#A28 INTEGERS 9 (2009), 343-352

ON RELATIVELY PRIME SETS

Mohamed Ayad
Laboratoire de Math. Pures et Appliquées, Université du Littoral, Calais, France
Ayad@lmpa.univ-littoral.fr
Omar Kihel[1]
Department of Mathematics, Brock University, St. Catharines, Ontario, Canada
okihel@brocku.ca

Abstract

Functions counting the number of subsets of $\{1, 2, \ldots, n\}$ having particular properties are defined by Nathanson. Here, generalizations in two directions are given.

Received: 10/1/08, Revised: 3/20/09, Accepted: 3/30/09

1. Introduction

A nonempty subset A of $\{1, 2, \ldots, n\}$ is said to be relatively prime if $\gcd(A) = 1$. Nathanson [2] defined $f(n)$ to be the number of relatively prime subsets of $\{1, 2, \ldots, n\}$ and, for $k \geq 1$, $f_k(n)$ to be the number of relatively prime subsets of $\{1, 2, \ldots, n\}$ of cardinality k. By analogy with Euler's phi function $\phi(n)$ that counts the number of positive integers a in the set $\{1, 2, \ldots, n\}$ such that $\gcd(a, n) = 1$, Nathanson [2] defined $\Phi(n)$ to be the number of nonempty subsets A of the set $\{1, 2, \ldots, n\}$ such that $\gcd(A)$ is relatively prime to n, and for an integer $k \geq 1$, $\Phi_k(n)$ to be the number of subsets A of the set $\{1, 2, \ldots, n\}$ such that $\gcd(A)$ is relatively prime to n and $\text{card}(A) = k$. He obtained explicit formulas for these four functions and deduced asymptotic estimates [2].

The functions $f(n)$, $f_k(n)$, $\Phi(n)$ and $\Phi_k(n)$ have been generalized by El Bachraoui [1] to subsets $A \subseteq \{m + 1, m + 2, \ldots, n\}$ where m is any nonnegative integer. His proofs use an extension of generalized convolutions and the Möbius inversion formula to functions of several variables. Nathanson and Orosz [3] used El Bachraoui's result to obtain simple explicit formulas and asymptotic estimates. A natural extension of this problem is to generalize the previous functions to subsets of the set $\{a, a + b, \ldots, a + (n - 1)b\}$ where a and b are any integers. Nathanson [2] considered the special case $(a, b) = (1, 1)$, and El Bachraoui [1] and Nathanson and Orosz [3] considered the case $(a, b) = (m + 1, 1)$ where m is any non-negative integer. In [1] and [2], the proofs made use of the fact that the mapping $A \to \frac{1}{d}A$ is a one-to-one correspondence between the subsets of $\{m, \ldots, n\}$ containing m and having gcd $= d$ (dividing m), and the relatively prime subsets of $\{\frac{m}{d}, \ldots, [\frac{n}{d}]\}$ which contain $\frac{m}{d}$. Their methods seem not to generalize to the case where a and b are any two integers.

In the first part of this paper, we generalize the four functions $f(n)$, $f_k(n)$, $\Phi(n)$ and $\Phi_k(n)$ to subsets of the set $\{a, a + b, \ldots, a + (n - 1)b\}$ where a and b are any

[1]Research partially supported by NSERC.

integers. We give in Theorem 3.1 and Theorem 3.4 explicit formulas for the generalized functions we define. We show in Corollary 3.6, that the results of Nathanson [2], El Bachraoui [1] and Nathanson and Orosz [3] can be deduced as particular cases from Theorem 3.1 and Theorem 3.4.

One can easily recognize that $\Phi(n)$ represents the number of primitive elements of the field $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$. In the second part of this paper, among other results, we define a new function $\Psi(n,m)$ generalizing $\Phi(n)$ such that $\Psi(n,p)$ represents the number of primitive elements of $\mathbb{F}_{p^n}$ over $\mathbb{F}_p$.

2. Relatively Prime Subsets and a Phi Function for Subsets of $\{m,\, m+1,\, \ldots,\, l\}$

Let $[x]$ denote the greatest integer less than or equal to x, and $\mu(n)$ the Möbius function. Nathanson [2] proved the following two theorems.

