Annales Mathematicae et Informaticae
***33** (2006) pp. 45–56*
http://www.ektf.hu/tanszek/matematika/ami

On prime divisors of remarkable sequences

Ferdinánd Filip[a], Kálmán Liptai[b1], János T. Tóth[c2]

[a]Department of Mathematics University of J. Selye
e-mail: filip.ferdinand@seznam.cz

[b]Institute of Mathematics and Informatics Eszterházy Károly College
e-mail: liptaik@ektf.hu

[c]Department of Mathematics University of Ostrava
e-mail: toth@osu.cz

Submitted 10 November 2006; Accepted 18 December 2006

Abstract

In this paper we study sequences of the form $(a^n+b)_{n=1}^{\infty}$, where $a, b \in \mathbb{N}$. We prove many interesting results connection with sequences with infinitely many prime divisors.

Keywords: prime divisors, Dirichlet's theorem

MSC: 11N13

1. Introduction

There are many mathematical problems when we investigate the divisibility of sequences by a prime. We usually find this kind of interesting examples in national mathematical competitions and in the International Math Olympiad. In this paper we study sequences of the form $(a^n + b)_{n=1}^{\infty}$, where $a, b \in \mathbb{N}$. We prove some results concerning with sequences with infinitely many prime divisors. Moreover we characterize these sequences. Some of our theorems assert that there are infinitely many prime divisors of a sequence. These statements come from easily from the theory of S-units, but in this paper we use only elementary methods to get our results. We mention that our results help to generalize problems which can be found in some exercise books for students.

[1]Research supported by the Hungarian National Foundation for Scientific Research Grant. No. T 048945 MAT

[2]Research supported by Grant ČR 201/04/0381/2

Let $A = \{a_1 < a_2 < \cdots < a_n < \cdots\} \subseteq \mathbb{N}$ be a given set and let us denote by $A(x)$ the number of the elements of A not exceeding x. Let us suppose for any natural number k there is a positive real number x_k such that for all $x > x_k$ the inequality $A(x) > (\log x)^k$ holds. In this case there are infinitely many different prime divisors of the elements of A (see [3], p. 102).

Further we shall study the sequences of positive integers where the previous condition is not true. Let a, b be natural numbers with $a > 1$ and $(a, b) = 1$. Obviously the sequences

$$(a^n + b)_{n=1}^{\infty} \tag{1.1}$$

do not fulfill the above condition, since

$$A(x) = \left[\frac{\log(x-b)}{\log a}\right] \quad \text{if} \quad x > b + 1.$$

In what follows we show that sequences (1.1) have infinitely many different prime divisors. In the special case, when $a = 10$ and $b = 3$ we proved (in [6]) that the sequence $(10^n + 3)_{n=1}^{\infty}$ has infinitely many prime divisors, moreover for infinitely many primes p there are infinitely many $n \in \mathbb{N}$ such that $p \mid 10^n + 3$.

2. Results

First we prove that there are subsequences of sequences (1.1) which have infinitely many prime divisors.

Theorem 2.1. *Let a, b, c, d be natural numbers, $(a, b) = 1$ and $a > 1$. Then there are infinitely many prime divisors of the sequences*

$$(a^{c+(n-1)d} + b)_{n=1}^{\infty}. \tag{2.1}$$

Proof. First we suppose that sequence (2.1) has only finitely many prime divisors. Let us denote these primes by $q_1 < q_2 < \cdots < q_k$. Let us denote by $q_1 < q_2 < \cdots < q_l$ the prime divisors of sequence (2.1) which are divisors of $a^c + b$ as well and $q_{l+1} < q_{l+2} < \cdots < q_k$ which are not divisors of $a^c + b$. Let us denote by α_s for all $1 \leqslant s \leqslant l$ and $s \in \mathbb{N}$ the least natural number such that

$$q_s^{\alpha_s} > a^c + b.$$

Let

$$M = q_1^{\alpha_1} q_2^{\alpha_2} \cdots q_l^{\alpha_l} q_{l+1} q_{l+2} \cdots q_k$$

be a product of prime powers. In this case $(a, M) = 1$ since $(a, b) = 1$. By the theorem of Euler we have

$$M \mid a^{n\varphi(M)} - 1 \tag{2.2}$$

for all $n \in \mathbb{N}$.

