THE MULTIPLICATIVE GROUP GENERATED BY THE LEHMER NUMBERS

Florian Luca
IMATE de la UNAM, Ap. Postal 61-3 (Xangari)
CP 58 089, Morelia, Michoacán, México
e-mail: fluca@matmor.unam.mx

Štefan Porubský
Institute of Computer Science, Academy of Sciences of the Czech Republic
Pod Vodárenskou věží 2, 192 07 Prague 8
e-mail: Stefan.Porubsky@cs.cas.cz
(Submitted December 2000)

1. INTRODUCTION

Let $(u_n)_{n\geq 0}$ be a sequence of positive integers. We denote by $G(u)$ the multiplicative subgroup of $\mathbf{Q}_+^*$ generated by all the members of $(u_n)_{n\geq 0}$. That is,

$$G(u) = \{u_{n_1}^{\alpha_1} \cdot u_{n_2}^{\alpha_2} \cdot \ldots \cdot u_{n_s}^{\alpha_s} | s \geq 0,\ 0 \leq n_1 < n_2 < \cdots < n_s, \text{and } \alpha_i \in \mathbf{Z}^* \text{ for } i = 1, 2, \ldots, s\}. \tag{1.1}$$

In some cases, the group $G(u)$ is very easy to understand. For example, if $(u_n)_{n\geq 0}$ is a geometrical progression of first term u_0 and ratio $r = u_1/u_0$, then

$$G(u) = \{u_0^{\alpha} r^{\beta} | \text{for some } \alpha,\ \beta \in \mathbf{Z}\}. \tag{1.2}$$

For a sequence $(u_n)_{n\geq 0}$ we also denote by

$$U = \{m \in \mathbf{N} | m = u_n \text{ for some } n \geq 0\}. \tag{1.3}$$

That is, U is the range of the sequence $(u_n)_{n\geq 0}$. In this paper, we look at the set $G(u) \cap \mathbf{N}$. Certainly, $U \subseteq G(u) \cap \mathbf{N} \subseteq \mathbf{N}$. It is easy to see that the extreme cases of the above inclusions can occur in some non-trivial instances. For example, if $u_n = n!$ for all $n \geq 0$, then $m = u_m/u_{m-1}$ for all $m \geq 1$, therefore $G(u) = \mathbf{N}$. However, if $(u_n)_{n\geq 0}$ is an arithmetical progression of first term 1 and difference $k > 1$, then $G(u) \cap \mathbf{N} = U$. Indeed, notice that $1 = u_0 \in U$, and that if we write some $m \in G(u) \cap \mathbf{N},\ m \neq 1$ as

$$m = \prod_{i=1}^{s} u_{n_i}^{\alpha_i}, \quad \text{for some } s \geq 1 \text{ and } \alpha_i \in \mathbf{Z}^* \text{ for } i = 1, 2, \ldots, s, \tag{1.4}$$

then we can rearrange equation (1.4) as

$$m \prod_{\substack{1\leq i\leq s \\ \alpha_i<0}} u_{n_i}^{-\alpha_i} = \prod_{\substack{1\leq i\leq s \\ \alpha_i>0}} u_{n_i}^{\alpha_i}. \tag{1.5}$$

We may now reduce equation (1.5) modulo k and get $m \equiv 1 \pmod{k}$, therefore $m \in U$. While both the group $G(u)$ and the semigroup $G(u) \cap \mathbf{N}$ are very easy to understand for the above mentioned sequences $(u_n)_{n\geq 0}$, not the same is true when $(u_n)_{n\geq 0}$ is a non-degenerate linearly recurrent sequence. In this note, we investigate the group $G(u)$ and the semigroup $G(u) \cap \mathbf{N}$ when $(u_n)_{n\geq 0}$ is a *Lehmer sequence*.

