PROCEEDINGS OF THE YEREVAN STATE UNIVERSITY

Physical and Mathematical Sciences 2016, № 2, p. 22–27

M a t h e m a t i c s

ON THE P_1 PROPERTY OF SEQUENCES OF POSITIVE INTEGERS

T. L. HAKOBYAN *

Chair of Algebra and Geometry YSU, Armenia

In this paper we introduce the concept of P_1 property of sequences, consisting of positive integers and prove two criteria revealing this property. First one deals with rather slow increasing sequences while the second one works for those sequences of positive integers which satisfy certain number theoretic condition. Additionally, we prove the unboundedness of common divisors of distinct terms of sequences of the form $(2^{2^n}+d)_{n=1}^{\infty}$ for integers $d \neq 1$.

MSC2010: Primary 11A00; Secondary 11A05, 11A41, 11A51.

Keywords: Fermat's number, prime number, greatest common divisor, Chinese Remainder Theorem.

Introduction. It is known that for any non constant polynomial P with integer coefficients there exist infinitely many primes, dividing at least one term from the sequence $(P(n))_{n=1}^{\infty}$ [1]. In this respect we are interested if there is a general phenomenon behind this fact. It turns out that the answer is positive and somehow depends on the rate of growth of the given sequence . To be more precise we give the definition of P_1 property of sequences of positive integers.

D e f i n i t i o n 1. We say that a sequence $(n_k)_{k=1}^{\infty}$ of positive integers has the $\mathbb{P}_1$ property (denote $(n_k)_{k=1}^{\infty} \in \mathbb{P}_1$), if there are infinitely many primes dividing at least one term of the sequence.

To formulate our results we need one more definition.

D e f i n i t i o n 2. Suppose $S = \{p_1, p_2, ..., p_n\}$ is a finite set consisting of prime numbers, where $n \in \mathbb{N}$. We define $\hat{S} = \{{p_1}^{k_1} {p_2}^{k_2} \cdot \ldots \cdot {p_n}^{k_n} | k_1, k_2, ..., k_n \in \mathbb{Z}_+\}$ and arrange the set $\hat{S}$ as an increasing sequence, which is denoted by $(n_k(S))_{k=1}^{\infty}$.

In this paper we prove the following theorem.

T h e o r e m 1. $\lim\limits_{k\to\infty} \dfrac{\ln(\ln(n_k(S)))}{\ln(k)} = \dfrac{1}{n}$.

The next result which is concerning P_1 property, that is proved in this paper, is motivated by sequences $(a_n)_{n=1}^{\infty}$ of positive integers satisfying $\gcd(a_k, a_l) = a_{\gcd(k,l)}$ for all positive integers k and l.

* E-mail: tigran19931026@gmail.com

Theorem 2. Suppose $(n_k)_{k=1}^{\infty}$ and $(m_k)_{k=1}^{\infty}$ are sequences of positive integers. Then $(n_k)_{k=1}^{\infty} \in \mathbb{P}_1$, if the following conditions hold.

1. $\lim\limits_{k\to\infty} n_k = \infty$;
2. $(m_k)_{k=1}^{\infty}$ is increasing;
3. $\gcd(n_k, n_{k+l}) < m_l$ for all positive integers k and l.

In this paper we also deal with sequences of the form $a_n = 2^{2^n} + d$, where $d \in \mathbb{Z}$. Recall that a Fermat number is a positive integer of the form $F_n = 2^{2^n} + 1$ for some nonnegative integer n. It is well known that $\gcd(F_k, F_l) = 1$, whenever $k \neq l$. For the proof we refer to [2] (Chapter 1, Theorem 13). In this way a natural question arises. Whether this result is true for sequences $a_n = 2^{2^n} + d$ for odd integers d? In this paper we prove a theorem, which gives a negative answer to this question.

Theorem 3. For any integer $d \neq 1$ and positive integer m there exist distinct elements a_k and a_l in the sequence $a_n = 2^{2^n} + d$ such that $\gcd(a_k, a_l) > m$.

Proof of Theorem 1. Suppose we have positive numbers $w_1, w_2, \dots, w_n > 0$, where $n \in \mathbb{N}$.