Now we investigate the sequence

$$(a^{c+m\varphi(M)d}+b)_{m=1}^{\infty} \tag{2.3}$$

which is obviously a subsequence of sequence (2.1).

Let q be a prime divisor of sequence (2.3) that is

$$a^{m\varphi(M)d+c}+b\equiv 0 \pmod{q} \tag{2.4}$$

for some $m\in\mathbb{N}$. It follows from (2.2) that

$$a^{m\varphi(M)d}-1\equiv 0 \pmod{q}. \tag{2.5}$$

Using (2.4) and (2.5) we have

$$a^{m\varphi(M)d+c}+b=a^{m\varphi(M)d}(a^c-1)+a^{m\varphi(M)d}-1+b+1\equiv a^c+b \pmod{q}.$$

It is clear that $q\mid a^c+b$, it follows that $q\in\{q_1,q_2,\dots,q_l\}$, that is

$$a^{m\varphi(M)d+c}+b=q_1^{\beta_{m_1}}q_2^{\beta_{m_2}}\cdots q_l^{\beta_{m_l}}$$

where $\beta_{m_j}\geqslant 0$ for all $m\in\mathbb{N}$ and $1\leqslant j\leqslant l$.

We show that for all $m\in\mathbb{N}$ and $1\leqslant j\leqslant l$ we have $\beta_{m_j}<\alpha_j$. Let $1\leqslant j\leqslant l$, m be arbitrary natural numbers and $\beta_{m_j}\geqslant\alpha_j$ then

$$q_j^{\alpha_j}\mid a^{m\varphi(M)d+c}+b,$$

that is

$$a^{m\varphi(M)d+c}+b\equiv 0 \pmod{q_j^{\alpha_j}}.$$

Since $q_j^{\alpha_j}\mid M$, it follows from (2.2) that $a^{m\varphi(M)d}-1\equiv 0 \pmod{q_j^{\alpha_j}}$ and

$$a^{m\varphi(M)d+c}+b=a^{m\varphi(M)d}(a^c-1)+a^{m\varphi(M)d}-1+b+1\equiv a^c+b \pmod{q_j^{\alpha_j}},$$

that is $q_j^{\alpha_j}\mid a^c+b$, which is contradiction since $q_j^{\alpha_j}>a^c+b$. It follows that for all terms of (2.3) we have

$$a^{m\varphi(M)d+c}+b<q_1^{\alpha_1}q_2^{\alpha_2}\cdots q_l^{\alpha_l}\leqslant M\,.$$

In this way we obtained a contradiction since sequence (2.3) is not bounded. □

In the sequel we prove an interesting property of the prime divisors of sequence (2.1).

Theorem 2.2. *If $m\in\mathbb{N}$ is a divisor of a term of sequence* (2.1) *then m divides infinitely many terms of sequence* (2.1).

Proof. Let $m \in \mathbb{N}$ be a divisor of a term of sequence (2.1). Let us denote by n_0 the least non-negative number which

$$m \mid a^{c+n_0 d} + b\,. \tag{2.6}$$

Since $(a, m) = 1$, there exists a power h_m of $a \pmod m$. The number m divides $a^n - 1$ if and only if $h_m \mid n$.

Let us consider the sequence

$$(a^{n_k d+c} + b)_{n=1}^{\infty} \tag{2.7}$$

where

$$n_k = (k-1)\frac{h_m}{(h_m, d)} + n_0\,.$$

Obviously sequence (2.7) is a subsequence of sequence (2.1).

