#A14 INTEGERS 9 (2009), 163-166

THE NUMBER OF RELATIVELY PRIME SUBSETS OF $\{1, 2, \ldots, N\}$

Mohamed Ayad
Lab. de Math. Pures et Appliquées, Université du Littoral, Calais, F6228 France
Mohamed.Ayad@lmpa.univ-littoral.fr

Omar Kihel[1]
Department of Mathematics, Brock University, St. Catharines, Ontario, CANADA L2S 3A1 okihel@brocku.ca

Received: 7/11/08, Revised: 2/27/09, Accepted: 3/11/09

Abstract

A nonempty subset $A \subseteq \{1, 2 \ldots, n\}$ is relatively prime if $\gcd(A) = 1$. Let $f(n)$ denote the number of relatively prime subsets of $\{1, 2 \ldots, n\}$. The sequence given by the values of $f(n)$ is sequence A085945 in Sloane's On-Line Encyclopedia of Integer Sequences. In this article we show that $f(n)$ is never a square if $n \geq 2$. Moreover, we show that reducing the terms of this sequence modulo any prime $l \neq 3$ leads to a sequence which is not periodic modulo l.

1. Introduction

Nathanson defined a nonempty subset A of $\{1, 2 \ldots, n\}$ to be relatively prime if $\gcd(A) = 1$. Let $f(n)$ and $\Phi(n)$ denote respectively the number of relatively prime subsets of $\{1, 2 \ldots, n\}$ and the number of nonempty subsets A of $\{1, 2 \ldots, n\}$ such that $\gcd(A)$ is relatively prime to n. Exact formulas and asymptotic estimates are given by M. B. Nathanson in [5]. Generalizations may be found in [1], [2], [3], [4] and [6]. Let $[x]$ denote the greatest integer less than or equal to x and $\mu(n)$ the Mobius function. Nathanson [5] proved the following theorem.

Theorem 1. *The following hold:*

(i) For all positive integers n,

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

(ii) For all integers $n \geq 2$,

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

It is worth mentioning that from formula (2), we see that $\Phi(n)$ is equal to the number of primitive elements of the field $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$. In [1], a new function$\Psi(n, p)$

[1]Research partially supported by NSERC.

generalizing Φ is defined such that $\Psi(n,p)$ represents the number of primitive elements of $\mathbb{F}_{p^n}$ over $\mathbb{F}_p$, where p is any prime number. In [7, Example 1, p. 62], the function $\Phi(n)$ is defined as the number of primitive $0-1$ strings of length n.

The first result of this paper is the following:

Theorem 2. *$f(n)$ is never a square if $n \geq 2$.*

Question Is there any perfect power other than $f(1) = 1$?

Indeed we were unable to prove that there is no term of the sequence which is a cube other than the first term.

Our second result concerns the study of the sequence $f(n)$ if one reduces its terms modulo a fixed prime. Let l be a prime number. We say that the sequence $f(n)$ is periodic modulo l, starting from some integer $N = N(l)$, if there exists an integer $T \geq 1$ such that $f(n+T) \equiv f(n) \pmod{l}$ for any $n \geq N$. Lemma 2 below shows that $f(n)$ is periodic modulo 3 starting from $N = 2$.

Theorem 3. *Let l be a prime such that $l \neq 3$. Then $f(n)$ is not periodic modulo l.*

2. Proof of Theorem 2

For the proof of Theorem 2 we need two lemmas.

Lemma 1. *For any integer $n \geq 1$, we have*

$$f(n+1) - f(n) = \frac{1}{2}\Phi(n+1). \tag{3}$$

Proof. Let $E(n+1)$ be the set consisting of the nonempty subsets A of $\{1, 2, \ldots, n+1\}$ such that $\gcd(A)$ is coprime to $n+1$. Let $E_0(n+1)$ and $E_1(n+1)$ be two sets that partition $E(n+1)$ such that an element A of $E(n+1)$ belongs to $E_1(n+1)$ if it contains $n+1$. It is easy to see that $E_0(n+1)$ and $E_1(n+1)$ are of the same size. Moreover, by the very definition of $f(n)$, $f(n+1) - f(n)$ represents the cardinality of $E_1(n+1)$ and the result follows. $\square$

Lemma 2. *For any $n \geq 3$, $\Phi(n) \equiv 0 \pmod{3}$.*

Proof. If n is odd then for any $d \mid n$, $2^{n/d} \equiv -1 \pmod{3}$; hence (2) yields

$$\Phi(n) \equiv -\sum_{d \mid n} \mu(d).$$

It is well-known that $\sum_{d \mid n} \mu(d) = 0$ if $n \geq 2$; hence the result follows in the case n is odd. Suppose now that the integer n is even and write it in the form $n = 2^k n'$, where $k \geq 1$ and n' is odd. We suppose that $n' \geq 3$. Equation (2) may be written in the form

$$\Phi(n) = \sum_{d|n'} \mu(d) 2^{2^k n'/d} + \sum_{d|n'} \mu(2d) 2^{2^k n'/2d} + \cdots + \sum_{d|n'} \mu(2^k d) 2^{2^k n'/2^k d}. \quad (4)$$