Theorem 1. *For all positive integers n and for $k \geq 1$,*

$$f(n) = \sum_{d=1}^{n} \mu(d)\left(2^{[n/d]} - 1\right)$$

and

$$f_k(n) = \sum_{d=1}^{n} \mu(d) \binom{[n/d]}{k}.$$

Theorem 2. *For all positive integers $n \geq 2$ and $k \geq 1$*

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

and

$$\Phi_k(n) = \sum_{d|n} \mu(d) \binom{\frac{n}{d}}{k}.$$

Theorem 1 implies that $f(n) \sim 2^n$ as $n \to \infty$, which means that almost all finite sets of integers are relatively prime.

Theorems 1 and 2 have been generalized by El Bachraoui [1] to subsets of the set $\{m+1,\, m+2,\, \ldots,\, l\}$ for arbitrary non-negative integers $m < l$. Using an extension of the Möbius inversion formula to functions of many variables and generalized convolutions, El Bachraoui [1] obtained explicit formulas for the generalized functions he defined and Nathanson and Orosz [3] simplified them. They proved in [1], [3] the following two theorems.

Theorem 3. *For non-negative integers $m < l$ and for $k \geq 1$, let $f(m,l)$ denote the number of relatively prime subsets of $\{m+1,\, m+2,\, \ldots,\, l\}$ and $f_k(m,l)$ denote the number of relatively prime subsets of $\{m+1,\, m+2,\, \ldots,\, l\}$ of cardinality k. Then*

$$f(m,l) = \sum_{d=1}^{l} \mu(d) \left(2^{\left[\frac{l}{d}\right] - \left[\frac{m}{d}\right]} - 1 \right)$$

and

$$f_k(m,l) = \sum_{d=1}^{l} \mu(d) \binom{[l/d] - [m/d]}{k}.$$

Theorem 4. *For non-negative integers $m < l$ and for $k \geq 1$, let $\Phi(m,l)$ denote the number of subsets of the set $\{m+1,\, m+2,\, \ldots,\, l\}$ such that $\gcd(A)$ is relatively prime to n, and $\Phi_k(m,l)$ denote the number of subsets of the set $\{m+1, m+2, \ldots, l\}$ of cardinality k such that $\gcd(A)$ is relatively prime to n. Then*

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

and

$$\Phi_k(m,l) = \sum_{d|l} \mu(d) \binom{\frac{l}{d} - \left[\frac{m}{d}\right]}{k}.$$

3. Relatively Prime Subsets and a Phi Function for Subsets of $\{a,\, a+b,\, \ldots,\, a+(n-1)b\}$

It is natural to ask whether one can generalize the formulas obtained by Nathanson [2], El Bachraoui [1], and Nathanson and Orosz [3] to subsets of a set $A = \{a,\, a+b,\, \ldots,\, a+(n-1)b\}$, where a, b, and n are any integers. The purpose of this section is to generalize Theorems 2.1, 2.2, 2.3 and 2.4 to the general case where a and b are any integers. The generalization is given in Theorem 3.1 and Theorem 3.5.

Theorem 5. *For all positive integers n, a and b, let $f^{(a,b)}(n)$ denote the number of relatively prime subsets of $\{a,\, a+b,\, \ldots,\, a+(n-1)b\}$ and $f_k^{(a,b)}(n)$ denote the number of relatively prime subsets of $\{a, a+b, \ldots, a+(n-1)b\}$ of cardinality k. Suppose that $\gcd(a,b) = 1$, then*

$$f^{(a,b)}(n) = \sum_{\substack{d=1 \\ \gcd(b,d)=1}}^{a+(n-1)b} \mu(d) \left(2^{[n/d]+\varepsilon_d} - 1 \right)$$

and

$$f_k^{(a,b)}(n) = \sum_{\substack{d=1 \\ \gcd(b,d)=1}}^{a+(n-1)b} \mu(d) \binom{[n/d]+\varepsilon_d}{k} \tag{1}$$

where

$$\varepsilon_d = \begin{cases} 0 & \text{if } d \mid n, \\ 1 & \text{if } d \nmid n \text{ and } (-ab^{-1}) \bmod d \in \left\{0,\ldots,n-\left[\frac{n}{d}\right]d-1\right\}, \\ 0 & \text{otherwise.} \end{cases}$$

If $\gcd(a,b) \neq 1$, it is easy to see that $f^{(a,b)}(n) = f_k^{(a,b)}(n) = 0$.

To prove Theorem 5, we need the following lemma.

