Investigation of a Primality Criterion within an Arithmetic Progression

Mar Detic

Abstract

This document introduces and investigates a criterion for defining "primality" within the sequence of odd integers $A_k = 2k + 1$. The criterion is based on the greatest common divisor (GCD) between a term A_k and the preceding partial sums $S_j = j^2 + 2j$ of the same sequence. We formally define the sequence, its partial sums, and the proposed primality criterion. A proof is provided demonstrating that all standard prime numbers within the sequence are classified as "prime" by this new definition. Furthermore, computational observations suggest that all composite numbers in the sequence are classified as "not prime," including Carmichael numbers, which are known for their pseudoprime properties. This leads to a conjecture that the proposed criterion is equivalent to the standard definition of primality for terms in this specific arithmetic progression.

1 Introduction

This document explores a unique definition of "primality" applied to terms within a specific arithmetic progression. We define the terms of the series and its partial sums, then introduce a primality criterion based on the Greatest Common Divisor (GCD) between terms and preceding partial sums. Finally, we examine the relationship between this definition and the standard definition of prime numbers.

2 Definitions

Definition 1 (The Sequence of Terms (A_k))**.** *Let A_k be the sequence of odd integers greater than or equal to 3, defined for $k \in \mathbb{Z}^+$ as:*

$$A_k = 2k + 1$$

The sequence begins: $3, 5, 7, 9, 11, 13, 15, 17, 19, 21, 23, 25, \ldots$

Definition 2 (The Sequence of Partial Sums (S_n))**.** *Let S_n be the sum of the first n terms of the sequence A_k. This sum can be expressed as a polynomial in* *n:*

$$S_n = \sum_{i=1}^{n}(2i+1) = n^2 + 2n$$

Derivation: $S_n = 2\sum_{i=1}^{n} i + \sum_{i=1}^{n} 1 = 2\left(\frac{n(n+1)}{2}\right) + n = n(n+1) + n = n^2 + n + n = n^2 + 2n$.

Definition 3 (Prime Criterion)**.** *A term A_k from the sequence is defined as "prime" if and only if for every integer j such that $1 \leq j < k$, the greatest common divisor (GCD) of S_j and A_k is equal to 1. That is:*

$$\forall j \in \{1, 2, \ldots, k-1\} : \gcd(S_j, A_k) = 1$$

Definition 4 (Not Prime Criterion)**.** *A term A_k from the sequence is defined as "not prime" if there exists at least one integer j such that $1 \leq j < k$ for which the greatest common divisor of S_j and A_k is greater than 1. That is:*

$$\exists j \in \{1, 2, \ldots, k-1\} : \gcd(S_j, A_k) > 1$$

3 Relationship to Standard Prime Numbers

We now investigate how this definition of "primality" aligns with the standard definition of a prime number.

Proposition 1. *If a term A_k is a standard prime number, then A_k is "prime" according to the criterion.*

Proof. Let $A_k = p$ be a standard prime number. We aim to demonstrate that for every j such that $1 \leq j < k$, $\gcd(S_j, p) = 1$.

We know that $S_j = j(j+2)$. For $\gcd(S_j, p)$ to be greater than 1, since p is a prime number, it must be that p divides S_j. By Euclid's Lemma, if p divides $j(j+2)$, then p must divide j or p must divide $(j+2)$.

From the definition of A_k, we have $A_k = 2k+1 = p$, which implies $k = (p-1)/2$. The range for j is $1 \leq j < k$, meaning $1 \leq j < (p-1)/2$.

1. **Consider the case where p divides j:** If p divides j, then j must be a multiple of p. Since $j \geq 1$, this would imply $j \geq p$. However, our condition $j < (p-1)/2$ implies $j < p$ for all prime $p \geq 3$. Specifically, for $p = 3$, $k = 1$, so there are no $j < 1$. For $p \geq 5$, $(p-1)/2 < p$. Thus, $j \geq p$ contradicts $j < (p-1)/2$. Therefore, p cannot divide j.

2. **Consider the case where p divides $(j+2)$:** If p divides $(j+2)$, then $(j+2)$ must be a multiple of p. Since $j \geq 1$, $j+2 \geq 3$. This would imply $j+2 \geq p$. However, from $j < (p-1)/2$, we can deduce $j+2 < (p-1)/2 + 2 = (p-1+4)/2 = (p+3)/2$. For any prime $p > 3$, we have $(p+3)/2 < p$. (e.g., for $p = 5$, $(5+3)/2 = 4 < 5$; for $p = 7$, $(7+3)/2 = 5 < 7$). Thus, for $p > 3$, $j+2 \geq p$ contradicts $j+2 < (p+3)/2$. Therefore, p cannot divide $(j+2)$.

