František Marko

A note on pseudoprimes with respect to abelian linear recurring sequence

*Mathematica Slovaca*, Vol. 46 (1996), No. 2-3, 173--176

Persistent URL: http://dml.cz/dmlcz/130462

Math. Slovaca, **46** (1996), No. 2–3, 173–176

Mathematica Slovaca


*Dedicated to Professor Tibor Šalát on the occasion of his 70th birthday*

# A NOTE ON PSEUDOPRIMES WITH RESPECT TO ABELIAN LINEAR RECURRING SEQUENCE

František Marko

(*Communicated by Stanislav Jakubec*)

ABSTRACT. It is proved that for any finite system of simple abelian linear recurring sequences $\{a_n^i\}$, $i \in I$, and arbitrary integer $l \geq 3$ Schinzel's conjecture H implies the existence of infinitely many composite numbers $n$ which are a product of $l$ different primes and satisfy $a_{ns}^i \equiv a_s^i \pmod n$ for every natural number $s$.

We start with the following question of Perrin (see [6]):

Does there exist a composite index $n$ with $a_n \equiv 0 \pmod n$ in the linear recurring sequence $\{a_n\}$ of integers defined by $a_{n+3} = a_{n+1} + a_n$ and the initial conditions $a_0 = 3$, $a_1 = 0$, $a_2 = 2$?

The answer is affirmative, and concrete values of $n$ are given in [5], [1] and [2]. In [1], Perrin's question was generalized to certain congruences among the members of some third order linear recurring sequences. Authors of [1] also consider other properties of terms of linear recurring sequences in order to use them in primality testing.

In [3], one can find the following definition which is based on the above mentioned congruences:

**Definition 1.** Let $\{a_n\}$ be a linear recurring sequence. An integer $n$ is called *pseudoprime with respect to* $\{a_n\}$ if $a_{ns} \equiv a_s \pmod n$ for every natural number $s$.

The fact that Schinzel's conjecture H implies the existence of infinitely many pseudoprimes with respect to simple abelian linear recurrent sequences was

AMS Subject Classification (1991): Primary 11A99, 11B37.
Key words: linear recurrence, pseudoprime, Carmichael number.

proved in [3]. Moreover, all pseudoprimes considered there are a product of two different primes.

The aim of this note is to prove that for any finite system of simple abelian linear recurring sequences $\{a_n^i\}$, $i \in I$, and arbitrary integer $l \geq 3$ Schinzel's conjecture H implies the existence of infinitely many common pseudoprimes with respect to $\{a_n^i\}$ which are a product of $l$ different primes.

Let $\{a_n\}$ be a $r$th order linear recurring sequence of integers satisfying the recurrence relation

$$a_{n+r} = b_{r-1}a_{n+r-1} + \cdots + b_0 a_n ,$$

where $b_0, \dots, b_{r-1}$ are integers.

The sequence $\{a_n\}$ is called *simple* if its characteristic polynomial $g(x) = x^r - b_{r-1}x^{r-1} - \cdots - b_0$ has only simple roots and is called *abelian* if the splitting field of $g(x)$ over the field $\mathbb{Q}$ of rational numbers is abelian over $\mathbb{Q}$.

The Schinzel's conjecture H states the following:

If $f_1(x), \dots, f_k(x)$ are irreducible polynomials with integral coefficients and positive leading coefficient such that the product $f_1(x) \dots f_k(x)$ has no constant factor greater than 1, then there exist infinitely many positive integers $x$ for which $f_1(x), \dots, f_k(x)$ are primes.

**THEOREM.** *Let $\{a_n^i\}$, $i \in I$, be a finite system of simple abelian linear recurring sequences. Then for any natural $l \geq 3$ Schinzel's conjecture* H *implies the existence of infinitely many pseudoprimes with respect to every $\{a_n^i\}$, which are Carmichael numbers and are a product of $l$ different primes.*

Proof. Put

$$C_l = p(2p-1)(3p-2)(6p-5)(12p-11)\dots\big(6\cdot 2^{l-4}(p-1)+1\big)$$

and suppose that each factor in this product is a prime.

First we will show that $C_l$ is a Carmichael number whenever $p \equiv 1 \pmod{6\cdot 2^{l-3}}$. It suffices to prove that, under this assumption, the number $C_l - 1$ is divisible by numbers $(p-1)$, $2(p-1)$, $3(p-1)$, $6(p-1), \dots, 6\cdot 2^{l-4}(p-1)$.

If $l = 3$, then $C_3 - 1 = (p-1)(6p^2 - p + 1)$, and $p \equiv 1 \pmod 6$ implies that $6p^2 - p + 1$ is divisible by $6$.

Denote by $h_l(x)$ the integral polynomial given by the formal equality $\dfrac{C_l - 1}{p-1} = h_l(p)$.

We proceed by induction. For $l = 3$ we have $h_3(1) = 6$, and $C_3 - 1$ is divisible by $6(p-1)$.

Next suppose that $h_l(1) = 6\cdot 2^{l-3}$, and $C_l - 1$ is divisible by $6\cdot 2^{l-3}(p-1)$ for some $l \geq 3$.