It is clear that all the sums in (4) but the first two are 0. For any $d \mid n'$ we have $2^{2^k n'/d} \equiv 1 \pmod 3$; hence $\sum_{d|n'} \mu(d) 2^{2^k n'/d} \equiv 0 \pmod 3$. We have $2^{2^{k-1} n'/d} \equiv 1 \pmod 3$ if $k \geq 2$ and $2^{2^{k-1} n'/d} \equiv -1 \pmod 3$ if $k = 1$. We deduce that $\sum_{d|n'} \mu(2d) 2^{2^k n'/2d} \equiv \pm \sum_{d|n'} \mu(2d) \equiv \mp \sum_{d|n'} \mu(d) \equiv 0 \pmod 3$ and the result follows in the case n is even and $n' \geq 3$.

The case $n' = 1$ may be proved similarly. □

Second Proof. Recall from [5] the following formula:

$$\sum_{d|n} \Phi(d) = 2^n - 1.$$

Suppose that the lemma is true for any $3 \leq m < n$. If n is even, then $2^n - 1 \equiv \Phi(1) + \Phi(2) + \Phi(n) \pmod 3$ and the result follows since $\Phi(1) = 1$, $\Phi(2) = 2$ and $2^n - 1 \equiv 0 \pmod 3$. A similar argument applies when n is odd.

Proof of Theorem 2 Lemmas 1 and 2 show that $f(n+1) \equiv f(n) \pmod 3$. Since $f(2) = 2$, we conclude by induction that for any $n \geq 2$, $f(n) \equiv 2 \pmod 3$; hence $f(n)$ is never a square if $n \geq 2$. □

3. Proof of Theorem 3

Suppose first that $l \geq 5$ and that the sequence $f(n)$ is periodic starting from some integer N and denote by T one of its periods. It is clear, by (3), that the sequence $\Phi(n)$ is also periodic and T is also a period for this sequence. Select two large prime numbers p and q such that $p \equiv 1 \pmod{(l-1)T}$ and $q \equiv -1 \pmod{(l-1)T}$. It is easy to see that $\Phi(p) = 2^p - 2$, $\Phi(q) = 2^q - 2$ and $\Phi(pq) = 2^{pq} - 2^p - 2^q + 2$, by (2). Hence, $\Phi(p) \equiv 0 \pmod l$, $\Phi(q) \equiv 2^{-1} - 2 \pmod l$ and $\Phi(pq) \equiv 0 \pmod l$. But $pq \equiv q \pmod T$; hence $\Phi(pq) \equiv 2^{-1} - 2 \pmod l$. It follows that $2^{-1} - 2 \equiv 0 \pmod l$, thus $l = 3$, which contradicts our hypothesis and the proof is complete when $l \geq 5$.

Suppose now that $l = 2$ and that $f(n)$ is periodic modulo 2 with period T starting from the integer N. Using (1), we see that $f(n) \equiv \sum_{d=1}^{n} \mu(d) \pmod 2$ and $f(n + T) \equiv \sum_{d=1}^{n+T} \mu(d) \pmod 2$. We deduce that, for $n \geq N$, $\sum_{d=1}^{n} \mu(d) \equiv \sum_{d=1}^{n+T} \mu(d) \pmod 2$. Then $\sum_{d=n+1}^{n+T} \mu(d) \equiv 0 \pmod 2$, whereupon $\mu(n+1) \equiv \mu(n+T+1) \pmod 2$; i.e. $\mu(n) \equiv \mu(n+mT) \pmod 2$ for every $n \geq N$ and m any positive integer. Choose a large square-free integer n_0 and a prime p such that $p \nmid T$.

It is clear that there exists a positive integer m such that $n_0 + mT \equiv 0 \pmod{p^2}$; hence $n_0 + mT$ is not square-free. Then, $\mu(n_0) \equiv 1 \pmod 2$ and $\mu(n_0 + mT) \equiv 0 \pmod 2$, which is a contradiction and the proof is complete.

Acknowlegement. We thank the referee for suggesting some corrections and for pointing us to reference [7].

References

[1] M. Ayad, O. Kihel, *On relatively prime sets*, preprint 2008.

[2] M. Ayad, O. Kihel, *On the Number of Subsets Relatively Prime to an Integer*, J. Integer Sequences **11** (2008), 08.5.5.

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

[4] M. El Bachraoui. *On the number of Subsets of* $[1,m]$ *Relatively Prime to* n *and Asymptotic Estimates*, Integers **8** (2008), A41.

[5] M. B. Nathanson. *Affine invariants, relatively prime sets, and a Phi function for subsets of* $\{1,2,\ldots,n\}$, Integers **7** (2007), A01.

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

[7] H. S. Wilf. *generatingfunctionology.* Academic Press, 1994.