Recall that if L and M are two non-zero coprime integers with $L - 4M \neq 0$, then the n^{th} Lehmer number corresponding to the pair (L, M) and denoted by P_n is defined as

$$P_n = \begin{cases} \frac{\alpha^n - \beta^n}{\alpha - \beta} & \text{for } n \equiv 1 (\text{mod } 2), \\ \frac{\alpha^n - \beta^n}{\alpha^2 - \beta^2} & \text{otherwise,} \end{cases} \tag{1.6}$$

where α and β are the two roots of the *characteristic equation*

$$x^2 - \sqrt{L}x + M = 0. \tag{1.7}$$

To avoid degenerate cases, we assume that α/β is not a root of 1. In what follows, we denote by $u_n = |P_n|$ and by $G = G(u)$. Our main results say that though the set G is topologically dense in the set of non-negative real numbers, its asymptotic density in the set of positive integers is zero. Before stating it, we introduce one more notation.

For every positive real number x let $G(x) = G \cap \mathbf{N} \cap (0, x)$. For every finite set of prime numbers $\mathcal{P}$, let $G_{\mathcal{P}}$ be the subgroup of $\mathbf{Q}_+^*$ generated by G and $\mathcal{P}$. If x is a positive real number, we denote $G_{\mathcal{P}}(x) = G_{\mathcal{P}} \cap \mathbf{N} \cap (0, x)$.

We have the following results.

Theorem 1: *The set G is dense in the set of non-negative real numbers.*

Theorem 2: *For any positive number δ there exists a computable constant C depending on δ, $\mathcal{P}$, L and M such that*

$$\#G_{\mathcal{P}}(x) < \frac{x}{(\log x)^{\delta}} \tag{1.8}$$

holds for all $x > C$.

The above Theorem 2 has the following immediate consequence.

Corollary 1:

(i) *Both the group G and the factor group $\mathbf{Q}_+^*/G$ are infinitely generated.*

(ii) *There exist infinitely many prime numbers p which do not belong to G.*

(iii) *There exist infintely many n's such that $n!$ does not belong to G.*

Since the group G is a subgroup of $\mathbf{Q}_+^*$, we know that G contains no torsion elements. However, this is not necessarily the case for the factor group $\mathbf{Q}_+^*/G$. Let $\overline{G} = \mathbf{Q}_+^*/G$. Since $\overline{G}$ is abelian, it follows that $\overline{G}$ has a torsion part, let's call it $T(\overline{G})$, and

$$F(\overline{G}) := \frac{\overline{G}}{T(\overline{G})} \tag{1.9}$$

is torsion free. The following result is slightly stronger version of the above Corollary.

Proposition: *The group $F(\overline{G})$ contains a free subgroup of infinite rank.*

The following Corollary follows from the above Proposition and is a stronger version of Corollary 1 (ii).

Corollary 2: *There exist infinitely many prime numbers p such that $p^k \notin G$ for any positive integer k.*

3. THE PROOFS

The Proof of Theorem 1: It is proved in Lemma 2 of [3] that if p and q are two coprime integers with $1 < p < q$, then each non-negative real number is a limit-point of the set of all fractions of the form $p^m q^{-n}$, where m and n are positive integers. Since for all positive integers k and s we have $(u_k, u_s) = u_{(k,s)}$, the above result applied to positive integers $u_s/u_{(k,s)}$ and $u_k/u_{(k,s)}$ proves Theorem 1.

We now proceed to the proof of Theorem 2.

In what follows, we recall the definition of a *primitive prime divisor* of a term of a Lehmer sequence. It is well known that $u_n | u_m$ whenever $n|m$. A *primitive prime divisor* of u_m is defined to be a prime number $p|u_m$ such that $p \nmid u_n$ for any $n < m$. Moreover, an *intrinsic primitive prime divisor* of u_m is defined to be a primitive prime divisor p of u_m such that p does not divide the discriminant $\Delta = L - 4M$ of $(u_n)_{n\geq 0}$. In order not to complicate the terminology, in what follows we will refer to an intrinsic primitive prime divisor of u_m as simply a primitive divisor of u_m. By results of Ward [5] for the case in which $(u_n)_{n\geq 0}$ has positive discriminant, and Bilu, Hanrot and Voutier [1] for the general case, we know that u_m has a primitive divisor for all $m > 30$. It is also well known that any primitive divisor p of u_m satisifies $p \equiv \pm 1 \pmod{m}$.

