ISRAEL JOURNAL OF MATHEMATICS, Vol. 61, No. 2, 1988

ON MEASURES SIMULTANEOUSLY 2- AND 3-INVARIANT

BY

RUSSELL LYONS†

Department of Mathematics, Stanford University, Stanford, CA 94305-2125, USA

ABSTRACT

Furstenberg has conjectured that the only continuous probability measure on the circle $\mathbf{T}=\mathbf{R}/\mathbf{Z}$ which is invariant under both $x\mapsto 2x$ and $x\mapsto 3x$ is Lebesgue measure. We shall show that under additional hypotheses, this is true. We also discuss related conjectures and theorems.

§1. Introduction

For any integer n, let $T_n : x\mapsto nx$ denote the indicated endomorphism of the circle group $\mathbf{T}=\mathbf{R}/\mathbf{Z}$. A set $E\subset\mathbf{T}$ is called *T_n-invariant* if $T_n(E)\subset E$. Furstenberg [2] showed that the only infinite closed set which is both T_2- and T_3-invariant is the whole circle. Indeed, more generally, call $S\subset\mathbf{Z}$ a *nonlacunary semigroup* if S is a multiplicative semigroup whose positive elements are not contained in any singly-generated semigroup — for example, $S=\{2^m3^n : m,n\geqq 0\}$. A set is *$S$-invariant* if it is T_n-invariant for all $n\in S$. Furstenberg showed that whenever S is a nonlacunary semigroup, the only infinite closed set which is S-invariant is the whole circle. Now two nonzero integers are called *multiplicatively independent* if they generate a nonlacunary semigroup, i.e., if their absolute values are not both powers of the same integer. Furstenberg has made the following conjecture, which is clearly stronger than the above theorem.

Let p and q be multiplicatively independent. If E is any infinite

(C1) *closed T_p-invariant set, then $T_q^nE\to\mathbf{T}$ in the Hausdorff metric.*

† Research partially supported by fellowships from the American Mathematical Society and the National Science Foundation.

Received March 25, 1987

Note that Furstenberg's theorem on S-invariant sets is equivalent to an assertion about measures. Indeed, recall that a Borel probability measure μ is said to be T_n-*invariant* if $\mu = T_n\mu$, where $(T_n\mu)(E) = \mu(T_n^{-1}E)$ for all measurable E. Thus, Furstenberg's theorem states that every continuous S-invariant measure has full support (i.e., supp $\mu = \mathbf{T}$) if S is any nonlacunary semigroup. He has conjectured, in fact, that

(C2) *The only continuous S-invariant (probability) measure is Lebesgue measure, λ, if S is a nonlacunary semigroup.*

Similarly, (C1) is equivalent to the conjecture that if μ is T_p-invariant, then supp $T_q^n\mu \to \mathbf{T}$. Furstenberg has again made the stronger conjecture that

(C3) *If p and q are multiplicatively independent and μ is any continuous T_p-invariant measure, then $T_q^n\mu \to \lambda$ weak*.*

We may formulate similar conjectures which do not involve invariance: Let $M_c^1(\mathbf{T})$ denote the continuous probability measures.

(C4) *If $\mu \in M_c^1(\mathbf{T})$ and S is a nonlacunary semigroup, then $\exists\, n_k \in S$ tending to ∞ such that $\hat{\mu}(n_k) \to 0$.*

(C5) *If $\mu \in M_c^1(\mathbf{T})$ and S is a nonlacunary semigroup, then $\exists\, n_k \in S$ such that $T_{n_k}\mu \xrightarrow{w^*} \lambda$.*

Clearly (C5)$\Rightarrow$(C4)$\Rightarrow$(C2). In fact, (C4)$\Rightarrow$(C5) as follows. Given $\mu \in M_c^1(\mathbf{T})$, apply (C4) to the measure $\Sigma_{1 \le j \le k} T_j(\mu * \tilde{\mu})$ to obtain an $n_k \in S$ satisfying $|\hat{\mu}(jn_k)| < k^{-1}$ for $1 \le j \le k$, where $\tilde{\mu}(E) = \mu(-E)$. This sequence $\{n_k\}$ is then such that $T_{n_k}\mu \xrightarrow{w^*} \lambda$. Also, one is almost able to conclude that (C2)$\Rightarrow$(C5) by considering a weak* limit point, ν, of

$$\sum_{\substack{n \in S' \\ n \le N}} T_n(\mu * \tilde{\mu}) \Big/ \sum_{\substack{n \in S' \\ n \le N}} 1,$$

where S' is any nonlacunary subsemigroup of S generated by two positive integers. Then ν is S'-invariant, but, unfortunately, not necessarily continuous.

