JOURNAL OF NUMBER THEORY **10**, 385–394 (1978)

Finite Measures Designed for Accuracy on Arithmetic Progressions

D. J. NEWMAN

Department of Mathematics, Temple University, Philadelphia, Pennsylvania 19122

AND

IAN RICHARDS

Department of Mathematics, University of Minnesota, Minneapolis, Minnesota 55455

Communicated by E. Hlawka

Received July 1, 1976

Anyone familiar with the so-called "sieving process" knows that it consists of repeated removals and insertions of various arithmetic progressions, and that the sizes of these progressions can only be estimated crudely. Motivated by these considerations we set ourselves the problem of producing a probability measure on $\{1, 2, 3,..., n\}$ such that "many" arithmetic progressions have measure "close to" $1/a$, where a is their common difference.

For example consider $n = 12$ and attach the measure (1/60, 1/30, 1/15, 1/10, 2/15, 3/20, 3/20, 2/15, 1/10, 1/15, 1/30, 1/60). The fact then is that *all* the A.P.'s with common difference $a \leqslant 6$ have *exactly* their "correct" measure $1/a$. For example the progression $5k + 2$ which is 2, 7, 12 has measure $1/30 + 3/20 + 1/60 = 1/5$; also the progression $3k + 1$, i.e., 1, 4, 7, 10 has the measure $1/60 + 1/10 + 3/20 + 1/15 = 1/3$, etc.

Now if we were to require of our measure that all A.P.'s of difference $a \leqslant m$ have *exactly* the *correct* measure, $1/a$, then we could only achieve this for $m \leqslant C(n^{1/2})$, C a constant (cf. Theorem 3 below). We find, however, that we can obtain *almost* exact agreement well past this point. Indeed we can get up to $m = n^{1-\epsilon}$ with errors of size $e^{-n^{\delta}}$, where δ lies somewhere between ϵ and 4ϵ.

For convenience we write $S_{a,b}$ to represent the A.P. $\{ak + b, -\infty < k < \infty\}$; more precisely, when considering measures μ supported on the finite set $\{1, 2, 3,..., n\}$, we mean by $S_{a,b}$ the intersection of the A.P. $\{ak + b\}$ with the interval $\{1,..., n\}$.

0022-314X/78/0104–0385$02.00/0

THEOREM 1. *Given n and m there exists a probability measure μ on $\{1, 2, 3,..., n\}$ such that*

$$| \mu[S_{a,b}] - 1/a | \leqslant e^{-n/m}$$

as long as $1 \leqslant a \leqslant m$.

We will also show that to some extent this construction is as good as can be.

THEOREM 2. *No measure μ on $\{1, 2,..., n\}$, positive or not, can satisfy*

$$| \mu[S_{a,b}] - 1/a | < e^{-C(n/m)^4}$$

for all a, b with $1 \leqslant a \leqslant m$ if $m > 20n^{3/4}$.

(Here $C = 1{,}000{,}000$. Note that taking $a = 1$ gives the total measure of $\{1, 2,..., n\}$ as being very close to 1.)

A case of interest is that of $m = n^{1-\epsilon}$, $0 < \epsilon < \frac{1}{4}$ where we conclude roughly that we can achieve $| \mu[S_{a,b}] - 1/a | \leqslant e^{-n^{\epsilon}}$ and that we cannot achieve $| \mu[S_{a,b}] - 1/a | \leqslant e^{-n^{4\epsilon}}$. The gap between ϵ and 4ϵ cannot be narrowed by our present methods, but our guess is that the truth is closer to ϵ, i.e., that Theorem 2 is the one that needs improvement. Indeed Theorem 1 has a rather simple proof while Theorem 2 has a complicated one, and this tends to make one believe that Theorem 1 is closer to the true state of affairs.

If we ask instead that all of the A.P's considered have *exactly* the right measure, then we obtain the following result.

THEOREM 3. *Given n and m, a necessary and sufficient condition for the existence of a nonzero signed measure μ on $\{1, 2, 3,..., n\}$ such that $\mu[S_{a,b}] = 1/a$ for all a, b with $a \leqslant m$ is*

$$\sum_{a=1}^{m} \varphi(a) \leqslant n \qquad (\textit{where } \varphi \textit{ denotes Euler's function}). \tag{*}$$

Note. Of course this allows us to compute, for any m, the smallest value of n which is compatible with it. Thus for $m = 6$, we obtain $n = 12$ as in the example at the beginning of this article. To construct the corresponding measure μ, we proceed as follows: First let μ_k denote the measure of the kth point. Then

$$\mu_k = \text{the coefficient of } z^k$$

in the polynomial $cz \cdot g_m(z)$, where

$$g_m(z) = \prod_{a=2}^{m} \Phi_a(z),$$

Φ_a denotes the ath cyclotomic polynomial, and $1/c$ is the least common multiple of all the numbers $\leqslant m$.