Definition 3. For any $W > 0$ we define

$$N(W; w_1, w_2, \dots, w_n) = \left| \left\{ (k_1, k_2, \dots, k_n) \in (\mathbb{Z}_+)^n \middle| \sum_{i=1}^{n} k_i w_i \leq W \right\} \right|.$$

Lemma 1. $$\frac{W^n}{n! \prod\limits_{i=1}^{n} w_i} \leq N(W; w_1, w_2, \dots, w_n) \leq \frac{\left(W + \sum\limits_{i=1}^{n} w_i\right)^n}{n! \prod\limits_{i=1}^{n} w_i}.$$

Proof. Consider the lattice Λ in $\mathbb{R}^n$, spanned over the basis $\{w_1 e_1, \dots, w_n e_n\}$, where $\{e_1, \dots, e_n\}$ is the standard basis of $\mathbb{R}^n$. Define

$$\Pi_r = \{(x_1, x_2, \dots, x_n) \in (\mathbb{R}_+)^n | \sum_{i=1}^{n} x_i \leq r\} \subset \mathbb{R}^n$$

for any $r > 0$. Then $N(W; w_1, w_2, \dots, w_n) = |\Lambda \cap \Pi_W|$ is the number of lattice points in the simplex Π_W.

Now for any point $x = (x_1, x_2, \dots, x_n) \in \Lambda \cap \Pi$ (i.e. for any solution) construct an open parallelotope $\Pi_x = \{(t_1, \dots, t_n) || t_i - x_i| < w_i/2,\ i = 1, 2, \dots, n\} \subset \mathbb{R}^n$ with a center at that point. Note that $\Pi_x \cap \Pi_y = \emptyset, \mathbb{V}(\Pi_x) = \prod\limits_{i=1}^{n} w_i$ for all $x, y \in \Lambda \cap \Pi_W$, $x \neq y$, where $\mathbb{V}$ stands for the volume.

Set $\Delta = \sum\limits_{i=1}^{n} w_i, v = (w_1/2, \dots, w_n/2) \in \mathbb{R}^n$ and $\Pi_{r,v} = \{x - v | x \in \Pi_r\}$ (shift of the simplex Π_r by vector v). Note that $\Pi_W \subset \bigcup\limits_{x \in \Lambda \cap \Pi_W} \Pi_x \subset \Pi_{W+\Delta, v}$.

Comparing volumes yields $\dfrac{W^n}{n!} \leq N(W; w_1, w_2, ..., w_n) \prod_{i=1}^{n} w_i \leq \dfrac{(W + \sum_{i=1}^{n} w_i)^n}{n!}$.

It remains only to divide all the parts of the inequality by $\prod_{i=1}^{n} w_i$. □

One can find an additional information concerning Lemma 1 in [1, 3].

Definition 4. For any $l \in N$ we set $t_l = |\{k | n_k(S) \leq l\}|$.

Observe that due to Definition 2.

$$t_l = \left| \left\{ (k_1, k_2, ..., k_n) \in (\mathbb{Z}_+)^n | \prod_{i=1}^{n} p_i^{k_i} \leq l \right\} \right| =$$
$$= \left| \left\{ (k_1, k_2, ..., k_n) \in (\mathbb{Z}_+)^n | \sum_{i=1}^{n} \ln(p_i) k_i \leq \ln(l) \right\} \right| =$$
$$= N(\ln(l); \ln(p_1), \ln(p_2), ..., \ln(p_n)),$$

As a consequence of Lemma 1, we get that there exist constants $c_1 > 0$ and $c_2 > 0$ such that $c_1 W^n < N(W; w_1, w_2, ..., w_n) < c_2 W^n$ for all $W > \ln(2)$. Therefore, for some constants $a > 0$ and $b > 0$ the inequality

$$a(\ln(l))^n < N(\ln(l); \ln(p_1), \ln(p_2), ..., \ln(p_n)) < b(\ln(l))^n$$

holds for all $l \geq 2$. Substituting $l = n_k(S)$ for $k = 2, 3, ...$, we obtain

$$a(\ln(n_k(S)))^n < t_{n_k(S)} < b(\ln(n_k(S)))^n$$

and, therefore, $\ln(a) + n\ln(\ln(n_k(S))) < \ln(t_{n_k(S)}) < \ln(b) + n\ln(\ln(n_k(S)))$. Using that $(n_k(S))_{k=1}^{\infty}$ is an increasing sequence, we conclude that $t_{n_k(S)} = k$ for all $k \in \mathbb{N}$. As a result

$$\ln(a) + n\ln(\ln(n_k(S))) < \ln(k) < \ln(b) + n\ln(\ln(n_k(S)))$$

for all $k \geq 2$, $k \in \mathbb{N}$ and so

$$\limsup_{k\to\infty} \frac{\ln(\ln(n_k(S)))}{\ln(k)} \leq 1/n \leq \liminf_{k\to\infty} \frac{\ln(\ln(n_k(S)))}{\ln(k)},$$

which shows that $\lim\limits_{k\to\infty} \dfrac{\ln(\ln(n_k(S)))}{\ln(k)} = \dfrac{1}{n}$. □

Corollary 1. If $(n_k)_{k=1}^{\infty}$ is an increasing sequence of positive integers and $\liminf\limits_{k\to\infty} \dfrac{\ln(\ln(n_k))}{\ln(k)} = 0$, then $(n_k)_{k=1}^{\infty} \in \mathbb{P}_1$.