We note, in any case, that (C4) and (C5) are true when $S = \mathbf{Z}$. Here we shall establish special cases of conjectures (C1), (C2), and (C3).

We thank Bernard Host and François Parreau for useful discussions.

§2. Exact measures

Recall that a measure μ is called *T-exact* (or *K-mixing* for T) if

$$\forall g \in L^2(\mu) \quad \lim_{n\to\infty} \sup_{\substack{f\in L^2(\mu)\\ \|f\|_2\leqq 1}} |\langle T^n f, g\rangle - \langle f, 1\rangle\langle 1, g\rangle| = 0,$$

where $\langle f, g\rangle$ denotes $\int f\bar{g}\, d\mu$. Observe that $(T_n\mu)^\wedge(r) = \hat{\mu}(nr)$. Thus, if μ is T_p-exact, then

$$\forall b \in \mathbf{Z} \quad \lim_{n\to\infty} \sup_{a\in\mathbf{Z}} |\hat{\mu}(ap^n + b) - \hat{\mu}(a)\hat{\mu}(b)| = 0.$$

THEOREM 1. *Let $\mu \in M_c^1(\mathrm{T})$ be S-invariant, where S is a nonlacunary semigroup generated by relatively prime integers p, q. If μ is T_p-exact, then $\mu = \lambda$.*

We require two lemmas concerning elementary number theory.

LEMMA 2. *Let $p, q > 1$ be relatively prime. There exist A, d, L with $L \geqq 2$ and $(d, p) = 1$ such that*

$$q^A = dp^L + 1.$$

PROOF. Choose A_1 and d_0 so that $q^{A_1} = d_0p^2 + 1$ and write $d_0 = d_1p^l$ with $p \mid d_1$. If $(d_1, p) = 1$, we are done. Otherwise, choose p_1 so that $d_1p_1 = d_2'p$ with $(d_2', p) < (d_1, p)$. Put $A_2 = p_1A_1$, so that for some d', d_2,

$$\begin{aligned} q^{A_2} &= (d_1p^{2+l} + 1)^{p_1} = d'p^{4+2l} + d_2'p^{3+l} + 1 \\ &= d_2p^{3+l} + 1. \end{aligned}$$

Since $(d_2, p) = (d_2', p) < (d_1, p)$, we can repeat this process until, after a finite number of steps, we obtain the desired equation. ■

LEMMA 3. *Let $p, q > 1$ be relatively prime and let A be the smallest positive integer such that d and L exist satisfying Lemma 2. Then for all $l \geqq L$, the order of q modulo p^l is $p^{l-L}A$ and $q^x \equiv b \pmod{p^l}$ has a solution in x iff $q^x \equiv b$ $\pmod{p^L}$ does.*

PROOF. Let r_l denote the order of q modulo p^l. We have, by induction on $l \geqq L$, that

$$\text{(1)} \qquad q^{p^{l-L}A} = d_l\, p^l + 1, \qquad (d_l, p) = 1.$$

Hence $r_l \mid p^{l-L}A$. Furthermore, if $p^{l-L}A = r_ls_l$, let

$$q^{r_l} = d_l'\, p^l + 1.$$

Then

$$q^{r_l s_l} = d_l'' p^{2l} + s_l d_l' p^l + 1. \tag{2}$$

Comparison with (1) shows that $(d_l', p) = 1$. When $l = L$, this means that $r_L = A$ by choice of A. Thus, for $l > L$, we have $A = r_L \mid r_l$. But comparison of (2) and (1) also shows that $(s_l, p) = 1$, whence from $p^{l-L}A = r_l s_l$, it follows that $s_l = 1$. Thus $r_l = p^{l-L}A$ and the rest of the lemma follows easily. ∎

When p is prime, Lemma 3 is a familiar fact in p-adic number theory.

