ACTA ARITHMETICA
LXII.1 (1992)
æ

On certain solutions of the diophantine equation $x - y = p(z)$

by

R. Nair (Liverpool)

Introduction. Given a subset S of $\mathbb{Z}$ and a sequence $I = (I_n)_{n=1}^{\infty}$ of intervals of $\mathbb{Z}$ strictly increasing in length, let

$$b(S, I) = \limsup_{|I_n| \to \infty} \frac{|S \cap I_n|}{|I_n|}$$

and let

$$b(S) = \sup_I b(S, I)\,,$$

where the supremum is taken over all possible sequences of intervals I. We say S has *positive Banach density* if $b(S) > 0$. Here and hence forth for a set B we allow $|B|$ to represent its cardinality. We say a subset A of $\mathbb{N}$ is *intersective* if for each subset S of $\mathbb{N}$ with $b(S)$ positive the set $A \cap (S - S)$ is non-empty. Here $S - S$ denotes the set $\{x - y : x, y \in S\}$. In Section 1 of this note we use ergodic theory to prove the following theorem.

Theorem 1. *Let ψ be a polynomial with integer coefficients and let*

$$P_\psi = \{\psi(p) : p \text{ a rational prime}\}\,.$$

Then a necessary and sufficient condition on ψ to ensure that P_ψ is intersective is that for each non-zero integer n, there exists another integer m_n, coprime to it, such that n divides $\psi(m_n)$.

Let

$$N_\psi = \{\psi(n) : n \text{ a positive integer}\}.$$

The fact that the set N_ψ is intersective for any polynomial ψ with $\psi(0) = 0$ and mapping the integers to themselves is proved by H. Furstenberg [4, p. 74], using ergodic theory. In the special case $\psi(x) = x^2$, this had been shown earlier by H. Furstenberg [3] and A. Sárközy [10] using ergodic theory and analytic number theory respectively. Later, in response to a question of P. Erdős, Sárközy [11] proved P_ψ is intersective in the special case $\psi(x) =$

$x-1$. His method in [11] is a more complicated version of the technique in [7]. This result of Sárközy'sand also Theorem 7 which follows are also obtained in the work of T. Kamae and M. Mendès France [6] though by still further different methods. It should be said Sárközy's methods are quantitative in that if S_N denotes $S \cap [1, N]$ lower bounds are found for $|A \cap (S_N - S_N)|$. Our proof of Theorem 1 is a variant of Furstenberg's approach.

Suppose M is a countable commutative monoid with binary operation indicated by the plus sign $+$. Suppose $\mathcal{A} = \{A_n\}_{n=1}^{\infty}$ is a collection of subsets of M and consider the following properties of $\mathcal{A}$:

(i) if $m < n$ then $A_m \subseteq A_n$;
(ii) $|A_n|$ is finite for each n and also tends to infinity as n does;
(iii) for each h in M

$$\lim_{n\to\infty} \frac{|A_n \triangle (A_n + h)|}{|A_n|} = 0\,,$$

where $\triangle$ denotes the symmetric difference and $A_n + h$ denotes the set $\{k + h : k \in A_n\}$; and

(iv) there exists $K > 0$ such that $|A_n A_n^{-1}| \le K|A_n|$ for each n, where $A_n A_n^{-1}$ denotes the set

$$\{k \in A_n : k + l \in A_n \text{ for some } l \text{ in } A_n\}\,.$$

We introduce two notions of density on M associated with $\mathcal{A}$. Given a subset E of M, for $\mathcal{A}$ satisfying conditions (i) and (ii) we say

$$d_{\mathcal{A}}^{*}(E) = \limsup_{n\to\infty} \frac{|E \cap A_n|}{|A_n|},$$

denotes its *upper density along* $\mathcal{A}$. If the above limit exists we say E has *density along* $\mathcal{A}$ denoted by $d_{\mathcal{A}}(E)$. We say a set E contained in M has *positive upper Banach density* on M if there exists a collection of subsets $\mathcal{A}$ of M satisfying (ii) and (iii) such that

$$b(E, \mathcal{A}) = \limsup_{n\to\infty} \frac{|E \cap A_n|}{|A_n|} > 0\,.$$

Let $b(E) = \sup_{\mathcal{A}} b(E, \mathcal{A})$ where the supremum is taken overall collections of subsets $\mathcal{A}$ satisfying (ii) and (iii). We refer to $b(E)$ as the *upper Banach density* of E *along* $\mathcal{A}$. In Section 2 we prove the following theorem:

THEOREM 2. *Suppose the subset E of M has positive Banach density $b(E)$. Then if $\mathcal{A}$ satisfies conditions* (i)–(iv) *there exists a subset R of M with $d_{\mathcal{A}}(R) \ge b(E)$ such that for each finite subset $\{n_1, \ldots, n_k\}$ of R we have*

$$b(E \cap (E + n_1) \cap \ldots \cap (E + n_k)) > 0\,.$$

The existence of $d_{\mathcal{A}}(E)$ is part of the statement of Theorem 2. In the special case where $M=\mathbb{Z}$ and $\mathcal{A}$ is given by $A_n=[1,n]\cap\mathbb{Z}$ $(n=1,2,\ldots)$ Theorem 2 was proved by V. Bergelson in [1]. His proof depends on G. Birkhoff's pointwise ergodic theorem. The extension to Theorem 2 is made possible by the generalisation of Birkhoff's theorem due to A. A. Tempel'man [7, p. 224]. Besides Bergelson's theorem, there are a variety of contexts to which Theorem 2 applies. We mention three.

(a) $M=\mathbb{Z}^m$ for some natural number m, with $\mathcal{A}$ given by $A_n=C_n\cap\mathbb{Z}^m$ $(n=1,2,\ldots)$ where C_n is a bounded convex subset of $\mathbb{R}^m$ tending to infinity in all directions as n does.

(b) $M=\mathbb{Z}$ with $\mathcal{A}$ given by $A_n=[1,n]\cap\mathbb{Z}\bigcup_{k=1}^{\infty}[d_k,e_k]$ $(n=1,2,\ldots)$, where $(d_k)_{k=1}^{\infty}$ and $(e_k)_{k=1}^{\infty}$ are strictly increasing sequences such that $d_{k-1}=O(e_k)$.

(c) $M=\mathbb{D}_2$ where $\mathbb{D}_2$ denotes the dyadic rationals in $[0,1)$ with addition modulo one and $\mathcal{A}$ given by

$$A_n=\left\{\frac{a_1}{2}+\ldots+\frac{a_n}{2^n}:a_i\in\{0,1\}\right\}\quad (n=1,2,\ldots).$$

Note that in example (b) if $e_k=o(d_k)$ and $(a_k)_{k=1}^{\infty}$ denotes $\bigcup_{k=1}^{\infty}[d_k,e_k]$ then

$$\lim_{N\to\infty}\frac{|(a_k)_{k=1}^{\infty}\cap[1,N]|}{N}=0.$$

This means that even in $\mathbb{Z}$ Theorem 2 gives more information than in Bergelson's theorem. If M_1 and M_2 with systems of subsets $\mathcal{A}_1=(A_{1,n})_{n=1}^{\infty}$ and $\mathcal{A}_2=(A_{2,n})_{n=1}^{\infty}$ respectively satisfy conditions (i)–(iv) then so does the direct product monoid $M_1\times M_2$ with the system of subsets $\mathcal{A}=(A_{1,n}\times A_{2,n})_{n=1}^{\infty}$ where $A_{1,n}\times A_{2,n}$ denotes the Cartesian product of $A_{1,n}$ and $A_{2,n}$ $(n=1,2,\ldots)$. This last remark and the fact that the examples (b) and (c) satisfy (i)–(iv) are readily justified and their verification we leave to the reader. The fact that example (a) satisfies (i)–(iv) is verified in [8].

1. Suppose (X,β,μ) is a probability space and suppose the measurable transformation $T:X\to X$ is measure preserving, that is, $\mu(T^{-1}B)=\mu(B)$ for each B in β. Here $T^{-1}B$ denotes $\{x\in X:Tx\in B\}$. We say a subset A of $\mathbb{N}$ is a *set of (Poincaré) recurrence* if for each B in β with $\mu(B)$ positive, there exists m in A such that $\mu(B\cap T^{-m}B)$ is positive. The proof of Theorem 1 is transformed into a problem in ergodic theory by the following result [2].

Theorem 3. *A subset A of $\mathbb{N}$ is a set of recurrence if and only if it is a set of intersectivity.*

For a real number x let $\langle x\rangle$ denote its fractional part. To complete the proof of Theorem 1 we need the following subsidiary result.