Remark 1. A close result was previously proved in [4]. The result was formulated for almost injective sequences, i.e. for the sequences $(n_k)_{k=1}^{\infty}$ of positive integers for which there exists a constant c such that $|\{k | n_k = m\}| \leq c$ for all positive integers m. This definition of almost injective sequences was inspired by non constant polynomials P, since they attain any value at most $c = \deg(P)$ times. Our result is independent of [4].

Proof. Suppose to the contrary that $(n_k)_{k=1}^{\infty} \notin \mathbb{P}_1$. This means that there is a finite set S consisting of prime numbers such that $(n_k)_{k=1}^{\infty}$ is a subsequence of $(n_k(S))_{k=1}^{\infty}$. Hence

$$\liminf_{k\to\infty} \frac{\ln(\ln(n_k))}{\ln(k)} \geq \liminf_{k\to\infty} \frac{\ln(\ln(n_k(S)))}{\ln(k)} = \frac{1}{|S|} > 0,$$

which is a contradiction. □

Corollary 2. For any non constant polynomial P with integer coefficients the sequence $(P(n))_{n=1}^{\infty} \in P_1$.

Proof. The sequence $(P(n))_{n=1}^{\infty}$ is eventually increasing and $\lim\limits_{n\to\infty} \dfrac{\ln(\ln(P(n)))}{\ln(n)} = 0$. It remains to use Corollary 1. $\square$

We would also like to give a purely number theoretic proof of this fact.

Proof. Suppose that the finite set $S = \{p_1, p_2, ..., p_n\}$ contains all possible prime factors of all numbers $P(n)$, $n \in \mathbb{N}$, where P is the given polynomial. For $j \in \{1, 2, .., n\}$ we define $k_j = \min_{n\in\mathbb{N}} \nu_{p_j}(P(n))$.

Suppose also that $k_j = \nu_{p_j}(P(s_j))$ for each $j \in \{1, 2, .., n\}$. By the Chinese Remainder Theorem, there is a positive integer n such that $n \equiv s_j (\mod {p_j}^{k_j+1})$ for all $j \in \{1, 2..., n\}$. From this it follows that $P(n) \equiv P(s_j) (\mod {p_j}^{k_j+1})$ for all $j \in \{1, 2..., n\}$. Consequently, $P(n)$ is not divisible by ${p_j}^{k_j+1}$ for all $j \in \{1, 2..., n\}$. Hence, $P\Big(n + s\prod_{j=1}^{n} {p_j}^{k_j+1}\Big)$ is not divisible by ${p_j}^{k_j+1}$ for all $j \in \{1, 2..., n\}$ and $s \in \mathbb{N}$. As a result we obtain $P\Big(n + s\prod\limits_{j=1}^{n} {p_j}^{k_j+1}\Big) \leq \prod\limits_{j=1}^{n} {p_j}^{k_j}$ for all $s \in \mathbb{N}$. The latter assertion is a contradiction to the fact that P is a non constant polynomial. $\square$

Proof of Theorem 2. Suppose $(n_k)_{k=1}^{\infty} \notin \mathbb{P}_1$. Then there is a finite set $S =$ $= \{p_1, p_2, ..., p_n\}$, consisting of prime numbers such that any term of the sequence $(n_k)_{k=1}^{\infty}$ is a product of some elements (not necessarily distinct) from the set S. As the sequence $(n_k)_{k=1}^{\infty}$ tends to infinity, it is unbounded, so there is at least one prime $p \in S$ such that the sequence $(\nu_p(n_k))_{k=1}^{\infty}$ is unbounded, where $\nu_p(m) = \max\{k | m \vdots p^k\}$ for any integer m and prime p. WLOG we may assume that the set of all such primes $p \in S$ is $\{p_1, p_2, ..., p_l\}$, for some $1 \leq l \leq s$.