For every finite set of prime numbers $\mathcal{P}$ we denote by

$$M_{\mathcal{P}} = \max(30, p+1 | p \in \mathcal{P}). \tag{2.1}$$

When $\mathcal{P}$ is empty, we simply set $M = M_{\emptyset} = 30$. From the above remarks, it follows that whenever $n > M_{\mathcal{P}}$, u_n has primitive divisors and none of them belongs to $\mathcal{P}$.

We begin by pointing out a large free subgroup of G.

Lemma 1:

(i) *Let G_1 be the subgroup of G generated by the set $\{u_n\}_{1\leq n\leq 30}$ and G_2 be the subgroup of G generated by the set $\{u_n\}_{n>30}$. Then, G_2 is free on the set of generators $\{u_n\}_{n>30}$ and G is the direct product of G_1 and G_2.*

(ii) *Let $G_{1,\mathcal{P}}$ be the subgroup of $G_{\mathcal{P}}$ generated by the set $\mathcal{P} \cup \{u_n\}_{n\leq M_{\mathcal{P}}}$ let $G_{2,\mathcal{P}}$ be the subgroup of $G_{\mathcal{P}}$ generated by the set $\{u_n\}_{n>M_{\mathcal{P}}}$. Then, $G_{2,\mathcal{P}}$ is free on the set of generators $\{u_n\}_{n>M_{\mathcal{P}}}$ and $G_{\mathcal{P}}$ is the direct product of $G_{1,\mathcal{P}}$ and $G_{2,\mathcal{P}}$.*

The Proof of Lemma 1: We prove only (i) as the proof of (ii) is entirely similar. It is clear that G is the product of G_1 and G_2. In order to prove that this product is direct and that G_2 is indeed free on the indicated set of generators, it suffices to show that if

$$\prod_{i=1}^{s} u_{n_i}^{\alpha_i} = 1, \qquad \text{for some } s \geq 1, \ \ \alpha_i \in \mathbf{Z}^* \text{ and } n_1 < n_2 < \cdots < n_s, \tag{2.2}$$

then $n_s \leq 30$. But this follows right away because u_n has a primitive divisor of $n > 30$.

Let $g \in G_{\mathcal{P}} \setminus G_{1,\mathcal{P}}$. By the definition of $G_{\mathcal{P}} \setminus G_{1,\mathcal{P}}$, it follows that one may write

$$g = \prod_{p \in \mathcal{P}} p^{\beta_p} \prod_{i=1}^{s} u_{n_i}^{\alpha_i}, \tag{2.3}$$

where $\beta_p \in \mathbf{Z}$ for all $p \in \mathcal{P}$, $s \geq 1, \alpha_i \in \mathbf{Z}^*$ for $i = 1, 2, \ldots, s$ and $n_1 < n_2 < \cdots < n_s$ with $n_s > M_{\mathcal{P}}$. Of course, the above representation (2.3) for g need not be unique. However, by Lemma 1 above, we get that both the index n_s and the exponent α_s of u_{n_s} do not depend on the representation of g of the form (2.3). Thus, we may define two functions $f, h : G_{\mathcal{P}} \setminus G_{1,\mathcal{P}} \to \mathbf{Z}$ by $f(g) = n_s$ and $h(g) = \alpha_s$. We also extend the function f to the whole $G_{\mathcal{P}}$ by simply setting $f(g) = M_{\mathcal{P}}$ when $g \in G_{1,\mathcal{P}}$.

The following observation is relevant in what follows.

Lemma 2: *Assume that $g \in G_{\mathcal{P}} \setminus G_{1,\mathcal{P}}$. If $g \in \mathbf{N}$, then $h(g) > 0$.*

The Proof of Lemma 2: This is almost obvious. Indeed, assume that g is given by formula (2.3) and that $\alpha_s < 0$. Since $n_s > M_{\mathcal{P}}$, it follows that u_{n_s} has primitive divisors. Pick a primitive divisor q of u_{n_s}. By the remarks preceeding Lemma 1, we know that $q \notin \mathcal{P}$. Since $g \in \mathbf{N}$ and $\alpha_s < 0$, formula (2.3) implies that

$$q \Big| \prod_{p \in \mathcal{P}} p \prod_{1 \leq j < n_s} u_j, \tag{2.4}$$

which is obviously impossible.

