**Bilkent University**
**Department of Mathematics**

# Problem Of The Month

February 2021

**Problem:**

Let $(a_n)_{n=1}^{\infty}$ be a sequence of integers with $a_1 = 1, a_2 = 2$ and

$$a_{n+2} = a_{n+1}^2 + (n+2)a_{n+1} - a_n^2 - na_n$$

for all $n \geq 1$. We say that a prime number is *good* if it divides at least one term of this sequence.

a) Show that there exist infinitely many good prime numbers.

b) Find three not good prime numbers.

**Solution:**

Let us define a sequence $(b_n)_{n=1}^{\infty}$ by $b_1 = 1$ and $b_{n+1} = a_n^2 + na_n$ for all $n \geq 1$. Then

$$a_{n+2} - a_{n+1} = a_{n+1}^2 + (n+1)a_{n+1} - a_n^2 - na_n = b_{n+2} - b_{n+1}.$$

We also have $a_1 = b_1 = 1$ and $a_2 = b_2 = 2$. Hence, we conclude that $a_n = b_n$ for all $n \geq 1$. Then we get $a_{n+1} = b_{n+1} = a_n(a_n + n)$ for all $n \geq 1$. Assume that the set of all prime numbers dividing at least one element of the sequence are finite. Denote these primes by $p_1, p_2, \ldots, p_k$. Since $a_n \mid a_{n+1}$, we have $a_n \mid a_m$ for all $m \geq n$. This means that if $p_i \mid a_n$ for some $i, n$, then $p_i \mid a_m$ for all $m \geq n$. Therefore, there exists an index $N$ for which $p_1 \cdot p_2 \cdots p_k \mid a_n$ for all $n > N$. Take an index $\ell$ satisfying $\ell > N + 1$ and $\ell \equiv 2 \pmod{p_1 \cdot p_2 \cdots p_k}$. In this case, we get $a_\ell = a_{\ell-1}(a_{\ell-1} + \ell - 1)$ and the expression $a_{\ell-1} + \ell - 1$ is not divisible by $p_i$ for all $i = 1, 2, \ldots, k$. Since $a_{\ell-1} + \ell - 1 > 1$ we obtain that $a_\ell$ should have a prime divisor different from $p_1, p_2, \ldots, p_k$, which is a contradiction.

b) We will show that the primes $3, 5, 19$ do not divide any term of $(a_n)_{n=1}^{\infty}$ and hence are not good primes. By using of $a_{n+1} = a_n(a_n + n)$ it can be readily shown that if for a given prime number $p$ and some integer $m$ we have $a_m \equiv a_{m+p} \pmod{p}$, then $a_\ell \equiv a_{\ell+p} \pmod{p}$ for all $\ell \geq m$. Hence, after the index $m$, the sequence becomes periodic modulo $p$. Hence, if for some index $m$, $p \not| a_n$ for all $n < m+p$, then we conclude that $p \not| a_n$ for all $n$.

Let us consider the sequence $(a_n)$ modulo $3, 5$ and $19$ and find $p$ and $m$ satisfying $a_m \equiv a_{m+p} \pmod{p}$:

$a_1, a_2, a_3, a_4 \equiv 1, 2, 2, 1 \pmod{3}$ so $m = 1, p = 3$.

$a_1, a_2, a_3, a_4, a_5, a_6 \equiv 1, 2, 3, 3, 1, 1 \pmod{5}$ so $m = 1, p = 5$.

$a_1, a_2, \ldots, a_{25} \equiv 1, 2, 8, 12, 2, 14, 14, 9, 1, 10, 10, 1, 13, 15, 17, 12, 13, 10, 14, 6, 4, 5, 2, 12, 14 \pmod{19}$ so $m = 6, p = 19$.

We are done.