THEOREM 4. *If α is irrational, $\theta(x)$ is a non-constant polynomial with integer coefficients and for coprime integers c and d, $(q_k)_{k=1}^{\infty}$ are the primes congruent to c modulo d, then $(\langle\alpha\theta(q_k)\rangle)_{k=1}^{\infty}$: is uniformly distributed modulo one. Equivalently by Weyl's criteria*

$$\lim_{N\to\infty}\frac{1}{N}\sum_{k=1}^{N}e^{2\pi ih\alpha\theta(q_k)}=0\,, \tag{1}$$

for each h in $\mathbb{Z}\setminus\{0\}$.

Let

$$\theta^*(x)=\alpha_k x^k+\ldots+\alpha_1 x+\alpha_0\,,$$

with at least one of $\alpha_1,\ldots,\alpha_k$ irrational, then using the same method as that used to prove Theorem 4, we can actually prove $(\langle\theta^*(q_k)\rangle)_{k=1}^{\infty}$ is uniformly distributed modulo one. The proof is adapted from that used to show that if $(p_k)_{k=1}^{\infty}$ is the full sequence of rational primes, $(\langle\theta^*(p_k)\rangle)_{k=1}^{\infty}$ is uniformly distributed modulo one [9].

Because θ has integer coefficients, in proving (1) we may assume without loss of generality that $h=1$. The first lemma we need is Dirichlet's theorem on diophantine approximation.

LEMMA 5. *Suppose α is irrational. Then for each $Q\ge 1$, there exists a rational $\xi=a/q$ with $(a,q)=1$ and $1\le q\le Q$, such that*

$$|\alpha-\xi|\le\frac{1}{qQ}\,.$$

Let $Q=N^k(\log N)^{-u}$ with N large, $u>0$ and k the degree of θ. Also for the rational ξ in reduced form a/q let

$$M\left(\frac{a}{q}\right)=\left\{\alpha\in[0,1):\left\|\alpha-\frac{a}{q}\right\|<\frac{1}{qQ}\right\},$$

where $\|a_1-a_2\|=\min(|a_1-a_2|,|a_1+1-a_2|)$. Let $M=\bigcup_{\xi}M(\xi)$, where the union is taken over all $\xi=a/q$ with $1\le q\le(\log N)^u$. Classically the sets $M(\xi)$ are called major arcs and the connected components of $[0,1)\setminus M$ are known as the minor arcs. The following lemma, due to L. K. Hua [5], proves (1) on the minor arcs.

LEMMA 6. *Let $\alpha=\beta+a/q$ with $(a,q)=1$ and $\delta=|\beta|N^k$. Then if $\max(q,\delta)\ge(\log N)^u$,*

$$\left|\frac{1}{\pi_{N,c,d}}\sum_{1\le q_k\le N}e^{2\pi i\alpha\theta(q_k)}\right|\le C((\log N)^{-\zeta})\,,$$

with $\zeta>0$. Here $\pi_{N,c,d}$ denotes the number of primes congruent to $c \bmod d$ lying in $[1,N]$.

In Lemma 6 and henceforth C denotes an absolute positive constant not necessarily the same at each occurrence. To prove (1) on the major arcs we argue as follows. Let

$$T_N = \sum_{1\le q_k\le N} e^{2\pi i\alpha\theta(q_k)} \qquad (N=1,2,\ldots)$$

with α in M and let

$$R_N = \sum_{1\le q_k\le N} e^{2\pi i a q^{-1}\theta(q_k)} \qquad (N=1,2,\ldots)$$

with $R_0 = 0$. This means that

$$\begin{aligned} T_N &= \sum_{1\le n\le N} e^{2\pi i\beta\theta(n)}\{R_n - R_{n-1}\} \\ &= \sum_{1\le n\le N-1} R_n\{e^{2\pi i\beta\theta(n)} - e^{2\pi i\beta\theta(n+1)}\} + R_N e^{2\pi i\beta\theta(N)}\,. \end{aligned}$$