We show that m divides only those terms of sequence (2.1) which are the terms of (2.7) as well.

a) First we prove that m divides all terms of sequence (2.7). Obviously we have

$$\begin{aligned} a^{n_k d+c} + b &= a^{n_k d+c} + b - a^{n_0 d+c} + a^{n_0 d+c} = \\ &= a^{n_0 d+c}(a^{(n_k-n_0)d} - 1) + a^{n_k 0+c} + b = \\ &= a^{n_0 d+c}\big(a^{(k-1)\frac{h_m d}{(h_m,d)}} - 1\big) + a^{n_0 d+c} + b. \end{aligned} \tag{2.8}$$

Using that $\frac{d}{(h_m,d)}$ is an integer number and the definition of h_m we have

$$a^{(k-1)\frac{d}{(h_m,d)}h_m} - 1 \equiv 0 \pmod m.$$

It follows that

$$a^{n_k d+c} + b \equiv a^{n_0 d+c} + b \pmod m,$$

that is m divides all terms of (2.7).

b) Secondly we prove that if m divides a term of sequence (2.1) then this term is a term of sequence (2.7).

Let us choose $n \in \mathbb{N}$ such that $m \mid a^{nd+c_1} + b$. Obviously $n \geqslant n_0$. Then we have

$$m \mid a^{nd+c_1} + b - \big(a^{n_0 d+c_1} + b\big) = a^{n_0 d+c_1}\big(a^{d(n-n_0)} - 1\big)\,.$$

Since $(a, m) = 1$, therefore $m \mid a^{d(n-n_0)} - 1$. Using the definition of h_m we have $h_m \mid d(n - n_0)$, and

$$n = (k-1)\frac{h_m}{d} + n_0 \tag{2.9}$$

for some $k \in \mathbb{N}$. From equation (2.9) we deduce

$$n = \left((k-1)\frac{\frac{h_m}{(h_m,d)}}{\frac{d}{(h_m,d)}}\right) + n_0\,.$$

Using that $\left(\frac{h_m}{(h_m,d)}, \frac{d}{(h_m,d)}\right) = 1$, we have that n is an integer if and only if the fraction $\frac{k-1}{\frac{d}{(h_m,d)}}$ is also an integer. Consequently

$$k - 1 = (l-1)\frac{d}{(h_m, d)}\,,$$

and

$$n = (l-1)\frac{h_m}{(h_m, d)} + n_0.$$

Now the theorem is proved. □

In the previous theorems we investigated such subsequences of sequences (1.1) where the powers formed arithmetic progressions. It is known that the asymptotic density of sets of terms of arithmetic progressions are greater than zero, more exactly it equals the reciprocal of the difference. This means that sequence (2.1) is such a subsequence of (1.1) which contains relatively "many" terms of sequence (1.1). In what follows we are looking for subsequences of (1.1) where the density of the set of powers is zero, but they have infinitely many prime divisors. We give two sequences possessing the above conditions. In one of them the powers run through the set of primes and in the other the powers equal the values of Euler's function φ. It is known fact that the asymptotic density of the set of primes and the set of values of Euler's function are zero.

Theorem 2.3. *Let a, b be natural numbers with $(a, b) = 1$ and $a > 1$. Let us denote by p_n the n-th prime number. Then the sequence*

$$(a^{p_n} + b)_{n=1}^{\infty} \tag{2.10}$$

has infinitely many prime divisors.

Proof. Let us suppose that sequence (2.10) has only finitely many prime divisors, namely $q_1, q_2, \ldots, q_k$. We discuss two cases.

We consider first that there are prime divisors of the terms of sequence (2.10) which divide $a + b$. Let us denote by $q_1 < \cdots < q_l$ the divisors of $a + b$ and $q_{l+1} < \cdots < q_k$ which are not divisors of $a + b$. Let us denote by α_s for all $1 \leqslant s \leqslant l$ the least natural number which

$$q_s^{\alpha_s} > a + b\,.$$

Put

$$M = q_1^{\alpha_1} q_2^{\alpha_2} \cdots q_l^{\alpha_l} q_{l+1} \cdots q_k.$$

In this case $(a, M) = 1$ since $(a, b) = 1$. It follows from Euler's theorem that

$$a^{n\varphi(M)} - 1 \equiv 0 \pmod{M} \tag{2.11}$$

for all $n \in \mathbb{N}$. Using the theorem of Dirichlet we get that there are infinitely many prime numbers in the sequence $(n\varphi(M)+1)_{n=1}^{\infty}$. Let us denote these prime numbers by $p_1' < p_2' < \cdots p_n' < \cdots$. Obviously the sequence

