NOTA ELEVULUI

Sequences of coprime integers

Matei-Pavel DUMITRESCU[1]

Abstract. In this note, motivated by Problem 2, ITYM 2021, we attempt to answer several questions concerning sequences of coprime integers.

Keywords: coprime integers, Chinese remainder theorem.

MSC 2010: 11A07, 11A51.

1. Introduction

Definition 1.1. *Let $n \in \mathbb{N}$. A finite or infinite sequence of positive integers (hereinafter called a SPI) $a_1, a_2, \dots, a_k, \dots$ is called n-prime if $a_1+n, a_2+n, \dots, a_k+n, \dots$ are pairwise coprime.*

Since a n-prime SPI remains n-prime after any rearrangement, we can suppose without any loss of generality that all SPIs that follow are increasing. Having in mind the statement of Problem 2, ITYM 2021, which leads to an inquiry about the properties of n-prime SPIs, we seek to answer the following questions.

Question 1. Which SPI are n-prime for all $n \in \mathbb{N}$?

Question 2. Is there a SPI that is not n-prime for any $n \in \mathbb{N}$?

Question 3. What are the necessary and sufficient conditions for a SPI to be n-prime for infinitely many $n \in \mathbb{N}$?

To answer these questions, the following result, called *Chinese remainder theorem*, is of interest.

Theorem 1.1. If $n_1, n_2, \dots, n_q$ are pairwise coprime integers greater than 1, then for any integers $r_1, r_2, \dots, r_q$ the system $x \equiv r_i \pmod{n_i}$, $1 \leq i \leq q$, has a solution. Furthermore, any two solutions are congruent modulo N, where $N = n_1 n_2 \cdots n_q$.

Given two integers a, b, we denote their greatest common divisor as (a, b) and observe that $(a, b) = (a, b-a)$. Also, let p be a prime number and let $a_1, a_2, \dots, a_k$ be a finite SPI. Denote by L_p the associated sequence of remainders mod p. We shall also employ the following auxiliary results.

Lema 1.1. If L_p does not contain all possible remainders mod p or contains a remainder that appears only once, then there is a remainder r_p mod p such that for every n satisfying $n \equiv r_p \pmod{p}$ it follows that (a_i+n, a_j+n) is not divisible by p for any $1 \leq i, j \leq k$, $i \neq j$.

Proof. Let v be a remainder mod p that either does not appear in L_p or appears only once and let r_p be the remainder of $p-v$ mod p. If we choose n so that $n \equiv r_p$ (mod p), then at most one of the numbers $a_1+n, a_2+n, \dots, a_k+n$ is divisible by p, which finishes the proof.

Lema 1.2. If L_p contains all possible remainders mod p at least twice, then $a_1, a_2, \dots, a_k$ is not n-prime for any $n \in \mathbb{N}$.

Proof. If every remainder mod p appears at least twice, then for every $n \in \mathbb{N}$ at least two terms of the sequence $a_1+n, a_2+n, \dots, a_k+n$ will be divisible by p, hence the conclusion.

[1]Student, National College Iaşi; *matei.dumitrescu@gmail.com.*

2. Answers to the questions

Answer to Question 1. Case 1: Sequences of 2 numbers. Given a SPI a_1, a_2 that is n-prime for all $n \in \mathbb{N}$, we observe that $(a_1 + n, a_2 + n) = (a_1 + n, a_2 - a_1)$. If $a_2 - a_1 > 1$, we can choose $n = p(a_2 - a_1) - a_1$, with $p \in \mathbb{N}$ large enough, which leads to $(a_1 + n, a_2 + n) = (p(a_2 - a_1), a_2 - a_1) = a_2 - a_1 > 1$, contradiction. Consequently, $a_2 - a_1 = 1$, so a_1, a_2 are consecutive, and then it is easy to see that a SPI a_1, a_2 of consecutive numbers is n-prime for all $n \in \mathbb{N}$.

Case 2: Sequences of at least 3 numbers. Given a SPI $a_1, a_2, \ldots, a_k, \ldots$ of at least 3 numbers that is n-prime for all $n \in \mathbb{N}$, we observe by the argument employed in Case 1 that the positive integers in the sequence are pairwise consecutive. Since the sequence contains at least 3 numbers, this is impossible.

Answer to Question 2. Case 1: Sequences of at least 4 numbers. A SPI a_1, $a_2, \ldots, a_k, \ldots$ of at least 4 numbers that contains at least 2 even and 2 odd numbers is not n-prime for any $n \in \mathbb{N}$, since $a_1 + n$, $a_2 + n, \ldots, a_k + n, \ldots$ contains at least 2 even numbers regardless of the parity of n.

Case 2: Sequences of 2 numbers. Given an arbitrary SPI a_1, a_2, take $n_0 = q(a_2 - a_1) - a_1 + 1$ for $q \in \mathbb{N}$ large enough. Then $(a_1 + n_0, a_2 + n_0) = (a_1 + n_0, a_2 - a_1) = (q(a_2 - a_1) + 1, a_2 - a_1) = 1$, so the SPI a_1, a_2 is n_0-prime.

Case 3: Sequences of 3 numbers. Given a SPI a_1, a_2, a_3, we observe that the conditions of Lemma 1.1 are satisfied for any prime p, since $p \geq 2$ and L_p only has 3 numbers. Note that $(a_i + n, a_j + n) = (a_i + n, a_j - a_i)$, $1 \leq i, j \leq 3$, $i \neq j$, so we only need to consider the possible prime divisors at most equal to $a_3 - a_1$.

For every prime p_i at most equal to $a_3 - a_1$, we obtain a corresponding r_{p_i} from Lemma 1.1. Using the Chinese remainder theorem, there is $n_0 \in \mathbb{N}$ such that $n \equiv r_{p_i}$ (mod p_i) for every prime p_i at most equal to $a_3 - a_1$. Consequently, by Lemma 1.1, $(a_i + n, a_j + n)$ is not divisible by any prime p_i at most equal to $a_3 - a_1$ (and in fact, by the above considerations, by any prime p) for all $1 \leq i, j \leq 3$, $i \neq j$ and therefore all pairs are coprime. It follows that the SPI a_1, a_2, a_3 is n_0-prime.

Answer to Question 3. Let a_1, $a_2, \ldots, a_k$ be a finite SPI that is n_0-prime for some $n_0 \in \mathbb{N}$. Let P be the product of all prime numbers at most equal to $a_k - a_1$. Having in view that for all $q \in \mathbb{N}$ and all $1 \leq i, j \leq k$, $i \neq j$, one has $(a_i + n_0 + qP, a_j + n_0 + qP) = (a_i + n_0 + qP, a_j - a_i) = (a_i + n_0, a_j - a_i) = (a_i + n_0, a_j + n_0)$, it follows that the sequence is also $n_0 + qP$-prime, for all $q \in \mathbb{N}$. It follows that a finite SPI is either n-prime for infinitely many n or is not n-prime for any n.

Consequently, having also in view Lemma 1.2, it follows that the required necessary and sufficient condition is that the hypotheses of Lemma 1.1 hold for some (or all) prime p (or, equivalently for primes at most equal to $a_k - a_1$). If a_1, $a_2, \ldots, a_k, \ldots$ is an infinite SPI, the necessary and sufficient condition stays conceptually the same, but has to be satisfied for any finite subsequence of a_1, $a_2, \ldots, a_k, \ldots$.

References

1. **Petru Minuţ** - *Number theory* (Romanian), Crenguţa Gâldău Publishing House, Iaşi, 1997.
2. ******* - Problem 2, ITYM 2021.