By the Chinese remainder theorem the congruences $x \equiv c \pmod d$ and $x\equiv m \pmod q$ have a solution $x\equiv l \pmod{[d,q]}$ if and only if $[d,q]$ divides $m-c$. This solution is unique. Here $[d,q]$ denotes the least common multiple of the natural numbers d and q. As a consequence we have

$$R_N = e^{2\pi i a q^{-1}\theta(c)}\pi_{N,l,[d,q]} + O(1)\,.$$

The prime number theorem for arithmetic progressions says

$$\pi_{N,l,[d,q]} = \frac{\pi_N}{\phi([d,q])} + O(Ne^{-C(\log N)^{1/2}})\,.$$

Here π_N denotes the number of primes in $[1,N]$ and ϕ denotes the Euler totient function. This means $T_N = T_1 + T_2$ where

$$T_1 = \frac{e^{2\pi i a q^{-1}\theta(c)}}{\phi([d,q])}\Big(\sum_{1\le n\le N-1} \pi_n\{e^{2\pi i\beta\theta(n)} - e^{2\pi i\beta\theta(n+1)}\} + \pi_N e^{2\pi i\beta\theta(N)}\Big)$$

and

$$T_2 = O\Big(Ne^{-C(\log N)^{1/2}} \sum_{1\le n\le N} |e^{2\pi i\beta\theta(n)} - e^{2\pi i\beta\theta(n+1)}| + 1\Big)\,.$$

Now because

$$|e^{2\pi i\beta\theta(n)} e^{2\pi i\beta\theta(n+1)}| \le C|\beta||(\theta(n+1)-\theta(n))|\,,$$

and because $\theta(n+1)-\theta(n)$ does not change sign for large enough n we have

$$T_2 = O(|\beta|N^{k+1}e^{-C(\log N)^{1/2}})\,,$$

which on the major arcs is

$$= O(Ne^{-C(\log N)^{1/2}})\,.$$

In addition summation by parts gives

$$T_1 = \frac{e^{2\pi i a q^{-1}\theta(c)}}{\phi([d,q])}\Big(\sum_{1\le n\le N-1}\{\pi_n - \pi_{n-1}\}e^{2\pi i\beta\theta(n)}\Big).$$

So, using the fact from elementary number theory that $q(\log\log q)^{-1} = O(\phi(q))$, we have

$$T_N = \frac{1}{\phi([d,q])}O\Big(\sum_{1\le n\le N}\{\pi_n - \pi_{n-1}\}\Big) = O\left(\pi_N\frac{\log\log q}{q}\right).$$

Now note that for ξ which is rational, the major arc centred on it gets smaller as N tends to infinity. This means that if α is in the major arc centred on $\xi = a/q$ then $q = q(N)$ tends to infinity as N does. Thus $T_N/\pi_{N,c,d}$ tends to zero as N tends to infinity on the major arcs, completing the proof of Theorem 4. ∎

Proof of Theorem 1. *Sufficiency of conditions on* ψ. By Theorem 3, it is sufficient to show that if (X,β,μ) is any probability space and $T : X\to X$ is any measurable and measure preserving transformation of it, for any B in β with $\mu(B) > 0$ there exists m in P_ψ such that $\mu(B\cap T^{-m}B) > 0$. To do this we argue as follows.

For f in $L^p(X,\beta,\mu)$ ($p\ge 1$), let $U : L^p\to L^p$ be the Koopman unitary operator defined by $Uf(x) = f(Tx)$. If $\langle\ \rangle$ denotes the standard inner product on L^2 then $(\langle U^n f, f\rangle)_{n=1}^{\infty}$ is a positive definite sequence, hence by Bochner's theorem, there exists a measure w_f, dependent on f, on the unit circle $\mathbb{T}$ such that

$$\langle U^n f, f\rangle = \int_{\mathbb{T}} z^n\,dw_f(z) \qquad (n = 1,2,\ldots).$$

Now for each natural number N, $(1/N)\sum_{n=1}^{N} z^n$ equals 1 if z does, and it tends to 0 for all other z on $\mathbb{T}$ as N tends to infinity. This means that if

$$A_n f(x) = \frac{1}{N}\sum_{n=1}^{N} f(T^n x) \qquad (N = 1,2,\ldots),$$

then $\langle A_N f, f\rangle$ tends to $w_f(\{1\})$ as N tends to infinity. By the mean ergodic theorem however, for f in L^2, if $\Pi_T f$ is the projection of f onto the T-invariant subspace of L^2, then $A_N f$ tends to $\Pi_T f$ in both L^1 and L^2 norms as N tends to infinity. This means that $\langle \Pi_T f, f\rangle = w_f(\{1\})$ and so, by Cauchy's inequality,

$$w_f(\{1\}) = \langle \Pi_T f, f\rangle = \langle \Pi_T f, \Pi_T f\rangle \ge \Big|\int \Pi_T f\,d\mu\Big|^2 = \Big|\int_X f\,d\mu\Big|^2. \tag{2}$$