Lemma 6. *For an integer $d \geq 1$, and for nonzero integers a and b with $\gcd(a,b)=1$, let $A_d = \{x = a+ib \text{ for } i = 0,\ldots,(n-1);\ d \mid x\}$.*

(i) *If gcd $(b,d) \neq 1$, then $|A_d| = 0$.*

(ii) *If gcd $(b,d) = 1$, then $|A_d| = \left[\frac{n}{d}\right] + \varepsilon_d$ where*

$$\varepsilon_d = \begin{cases} 0 & \text{if } d \mid n, \\ 1 & \text{if } d \nmid n \text{ and } (-ab^{-1}) \bmod d \in \left\{0,\ldots,n-\left[\frac{n}{d}\right]d-1\right\}, \\ 0 & \text{otherwise.} \end{cases}$$

Proof. (i) If $\gcd(b,d) \neq 1$, then no element of the arithmetic sequence a, $a+b$, $\ldots$, $a+(n-1)b$ is divisible by d because we supposed that $\gcd(a,b)=1$, i.e., A_d is empty and $|A_d| = 0$.

(ii) We suppose that $\gcd(d,b)=1$. If $d \mid n$ then $|A_d| = \left[\frac{n}{d}\right]$. If $d \nmid n$ and $d \leq n$, then every d consecutive terms of the arithmetic sequence a, $a+b$, $\ldots$, $a+(n-1)b$ constitute a complete set of residues mod d. Hence, the sequence a, $a+b$, $\ldots$, $a+\left(\left[\frac{n}{d}\right]d-1\right)b$ contains exactly $\left[\frac{n}{d}\right]$ terms divisible by d. Then $|A_d| = \left[\frac{n}{d}\right]+1$ if and only if one term $a+tb \equiv 0 \pmod d$ for a certain $t \in \left\{\left[\frac{n}{d}\right]d,\ldots,n-1\right\}$. Then $|A_d| = \left[\frac{n}{d}\right]+1$ if and only if $(-ab^{-1}) \bmod d \in \left\{0,\ldots,n-\left[\frac{n}{d}\right]d-1\right\}$, otherwise $|A_d| = \left[\frac{n}{d}\right]$. If $d > n$, the proof is similar. $\square$

Proof of Theorem 3.1. Let $A_d = \{x = a+ib \text{ for } i=0,\ldots,(n-1);\ d \mid x\}$, and $\mathcal{P}(A_d) = \{\text{the nonempty subsets of } A_d\}$. Then

$$f^{(a,b)}(n) = (2^n-1) - \left| \bigcup_{p \text{ prime}} \mathcal{P}(A_p) \right|.$$

The principle of inclusion-exclusion implies that

$$\begin{aligned} f^{(a,b)}(n) &= (2^n-1) - \Big(\sum |\mathcal{P}(A_p)| \\ &- \sum |\mathcal{P}(A_p) \cap \mathcal{P}(A_q)| \\ &+ \sum |\mathcal{P}(A_p) \cap \mathcal{P}(A_q) \cap \mathcal{P}(A_r)| - \dots \Big), \end{aligned}$$

where p, q and r are distinct primes. Clearly, if $p_1, \dots, p_t$ are distinct primes, then

$$\left| \bigcap_{i=1}^{t} \mathcal{P}(A_{p_i}) \right| = \left| \mathcal{P}(A_{\prod_{i=1}^{t} p_i}) \right|.$$

Thus,

$$f^{(a,b)}(n) = \sum_{d=1}^{a+(n-1)b} \mu(d) |\mathcal{P}(A_d)|.$$

Then Lemma 6 implies that

$$f^{(a,b)}(n) = \sum_{\substack{d=1 \\ \gcd(b,d)=1}}^{a+(n-1)b} \mu(d) \left(2^{[n/d]+\varepsilon_d} - 1 \right).$$

The proof for Formula (1) is similar. □

Theorem 7. *For all positive integers a and b such that* $\gcd(a,b) = 1$*,*

$$\lim_{n\to\infty} \frac{f^{(a,b)}(n)}{2^n} = 1.$$

Proof. It is easy to see that $(2^n-1) - (a+(n-1)b-1)\left(2^{n/2+1}-1\right) \le f^{(a,b)}(n) \le (2^n-1)$. Then

$$\lim_{n\to\infty} \frac{f^{(a,b)}(n)}{2^n} = 1.$$

□

Remark 8. *One can obtain better bounds for $f^{(a,b)}(n)$ but we were interested in showing only that almost all subsets of the set $\{a, a+b, \dots, a+(n-1)b\}$ are relatively prime.*