The Proof of Theorem 2: We assume that $|\alpha| \geq |\beta|$. Notice that $|\alpha| > 1$. For any $n > 30$, we denote by $Pr(n)$ the primitive part of u_n. That is, $Pr(n)$ is the product of all the primitive prime divisors of u_n at the powers at which they appear in the prime factor decomposition of u_n. It is well known (see [4]), that if we denote by ζ_i all the primitive roots of unity of order n for $i = 1, 2, \ldots, \phi(n)$, then

$$Pr(n) = \frac{|\Phi_n(\alpha, \beta)|}{q(n)}, \tag{2.5}$$

where

$$\Phi_n(X, Y) = \prod_{i=1}^{\phi(n)} (X - \zeta_i Y) \in \mathbf{Z}[X, Y]$$

is the homogenized version of the n^{th} cyclotomic polynomial and $q(n)$ is either 1 or the largest prime factor of n. We also denote by $Pr_{\mathcal{P}}(n)$ the primitive part of u_n which is coprime to all the prime numbers $p \in \mathcal{P}$. By using linear forms in logarithms, both complex and p-adic

with respect to the primes $p \in \mathcal{P}$ (see [4]), it follows easily that there exist two effectively computable constants c_1 and c_2 depending on L, M and $\mathcal{P}$ such that

$$Pr_{\mathcal{P}}(n) > |\alpha|^{\phi(n)-c_1 d(n)\log n}, \quad \text{whenever } n > c_2, \tag{2.6}$$

where $d(n)$ is the number of divisors of n. Since $d(n) < n^{\epsilon}$ for every $\epsilon > 0$ provided that n is large enough (with respect to ϵ) and since

$$\phi(n) > \frac{c_3 n}{\log\log n}, \quad \text{whenever } n > c_4 \tag{2.7}$$

for some absolute constants c_3 and c_4, it follows that there exists a constant c_5 (depending on L, M and $\mathcal{P}$) such that

$$Pr_{\mathcal{P}}(n) > e^{\sqrt{n}}, \quad \text{whenever } n > c_5. \tag{2.8}$$

We may assume that $c_5 > 30$.

We now look at the elements $g \in G_{\mathcal{P}} \cap \mathbf{N}$. Let y be a very large positive real number ($y > 30$), and set

$$A(y) = \{g \in G_{\mathcal{P}} \cap \mathbf{N} | f(g) < y\}, \tag{2.9}$$

and

$$B(y) = \{g \in G_{\mathcal{P}} \cap \mathbf{N} | f(g) \geq y\}, \tag{2.10}$$

Certainly, $G_{\mathcal{P}} \cap \mathbf{N} = A(y) \cup B(y)$ holds for every y. For a real number x set $A(x,y) = A(y) \cap (0,x)$ and $B(x,y) = B(y) \cap (0,x)$. Thus, in order to bound the cardinality of $G_{\mathcal{P}}(x)$, it suffices to bound both the cardinality of $A(x,y)$ and $B(x,y)$.

We start by bounding the cardinality of $A(x,y)$. Assume that $q_1 < q_2 < \cdots < q_k$ are all the possible prime factors of an integer $g \in A(x,y)$. Then,

$$\prod_{i=1}^{k} q_i | \prod_{p \in \mathcal{P}} p \cdot \prod_{j \leq y} u_j. \tag{2.11}$$

Since $\mathcal{P}$ is fixed and since $u_n < (2|\alpha|)^n$ holds for all $n \geq 1$, it follows that there exists a constant c_6 (depending on L, M and $\mathcal{P}$) such that

$$\prod_{i=1}^{k} q_i < e^{c_6 y^2}. \tag{2.12}$$

From the Prime Number Theorem, we know that there exists an absolute constant $c_7 > 0$ such that

$$e^{c_7 k} < \prod_{i=1}^{k} q_i. \tag{2.13}$$

Hence,

$$k < c_8 y^2, \tag{2.14}$$

where $c_8 = c_6/c_7$. Assume now that $g \in A(x,y)$ has the prime factor decomposition

$$g = \prod_{i=1}^{k} q_i^{\mu_i}, \qquad \text{where } \mu_i \geq 0 \text{ for } i = 1, 2, \ldots, k. \tag{2.15}$$

Since $g \leq x$, it follows that

$$\mu_i \leq \frac{\log x}{\log q_i} \leq \frac{\log x}{\log 2} \qquad \text{for all } i = 1, 2, \ldots, k. \tag{2.16}$$

From inequalities (2.14) and (2.15), it follows that there exists a constant c_9 such that

$$\#A(x,y) < (\log x)^{c_9 y^2}, \qquad \text{for all } x \geq 3. \tag{2.17}$$

The above inequality (2.17) holds for all $y > 30$.