Let L_s $(s = 1, 2, \ldots)$ be the subset of P_ψ of elements which are multiples of the least common multiple of the first s positive integers. In addition, let $L_{s,n} = L_s \cap [1, n]$ $(n = 1, 2, \ldots)$ and let

$$F_k = \{a/q : 1 \le a < q \le k,\ (a, q) = 1\} \qquad (k = 1, 2, \ldots)$$

(that is, the k th Farey dissection). Let F_k^c denote the complement of F_k in $\mathbb{Q} \cap (0, 1)$ and finally let $w_t = w_r + w_i$ denote the decomposition of w_f into a part with only atoms at the rationals and a part with no atoms at the rationals respectively. Then for any positive v

$$\begin{aligned}\langle U^v f, f\rangle = {} & \int_{\mathbb{T}} z^v \, dw_i(z) + w_r(\{1\}) \\ & + \Big(\sum_{a/q \in F_{k_0}} + \sum_{a/q \in F_{k_0}^c} \Big) e^{2\pi i a v q^{-1}} w_r(\{e^{2\pi i a q^{-1}}\}),\end{aligned}$$

where $k_0 = k_0(\varepsilon)$ has been chosen so that the second sum on the right is less than $\varepsilon > 0$ in absolute value. This means that

$$\frac{1}{|L_{k_0,n}|} \sum_{v \in L_{k_0,n}} \langle U^v f, f\rangle = w_r(\{1\}) + \sum_{a/q \in F_{k_0}} w_r(e^{2\pi i a q^{-1}}) \tag{3}$$

$$+ \sum_{a/q \in F_{k_0}^c} w_r(\{e^{2\pi i a q^{-1}}\}) \bigg(\frac{1}{|L_{k_0,n}|} \sum_{v \in L_{k_0,n}} e^{2\pi i v a q^{-1}} \bigg) \tag{4}$$

$$+ \int_{\mathbb{T}} \bigg(\frac{1}{|L_{k_0,n}|} \sum_{v \in L_{k_0,n}} e^{2\pi i v \alpha} \bigg) dw_i(e^{2\pi i \alpha}). \tag{5}$$

Let s^* denote the least common multiple of the first s natural numbers and let

$$M_{s,n,r} = \{\psi(p) : \text{ prime } p \equiv r \pmod{s^*}\} \cap [1, n].$$

Because of the assumptions on ψ in the statement of Theorem 1,

$$L_{s,n} = \bigcup_{r \in g_{s^*}} M_{s,n,r},$$

where g_{s^*} denotes the non-empty set of reduced residues mod s^* such that $\psi(r) \equiv 0 \pmod{s^*}$. This means that

$$\sum_{v \in L_{k_0,n}} e^{2\pi i v \alpha} = \sum_{r \in g_{k_0^*}} \sum_{v \in M_{k_0,n,r}} e^{2\pi i v \alpha},$$

which using Theorem 3 is

$$= o\Big(\sum_{r \in g_{k_0^*}} |M_{k_0,n,r}| \Big) = o(|L_{k_0,n}|).$$

Thus (5) tends to zero as n tends to infinity. In addition the expression (4)is less than ε in absolute value. Hence if we set $f = \chi_B$ (the characteristic function of B), using (2) we obtain

$$\liminf_{n\to\infty} \frac{1}{|L_{k_0,n}|} \sum_{v\in L_{k_0,n}} \mu(B\cap T^{-v}B) \geq \mu^2(B) - \varepsilon$$

as required.

Necessity of the conditions on ψ. For fixed positive integers n and l and each positive integer k ($k = 1, 2, \ldots$) let $S \equiv kn\mathbb{Z} + l$. Clearly S has positive upper Banach density, thus if P_ψ is intersective it contains infinitely many non-zero multiples of n. This means that there are primes p such that n divides $\psi(p)$ with p strictly greater than n. So that on setting m_n to be one such prime p we have shown that the intersectivity of P_ψ implies ψ satisfies the conditions on it in Theorem 1. ∎

Examination of the first part of the proof of Theorem 1 shows that the only property of $(u_t)_{t=1}^\infty = P_\psi$ used is the following fact. For each natural number s there exists an infinite sequence $(u_{s,t})_{t=1}^\infty$ of multiples of the least common multiple of the numbers $\{1, 2, \ldots, s\}$ contained in $(u_t)_{t=1}^\infty$ such that for each irrational real number α we have $N^{-1}\sum_{t=1}^N e^{2\pi i u_{s,t}\alpha}$ tending to zero as N tends to infinity. In consequence, any sequence $(u_t)_{t=1}^\infty$ with this property is intersective. As a result if, instead of Theorem 4, we use the fact that $(\langle\theta^*(n)\rangle)_{n=1}^\infty$ is uniformly distributed modulo one[12], we get a virtually identical proof of the following theorem.

