PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 127, Number 7, Pages 1951–1956
S 0002-9939(99)04742-5
Article electronically published on February 18, 1999

A GENERALIZATION OF FURSTENBERG'S DIOPHANTINE THEOREM

BRYNA KRA

(Communicated by Mary Rees)

ABSTRACT. We obtain a generalization of Furstenberg's Diophantine Theorem on non-lacunary multiplicative semigroups. For example we show that the sets of sums $\{(p_1^n q_1^m + p_2^n q_2^m)\alpha : n, m \in \mathbb{N}\}$ and $\{(p_1^n q_1^m + 2^n)\alpha : n, m \in \mathbb{N}\}$ are dense in the circle $\mathbb{T} = \mathbb{R}/\mathbb{Z}$ for all irrational α, where (p_i, q_i) are distinct pairs of multiplicatively independent integers for $i = 1, 2$.

1. INTRODUCTION

A basic question in Diophantine approximation is which subsets of the natural numbers $\mathbb{N}$ are allowable denominators. More specifically, for which $\Delta \subset \mathbb{N}$, given irrational α and $\epsilon > 0$, can we find $n \in \Delta$ and $m \in \mathbb{Z}$ so that

$$|\alpha - m/n| < \epsilon/n?$$

A sufficient condition that Δ be a set of denominators is that $\{n\alpha \,(\mathrm{mod}\ 1) : n \in \Delta\}$ be dense in the circle $\mathbb{T} = \mathbb{R}/\mathbb{Z}$ for all irrational α.

The most basic such result is that $\{n\alpha : n \in \mathbb{N}\}$ is dense (even uniformly distributed) in $\mathbb{T}$ for all irrational α. We assume throughout that all expressions are considered on the circle (i.e. modulo 1) and omit explicit reference to this. A Theorem of G. H. Hardy and J. E. Littlewood's [6] generalized this result, showing that for any positive integer k, $\{n^k\alpha : n \in \mathbb{N}\}$ is dense in $\mathbb{T}$ for all irrational α. H. Furstenberg [5] generalized this to pairs of multiplicatively independent integers. Positive integers p and q are said to be *multiplicatively independent* if they are not both integer powers of the same integer.

Theorem 1.1 (Furstenberg)**.** *If $p, q > 1$ are multiplicatively independent integers, then $\{p^n q^m \alpha : n, m \in \mathbb{N}\}$ is dense in $\mathbb{T}$ for all irrational α.*

Given a positive integer p, a subset $A \subset \mathbb{T}$ is said to be *p-invariant* if $pa \in A$ for all $a \in A$. An equivalent formulation of Theorem 1.1 needed below is that any closed, infinite subset of $\mathbb{T}$ that is both p and q-invariant must be all of $\mathbb{T}$. More generally, a closed subset of $\mathbb{T}$ that is both p and q-invariant is either a finite set of (necessarily) rational points or is all of $\mathbb{T}$.

More recently, M. Boshernitzan [4] offered an elementary and elegant proof of this result, and we make use of some of these ideas in the proof of our main theorem.

Received by the editors March 19, 1997 and, in revised form, October 2, 1997.
1991 *Mathematics Subject Classification.* Primary 11J71, 54H20.
Key words and phrases. Topological dynamics, distribution modulo 1.

D. Berend [1], [2] generalized Theorem 1.1 to the torus and provided many other examples of denominators, based on multiplicative properties of the sequence of natural numbers. The main result of this paper is a generalization of Theorem 1.1 in an additive sense. We show:

Theorem 1.2. *Let $k \in \mathbb{N}$. Let $p_i, q_i \in \mathbb{N}$ with $1 < p_i < q_i$ for $i = 1, \dots, k$ and assume that $p_1 \leq p_2 \leq \dots \leq p_k$. Assume that the pairs p_i, q_i are multiplicatively independent for $i = 1, \dots, k$. Then for distinct $\alpha_1, \dots, \alpha_k \in \mathbb{T}$ with at least one $\alpha_i \notin \mathbb{Q}$,*

$$\left\{ \sum_{i=1}^{k} p_i^n q_i^m \alpha_i : n, m \in \mathbb{N} \right\}$$

is dense in $\mathbb{T}$.