We now bound the cardinality of $B(x,y)$ for y large enough.

Assume that $y > M_{\mathcal{P}}$ and assume that $g \in B(x,y)$. From the definition of $B(x,y)$, it follows that $f(g) \geq y$. Moreover, from Lemma 2, it follows that $h(g) > 0$. By writing

$$g = \prod_{p \in \mathcal{P}} p^{\beta_p} \prod_{i=1}^{s} u_{n_i}^{\alpha_i}, \tag{2.18}$$

where $\beta_p \in \mathbf{Z}, s \geq 1, \alpha_i \in \mathbf{Z}^*$ for $i = 1, 2, \ldots, s$ and $n_1 < n_2 < \cdots < n_s$, with $n_s = f(g) > y$ and $\alpha_s = h(g) > 0$, we get that the positive integer g is a multiple of $Pr_{\mathcal{P}}(f(g))$. There are at most

$$\frac{x}{Pr_{\mathcal{P}}(f(g))}$$

positive integers less than x which are multiples of $Pr_{\mathcal{P}}(f(g))$. Hence, this argument shows that the cardinality of $B(x,y)$ is bounded above by

$$\#B(x,y) \leq \sum_{t \geq y} \frac{x}{Pr_{\mathcal{P}}(t)}. \tag{2.19}$$

We now assume that $y > c_5$ and use the lower bound (2.8) on $Pr_{\mathcal{P}}(t)$ for $t \geq y > c_5$ to infer that

$$\#B(x,y) \leq \sum_{t \geq y} \frac{x}{e^{\sqrt{t}}}. \tag{2.20}$$

By inequality (2.20), it follows that there exists an absolute constant c_{10} such that

$$\#B(x,y) < \frac{c_{10}\sqrt{y}}{e^{\sqrt{y}}} \cdot x. \tag{2.21}$$

Combining inequalities (2.17) and (2.21), we get that

$$G_{\mathcal{P}}(x) < (\log x)^{c_9 y^2} + \frac{c_{10}\sqrt{y}}{e^{\sqrt{y}}} \cdot x, \qquad \text{provided that } x \geq 3 \text{ and } y \geq c_5. \tag{2.22}$$

All it remains to show is that one may choose y (depending on x) such that

$$(\log x)^{c_9 y^2} + \frac{c_{10}\sqrt{y}}{e^{\sqrt{y}}} \cdot x < \frac{x}{(\log x)^{\delta}}. \tag{2.23}$$

To see how (2.23) holds, we choose any $\epsilon > 0$ small enough and set

$$y = (\log x)^{\frac{1}{2}-\epsilon}. \tag{2.24}$$

Clearly, $y \geq c_5$ when x is large enough. Moreover, the inequality

$$(\log x)^{c_9 y^2} < \frac{x}{2(\log x)^{\delta}} \tag{2.25}$$

is equivalent to

$$(c_9 y^2 + \delta) \log\log x < \log x - \log 2,$$

or

$$(c_9 (\log x)^{1-2\epsilon} + \delta) \log\log x < \log x - \log 2,$$

which certainly holds for x large enough. Finally, the inequality

$$\frac{c_{10}\sqrt{y}}{e^{\sqrt{y}}} \cdot x < \frac{x}{2(\log x)^{\delta}} \tag{2.26}$$

is equivalent to

$$\log 2c_{10} + \frac{1}{2}\log y + \delta \log\log x < \sqrt{y},$$

or

$$\log 2c_{10} + \left(\frac{1}{2}\left(\frac{1}{2} - \epsilon\right) + \delta\right) \log\log x < (\log x)^{\frac{1}{4} - \frac{\epsilon}{2}},$$

which is again satisfied for x large enough. Inequalities (2.25) and (2.26) imply inequality (2.23).