Theorem 9. *For positive integers a, b and n, let $\Phi^{(a,b)}(n)$ denote the number of subsets A of $\{a, a+b, \dots, a+(n-1)b\}$ such that* $\gcd(A)$ *is relatively prime to n, and $\Phi_k^{(a,b)}(n)$ denote the number of subsets A of $\{a, a+b, \dots, a+(n-1)b\}$ such that* $\gcd(A)$ *is relatively prime to n and* $\mathrm{card}(A) = k$*. Suppose that* $\gcd(a,b) = 1$*. Then*

$$\Phi^{(a,b)}(n) = \sum_{\substack{d|n \\ \gcd(b,d)=1}} \mu(d) \left(2^{\frac{n}{d}} - 1 \right)$$

and

$$\Phi_k^{(a,b)}(n) = \sum_{\substack{d|n \\ \gcd(b,d)=1}} \mu(d) \begin{pmatrix} \frac{n}{d} \\ k \end{pmatrix}. \tag{2}$$

Proof. It is easy to see that $\Phi^{(a,b)}(n) = (2^n - 1) - \left|\bigcup_{p \text{ prime}, p|n} \mathcal{P}(A_p)\right|$ where $A_d = \{a \le x \le a + (n-1)b : d \mid x\}$. Using the principle of inclusion-exclusion and the same idea as in the proof of Theorem 3.1, one obtains from above that

$$\Phi^{(a,b)}(n) = \sum_{d|n} \mu(d)|\mathcal{P}(A_d)|.$$

It was proved in Lemma 3.2 that if $\gcd(b,d) = 1$, then $|A_d| = \left(\left[\frac{n}{d}\right] + \varepsilon_d\right)$, and since $d \mid n$, $\varepsilon_d = 0$. Then

$$\Phi^{(a,b)}(n) = \sum_{\substack{d \mid n \\ \gcd(b,d)=1}} \mu(d) \left(2^{\frac{n}{d}} - 1\right).$$

The proof for Formula 2 is similar. $\square$

Corollary 10. *The formulas for $f(m,k)$, $f_k(m,l)$, $\Phi(m,l)$ and $\Phi_k(m,l)$ obtained in [1], [2], [3] are consequences of Theorem 5 and Theorem 7.*

Proof. We will prove the corollary for $f(m,k)$ only. For the other formulas, the proof is similar. Let $a = m+1$, $b = 1$, $l = a + (n-1)b = n + m$. Then $n = l - m$,

$$f(m,l) = f^{(m+1,1)}(n) = \sum_{d=1}^{l} \mu(d) \left(2^{\left[\frac{l-m}{d}\right]+\varepsilon_d} - 1\right).$$

All we need to prove is that $\left[\frac{l-m}{d}\right] + \varepsilon_d = \left[\frac{l}{d}\right] - \left[\frac{m}{d}\right]$.
If $d \mid (l-m)$, then $\varepsilon_d = 0$ and it is easy to see that $\left[\dfrac{l-m}{d}\right] = \left[\dfrac{l}{d}\right] - \left[\dfrac{m}{d}\right]$, and the result follows.
If $d \nmid (l-m)$, let $l = \left[\dfrac{l}{d}\right] d + x$ and $m = \left[\dfrac{m}{d}\right] d + y$ with $0 \le x, y \le d-1$. Since $d \nmid (l-m)$, then $x \ne y \bmod d$.

- If $x < y$, then $\left[\frac{l-m}{d}\right] = \left[\frac{l}{d}\right] - \left[\frac{m}{d}\right] - 1$. From the definition, $\varepsilon_d = 1$ if $-(m+1) \pmod d \in \left\{0, \ldots, l - m - \left[\frac{l-m}{d}\right] d - 1\right\}$; otherwise $\varepsilon_d = 0$. Then,

$$\begin{aligned} l - m - \left[\tfrac{l-m}{d}\right] d - 1 &= \left[\tfrac{l}{d}\right] d + x - \left(\left[\tfrac{m}{d}\right] d + y\right) - \left(\left[\tfrac{l}{d}\right] - \left[\tfrac{m}{d}\right] - 1\right) d - 1 \\ &= x - y + d - 1. \end{aligned}$$