The assumptions that the p_i are non-decreasing and that $p_i < q_i$ only clarify the expressions we are summing, as arbitrary expressions can be reordered. In terms of Diophantine approximation, the main interest is when all of the α_i are equal, as then the set of sums forms a set of denominators.

More recently, D. Meiri [7] gave an alternate proof of portions of Theorem 1.2, using measure theoretic methods.

We start with some simpler sequences of integers that give dense expressions on the circle.

2. Summands involving one of the indices

First we show that we can add expressions solely dependent on one of the indices to expressions of the form in Theorem 1.1. The lemma has appeared in other forms previously (see [3]). This proof is joint with E. Glasner.

Lemma 2.1. *Let $\epsilon > 0$ and $p, q > 1$ be multiplicatively independent integers. Let A be an infinite p-invariant subset of $\mathbb{T}$. Then there exists $n \in \mathbb{N}$ such that $q^n A$ is ϵ-dense.*

Proof. Without loss, we can replace A by its closure. We consider all limits taken in the set of all subsets of $\mathbb{T}$, endowed with the Hausdorff metric. Let

$$\mathcal{A} = \overline{\{q^n A : n \in \mathbb{N}\}}.$$

Since A is p-invariant, so is each $X \in \mathcal{A}$. Let $B = \bigcup_{X \in \mathcal{A}} X$. Then B is infinite, since it contains A and is closed in $\mathbb{T}$, since $\mathcal{A}$ is closed in the Hausdorff topology. Furthermore, B is both p and q-invariant. By the second formulation of Theorem 1.1, $B = \mathbb{T}$. In particular there exists $\alpha \in B$ so that the closure $\overline{\{p^n \alpha : n \in \mathbb{N}\}} = \mathbb{T}$. By definition, $\alpha \in X$ for some $X = \lim q^{n_i} A$, where the limit is taken along some sequence $\{n_i\}$. Since X is p-invariant, $X \supseteq \overline{\{p^n \alpha : n \in \mathbb{N}\}}$, and so $X = \mathbb{T}$. Thus along the sequence n_i, $q^{n_i} A$ is ϵ-dense for sufficiently large n_i. □

Corollary 2.2. *Let $p, q > 1$ be multiplicatively independent integers and let r_m be any sequence of real numbers. Then for any irrational α*

$$\{p^n q^m \alpha + r_m : n, m \in \mathbb{N}\}$$

is dense in $\mathbb{T}$.

Proof. Fix $\epsilon > 0$. Let $A = \{p^n\alpha : n \in \mathbb{N}\}$. By Lemma 2.1, there exists m so that $q^m A$ is ϵ-dense. Since $q^m A + r_m$ is a translate of an ϵ-dense set, it is also ϵ-dense. □

As an immediate corollary, we have that expressions such as

$$\{p^n q^m \alpha + 2^n \beta : n, m \in \mathbb{N}\}$$

and

$$\{p^n q^m \alpha + n^2 \beta : n, m \in \mathbb{N}\}$$

are dense in the circle, so long as $p, q > 1$ are multiplicatively independent integers and α is irrational.

Corollary 2.3. *Let $k \in \mathbb{N}$. Let $p_i, q_i > 1$ be pairs of multiplicatively independent integers for $i = 1, \dots, k$. Let $\alpha \notin \mathbb{Q}$ and $\beta_2, \dots, \beta_k \in \mathbb{Q}$ for $i = 2, \dots, n$. Then the set*

$$\left\{ p_1^n q_1^m \alpha + \sum_{i=2}^{k} p_i^n q_i^m \beta_i : n, m \in \mathbb{N} \right\}$$

is dense in $\mathbb{T}$.