PROOF OF THEOREM 1. We may clearly assume that p and q are positive. By Lemma 3, there exists a sequence of integers $n_j \to \infty$ ($j \geqq L$) such that

$$q^{n_j} \equiv p^j + 1 \pmod{p^{2j}}.$$

Write

$$q^{n_j} = d_j p^{2j} + p^j + 1.$$

Then for all $m \in \mathbf{Z}$,

$$\begin{aligned}\hat{\mu}(m) &= \hat{\mu}(mq^{n_j}) = \hat{\mu}([md_j p^j + m]p^j + m) \\ &= \lim_{j\to\infty} \hat{\mu}(md_j p^j + m)\hat{\mu}(m) \\ &= \left[\lim_{j\to\infty} \hat{\mu}(md_j)\right]\hat{\mu}(m)^2.\end{aligned}$$

Therefore, if $\hat{\mu}(m) \neq 0$, we obtain

$$1 = \hat{\mu}(m) \lim_{j\to\infty} \hat{\mu}(md_j).$$

But $|\hat{\mu}| \leqq 1$, whence $|\hat{\mu}(m)| = 1$. If $m \neq 0$, this implies that μ is discrete. Thus $\hat{\mu}(m) = 0$ for all $m \neq 0$ and $\mu = \lambda$. ∎

Under similar hypotheses, we can prove a weak version of Conjecture (C3).

THEOREM 4. *Let $p, q > 1$ be relatively prime integers and let $\mu \in M_c^1(\mathbf{T})$ be T_p-exact. Then there exist $n_j \to \infty$ ($j \geqq L$) such that $T_q^{n_j}\mu \xrightarrow{w^*} \lambda$.*

PROOF. Choose $n_j \to \infty$ ($j \geqq L$) such that

$$q^{n_j} \equiv p^{j(j-1)} + p^{j(j-2)} + \cdots + p^j + 1 \pmod{p^{j^2}}.$$

Then with appropriate d_j, we have for all $m \in \mathbf{Z}$,

$$\begin{aligned}\lim_{j\to\infty} \hat{\mu}(mq^{n_j}) &= \lim_{j\to\infty} \hat{\mu}(md_j p^{j^2} + mp^{j(j-1)} + \cdots + mp^j + m) \\ &= \hat{\mu}(m) \lim_{j\to\infty} \hat{\mu}(md_j p^{j(j-1)} + mp^{j(j-2)} + \cdots + m)\end{aligned}$$

$$= \hat{\mu}(m)^2 \lim_{j\to\infty} \hat{\mu}(md_j p^{j(j-2)} + mp^{j(j-3)} + \cdots + m)$$

$$= \cdots.$$

Therefore $\lim_{j\to\infty} |\hat{\mu}(mq^{n_j})| \leq |\hat{\mu}(m)|^l$ for any given l. Since $|\hat{\mu}(m)| < 1$ for $m \neq 0$, it follows that $\lim_{j\to\infty} \hat{\mu}(mq^{n_j}) = 0$ for $m \neq 0$. In other words, $T_q^{n_j}\mu \xrightarrow{w^*} \lambda$. ■

For many specific measures, such as infinite convolutions and Riesz products, we may obtain the full conclusion of (C3). Let $e(x)$ denote $e^{2\pi i x}$.

THEOREM 5. *Let p, q be multiplicatively independent and let $\nu \in M_c^1(\mathbf{T})$ be T_p-invariant and T_p-exact. Suppose that if $\{e(m_j x)\}_{j\geq 1}$ is any sequence not converging to zero weak* in $L^\infty(\nu)$, then there is a subsequence $\{m_j'\}$ of $\{m_j\}$ and integers b, a_j, n_j such that $n_j \to \infty$ and $m_j' = a_j p^{n_j} + b$. Then $T_q^n \mu \xrightarrow{w^*} \lambda$ for any probability measure μ absolutely continuous with respect to a measure of the form $\delta(t) * T_r \nu$ ($t \in \mathbf{T}$, $r \in \mathbf{Z}^*$).*

See Lyons [3] for a discussion of measures satisfying these hypotheses. As a consequence, for example, if E is any subset of the Cantor middle-thirds set having positive Cantor–Lebesgue measure, then $T_2^n E \to \mathbf{T}$.