Theorem 7. *Let ψ be a polynomial with integer coefficients and $N_\psi = \{\psi(n) : n \in \mathbb{Z}\}$. Then N_ψ is intersective if and only if for each non-zero integer n, there exists an element m_n of N_ψ such that n divides m_n.*

2. The proof of Theorem 2 hinges on the following form of an ergodic theorem of A. A. Tempel'man.

Theorem 8. *Suppose $\{T_m\}_{m\in M}$ is a countable commutative monoid under composition of measurable measure preserving transformations of the measure space (X, β, μ) indexed by elements m of the countable commutative monoid M. Suppose $\mathcal{A}$ is a collection of subsets of M that satisfy conditions* (i)–(iv). *Then for each integrable function f on (X, β, μ) we have*

$$\lim_{n\to\infty} \frac{1}{|A_n|} \sum_{m\in A_n} f(T_m x) = f^*(x)\,,$$

and for each $m \in M$, $f^*(T_m x) = f^*(x)$ μ -almost everywhere,with

$$\int_X f^*(x) d\mu = \int_X f(x)\, d\mu\,.$$

By $\{T_m\}_{m\in M}$ being a monoid under composition we mean that for each x in X we have $T_{m_1}(T_{m_2}(x)) = T_{m_1+m_2}(x)$.

To prove Theorem 2 we use the following result which is a straightforward generalisation of a result of V. Bergelson [1] produced here for completeness.

THEOREM 9. *Suppose $\{T_m\}_{m\in M}$ is a countable commutative monoid of measure preserving transformations acting on the probability space (X,β,μ). For B in β with $\mu(B) = a > 0$ and for each m in M let B_m denote T_mB. Then if $\mathcal{A}$ satisfies* (i)–(iv) *there exists a subset R of M with $d_{\mathcal{A}}(R) \geq a$ such that for each finite subset F of R we have $\mu(\bigcup_{m\in F} B_m) > 0$.*

Proof. For finite subsets F of M let $B_F = \bigcap_{m\in F} B_m$. Let $\mathcal{C}$ denote the necessarily countable set of products of finitely many characteristic functions of the form I_{B_m}. For each function f in $\mathcal{C}$ let N_f denote the set $\{x : \|f(x)| > ||f||_\infty\}$ and let $N = \bigcup_{f\in\mathcal{C}} N_f$. Now if $(X\setminus N)\cap B_F \neq \emptyset$ then $\mu(B_F) > 0$ because if x is in $(X\setminus N)\cap B_F$, letting $f = \prod_{m\in F} I_{B_m}$ and assuming $\mu(B_F) = 0$ we have $||f||_\infty = 0$. This means x is in N_f, which is a contradiction. Thus removing N from X if necessary, we may assume without loss of generality that if $B_F \neq \emptyset$ then $\mu(B_F) > 0$.

By Tempel'man's theorem

$$\lim_{N\to\infty} \frac{1}{|A_N|} \sum_{m\in A_N} I_{B_m}(x) = f^*(x)$$

with $f^*(T_mx) = f^*(x)$ for each m in M μ-almost everywhere and $\int_X f^*(x)d\mu = a$. Because (X,β,μ) is a probability space there exists an x_0 in X such that $f^*(x_0) \geq a$. Let R be the set $\{m \in M : x_0 \in B_m\}$. It follows $d_{\mathcal{A}}(R) \geq a$ and as x_0 is in B_m for each m in R we have $\mu(B_F) > 0$ for every finite subset F of R. ■

We now complete the proof of Theorem 2.