Since p cannot divide j and p cannot divide $(j+2)$, it follows that p cannot divide their product $S_j = j(j+2)$. Consequently, $\gcd(S_j, p) = 1$ for all $1 \leq j < k$. This concludes the proof that if A_k is a standard prime number, it satisfies the "prime" criterion. □

4 Observations on Composite Numbers

While the proposition above proves that all standard prime numbers within the sequence A_k will be classified as "prime" by the definition, it's also insightful to observe how composite numbers are classified.

Through computational checks of initial terms, we've observed that all composite numbers of the form $A_k = 2k + 1$ are classified as "not prime" by the criterion.

- If A_k is a multiple of 3 (e.g., $A_4 = 9$, $A_7 = 15$, $A_{10} = 21$), then $\gcd(S_1, A_k) = \gcd(3, A_k) = 3 > 1$. Thus, all multiples of 3 are correctly identified as "not prime".
- For other composite numbers, such as $A_{12} = 25$, which is 5^2: $\gcd(S_3, A_{12}) = \gcd(15, 25) = 5 > 1$. Hence, $A_{12} = 25$ is "not prime".
- For $A_{24} = 49$, which is 7^2: $\gcd(S_5, A_{24}) = \gcd(35, 49) = 7 > 1$. Hence, $A_{24} = 49$ is "not prime".

This pattern suggests that any odd composite number A_k will likely share a common factor with at least one preceding partial sum S_j. This is because the prime factors of $S_j = j(j+2)$ cover an increasing range of integers as j increases, making it probable to find a shared factor with any composite A_k.

5 Efficiency Against Carmichael Numbers

Carmichael numbers are composite numbers that are known for their pseudoprime properties; they satisfy the congruence relation of Fermat's Little Theorem for all bases coprime to them, often making them difficult to distinguish from primes using certain probabilistic primality tests. We investigate how the proposed criterion classifies these numbers.

All Carmichael numbers are odd and greater than 1, so they are terms in our sequence $A_k = 2k + 1$. Let's test the first few Carmichael numbers using our criterion:

1. $A_{280} = 561$**:** The number 561 is a Carmichael number. It can be expressed as $A_{280} = 2(280) + 1$. Its prime factorization is $3 \times 11 \times 17$. We compute $\gcd(S_1, A_{280}) = \gcd(3, 561)$. Since 561 is divisible by 3, $\gcd(3, 561) = 3$. As $\gcd(3, 561) = 3 > 1$, according to our criterion, $A_{280} = 561$ is classified as **"not prime"**.

2. $A_{552} = 1105$**:** The number 1105 is a Carmichael number, and $A_{552} = 2(552) + 1$. Its prime factorization is $5 \times 13 \times 17$. Consider $j = 3$, $S_3 = 3^2 + 2(3) = 9 + 6 = 15$. We compute $\gcd(S_3, A_{552}) = \gcd(15, 1105)$. Since $15 = 3 \times 5$ and $1105 = 5 \times 221$, they share a common factor of 5. Thus, $\gcd(15, 1105) = 5$. As $\gcd(15, 1105) = 5 > 1$, according to our criterion, $A_{552} = 1105$ is classified as **"not prime"**.

3. $A_{864} = 1729$**:** The number 1729 is a Carmichael number, and $A_{864} = 2(864) + 1$. Its prime factorization is $7 \times 13 \times 19$. Consider $j = 5$, $S_5 = 5^2 + 2(5) = 25 + 10 = 35$. We compute $\gcd(S_5, A_{864}) = \gcd(35, 1729)$. Since $35 = 5 \times 7$ and $1729 = 7 \times 247$, they share a common factor of 7. Thus, $\gcd(35, 1729) = 7$. As $\gcd(35, 1729) = 7 > 1$, according to our criterion, $A_{864} = 1729$ is classified as **"not prime"**.

These examples demonstrate that the proposed primality criterion successfully classifies Carmichael numbers as "not prime." This provides further evidence for the robustness and accuracy of the criterion in identifying composite numbers, even those that exhibit pseudoprime behavior in other primality tests.

Conjecture 1. *A term A_k is "prime" by the criterion if and only if A_k is a standard prime number.*

Based on our analysis, the evidence strongly supports this conjecture. While proving the converse (that if A_k is "prime" by the criterion, then it must be a standard prime number) requires a more rigorous number-theoretic argument for all cases, the criterion appears to be a very effective filter for standard prime numbers within the sequence $2k + 1$.