Theorem 2 is therefore proved.

The Proof of Corollary 1:

(i). The fact that G is infinitely generated follows from Lemma 1. Assume now that $\mathbf{Q}_+^*/G$ is finitely generated. It now follows that there exists a finite set of prime numbers, call it $\mathcal{P}$, such that $G_{\mathcal{P}} = \mathbf{Q}_+^*$. It now follows that $G_{\mathcal{P}} \cap \mathbf{N} = \mathbf{N}$, which contradicts the Theorem 2.

(ii). If there are only finitely many prime numbers p not belonging to G, then $\mathbf{Q}_+^*/G$ is finitely generated, which contradicts (i).

(iii). Assume that there exists $n_0 \in \mathbf{N}$ such that $n! \in G$ for all $n > n_0$. Since $n = n!/(n-1)! \in G$, whenever $n > n_0 + 1$, it follows that $\mathbf{Q}_+^*/G$ is finitely generated, which contradicts (i).

We now give the proof of the Proposition. This proof is based on the following Lemma due to Schinzel (see [2]).

Lemma 3: *There exists a strictly increasing sequence of integers $(m_i)_{i\geq 1}$ with $m_1 > 30$ such that u_{m_i}, has at least two primitive divisors.*

Using Lemma 3 above and the Axiom of Choice, it follows that one may select an infinite set of prime numbers $\mathcal{Q} = \{q_i\}_{i\geq 1}$ such that q_i is a primitive divisor of u_{m_i} for all $i \geq 1$. We introduce on $\mathcal{Q}$ the order relation induced by the natural ordering of the *orders of apparition* m_i's of the q_i's and denote this by $q_i \prec q_{i+1}$ for all $i \geq 1$. Based on Lemma 3 above, we infer the following auxiliary result.

Lemma 4: *With the above notations, let G_3 be the subgroup of $\mathbf{Q}_+^*$ generated by the set $\mathcal{Q}$. Then, $G \cap G_3 = \{1\}$.*

The Proof of Lemma 4: Assume that this is not so and let $g \in G \cap G_3 \setminus \{1\}$. It follows that

$$g = \prod_{i=1}^{s} u_{n_i}^{\alpha_i} = \prod_{j=1}^{t} q_{k_j}^{\beta_j}, \tag{2.27}$$

where $s \geq 1, t \geq 1, n_1 < n_2 < \cdots < n_s, k_1 < k_2 < \cdots < k_t$ and $\alpha_i, \beta_j \in \mathbf{Z}^*$ for $i = 1, 2, \ldots, s$ and $j = 1, 2, \ldots, t$. We first show that $n_s = m_{k_t}$. Indeed, since $q_{k_t} | \prod_{i=1}^{s} u_{n_i}$, and q_{k_t} is a primitive divisor of $u_{m_{k_t}}$, it follows that there exists some i with $1 \leq i \leq s$ such that $m_{k_t} | n_i$. In particular, $n_s \geq m_{k_t}$. Assume that $n_s > m_{k_t}$. Since $m_{k_t} \geq m_1 > 30$, it follows that u_{n_s} has a primitive divisor, call it q. Since q is a primitive divisor of u_{n_s} and $n_s > n_i$ for all $i < s$, it follows that $q = q_{k_j}$ for some $j \leq t$. But this impossible because q_{k_j} is a primitive divisor of $u_{m_{k_j}}$ and $m_{k_j} \leq m_{k_t} < n_s$. Thus, $n_s = m_{k_t}$. Now u_{n_s} has at least two primitive prime divisors. Pick a primitive prime divisor q of u_{n_s} different than q_{k_t}. Arguments similar to the preceeding ones show that $q \not| u_{n_i}$ for $i < s$ and $q \neq q_{k_j}$ for any $j \leq t$. This contradicts formula (2.27).

The Proof of the Proposition: The proof of the Proposition is contained in Lemma 3. Indeed, by Lemma 3, it follows easily that the factor group $\overline{G} = \mathbf{Q}_+^*/G$ contains the subgroup

$GG_3/G \cong G_3$. This subgroup is free on the basis $\{qG|q \in \mathcal{Q}\}$. Thus, this subgroup can be identified with a subgroup of $F(\overline{G})$ and therefore $F(\overline{G})$ has a free subgroup of infinite rank.