PROOF. Let $\{n_j\}$ be any sequence such that for every $r \in \mathbf{Z}$, $\{e(-rq^{n_j}x)\}_{j\geq 1}$ has a weak* limit in $L^\infty(\mu)$, call it $\hat{\sigma}_x(r)$. It was shown in Lyons [3] that $\sigma_x = \lambda$ μ-a.e. unless a subsequence $\{n_j'\}$ of $\{n_j\}$ exists with $q^{n_j'}$ of the form

$$q^{n_j'} = \sum_{k=1}^{K} a_k p^{\alpha_k^{(j)}},$$

where K and $a_1, \ldots, a_K$ are fixed. But Senge and Straus [7] (see also Stewart [8]) have shown this to be impossible. Therefore $\sigma_x = \lambda$ μ-a.e. and thus $e(-rq^n x) \xrightarrow{w^*} 0$ in $L^\infty(\mu)$ for $r \neq 0$. Integration shows that $T_q^n \mu \xrightarrow{w^*} \lambda$. ■

It is interesting to note that if Conjecture (C3) is true, then we may obtain the number-theoretic fact used in the proof of Theorem 5 merely by applying Theorem 1 of Lyons [3] to the measure

$$\mu = \mathop{*}_{k\geq 1} [\tfrac{1}{3}\delta(0) + \tfrac{2}{3}\delta(p^{-k})].$$

This is quite surprising, in view of the fact that Senge and Straus used methods from transcendence theory.

Theorem 5 suggests an additional conjecture:

If S is a nonlacunary semigroup and $\mu \in M_c^1(\mathbf{T})$, then there is a sequence $\{n_k\} \subset S$ such that for all $\nu \in M^1(\mathbf{T})$ with $\nu \ll \mu$, $T_n \nu \xrightarrow{w^*} \lambda$. Equivalently, given S and μ, there is $\{n_k\} \subset S$ such that for $r \neq 0$, $e(-rn_k x) \to 0$ weak in $L^\infty(\mu)$.* (C6)

Again, (C6) is known when $S = \mathbf{Z}$ (Lyons [4]).

A similar possibility was mentioned to us by Benjamin Weiss:

Let p and q be multiplicatively independent positive integers. If $\mu \in M_c^1(\mathbf{T})$ is T_p-invariant, then μ-a.e. x is normal in base q; i.e., for $r \neq 0$,

$$\lim_{K \to \infty} \frac{1}{K} \sum_{k=1}^{K} e(-rq^k x) = D \qquad \mu\text{-a.e.} \tag{C7}$$

This conjecture has been established for certain infinite convolution measures and Riesz products (Schmidt [6], Pearce and Keane [5], Brown, Moran and Pearce [1]).

References

1. Gavin Brown, William Moran and Charles E. M. Pearce, *Riesz products and normal numbers*, J. London Math. Soc. (2) **32** (1985), 12–18.

2. Harry Furstenberg, *Disjointness in ergodic theory, minimal sets, and a problem in diophantine approximation*, Math. Systems Theory **1** (1967), 1–49.

3. Russell Lyons, *Mixing and asymptotic distribution modulo* 1, Ergodic Theory Dynamical Systems (to appear).

4. Russell Lyons, *The local structure of some measure-algebra homomorphisms*, in preparation.

5. C. E. M. Pearce and M. S. Keane, *On normal numbers*, J. Austral. Math. Soc. (A) **32** (1982), 79–87.

6. Wolfgang Schmidt, *On normal numbers*, Pacific J. Math. **10** (1960), 661–672.

7. H. G. Senge and E. G. Straus, *PV-numbers and sets of multiplicity*, Per. Math. Hung. **3** (1–2) (1973), 93–100.

8. C. L. Stewart, *On the representation of an integer in two different bases*, J. Reine Angew. Math. **319** (1980), 63–72.