$$(a^{p_n'} + b)_{n=1}^{\infty} \tag{2.12}$$

is a subsequence of sequence of (2.10). Let q be a prime divisor of sequence of (2.12). Obviously $q \in \{q_1, q_2, \ldots, q_k\}$, moreover

$$a^{p_i'} + b \equiv 0 \pmod{q} \tag{2.13}$$

for some $i \in \mathbb{N}$. It follows from (2.11) and (2.13) that

$$0 \equiv a^{p_i'} + b \equiv a^{p_i'-1}(a-1) + a^{p_i'-1} + b \equiv a + b \pmod{q}.$$

Thus $q \mid a+b$ and $q \in \{q_1, q_2, \ldots, q_l\}$. In other words $a^{p_i'} + b$ can be written in the form

$$a^{p_i'} + b = q_1^{\beta_{i,1}} q_2^{\beta_{i,2}} \cdots q_l^{\beta_{i,l}}$$

where $\beta_{i,j} \geqslant 0$ for all $1 \leqslant j \leqslant l$ natural numbers.

Now we show that $\beta_{i,j} < \alpha_j$ for all $1 \leqslant j \leqslant l$. If $\beta_{i,j} \geqslant \alpha_j$ for some $1 \leqslant j \leqslant l$ then

$$a^{p_i'} + b \equiv 0 \pmod{q_j^{\alpha_j}}$$

moreover using (2.11) and $q_j^{\alpha_j} \mid M$ we have

$$a^{p_i'-1} \equiv 1 \pmod{q_j^{\alpha_j}}.$$

It follows from the previous congruence that

$$0 \equiv a^{p_i'} + b \equiv a^{p_i'-1}(a-1) + a^{p_i'-1} + b \equiv a + b \pmod{q_j^{\alpha_j}}$$

which contradicts the fact that $q_j^{\alpha_j} > a + b$. In this way we get

$$a^{p_i'} + b < q_1^{\alpha_1} q_2^{\alpha_2} \cdots q_l^{\alpha_l} \leqslant M$$

for all $i \in \mathbb{N}$. Here we have obtained a contradiction since sequence (2.12) is not bounded.

In the second case we study when the terms of sequence (2.10) do not have such prime divisors which divide $a + b$. Put

$$L = q_1 q_2 \cdots q_k.$$

Since $(a, L) = 1$, therefore

$$a^{n\varphi(L)} - 1 \equiv 0 \pmod{L} \tag{2.14}$$

for all $n \in \mathbb{N}$. Let

$$Q = l\varphi(L) + 1$$

be a prime and q be a prime divisor of $a^Q + b$.

It follows from the definition of Q and from (2.14) that

$$a^{Q-1} \equiv 1 \pmod{q}$$

where $q \in \{q_1, q_2, \ldots, q_k\}$. Obviously

$$0 \equiv a^Q + b \equiv a^{Q-1}(a-1) + a^{Q-1} + b \equiv a + b \pmod{q},$$

which contradicts the fact that q is not a divisor of $a + b$. □

It is worth investigating that if a term of sequence (2.10) is divisible by a prime then this prime is a divisor of infinitely many terms of the sequence. The answer is not as obvious as before. First of all we prove a Lemma which help us in this case and other similar cases, too.

Lemma 2.4. *Let a, b be natural numbers with $(a, b) = 1$ and $a > 1$. If q is a prime divisor of sequence* (1.1) *then*

1. *There exists an exponent h_q of a with respect to q.*
2. *If q is a divisor of $a^k + b$ then q is a divisor of those terms of sequence* (1.1) *which can be given of the form*

$$a^{k+zh_p} + b$$

where $z \in \mathbb{Z}$ and $k + zh_p \geqslant 0$.

Proof. 1. The first statement is trivial. If $(a, b) = 1$ and q is a divisor of a term of sequence (1.1) then $(a, q) = 1$.