Definition 5. For any $1 \leq t \leq l$ and $M \in \mathbb{N}$ we define

$$A_t(M) \triangleq \{k | \nu_{p_t}(n_k) > M\} = (s_{M,t,j})_{j=1}^{\infty},$$
$$L \triangleq \max\{\nu_{p_j}(n_k) | l+1 \leq j \leq s,\ k \in \mathbb{N}\} < \infty, \quad l < s.$$

Corollary 3. For each $M \in \mathbb{N}$, one has that $\mathbb{N} = \bigcup\limits_{t=1}^{l} A_t(M) \cup A_M$ for the set

$$A_M = \{k | \nu_{p_t}(n_k) \leq M,\ t = 1, 2, ..., l\}.$$

It is finite, since $|A_M| \leq \left| \left\{ k | n_k \leq \prod\limits_{i=1}^{l} p_i^M \cdot \prod\limits_{j=l+1}^{s} p_j^L \right\} \right|$, where the latter product $T = \prod\limits_{j=l+1}^{s} p_j^L$ is assumed to be 1 if $l = s$.

Lemma 2. For sufficiently large M the inequality $s_{M,t,j+1} - s_{M,t,j} > l$ holds for all $t \in \{1, 2, ..., l\}$ and $j \in \mathbb{N}$.

Proof. We choose M large enough to satisfy $2^M > m_l$. Using that $p_t^M | n_{s_{M,t,j+1}}$ and $p_t^M | n_{s_{M,t,j}}$ we deduce that $m_{(s_{M,t,j+1} - s_{M,t,j})} > \gcd(n_{s_{M,t,j+1}}, n_{s_{M,t,j}}) \geq {p_t}^M \geq 2^M > m_l$. Since the sequence $\Big(m_t\Big)_{t=1}^{\infty}$ is increasing, we conclude that $s_{M,t,j+1} - s_{M,t,j} > l$. $\square$

Consequently for all $t \in \{1,2,...,l\}$, $N \in \mathbb{N}$, and sufficiently large M,

$$|A_t(M) \cap \{1,2,...,N\}| \leq \left[\frac{N}{l+1}\right] + 1,$$

where $[x]$ stands for the integer part of $x \in \mathbb{R}$. Therefore, for a fixed sufficiently large M

$$|A_M| \geq |\{1,2,...,N\} \setminus \bigcup_{t=1}^{l} A_t(M)| \geq$$

$$\geq N - \sum_{t=1}^{l} |A_t(M) \cap \{1,2,...,N\}| \geq N - l\left(\left[\frac{N}{l+1}\right] + 1\right) \geq \frac{N}{l+1} - l$$

for each positive integer N. From this inequality we infer that A_M is infinite, which is contrary to Corollary 3. The Proof of Theorem 2 is completed. □

Corollary 4. Let $(n_k)_{k=1}^{\infty}$ be a sequence of positive integers, which tends to infinity. If for each $l \in \mathbb{N}$ there is a constant $c_l \in \mathbb{N}$ such that $\gcd(n_k, n_{k+l}) \leq c_l$ for all positive integers k, then $(n_k)_{k=1}^{\infty} \in P_1$.

Proof. We define a sequence $(m_l)_{l=1}^{\infty}$ of positive integers by

$$m_l = \max\{c_1, c_2, ..., c_l\} + l$$

for all positive integers l. Now all conditions of Theorem 2 are satisfied and the Corollary is proved. □

Corollary 5. If an increasing sequence $(n_k)_{k=1}^{\infty}$ of positive integers satisfies $\gcd(n_k, n_l) = n_{\gcd(k,l)}$ for all positive integers k and l, then $(n_k)_{k=1}^{\infty} \in P_1$.

Proof. Let us set $c_l = n_l$ for each $l \in \mathbb{N}$, and observe that

$$\gcd(n_k, n_{k+l}) = n_{\gcd(k,k+l)} = n_{\gcd(k,l)} \leq n_l = c_l,$$

since $(n_k)_{k=1}^{\infty}$ is increasing. So the conditions of Corollary 4 are satisfied. □

Proof of Theorem 3. Suppose that there is an integer $d \neq 1$ and a positive integer m such that $\gcd(a_k, a_l) \leq m$ for all distinct elements a_k and a_l of this sequence. It follows that if for some positive integer ν and distinct positive integers k and l, $p^\nu | a_k$ and $p^\nu | a_l$, then $p^\nu \leq \gcd(a_k, a_l) \leq m$. Consequently for each prime p the sequence $(\nu_p(a_n))_{n=1}^{\infty}$ is bounded. Let us prove some auxiliary lemmas.

Lemma 3. If positive integers n and k are given, which satisfy $\nu_2(k) < n$, then there is a positive integer $l > n$ such that $(2^l - 2^n) \vdots k$.