Proof. Since $\beta_i \in \mathbb{Q}$, we can choose $l_2, \dots, l_k \in \mathbb{N}$ so that $p_i^{l_i}\beta_i \equiv \beta_i \pmod 1$ (or $p_i^{l_i}\beta_i \equiv 0 \pmod 1$) for $i = 2, \dots, k$. Then

$$\left\{ (p_1^{l_2 \cdot \ldots \cdot l_k})^n q_1^m \alpha + \sum_{i=2}^{k} (p_i^{l_2 \cdot \ldots \cdot l_k})^n q_i^m \beta_i : n, m \in \mathbb{N} \right\}$$

is a subset of the original sum and by choice of the l_i,

$$(p_i^{l_2 \cdot \ldots \cdot l_k})^n q_i^m \beta_i \equiv q_i^m \beta_i \pmod 1$$

for each i (or is 0). Letting $A = \{(p_1^{l_2 \cdot \ldots \cdot l_k})^n \alpha : n \in \mathbb{N}\}$ we can find $m \in \mathbb{N}$ by Lemma 2.1 so that $\{(p_1^{l_2 \cdot \ldots \cdot l_k})^n q_1^m \alpha : n, m \in \mathbb{N}\}$ is dense. The set considered in the statement of the corollary contains a translate of this one. □

3. Proof of the main theorem

We prove the main theorem via a series of lemmas. Throughout this section, we assume that $p_i, q_i > 1$ are pairs of multiplicatively independent integers.

We consider the actions of $M_1 = \begin{pmatrix} p_1 & 0 \\ 0 & p_2 \end{pmatrix}$ and $M_2 = \begin{pmatrix} q_1 & 0 \\ 0 & q_2 \end{pmatrix}$ on the 2-torus $\mathbb{T}^2$. A subset $A \subset \mathbb{T}^2$ is said to be invariant under the action of M if $MA \subset A$.

Given $A \subset \mathbb{T}^2$ and $x \in \mathbb{T}$, let

$$A_x = \{t \in \mathbb{T} : (t, x) \in A\}.$$

Lemma 3.1. *Let A be a non-empty, closed subset of $\mathbb{T}^2$, invariant under the actions of M_1 and M_2. Then $P = \{x \in \mathbb{T} : A_x \neq \emptyset\}$ is either $\mathbb{T}$ itself or is a finite set of rational points. Furthermore, if $r \in \mathbb{Q}$ and the denominator of r is relatively prime to p and q, then A_r is either empty, a finite set of rational points, or is $\mathbb{T}$ itself.*

Proof. Since A is non-empty, so is P. Since A is invariant under the actions of M_1 and M_2, P is invariant under multiplication by p_2 and q_2. By Theorem 1.1, P is either a finite set of (necessarily) rational points or is all of $\mathbb{T}$.

Given $r \in \mathbb{Q}$, assume that $A_r \neq \emptyset$. Since r is rational, we can find $u \in \mathbb{N}$ so that

$$p_2^u r \equiv q_2^u r \equiv r \pmod 1.$$

Then A_r is p_2^u- and q_2^u-invariant and non-empty. By Theorem 1.1, A_r is either a finite set of rationals or all of $\mathbb{T}$. □

Corollary 3.2. *Let $A \subset \mathbb{T}^2$ be non-empty, closed and invariant under the actions of M_1 and M_2. If all points of $A \cap \mathbb{Q}^2$ are isolated in A, then A is finite.*

Proof. Consider $A \backslash \mathbb{Q}^2$, the set A with all rational points removed. If this is empty, we are done. Otherwise $A \backslash \mathbb{Q}^2$ is a non-empty, closed subset of $\mathbb{T}^2$ that is invariant under the actions of M_1 and M_2 and so satisfies the conditions of Lemma 3.1. It follows immediately from Lemma 3.1 that any set satisfying the hypotheses must contain a point in $\mathbb{Q}^2$, a contradiction. Thus A is a closed collection of isolated points in a compact space, and so A is finite. □

Lemma 3.3. *Let A be a closed subset of $\mathbb{T}^2$, invariant under M_1 and M_2. Suppose that $(r, s) \in A \cap \mathbb{Q}^2$. Then there exist $n, m \in \mathbb{N}$ so that $A - (r, s)$ is invariant under M_1^n and M_2^m.*

By definition, $A - (r, s) = \{(x - r, y - s) : (x, y) \in A\}$.