2. Let q is a prime divisor of $a^k + b$. Let us denote by h_q an exponent of a with respect to q. Let us consider a term in the form $a^m + b$ of sequence (1.1). In this case q is a divisor of $a^m + b$ if and only if

$$(a^k + b) - (a^m + b) \equiv 0 \pmod{q}. \tag{2.15}$$

Using elementary conversions we have

$$(a^k + b) - (a^m + b) = a^{\min\{k,m\}}\big(a^{|m-k|} - 1\big).$$

Since $(a, q) = 1$ and h_q is an exponent of a we get that congruence (2.15) is valid if and only if h_q is a divisor of $|m-k|$. This statement is equivalent to our statement. □

Conclusion 2.5. If a prime q is a divisor of two different terms of sequence (2.10) then it is a divisor of infinitely many terms of the sequence.

Proof. Let q be a prime divisor of at least two different terms of sequence (2.10). Let us denote these terms by $a^{p_1}+b$ and $a^{p_2}+b$ where $p_1 < p_2$. It follows from Lemma 1 that

$$p_2 = p_1 + nh_q$$

for some natural number n. Since p_1 and p_2 are primes therefore $(p_1, h_q) = 1$. Using Dirichlet's theorem we have that there is a subsequence $(p'_n)_{n=1}^{\infty}$ with prime terms of the sequence $(p_1 + nh_q)_{n=1}^{\infty}$. It follows from Lemma 1 that q is a divisor of all terms of the sequence

$$(a^{p'_n} + b)_{n=1}^{\infty}.$$

□

Further we study a subsequence of (1.1) where the powers are the values of Euler's function φ. Similarly to the previous sequence the asymptotic density of the set of values of Euler's function φ equals zero. First we prove that there are infinitely many prime divisors of this sequence.

Theorem 2.6. *Let a, b be natural numbers where $(a, b) = 1$ and $a > 1$. Then there are infinitely prime divisors of the sequence*

$$(a^{\varphi(n)} + b)_{n=1}^{\infty}. \tag{2.16}$$

Proof. Let us suppose that there are only finitely many prime divisors of sequence (2.16) namely $q_1, q_2, \ldots, q_k$. We distinguish two cases.

In the first case we suppose that among the prime divisors of sequence (2.16) there are divisors which divide $b+1$. Let us denote these divisors by $q_1 < \cdots < q_l$ and the others by $q_{l+1} < \cdots < q_k$.

Let us denote by α_s for all s $(1 \leqslant s \leqslant l)$ the least natural number which

$$q_s^{\alpha_s} > b + 1\,.$$

Put

$$M = q_1^{\alpha_1} q_2^{\alpha_2} \cdots q_l^{\alpha_l} q_{l+1} \cdots q_k.$$

Obviously $(a, M) = 1$. It follows from Euler's theorem that

$$a^{n\varphi(M)} \equiv 1 \pmod{M} \tag{2.17}$$

for all natural numbers n. Let us consider an increasing sequence of prime numbers $(p_i)_{i=1}^{\infty}$ where $(p_i, M) = 1$ for all $i \in \mathbb{N}$. Since the Euler's function is multiplicative we have that the sequence

$$(a^{\varphi(p_i)\varphi(M)} + b)_{i=1}^{\infty} \tag{2.18}$$

is a subsequence of sequence (2.16).

It is obvious that the prime divisors of sequence (2.18) belong to the set

$$\{q_1, q_2, \ldots, q_k\}.$$

We choose one of them and let us denote it by q. It follows from (2.17) that

$$0 \equiv a^{\varphi(p_i)\varphi(M)} + b \equiv b + 1 \pmod{q},$$

that is q is a divisor of $b+1$ and $q \in \{q_1, q_2, \ldots, q_l\}$. Thus we have

$$a^{\varphi(p_i)\varphi(M)} + b = q_1^{\beta_{i,1}} q_2^{\beta_{i,2}} \cdots q_l^{\beta_{i,l}}$$

where $\beta_{i,j} \geqslant 0$ for all $1 \leqslant j \leqslant l$ and $i \in \mathbb{N}$.