But $-(m+1) = -\left[\frac{m}{d}\right] d - y - 1 \equiv d - y - 1 \bmod d$. Since $x \geq 0$, then, $-(m+1) \bmod d \in \{0, \ldots, x - y + d - 1\} = \left\{0, \ldots, l - m - \left[\frac{l-m}{d}\right] d - 1\right\}$. Hence $\varepsilon_d = 1$ and

$$\left[\frac{l-m}{d}\right] + \varepsilon_d = \left[\frac{l}{d}\right] - \left[\frac{m}{d}\right].$$

- If $x > y$, it is easy to see that

$$\left[\frac{l-m}{d}\right] = \left[\frac{l}{d}\right] - \left[\frac{m}{d}\right]$$

and

$$l - m - \left[\frac{l-m}{d}\right] d - 1 = x - y - 1.$$

But

$$0 \leq x - y - 1 \leq d - y - 1.$$

Then

$$-(m+1) \bmod d = d - y - 1 \notin \left\{0, \ldots, l - m - \left[\frac{l-m}{d}\right] d - 1\right\}.$$

Hence $\varepsilon_d = 0$ and

$$\left[\frac{l-m}{d}\right] + \varepsilon_d = \left[\frac{l}{d}\right] - \left[\frac{m}{d}\right].$$

Remark 11. If a and b are integers not necessary positive, one can easily deduce from Theorem 3.1 and Theorem 3.5, the formulas for $f^{(a,b)}(n)$, $f_k^{(a,b)}(n)$, $\Phi^{(a,b)}(n)$ $\Phi_k^{(a,b)}(n)$ and $\Phi_k^{(a,b)}(n)$.

Remark 12. Suppose in Theorem 3.5 that $\gcd(a,b) = \alpha \neq 1$.

(i) If $\gcd(\alpha, n) \neq 1$, then it is easy to show that $\Phi^{(a,b)}(n) = 0$ and $\Phi_k^{(a,b)}(n) = 0$.

(ii) If $\gcd(\alpha, n) = 1$. Let $a_\alpha = \frac{a}{\alpha}$ and $b_\alpha = \frac{b}{\alpha}$. Then, $\gcd(a_\alpha, b_\alpha) = 1$. Hence, $\Phi^{(a,b)}(n) = \Phi^{(a_\alpha, b_\alpha)}(n)$ and $\Phi_k^{(a,b)}(n) = \Phi_k^{(a_\alpha, b_\alpha)}(n)$.

4. Prime Applications

Let $E(n,m) = \{h : \{1, 2, \ldots, n\} \to \mathbb{Z}/m\mathbb{Z}\}$. For $h \in E(n,m)$, we define the support of h to be $\mathrm{supp}(h) = \{x \in \{1, 2, \ldots, n\}; h(x) \neq 0\}$, and $\gcd(h) = \gcd(\mathrm{supp}(h))$. We say that h is prime if $\gcd(h) = 1$.

Proposition 13. *Let $A \subset \{1, 2, \ldots, n\}$, then there exist $(m-1)^{|A|}$ elements $h \in E(n,m)$ such that supp$(h) = A$.*

Proof. It is clear that there is a one-to-one and onto correspondence between $\{h \in E(n,m), supp(h) = A\}$ and $\{g : A \to \mathbb{Z}/m\mathbb{Z}\backslash\{0\}\}$, hence the result. $\square$

From Proposition 4.1, we deduce that the mapping

$$E(n,2) \quad \xrightarrow{\theta} \quad \mathcal{P}(\{1,\, 2,\, \dots,\, n\}),$$

such that $\theta(h) = \mathrm{supp}(h)$, is bijective. Moreover, it maps the prime applications h to what Nathanson [2] calls relatively prime sets.

Let us denote by $F(n,m)$ (respectively $\Psi(n,m)$), the number of prime elements $h \in E(n,m)$ (respectively $h \in E(n,m)$ such that $\gcd(\gcd(h), n) = 1$). It is easy to see that $F(n,2) = f(n)$ and $\Psi(n,2) = \Phi(n)$.

Theorem 14. *For all positive integers n and $m \geq 2$,*

$$F(n,m) = \sum_{d=1}^{n} \mu(d)\big(m^{[n/d]} - 1\big)$$

and

$$\Psi(n,m) = \sum_{d|n} \mu(d) m^{n/d}. \tag{3}$$

Before proving Theorem 14, we need the following lemma.