The Proof of Corollary 2: This follows from the Proposition. Indeed, assume that there exist only finitely many prime numbers, call them $p_1, p_2, \ldots, p_s$, such that whenever q is a prime number with $q \neq p_i$ for any $i = 1, 2, \ldots, s$, there exists $k > 0$ (depending on q) such that $q^k \in G$. Since $q^k \in G$ is equivalent to the fact that the coset qG has exponent k in the factor group $\overline{G} = \mathbf{Q}_+^*/G$, it follows that $qG \in T(\overline{G})$, whenever $q \neq p_i$ for $i = 1, 2, \ldots, s$. Hence, $F(\overline{G})$ is finitely generated, which contradicts the Proposition.

3. AN EXAMPLE

The well known Fibonacci sequence $(F_n)_{n\geq 0}$ is given by $F_0 = 0, F_1 = 1$ and $F_{n+2} = F_{n+1} + F_n$ for all $n \geq 0$. The set of its terms $U = \{F_n\}_{n\geq 0}$ coincides with the set of terms of the Lehmer sequence corresponding to the pair $(L, M) = (1, 1)$. For this sequence, the only n's for which F_n does not have a primitive divisor are $n = 1, 2, 5, 6, 12$. Since $F_1 = F_2 = 1, F_5 = 5, F_6 = F_3^3$ and $F_{12} = F_3^4 F_4^2$, it follows, by Lemma 1 from the previous section, that the group G for the Fibonacci sequence is free having the set $\{F_n\}_{n\neq 1,2,6,12}$ as basis. Since we know that $G \cap \mathbf{N}$ has density zero, it follows that G does not contain all the positive integers. An easy computation shows that the first positive integer in $\mathbf{N} \setminus G$ is 37.

For this sequence, one can point out a nice structure by means of a *trace map*. That is, let $g \in G \setminus \{1\}$ and write g as

$$g = \prod_{i=1}^{s} u_{n_i}^{\alpha_i}, \tag{3.1}$$

for some $s \geq 1$, where $\alpha_i \in \mathbf{Z}^*$ and $3 \leq n_1 < n_2 < \ldots n_s$ are such that $n_i \neq 6$ or 12 for any $i = 1, 2, \ldots, s$. From the above arguments, we know that every $g \in G \setminus \{1\}$ can be represented in this way and that such a representation is unique. Thus, we may define the trace of g as

$$I(g) = \sum_{i=1}^{s} \alpha_i n_i. \tag{3.2}$$

When $g = 1$, we simply set $I(1) = 0$. It is easy to see that $I : G \to \mathbf{Z}$ is a group homomorphism whose kernel is $G_0 = \{g \in G|I(g) = 0\}$. Moreover, $G/G_0 \cong \mathbf{Z}$. The subgroup G_0 of G has a topological interpretation in the sense that it contains elements which are arbitrarily close to the identity 1 of G.

4. COMMENTS AND PROBLEMS

While our Theorem 2 guarantees that the density of the set $G \cap \mathbf{N}$ is zero, it seems reasonable to conjecture that, in fact, a much better upper bound for cardinality of the set $G_{\mathcal{P}}(x)$ than the one asserted at (1.8) holds. Thus, we propose the following problem.

Problem 1: *Prove that for every $\epsilon > 0$, there exists a computable constant C depending only on $\epsilon, \mathcal{P}, L$ and M such that*

$$\#\{m \in G_{\mathcal{P}} \cap \mathbf{N}|m \leq x\} < x^{\epsilon}$$

holds for all $x > C$.

Assume that $m_1 < m_2 < \cdots < m_n < \ldots$ are all the elements of $G \cap \mathbf{N}$. Our result shows that for every k, there exists a computable constant C_k such that $m_n > n(\log n)^k$ holds for all $n > C_k$. In particular, the series

$$\sum_{k \geq 1} \frac{1}{m_k} \tag{4.1}$$

is convergent. It is certainly a very difficult problem to decide whether or not the number given by (4.1) is rational or irrational (or algebraic, respectively, transcendental).