Henceforth we show that $\beta_{i,j} < \alpha_j$ for all $1 \leqslant j \leqslant l$ and $i \in \mathbb{N}$. If $\beta_{i,j} \geqslant \alpha_j$ for any $1 \leqslant j \leqslant l$ and for $i \in \mathbb{N}$, then we have

$$a^{\varphi(p_i)\varphi(M)} + b \equiv 0 \pmod{q_j^{\alpha_j}} \quad \text{and} \quad a^{\varphi(p_i)\varphi(M)} - 1 \equiv 0 \pmod{q_j^{\alpha_j}}.$$

It follows from the previous congruences that $q_j^{\alpha_j}$ is a divisor of $b+1$, this contradicts the fact that $q_j^{\alpha_j} > b+1$. Hence

$$a^{\varphi(p_i)\varphi(M)} + b < q_1^{\alpha_{i,1}} q_2^{\alpha_{i,2}} \cdots q_l^{\alpha_{i,l}} \leqslant M\,,$$

which is a contradiction since sequence (2.18) is not bounded.

In the second case we suppose that the divisors of sequence (2.16) are not divisors of $b+1$. Put

$$L = q_1 q_2 \cdots q_k.$$

Since $(a, L) = 1$, it follows from the Euler's theorem that

$$a^{\varphi(L)} - 1 \equiv 0 \pmod{L}. \tag{2.19}$$

Obviously $a^{\varphi(L)} + b$ is a term of sequence (2.16). Let q be a prime divisor of sequence (2.16). In this case

$$0 \equiv a^{\varphi(L)} + b \equiv a^{\varphi(L)} - 1 + b + 1 \equiv b + 1 \pmod{q},$$

that is q is a divisor of $b+1$ which is contradiction. □

Further we investigate when a prime divisor of sequence (2.16) divides infinitely many terms of sequence (2.16). This problem is more difficult than in case (2.10). We give two sufficient conditions.

Theorem 2.7. *If q is a prime divisor of sequence* (2.16) *and $b + 1 \equiv 0 \pmod{q}$, then q is a divisor of infinitely many terms of sequence* (2.16).

Proof. Let q be an odd prime divisor of sequence (2.16) with the condition $b+1 \equiv 0 \pmod{q}$. Since $(a, q) = 1$, it follows from the Euler's theorem that $a^{\varphi(q)} \equiv 1 \pmod{q}$. Obviously we have

$$a^{\varphi(q)} + b \equiv a^{\varphi(q)} - 1 + b + 1 \equiv 0 \pmod{q}.$$

Let $(p_n)_{n=1}^{\infty}$ be an arbitrary increasing sequence of prime numbers, where q is not a term of this sequence.

We show that q is a divisor of all terms of the sequence

$$(a^{\varphi(qp_n)}+b)_{n=1}^{\infty}.$$

Since φ is a multiplicative function and $(q,p_n)=1$ we have that

$$a^{\varphi(qp_n)}+b \equiv a^{\varphi(q)\varphi(p_n)}+b \equiv (a^{\varphi(q)})^{\varphi(p_n)}-1+b+1 \equiv 0 \pmod{q}$$

for all natural numbers n. □

Theorem 2.8. *Let q be a prime divisor of sequence* (2.16) *and the power of a is an odd number* $\pmod{q}$. *Then q is a divisor of infinitely many terms of sequence* (2.16).

Proof. Let q be such a prime divisor of sequence (2.16) that the power of a is odd $\pmod{q}$. Let us denote by n_0 the least natural number where q is a divisor of $a^{\varphi(n_0)}+b$. Since the power h_q of a is odd $\pmod{q}$ from the Dirichlet's theorem follows that the sequence

$$(kh_q+2)_{k=1}^{\infty} \tag{2.20}$$

contains infinitely many prime numbers. Let us choose a subsequence

$$(p_n')_{n=1}^{\infty}$$

of sequence (2.20) which terms are primes and not divisors of the number n_0. Since φ multiplicative we have that

$$a^{\varphi(n_0p_n')}+b = a^{\varphi(n_0)\varphi(p_n')}+b = a^{\varphi(n_0)(p_n'-1)}+b =$$

$$= a^{\varphi(n_0)(kh_q+1)}+b = a^{\varphi(n_0)+\varphi(n_0)kh_q}+b$$

for all $n \in \mathbb{N}$. Using Lemma 1 we have that q is a divisor of all terms of the sequence

$$(a^{\varphi(n_0p_n')}+b)_{n=1}^{\infty}.$$

□

Finally we show that there are infinitely many primes which do not divide any term of sequence (2.16). First we prove a more general theorem.

