\Psi_k([1, m], n) = \#\{A \subseteq [1, m] : m \in A, \ A = k, \text{ and } \gcd(A \cup \{n\}) = 1\}\). Then

(a) \[ \Psi([1, m], n) = \sum_{d|(m,n)} \mu(d)2^{m/d-1}. \]

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

**Proof.** (a) Let \(\mathcal{P}(m)\) denote the set of subsets of \([1, m]\) containing \(m\) and let \(\mathcal{P}(m, d)\) be the set of subsets \(A\) of \([1, m]\) such that \(m \in A\) and \(\gcd(A \cup \{n\}) = d\). It is clear that the set \(\mathcal{P}(m)\) of cardinality \(2^{m-1}\) can be partitioned using the equivalence 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 \(\mathcal{P}(m, d)\) and the set of subsets \(B\) of \([1, m/d]\) such that \(m/d \in B\) and \(\gcd(B \cup \{n/d\}) = 1\). Then \(\#\mathcal{P}(m, d) = \Psi([1, m/d], n/d)\). Thus,

\[ 2^{m-1} = \sum_{d|(m,n)} \#\mathcal{P}(m, d) = \sum_{d|(m,n)} \Psi([1, m/d], n/d), \]

which by the Möbius inversion formula extended to multivariable functions [1, Theorem 2(c)] is equivalent to

\[ \Psi([1, m], n) = \sum_{d|(m,n)} \mu(d)2^{m/d-1}. \]
(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

\[
\binom{m - 1}{k - 1} = \sum_{d|\langle m, n \rangle} \Psi_k([1, m/d], n/d)
\]

which by the Möbius inversion formula [1, Theorem 2(c)] is equivalent to

\[
\Psi_k([1, m], n) = \sum_{d|\langle m, n \rangle} \mu(d) \binom{m/d - 1}{k - 1}.
\]

\[\square\]

**Theorem 3.** We have

(a) $\Phi([1, m], n) = \sum_{d|n} \mu(d) 2^{m/d}$.

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

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

\[
\Phi([1, m], n) = \Phi([1, m + 1], n) - \Psi([1, m + 1], n)
\]

\[= \Phi([1, m + 2], n) - (\Psi([1, m + 2], n) + \Psi([1, m + 1], n))\]

\[= \Phi([1, n], n) - \sum_{i=1}^{n-m} \Psi([1, m + i], n)\]

\[= \sum_{d|n} \mu(d) 2^{n/d} - \sum_{i=1}^{n-m} \sum_{d|\langle m+i, n \rangle} \mu(d) 2^{(m+i)/d-1}\]

\[= \sum_{d|n} \mu(d) 2^{n/d} - \sum_{d|n} \mu(d) \sum_{i=1}^{n-m} 2^{(m+i)/d-1}\]

\[= \sum_{d|n} \mu(d) 2^{n/d} - \sum_{d|n} \mu(d) \sum_{j=[m/d]+1}^{n/d} 2^{j-1}\]

\[= \sum_{d|n} \mu(d) (2^{n/d} - 2^{[m/d]} (2^{n/d-[m/d]} - 1))\]

\[= \sum_{d|n} \mu(d) 2^{[m/d]}\].

(b) Similar to (a), repeatedly applying Lemma 2(b) together with Equation (2) we find

\[
\Phi_k([1, m], n) = \sum_{d|n} \mu(d) \binom{n/d}{k} - \sum_{i=1}^{n-m} \sum_{d|\langle m+i, n \rangle} \mu(d) \binom{(m+i)/d-1}{k-1}.
\]
Then
\[
\Phi_k([1,m], n) = \sum_{d \mid n} \mu(d) \left( \frac{n/d}{k} \right) - \sum_{d \mid n} \mu(d) \sum_{i=1}^{n-m} \left( \frac{(m+i)/d - 1}{k-1} \right)
\]
\[
= \sum_{d \mid n} \mu(d) \left( \frac{n/d}{k} \right) - \sum_{d \mid n} \mu(d) \sum_{j=[m/d]+1}^{n/d} \left( \frac{j-1}{k-1} \right)
\]
\[
= \sum_{d \mid n} \mu(d) \left( \frac{n/d}{k} - \sum_{j=1}^{n/d} \left( \frac{j-1}{k-1} \right) \right)
= \sum_{d \mid n} \mu(d) \left( \left( \frac{n/d}{k} \right) - \left( \frac{[m/d]}{k} \right) \right)
= \sum_{d \mid n} \mu(d) \left( \left[ \frac{m/d}{k} \right] \right),
\]
where the next-to-last identity follows by (1).