By hypothesis there exists a sequence of subsets $\{C_N\}_{N=1}^\infty$ of M satisfying (ii) and (iii) such that

$$b(E) = \lim_{N\to\infty} \frac{|E\cap C_N|}{|C_N|}$$

exists and is positive. Let $\mathit{\Lambda}$ denote the set $\{0,1\}$ and let $\mathit{\Omega}$ denote $\mathit{\Lambda}^M$, that is, the set of maps from M to $\mathit{\Lambda}$. By identifying I_E, the characteristic function of the set E in M, with its range we may think of $\xi = I_E$ as a point of $\mathit{\Omega}$. Let T_l be the shift on $\mathit{\Omega}$ defined by $T_lx(t) = x(t+l)$. Now let X denote the orbit closure of $\{T_m\xi : m \in M\}$ in $\mathit{\Omega}$ and let X_0 denote $\{x \in X : x(0) = 1\}$. If δ_x denotes the delta measure on the point x, for each natural number N let

$$\mu_N = \frac{1}{|C_N|} \sum_{m \in C_N} \delta_{T_m \xi}\,.$$

Because of the conditions (ii) and (iii) on $\{C_N\}_{N=1}^{\infty}$ there is a probability measure μ supported on X and preserved by elements of $\{T_n\}_{n\in M}$ which is a weak-star limit of the sequence of measures $\{\mu_N\}_{N=1}^{\infty}$. In addition, passing to a subsequence of $\{C_n\}_{n=1}^{\infty}$ if necessary, for every integrable function f on Ω we have

$$\int_{\Omega} f\,d\mu = \lim_{s\to\infty} \int_{\Omega} f\,d\mu_{N_s}\,.$$

This means

$$\mu(X_0) = \lim_{s\to\infty} \mu_{N_s}(X_0) = \frac{1}{|C_{N_s}|} \sum_{n\in C_{N_s}} \delta_{T_n\xi}(X_0) = b(E) > 0\,.$$

By Theorem 9 this also means that

$$\begin{aligned}
\mu(X_0 \cap T_{n_1}X_0 \cap \ldots \cap T_{n_k}X_0)& \\
&= \lim_{s\to\infty} \mu_{N_s}(X_0 \cap T_{n_1}X_0 \cap \ldots \cap T_{n_k}X_0) \\
&= \lim_{s\to\infty} \frac{1}{|C_{N_s}|} \sum_{n\in C_{N_s}} \delta_{T_n\xi}(X_0 \cap T_{n_1}X_0 \cap \ldots \cap T_{n_k}X_0) \\
&= b(E \cap (E+n_1) \cap \ldots \cap (E+n_k)) > 0
\end{aligned}$$

as required. ■

References

[1] V. Bergelson, *Sets of recurrence of $\mathbb{Z}^m$ -actions and properties of sets of differences in $\mathbb{Z}^m$* , J. London Math. Soc. (2) 31 (1985), 295–304.

[2] A. Bertrand-Mathis,*Ensembles intersectifs et recurrence de Poincaré*, Israel J. Math. 55 (1986), 184–198.

[3] H. Furstenberg,*Ergodic behaviour of diagonal measures and a theorem of Szemerédi on arithmetic progressions*, J. Analyse Math. 31 (1977), 204–256.

[4] —, *Recurrence in Ergodic Theory and Combinatorial Number Theory*, Princeton University Press, 1981.

[5] L. K. Hua, *Additive Theory of Prime Numbers*, Amer. Math. Soc.Transl. 13, 1965.

[6] T. Kamae and M. Mendès France,*Van der Corput's difference theorem*, Israel J. Math. 31 (1978),335–342.

[7] U. Krengel, *Ergodic Theorems*, de Gruyter Stud. Math. 6, 1985.

[8] R. Nair, *On strong uniform distribution*, Acta Arith. 56 (1990), 183–193.

[9] G. Rhin, *Sur la répartition modulo* 1 *des suites* $f(p)$, ibid. 23 (1973), 217–248.

[10] A. Sárközy, *On difference sets of sequences of integers*, *II*, Ann. Univ. Sci. Budapest. Eötvös Sect. Math. 21(1978), 45–53.

[11] A. Sárközy, *On difference sets of sequences of integers. III*, Acta Math. Acad. Sci. Hungar. 31 (3–4) (1978),355–386.

[12] H. Weyl, *Über die Gleichverteilung von Zahlenmod. Eins*, Math. Ann. 77 (1916), 313–352.

DEPARTMENT OF PURE MATHEMATICS UNIVERSITY OF LIVERPOOLP.O. BOX 147LIVERPOOL L69 3BX, U. K.

Received on 16.8.1991
and in revised form on 31.1.1992 (2164)