Proof. Without loss, assume that the denominators of r and s are relatively prime to p_1, q_1 and p_2, q_2, respectively, by multiplying by M_1 and M_2. Since $s, r \in \mathbb{Q}$, we can pick $n, m \in \mathbb{N}$ so that

$$p_1^n r \equiv q_1^m r \equiv r \pmod 1$$

and

$$p_2^n s \equiv q_2^m s \equiv s \pmod 1.$$

Then (r, s) is fixed under the actions of M_1^n and M_2^m. Since A is invariant under the actions of M_1^n and M_2^m, $A - (r, s)$ is also invariant under M_1^n and M_2^m. □

For the remainder of this section we define

$$X = \left\{ (p_1^n q_1^m \alpha_1, p_2^n q_2^m \alpha_2) \in \mathbb{T}^2 : n, m \in \mathbb{N} \right\},$$

where each coordinate of the vectors is considered modulo 1. Let S be the set of accumulation points of X. Thus both X and S are invariant under the actions of M_1 and M_2, and S is closed.

Finally, let $\rho_1 = \log p_2 / \log p_1$ and $\rho_2 = \log q_2 / \log q_1$.

Lemma 3.4. *Assume S and X are defined as above. If $(0, 0) \in S$ then one of the following holds:*

(1) $(0, 0)$ is isolated in S.
(2) S contains the whole x-axis or the whole y-axis.
(3) For some $c > 0$, S contains the curve $y = cx^\rho$, for $x > 0$, where $\rho = \rho_1 = \rho_2$.

Proof. Assume that $(0, 0)$ is not isolated in S. There is a sequence $(x_i, y_i) \to (0, 0)$ with $(x_i, y_i) \in S$. Apply M_1 and M_2 repeatedly to the sequence $\{(x_i, y_i)\}$. Both M_1 and M_2 expand sufficiently small neighborhoods of the origin, and so in the limit we obtain a sequence of points in S_0 invariant under both M_1 and M_2. Call the limiting sequence $A = \{(z_i, w_i)\}$. Since each iterate of the original sequence has the origin as an accumulation point, A also has the origin as an accumulation point.

M_1 leaves curves of the form $y = cx^\rho$, where c is a constant, invariant. Thus if $\rho_1 \neq \rho_2$, the only curves left invariant under the actions of both M_1 and M_2 are the x-axis and the y-axis. So for $\rho_1 \neq \rho_2$, A contains an infinite set of points approaching the origin either on the x-axis or on the y-axis.

Let us assume that the approach to $(0,0)$ lies on the y-axis. (The proof for the approach to $(0,0)$ lying on the x-axis is identical.) Let T be the ordered semigroup generated by p_2 and q_2. Fixing $\epsilon > 0$, pick N large enough so that for all $i \geq N$, $t_{i+1}/t_i < 1 + \epsilon$. Choose $y \in S_0$ with $0 \neq |y| < \epsilon/t_N$. Then the finite subset of S

$$\{ty : t \in T, t_N \leq t \leq 1/|y|\}$$

is ϵ-dense on the y-axis, as can be seen by considering the differences $(t_{i+1} - t_i)y$. Since S is closed, it contains the entire y-axis.

Lastly, if $\rho = \rho_1 = \rho_2$, then A is contained in a curve of the form $y = cx^\rho$ for some constant c. Analogous to the situation when the approach to $(0,0)$ lies on one of the axes, we can pick a point within ϵ of $(0,0)$. By applying M_1 and M_2 to this point, we obtain an ϵ-dense set of points on the curve $y = cx^\rho$. As ϵ is arbitrary, the entire invariant curve $y = cx^\rho$ for $x > 0$ contained in S. □

Corollary 3.5. *Under the same assumptions, either* $(0,0)$ *is isolated in* S *or* $\{x + y : (x,y) \in S\} = \mathbb{T}$.