Theorem 2.9. *Let $a>1$ and $b>1$ be natural numbers where b is odd and $(a,b)=1$. Then there are infinitely many primes p which do not divide any term of sequence*

$$(a^{2n}+b)_{n=1}^{\infty} \tag{2.21}$$

Proof. Let p be an arbitrary prime. Then p is not a divisor of any term of sequence (2.21) if and only if there is no solution of the quadratic congruence $x^2 \equiv -b \pmod{p}$. Using the Jacobi's symbol we have

$$\left(\frac{-b}{p}\right) = -1.$$

Let p be an odd prime number where $(b, p) = 1$. Applying the law of quadratic reciprocity of Gauss we have

$$\left(\frac{-b}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{p}{p}\right) = (-1)^{\frac{p-1}{2}}\left(\frac{p}{b}\right) \ (-1)^{\frac{p-1}{2}\frac{b-1}{2}} = \left(\frac{p}{b}\right)(-1)^{\frac{p-1}{2}\frac{b+1}{2}}. \qquad (2.22)$$

We distinguish two cases.

First we suppose that $b = 4l + 1$ where l is a natural number. Let us consider primes of the form

$$p = 4bk + 2b + 1, \quad \text{where} \quad k \in \mathbb{N}.$$

It follows from the Dirichlet's theorem that there are infinitely many primes of the form as above since $(4b, 2b + 1) = 1$.

In this case $\left(\frac{p}{b}\right) = \left(\frac{1}{b}\right) = 1$ and $\frac{p-1}{2}\frac{b+1}{2}$ is odd natural number. Using (2.22) we have

$$\left(\frac{-b}{p}\right) = -1.$$

That is p doesn't divide any term of sequence (2.21).

In the second case we suppose that $b = 4l + 3$ where l natural number.
Let us consider primes of the form

$$p = 2bk + 2b - 1.$$

Using the previous method we get that there are infinitely many primes of this form. Obviously $\frac{b+1}{2}$ is even. Moreover

$$\left(\frac{p}{b}\right) = \left(\frac{-1}{b}\right) = (-1)^{\frac{b-1}{2}} = -1.$$

Using (2.22) we have equation

$$\left(\frac{-b}{p}\right) = -1.$$

That is p doesn't divide any term of sequence a (2.21). □

Conclusion 2.10. There are infinitely many primes which do not divide any term of sequence (2.16).

Proof. Using the previous theorem we get this statement since the Euler's function φ is even except those cases when $\varphi(1) = \varphi(2) = 1$. □

References

[1] Hardy, G. H., Wright, E. M., An introduction to the theory of numbers, Oxford, 1954.

[2] Sárközi, A., Számelmélet, Műszaki Könyvkiadó, Budapest, 1976.

[3] Sárközi, A., Surányi, J., Számelmélet feladatgyűjtemény, 13. kiadás, Tankönyvkiadó, Budapest, 1990.

[4] Sierpinsky, W., Elementary theory of numbers, PWN, Warszawa, 1964.

[5] Sierpinsky, W., 200 feladat az elemi számelméletből, Tankönyvkiadó, Budapest, 1964.

[6] Tóth, J., Egy számsorozat prímosztóiról, Polygon, Szeged III (2) (1993), 78–79.

Ferdinánd Filip
Department of Mathematics
University of J. Selye
SK-94501 Komárno
Rožníckej Školy 1514
Slovakia

Kálmán Liptai
Institute of Mathematics and Informatics
Eszterházy Károly College
H-3300 Eger
Leányka út 4.
Hungary

János T. Tóth
Department of Mathematics
University of Ostrava
CZ-701 03 Ostrava
30. dubna 22
Czech Republic