Bull. Aust. Math. Soc. **97** (2018), 11–14
doi:10.1017/S0004972717000843

NOTE ON LEHMER–PIERCE SEQUENCES WITH THE SAME PRIME DIVISORS

M. SKAŁBA

(Received 3 July 2017; accepted 17 July 2017; first published online 4 October 2017)

Abstract

Let $a_1, a_2, \ldots, a_m$ and $b_1, b_2, \ldots, b_l$ be two sequences of pairwise distinct positive integers greater than 1. Assume also that none of the above numbers is a perfect power. If for each positive integer n and prime number p the number $\prod_{i=1}^{m}(1-a_i^n)$ is divisible by p if and only if the number $\prod_{j=1}^{l}(1-b_j^n)$ is divisible by p, then $m = l$ and $\{a_1, a_2, \ldots, a_m\} = \{b_1, b_2, \ldots, b_l\}$.

2010 *Mathematics subject classification*: primary 11B50; secondary 11A15.

Keywords and phrases: Lehmer–Pierce sequences, power residues.

Let $a_1, a_2, \ldots, a_m$ and $b_1, b_2, \ldots, b_l$ be two sequences of pairwise distinct positive integers greater than 1. We associate with them the following two sequences:

$$x_n = \prod_{i=1}^{m}(1-a_i^n), \quad y_n = \prod_{j=1}^{l}(1-b_j^n). \tag{1}$$

They belong to the broader class of so-called *Lehmer–Pierce* sequences (see, for example, [2]).

For any natural number z, let $\operatorname{supp}(z)$ denote the set of all prime divisors of z. The main result of the paper is the following theorem.

Theorem 1. *Assume that for each $n \in \mathbb{N}$,*

$$\operatorname{supp}(x_n) \subseteq \operatorname{supp}(y_n). \tag{2}$$

Then, for any $i \in \{1, \ldots, m\}$ for which a_i is not a perfect power, there exists $j \in \{1, \ldots, l\}$ such that

$$b_j = a_i^t \quad \text{with } t \in \mathbb{N}.$$

We now introduce some useful terminology. We call a Lehmer–Pierce sequence (x_n) of type (1) *reduced* if and only if none of the a_i is a perfect power.

Theorem 2. *Assume that for each $n \in \mathbb{N}$, the relation (2) holds and that (x_n) is reduced. Then, for each $n \in \mathbb{N}$, the term y_n is divisible by x_n and y_n/x_n is a linear recurrence sequence.*

THEOREM 3. *Assume that for each* $n \in \mathbb{N}$,

$$\operatorname{supp}(x_n) = \operatorname{supp}(y_n) \tag{3}$$

and that both (x_n) *and* (y_n) *are reduced. Then* $m = l$, $\{a_1, a_2, \dots, a_m\} = \{b_1, b_2, \dots, b_l\}$ *and* $x_n = y_n$ *for each* $n \in \mathbb{N}$.

We need two lemmas.

LEMMA 4 [4, Corollary 1]. *Let* n *and* n_i *be positive integers with* $n_i \mid n$ *for* $1 \le i \le k$. *Let* K *be a number field,* $\alpha_i \in K^*$ $(1 \le i \le k)$ *and* $\beta_j \in K^*$ $(1 \le j \le l)$. *Let* $w_n(K)$ *be the number of nth roots of unity contained in* K *and assume that*

$$(w_n(K), \operatorname{lcm}[K(\zeta_q) : K]) = 1, \tag{4}$$

where the least common multiple is over all prime divisors q *of* n *and additionally* $q = 4$ *if* $4 \mid n$. *Consider the following implication.*

(i) *Solubility in* K *of the* k *congruences* $x^{n_i} \equiv \alpha_i \pmod{\mathfrak{p}}$ *implies solubility in* K *of at least one of the* l *congruences* $x^n \equiv \beta_j \pmod{\mathfrak{p}}$.

The implication (i) holds for almost all prime ideals $\mathfrak{p}$ *of* K *if and only if there exists an involution* σ *of the power set of* $\{1, \dots, l\}$ *such that for all* $A \subset \{1, \dots, l\}$,

$$|\sigma(A)| \equiv |A| + 1 \pmod 2$$

and

$$\prod_{j \in \sigma(A)} \beta_j = \prod_{j \in A} \beta_j \prod_{i=1}^{k} \alpha_i^{a_i n/n_i} \gamma^n,$$

where $a_i \in \mathbb{Z}$, $\gamma \in K^*$.

LEMMA 5. *Let* G *be a free abelian group. Then the equality*

$$\prod_{i=1}^{l} (1 - g_i) = 0 \quad \text{in the group ring } \mathbb{Z}[G]$$

implies that $g_i = e$ *for a certain* $i \in \{1, \dots, l\}$.

PROOF. Only a finite number of elements of G is involved and therefore we can assume that G is of finite rank, say $G = \mathbb{Z}^s$. Let us consider the homomorphism

$$h : \mathbb{Z}[G] \longrightarrow \mathbb{C}(z_1, \dots, z_s)$$

given on group elements by the formula

$$h(k_1, \dots, k_s) = z_1^{k_1} \cdots z_s^{k_s}.$$

It is clear that $g \neq e$ gives $h(g) \neq 1$ and hence the assertion follows. □

https://doi.org/10.1017/S0004972717000843 Published online by Cambridge University Press