Proof. If $(0,0)$ is not isolated in S, Lemma 3.4 shows that the sum obtained either contains a translate of an axis or contains all points from a continuous curve. In either case, the sum is all of $\mathbb{T}$. □

We combine these lemmas to prove Theorem 1.2.

Proof. (*Theorem 1.2*) Let $k = 2$. Assume that $\alpha_1 \notin \mathbb{Q}$. (The case that $\alpha_2 \notin \mathbb{Q}$ is analogous.) Theorem 1.1 shows that for any $x \in \mathbb{T}$ there exist sequences $n_i, m_i \to \infty$ so that $p_1^{n_i} q_1^{m_i} \alpha_1 \to x$. By compactness, there exists $y \in \mathbb{T}$ so that $(x,y) \in S$. In particular, S is infinite.

By Corollary 3.2, there is a non-isolated rational point of S. By Lemma 3.3, we can assume that this point is $(0,0)$. By Corollary 3.5, $\{x + y : (x,y) \in S\} = \mathbb{T}$.

Assume that we have proved the result for a sum of $k-1$ terms. Let

$$X = \{(p_1^n q_1^m \alpha_1, p_2^n q_2^m \alpha_2, \ldots, p_k^n q_k^m \alpha_k) : n, m \in \mathbb{N}\}$$

and let S be the accumulation points of this set. Without loss of generality assume that $\alpha_1 \notin \mathbb{Q}$. By the proof for $k = 2$ we have $(x, y, x_3, \ldots, x_k) \in S$ where x is a fixed point, y is any point in $\mathbb{T}$ and $x_3, \ldots, x_k$ depend on y. In the proof we showed that S contained an invariant curve, including the two axes as invariant curves. Defining $S_x = S - (x, 0, \ldots, 0)$ we have $(0, y, x_3, \ldots, x_k) \in S_x$ where y is an arbitrary point in $\mathbb{T}$ and $x_3, \ldots, x_k$ depend on the choice of y. Taking some $y \notin \mathbb{Q}$, the result for $k-1$ gives a dense set of sums. The set of sums obtained from elements of S is a translate of this one, and so is dense. □

Acknowledgments

I thank J. Cummings and H. Furstenberg for helpful discussions. I also thank the referee for suggestions on the organization of the paper.

References

[1] D. Berend. Multi invariant set on tori. *Trans. Amer. Math. Soc.*, 280:509–532, 1983. MR **85b:**11064

[2] D. Berend. Actions of sets of integers on irrationals. *Acta. Arith.*, 48:175–306, 1987. MR **89a:**11077

[3] D. Berend and M. D. Boshernitzan. Numbers with complicated decimal expansions. *Acta Math. Hungar.*, 66(1-2):113–126, 1995. MR **95m:**11073

[4] M.D. Boshernitzan. Elementary proof of Furstenberg's diophantine result. *Proc. Amer. Math. Soc.*, 122(1):67–70, 1994. MR **94k:**11085

[5] H. Furstenberg. Disjointness in ergodic theory, minimal sets, and a problem in diophantine approximation. *Math. Systems Theory*, 1:1–49, 1967. MR **35:**4369

[6] G.H. Hardy and J.E. Littlewood. The fractional part of $n^k\theta$. *Acta. Math.*, 37:155–191, 1914.

[7] D. Meiri. Entropy and uniform distribution of orbits in T^d. *to appear, Isr. J. Math.*, 1998.

Department of Mathematics, University of Michigan, East Hall, 525 East University Avenue, Ann Arbor, Michigan 49108-1109

E-mail address: bryna@math.lsa.umich.edu

Current address: IHES, 35, route de Chartres, 91440 Bures-sur-Yvette, France

E-mail address: kra@ihes.fr