Then

$$\begin{aligned} C_{l+1}-1 &= (C_l-1)\big(6\cdot 2^{l-3}(p-1)+1\big)+6\cdot 2^{l-3}(p-1) \\ &= (p-1)\left[(C_l-1)6\cdot 2^{l-3}+\frac{C_l-1}{p-1}+6\cdot 2^{l-3}\right], \end{aligned}$$

and we infer that $C_{l+1}-1$ is divisible by $p-1$, and $h_{l+1}(1)=6\cdot 2^{l-2}$. This means that the condition $p\equiv 1 \pmod{6\cdot 2^{l-2}}$ implies that $\dfrac{C_{l+1}-1}{p-1}$ is divisible by $6\cdot 2^{l-2}$.

Therefore, $C_l$ are Carmichael numbers provided $p\equiv 1 \pmod{6\cdot 2^{l-3}}$.

Now denote by $F$ an arbitrary natural number divisible by $6\cdot 2^{l-3}$ and all conductors of abelian fields $K_i$ which are the splitting fields of characteristic polynomials $g_i(x)$ of $\{a_n^i\}$ over $\mathbb{Q}$.

We define the polynomials $f_i(x)$ in the following way:

$$\begin{aligned} f_1(x) &= \;\; Fx+1\,; \\ f_2(x) &= 2Fx+1\,; \\ f_3(x) &= 3Fx+1\,; \\ f_4(x) &= 6Fx+1\,; \\ &\dots \\ f_l(x) &= 6\cdot 2^{l-4}Fx+1\,. \end{aligned}$$

Clearly, these polynomials satisfy the assumptions of Schinzel's conjecture H, and therefore this conjecture implies the existence of infinitely many natural $x_0$ such that all numbers

$$\begin{aligned} p &= f_1(x_0) = p_1\,; \\ 2p-1 &= f_2(x_0) = p_2\,; \\ 3p-2 &= f_3(x_0) = p_3\,; \\ 6p-5 &= f_4(x_0) = p_4\,; \\ &\dots \\ 6\cdot 2^{l-4}(p-1)+1 &= f_l(x_0) = p_l \end{aligned}$$

are primes.

Moreover, it can be assumed that the numbers $C=C_l=p_1\dots p_l$ do not ramify in any field $K_i$.

Every such $C$ is a Carmichael number because $F$ is divisible by $6\cdot 2^{l-3}$.

Each prime $p_j$ splits completely in each field $K_i$ because $p_j\equiv 1 \pmod F$, and $F$ is divisible by the conductor of the field $K_i$ over $\mathbb{Q}$.

Let $\wp_j$ be a prime divisor of the field $K_i$ which divides $p_j$. Using the generalized Euler criterion and the well-known expression for the terms $a_n = a_n^i$ of a simple linear recurring sequence as a linear combination over $K_i$ of the powers of the roots $\alpha_1, \dots, \alpha_r$ of its characteristic polynomial $g_i(x)$ we obtain

$$\begin{aligned} a_{Cs} &= c_1\alpha_1^{Cs} + \cdots + c_r\alpha_r^{Cs} \\ &\equiv c_1(\alpha_1^s)^{(p_j-1)\frac{C-1}{p_j-1}+1} + \cdots + c_r(\alpha_r^s)^{(p_j-1)\frac{C-1}{p_j-1}+1} \\ &\equiv c_1\alpha_1^s + \cdots + c_r\alpha_r^s = a_s \pmod{\wp_j}. \end{aligned}$$

Since each $\wp_j$ divides $p_j$ exactly in the first degree, and numbers $a_{Cs}$ and $a_s$ are rational integers, we obtain the congruence

$$a_{Cs} \equiv a_s \pmod{p_j}$$

for every $j = 1, \dots, l$.

Therefore

$$a_{Cs}^i \equiv a_s^i \pmod{C}$$

for each $i \in I$. □

## REFERENCES

[1] ADAMS, W.—SHANKS, D.: *Strong primality tests that are not sufficient*, Math. Comp. **39** (1982), 255–300.

[2] JAKUBEC, S.—NEMOGA, K.: *On a conjecture concerning sequences of the third order*, Math. Slovaca **36** (1986), 85–89.

[3] MARKO, F.: *Schinzel's conjecture* H *and divisibility in abelian linear recurring sequences*, Colloq. Math. **LIX** (1990), 1–7.

[4] MARKO, F.: *Pseudoprimes with Respect to Linear Recurring Sequences* (Slovak). Thesis, SAV, Bratislava, 1991.

[5] MILLER, J. C. P.—SPENCER BROWN, G.—SPENCER BROWN, D. J.: *The identification of prime numbers.* (Unpublished).

[6] PERRIN, R.: *"Item 1484"*, L'intermédiaire des math. **6** (1899), 76 77.

Received September 14, 1994

*Department of Mathematics*
*and Statistics*
*Carleton University*
*Ottawa, Ontario K1S 5B6*
*CANADA*