Proof of Theorem 1. Without loss of generality, assume that $i = 1$. Let q be a prime number and assume that a_1 is a qth power residue mod p, where p is also a prime number and $p \neq q$. If $p \not\equiv 1 \pmod q$, then all residues mod p are qth powers mod p and *a posteriori* there exists b_j, a qth power residue mod p. If $p \equiv 1 \pmod q$, then by Euler's criterion

$$a_1^{(p-1)/q} \equiv 1 \pmod p$$

and hence $x_{(p-1)/q} \equiv 0 \pmod p$ as well. Using the assumption (2) of the theorem, we infer that $y_{(p-1)/q} \equiv 0 \pmod p$ and further there exists j with $1 \leq j \leq l$ such that

$$b_j^{(p-1)/q} \equiv 1 \pmod p.$$

Using Euler's criterion once again, we see that b_j is a qth power residue mod p. So, we have verified that the implication (i) of Lemma 4 does hold for all $p \neq q$ ($K = \mathbb{Q}$, $k = 1$). The technical assumption (4) is obviously satisfied. Therefore, we conclude by Lemma 4 that there exist an involution $\sigma = \sigma(q)$ of the power set of $\{1, \ldots, l\}$ and integers $a(A), \gamma(A) \in \mathbb{Q}^*$ for $A \subset \{1, \ldots, l\}$ such that $|\sigma(A)| \equiv |A| + 1 \pmod 2$ and

$$\prod_{j\in\sigma(A)} b_j = a_1^{a(A)} \gamma(A)^q \prod_{j\in A} b_j. \tag{5}$$

Because there are only finitely many relevant involutions, there are an involution σ and an infinite set of primes Q such that (5) holds for $q \in Q$ with the same σ. Let $\mathcal{D}$ be the set of all prime divisors of the number $a_1 b_1 \cdots b_l$. For any prime $s \in \mathcal{D}$ and $u \in \mathbb{Q}^+$, let $\nu_s(u)$ be the s-adic exponent of u. For any $u \in \mathbb{Q}^+$, let $\nu(u) = (\nu_s(u))_{s\in\mathcal{D}}$ be the vector of exponents. For $q \in Q$, we obtain from (5) that

$$\dim_{\mathbb{F}_q}\Big(\nu\Big(\prod_{j\in\sigma(A)} b_j \cdot \prod_{j\in A} b_j^{-1}\Big), \nu(a_1)\Big) = 1.$$

Because Q is infinite, it follows that

$$\dim_{\mathbb{Q}}\Big(\nu\Big(\prod_{j\in\sigma(A)} b_j \cdot \prod_{j\in A} b_j^{-1}\Big), \nu(a_1)\Big) = 1.$$

Now we employ the assumption that a_1 is not a perfect power and get

$$\prod_{j\in\sigma(A)} b_j = a_1^{a(A)} \prod_{j\in A} b_j \quad \text{with } a(A) \in \mathbb{Z}.$$

The above 2^{l-1} equalities can be compactly rewritten as the equality

$$\prod_{j=1}^{l} (1 - \bar{b}_j) = 0$$

in the group ring $\mathbb{Z}[\mathbb{Q}^+/\langle a_1\rangle]$, where $\bar{b}_j$ denotes the image of $b_j \in \mathbb{Q}^+$ in the quotient group $\mathbb{Q}^+/\langle a_1\rangle$. Because a_1 is not a perfect power, the group $G = \mathbb{Q}^+/\langle a_1\rangle$ is free and, by Lemma 5,

$$\bar{b}_j = e \quad \text{in } Q^+/\langle a_1\rangle,$$

which gives $b_j = a_1^t$ with $t \in \mathbb{Z}$. □

Theorems 2 and 3 are immediate corollaries of Theorem 1.

https://doi.org/10.1017/S0004972717000843 Published online by Cambridge University Press

Theorem 2 can be considered as a variant of the so-called *quotient problem* (see, for example, [5, Theorem A] and also [3]): instead of assuming that $y_n/x_n \in \mathbb{Z}$ for infinitely many $n \in \mathbb{N}$, we require that $\mathrm{supp}(x_n) \subseteq \mathrm{supp}(y_n)$ (for each $n \in \mathbb{N}$) and obtain essentially the same conclusion that y_n/x_n assumes only integral values and is a linear recurrence sequence. It would be interesting to generalise Theorem 2 to any pair $(x_n), (y_n)$ of linear recurrence sequences or at least to dispense with the restriction that (x_n) should be reduced.

Theorem 3 can be compared with the following theorem of Barańczuk.

THEOREM 6 (Barańczuk [1, Corollary 1.4]). *Assume that $a_1, \dots, a_m$ are multiplicatively independent and also $b_1, \dots, b_l$ are multiplicatively independent. If, for each $n \in \mathbb{N}$, we have (3), then*

$$\{a_1, \dots, a_m\} = \{b_1, \dots, b_l\} \quad \textit{and} \quad x_n = y_n \quad \textit{or each } n.$$

In [1] a broader perspective is outlined, which applies also to our note.

References

[1] S. Barańczuk, 'On a generalization of the support problem of Erdös and its analogues for abelian varieties and K-theory', *J. Pure Appl. Algebra* **214** (2010), 380–384.

[2] G. Everest, A. van der Poorten, I. Shparlinski and T. Ward, *Recurrence Sequences*, Mathematical Surveys and Monographs, 104 (American Mathematical Society, Providence, RI, 2003).

[3] C. Sanna, 'Distribution of integral values for the ratio of two linear recurrences', *J. Number Theory* **180** (2017), 195–207.

[4] A. Schinzel and M. Skałba, 'On power residues', *Acta Arith.* **108** (2003), 77–94.

[5] U. Zannier, 'Diophantine equations with linear recurrences. An overview of some recent progress', *J. Théor. Nombres Bordeaux* **17**(1) (2005), 423–435.

M. SKAŁBA, Institute of Mathematics, University of Warsaw,
Banacha 2, 02-097 Warszawa, Poland
e-mail: skalba@mimuw.edu.pl

https://doi.org/10.1017/S0004972717000843 Published online by Cambridge University Press