Proof. Let $k = 2^a b$, where $a = \nu_2(k) < n$ and b be an odd number. Since

$$b | 2^{\phi(b)} - 1$$

(ϕ is the Euler's totient function), we get that $(2^{n+\phi(b)} - 2^n) \vdots 2^n b \vdots 2^a b = k$. We now set $l = n + \phi(b)$. The Lemma is proved. □

Lemma 4. If for some prime $p > m$ and positive integer n the relation $p | a_n$ holds, then $p \equiv 1 (\bmod\ 2^n)$.

Proof. Suppose $p \not\equiv 1 (\bmod\ 2^n)$. Then, by Lemma 1, there is some positive integer $l > n$ such that $(2^l - 2^n) \vdots (p-1)$. Consequently,

$$a_l - a_n = 2^{2^l} - 2^{2^n} = 2^{2^n}(2^{2^l - 2^n} - 1) \vdots 2^{2^n}(2^{p-1} - 1) = 2^{2^n - 1}(2^p - 2) \vdots p$$

by Fermat's little theorem. Since $p | a_n$, we thus get that $p | a_l$, and so

$$p \le \gcd(a_n, a_l) \le m,$$

which contradicts the conditions of the Lemma. □

Lemma 5. $|d|$ is a power of 2.

Proof. Let $a_n = 2^{k_n} b_n c_n$ for any positive integer n, where the prime divisors of b_n are precisely the odd prime divisors of a_n, which are less or equal to m. If there is no such prime, we set $b_n = 1$. From Lemma 2 it follows that $c_n \equiv 1 (\bmod\ 2^n)$ and so $a_n \equiv 2^{k_n} b_n (\bmod\ 2^n)$. On the other hand, $a_n = 2^{2^n} + d \equiv d (\bmod\ 2^n)$, hence $2^{k_n} b_n \equiv d (\bmod\ 2^n)$. As the number of primes not exceeding m is finite, and the sequence $(\nu_p(a_n))_{n=1}^{\infty}$ is bounded for each prime p, there exists some positive integer M such that $2^{k_n} b_n \le M$ for all $n \in \mathbb{N}$. In the long run we get $2^{k_n} b_n = d$ for all sufficiently large n (in particular $d \ne 0$, which was clear). From this we infer that

$$2^{2^n} + d = a_n = 2^{k_n} b_n c_n = d c_n \vdots d$$

and, therefore, $d | 2^{2^n}$ for all sufficiently large $n \in \mathbb{N}$. □

Lemma 6. For any sufficiently large positive integer n there is a positive integer $l_n > n$ such that $a_{l_n} \vdots a_n$.

Proof. For $d = -1$ one has that $a_{n+1} = 2^{2^{n+1}} - 1 \vdots 2^{2^n} - 1 = a_n$ and we are done. Now suppose $d \ne \pm 1$. In accordance with Lemma 5, $d = \pm 2^k$ for some positive integer k. Let us choose a positive integer $n > \nu_2(k)$, then $\nu_2(2^n - k) = \nu_2(k)$. Choose $l_n > n$ from Lemma 3, then $(2^{l_n} - 2^n) \vdots (2^n - k)$, and thereby $(2^{l_n} - k) \vdots (2^n - k)$. Since $\nu_2(2^{l_n} - k) = \nu_2(k) = \nu_2(2^n - k)$, the quotient $\dfrac{2^{l_n} - k}{2^n - k}$ is an odd integer, which means that

$$(2^{2^{l_n} - k} \pm 1) \vdots (2^{2^n - k} \pm 1).$$

Multiplying by 2^k, we obtain $a_{l_n} \vdots a_n$, depending on whether $d = 2^k$ or $d = -2^k$. □

One can infer from Lemma 6, that $a_n = \gcd(a_n, a_{l_n}) \le m$ for $n > \nu_2(k)$, which is a contradiction. □

Received 16.03.2016

REFERENCES

1. **Pólya G., Szegö G.** Problems and Theorems in Analysis. Part I, II. M.: Nauka, 1978 (in Russian).
2. **Chandrasekharan K.** Introduction to Analytic Number Theory. Springer, 1968.
3. **Manfred W.P.** A Remark on an Inequality for the Number of Lattice Points in a Simplex. // SIAM Journal on Applied Mathematics, 1971, v. 20, № 4, p. 638–641.
4. **Elsholtz Ch.** Prime Divisors of Thin Sequences. // The American Mathematical Monthly, 2012, v. 4, № 119, p. 331–333.