Another interesting question to investigate would be the distribution of the positive integers $(m_i)_{i \geq 1}$. By Theorem 2, we know that the set of those integers has density zero. One may ask how fast does the sequence $(m_i)_{i \geq 1}$ grow. For example, if it were true that the sequence of differences $m_{i+1} - m_i$ diverges to infinity with i, then we would get an alternative proof for the fact that $G \cap \mathbf{N}$ has density zero. Unfortunately, such a statement need not be true in general. Indeed, let $(F_n)_{n \geq 0}$ be the Fibonacci sequence mentioned above and let $(L_n)_{n \geq 0}$ be its Lucas companion sequence. Then the identity

$$F_n^2 - F_{n+1}F_{n-1} = (-1)^{n+1}, \quad \text{for all } n = 0, 1, \ldots \tag{4.2}$$

provides infinitely many examples of positive integers i for which $m_{i+1} - m_i = 1$. Moreover, either one of the identities

$$L_n^2 - 5F_n^2 = 4 \cdot (-1)^n,$$

or

$$L_{2n} - L_n^2 = 2 \cdot (-1)^{n+1}$$

which hold for all $n = 0, 1, \ldots$, together with the fact that $L_n = F_{2n}/F_n \in G$ for all $n \geq 1$, provides infinitely many examples of positive integers i for which $m_{i+1} - m_i \leq 4$. In our Proposition, we pointed out that the group $F(\overline{G})$ contains a free subgroup of infinite rank but we said nothing about the subgroup $T(\overline{G})$. Concerning the subgroup $T(\overline{G})$, we propose the following conjecture.

Problem 2: *Prove that* $T(\overline{G})$ *is finite.*

Finally, it could be of interest to analyze the dependence of the group G of the starting Lehmer sequence $(P_n)_{n \geq 0}$. More precisely, assume that $(P_n)_{n \geq 0}$ and $(P'_n)_{n \geq 0}$ are two Lehmer sequences. Let $u_n = |P_n|$ and $u'_n = |P'_n|$ and define G, G' and U, U' as before. We offer the following conjecture.

Problem 3: *Prove that if* $G \cap G'$ *is infinitely generated, then* $U \cap U'$ *is infinite.*

It is well-known, and it follows from the theory of linear forms in logarithms, that if $U \cap U'$ is infinite, then there exist two arithmetical progressions $(an + b)_{n \geq 0}$ and $(cn + d)_{n \geq 0}$ with $ab \neq 0$ such that $|P_{an+b} = |P'_{cn+d}|$ holds for all $n \geq 0$. Thus, Problem 3 above is just a generalization of this well known result from diophantine equations.

ACKNOWLEDGMENTS

This work was done while the first author visited the Mathematics Department of the University of Bielefeld. He would like to thank Andreas Dress and the entire Mathematics Department there for their hospitality during the period when this work was done as well as

the Alexander von Humboldt Foundation for support. The second author was supported by the research project CEZ: J19/98:223400007.

REFERENCES

[1] Y. Bilu, G. Hanrot and P.M. Voutier. "Existence of primitive Divisors of Lucas and Lehmer Numbers. With an appendix by M. Mignotte." *J. Reine Angew. Math.* **539** (2001): 75-122.

[2] A. Schinzel. "On Primitive Prime Divisors of Lehmer Numbers I." *Acta Arith.* **8** (1963): 213-223; II, *Acta Arith.* **8** (1963): 251-257, III *Acta Arith.* **15** (1968): 49-70.

[3] J. Smítal. "Remarks on Ratio Sets of Set of Natural Numbers." *Acta Fac. Rerum Natur. Univ. Comenianae* **25** (1971): 93-99.

[4] C.L. Stewart. "Primitive Divisors of Lucas and Lehmer Numbers." *Transcendence Theory: Advances and Applications* 79-92. Eds. A. Baker, D.W. Masser, Academic Press, 1977.

[5] M. Ward. "The Intrinsic Divisors of Lehmer Numbers." *Ann. of Math.* **62** (1955): 230-236.

AMS Classification Numbers: 11B05, 11B39, 11D85

✠ ✠ ✠