Lemma 15. *For any $d \geq 1$, let $B_d = \{h \in E(n,m), supp(h) \neq \emptyset; d \mid gcd(h)\}$. Then $|B_d| = m^{[n/d]} - 1$.*

Proof. If $d > n$, then clearly $B_d = \emptyset$. It is easy to see that the number of elements in $\{1,\, \dots,\, n\}$ that are divisible by d is equal to $[n/d]$. Notice that $h \in B_d$ if and only if $supp(h) \subset \{d,\, 2d,\, \dots,\, [\frac{n}{d}]d\}$. It follows from Proposition 13 that

$$\Big|B_d\Big| = \sum_{i=1}^{[n/d]} (m-1)^i \binom{[n/d]}{i} = m^{[n/d]} - 1.$$

$\square$

Proof of Theorem 14. As in the proof of Theorem 5, we will use the principle of inclusion-exclusion. We obtain

$$\begin{aligned} F(n,m) &= m^n - 1 - \Bigg|\bigcup_{q \text{ prime}} B_q\Bigg| = m^n - 1 - \sum_{d=2}^{n} -\mu(d)\Big|B_d\Big| \\ &= m^n - 1 + \sum_{d=2}^{n} \mu(d)\big|B_d\big|. \end{aligned}$$

Using Lemma 4.3, we obtain

$$F(n,m) = m^n - 1 + \sum_{d=2}^{n} \mu(d)\big(m^{[n/d]} - 1\big) = \sum_{d=1}^{n} \mu(d)\big(m^{[n/d]} - 1\big).$$

The proof for Formula 3 is similar. □

In what follows, we discuss the possible link between finite fields and $E(n,p)$. Notice that when $m = p$ is a prime, $\Psi(n,p)$ is the number of primitive elements of the finite field $\mathbb{F}_{p^n}$ over $\mathbb{F}_p$. Since $\big|E(n,p)\big| = \big|\mathbb{F}_{p^n}\big| = p^n$, it is natural to ask whether it is possible to define explicitly an operation $*$ such that $E(n,p)$ is a field under $+$ and $*$, where $+$ is the usual addition of applications. One answer may be the following:

Let $P_n(x)$ be a monic irreducible polynomial over $\mathbb{F}_p$ of degree n. Let

$$E(n,p) \quad \xrightarrow{\tau} \quad \mathbb{F}_p[x]/(P_n(x))$$

such that

$$\tau(g) = \sum_{i=1}^{n} g(i)x^{n-i}.$$

Let $g, h \in E(n,p)$, set $g * h = \tau^{-1}\big(\tau(g)\cdot\tau(h)\big)$. Then $(E(n,p), +, *)$ is a field and τ is an isomorphism.

The proof of this statement is straightforward.

Remark 16. Let p be a prime. The Formula 3 shows that $\Psi(n,p)$ is equal to the number of primitive element of $\mathbb{F}_{p^n}$ over $\mathbb{F}_p$. Consider any bijection from the set of primitive elements of $\mathbb{F}_{p^n}$ over $\mathbb{F}_p$ onto $\{h \in E(n,p);\ \gcd(\ \gcd(h), n) = 1\}$. Extend this bijection to $\mathbb{F}_{p^n}$ in order to obtain a bijection from $\mathbb{F}_{p^n}$ onto $E(n,p)$. By transferring the laws, $E(n,p)$ becomes a field and the bijection is an isomorphism of fields.

Question: Is it possible to construct an isomorphism of additive groups from $\mathbb{F}_{p^n}$ onto $E(n,p)$, which maps any primitive element onto some $h \in E(n,p)$, with $\gcd(\gcd(h), n) = 1$?

References

[1] M. El Bachraoui, *The number of relatively prime subsets and phi functions for* $\{m, m+1, \ldots, n\}$, Integers **7** (2007), #A43, 8 pp. (electronic).

[2] M. B. Nathanson, *Affine invariants, relatively prime sets, and a phi function for subsets of* $\{1, 2, \ldots, n\}$, Integers **7** (2007), #A1, 7 pp. (electronic).

[3] M. B. Nathanson, B. Orosz, *Asymptotic estimates for phi functions for subsets of* $\{M+1, M+2, \ldots, N\}$, Integers **7** (2007), #A54, 5 pp. (electronic).