**Corollary 4.** Let \( U(m, n) \) be the number of nonempty subsets of \([1, n]\) with elements in both \([1, m]\) and \([m, n]\) which are relatively prime to \( n \) and let \( U_k(m, n) \) be the number of such sets of cardinality \( k \). Then
\[
U(m, n) = \sum_{d \mid n} \mu(d) \left( 2^{n/d} - 2^{\lfloor (m-1)/d \rfloor} - 2^{n/d-[m/d]} \right)
\]
and
\[
U_k(m, n) = \sum_{d \mid n} \mu(d) \left( \left( \frac{n/d}{k} \right) - \left( \frac{[m-1]/d}{k} \right) - \left( \frac{n/d-[m/d]}{k} \right) \right).
\]

**Proof.** The are immediate from equations (2) and (3), Theorem 3, and the obvious facts that
\[
U(m, n) = \Phi([1,n], n) - \Phi([1,m-1], n) - \Phi([m+1,n], n)
\]
and
\[
U_k(m, n) = \Phi_k([1,n], n) - \Phi_k([1,m-1], n) - \Phi_k([m+1,n], n).
\]

3. Asymptotic Estimates

**Theorem 5.** Let \( p \) be the smallest prime divisor of \( n \) in the interval \([1,m]\). Then we have the following inequalities:
\[
(a) \quad 0 \leq 2^m - 2^{[m/p]} - \Phi([1,m], n) \leq m2^{[m/p]}.
\]
\[(b)\quad 0 \leq \left(\frac{m}{k}\right) - \left(\frac{\lfloor m/p \rfloor}{k}\right) - \Phi_k([1, m], n) \leq m\left(\frac{\lfloor m/p \rfloor}{k}\right).\]

**Proof.** (a) The number \(2^m - 2^{\lfloor m/p \rfloor}\) of sets consisting of multiples of \(p\) in \([1, m]\) is an upper bound for \(\Phi([1, m], n)\). As to the lower bound we have

\[
\Phi([1, m], n) - (2^m - 2^{\lfloor m/p \rfloor}) = \sum_{\substack{d|n \\text{ and } d > p}} \mu(d)2^{\lfloor m/d \rfloor} \leq m2^{\lfloor m/p \rfloor}.
\]

(b) The number \(\left(\frac{m}{k}\right) - \left(\frac{\lfloor m/p \rfloor}{k}\right)\) of sets consisting of multiples of \(p\) in \([1, m]\) and having cardinality \(k\) is an upper bound for \(\Phi_k([1, m], n)\). As to the lower bound we find

\[
\Phi_k([1, m], n) = \left(\frac{m}{k}\right) - \left(\frac{\lfloor m/p \rfloor}{k}\right) + \sum_{\substack{d|n \\text{ and } d > p}} \mu(d)\left(\frac{\lfloor m/d \rfloor}{k}\right)
\geq \left(\frac{m}{k}\right) - \left(\frac{\lfloor m/p \rfloor}{k}\right) - \sum_{\substack{d|n \\text{ and } d > p}} \left(\frac{\lfloor m/d \rfloor}{k}\right)
\geq \left(\frac{m}{k}\right) - \left(\frac{\lfloor m/p \rfloor}{k}\right) - m\left(\frac{\lfloor m/p \rfloor}{k}\right).
\]

\[\square\]

**Acknowledgment.** The author is grateful to the referee for valuable comments.

**References**