Now it is well known that

$$\sum_{a=1}^{m} \varphi(a) \sim (3/\pi^2) \cdot m^2,$$

and thus the asymptotic relationship between the number of points n and the "limit of accuracy" m is:

$$n \sim (3/\pi^2) \cdot m^2,$$

so

$$m \sim (\pi/3^{1/2}) \cdot n^{1/2}.$$

The optimal measure described above is unique. As Thomas Vehka has observed, it is not always positive. If we wish to have a positive measure, then we can obtain it by increasing the ratio n/m^2 by a constant factor, which for large m and n is asymptotic to $\pi^2/8$.

THEOREM 3a. *Given any n and m, there exists a probability measure μ on $\{1, 2,..., n\}$ such that $\mu[S_{a,b}] = 1/a$ for all a, b with $a \leqslant m$ provided that*

$$m \leqslant (8n/3)^{1/2} - 1.$$

Unlike Theorem 3, this result is probably not best possible. We suggest the problem: For large m and n, does there exist a nontrivial positive measure on $\{1, 2,..., n\}$ giving an exact equidistribution of mass on congruence classes (mod a) for all $a \leqslant m$, and where

$$n < (3/\pi^2) \cdot m^2 + o(m^2)?$$

The proof that the measure in Theorem 3 is not always positive is given at the end of this article.

Proofs of Theorems 1–3. In our proofs we will exploit the connection between the measures of A.P.'s and the values of the "*characteristic function*" at the roots of unity. Thus calling $\varphi(z) = \sum_1^n \mu_k z^k$ (where μ_k denotes the measure of the point k) we have the two-way relationship

(A) If ω is an ath root of unity then

$$\varphi(\omega) = \sum_{b=0}^{a-1} \mu[S_{a,b}]\, \omega^b,$$

(B) $$\mu[S_{a,b}] = \frac{1}{a} \sum_{\substack{\omega \text{ all } a\text{th} \\ \text{roots of } 1}} \omega^{-b} \varphi(\omega)$$

[(A) is trivial and (B) follows directly from (A) using the fact that $\sum_{\omega^a=1} \omega^v = \{a \text{ if } a \mid v \text{ or } 0 \text{ if not}\}$.]

From (A) we obtain

(I) If $|\mu[S_{a,b}] - 1/a| \leqslant \epsilon$ for all b then $|\varphi(\omega)| \leqslant a \cdot \epsilon$ for all ath roots of unity $\omega \neq 1$.

While (B) gives

(II) If $|\varphi(\omega)| \leqslant \epsilon$ for all ath roots of unity other than 1 and if $\varphi(1) = 1$ then $|\mu[S_{a,b}] - 1/a| < \epsilon$.

Let us fix an m and, for convenience, call W the set of all ath roots of unity for all $a \leqslant m$. Theorems 1 to 3 thus result from

THEOREM 1′. *There exists an nth degree polynomial $\varphi(z)$ with nonnegative coefficients having $\varphi(1) = 1$ and such that $|\varphi(z)| \leqslant 10e^{-(\pi/2)(n/m)}$ throughout $W - \{1\}$.*

THEOREM 2′. *If $\varphi(z) = \mu_n z^n + \cdots + \mu_1 z$ is any nth degree polynomial such that $|\varphi(z)| \leqslant e^{-10^6(n/m)^4}$ throughout $W - \{1\}$ and if $m > 20n^{3/4}$ then $|\varphi(1)| < \frac{1}{2}$.*

For Theorem 3, since we seek precision, it is convenient to replace the interval $\{1, 2, \ldots, n\}$ by $\{0, 1, \ldots, n-1\}$. Thus here the number of points n is one more than the degree of the corresponding polynomial.

THEOREM 3′. *$\varphi(z) = 0$ for all $z \in W - \{1\}$ if and only if the polynomial $\varphi(z)$ is divisible by*

$$g_m(z) = \prod_{a=2}^{m} \Phi_a(z), \qquad (**)$$

where Φ_a denotes the ath cyclotomic polynomial.

THEOREM 3a′. *The polynomial*

$$h_m(z) = \prod_{m/2<a\leqslant m} (1 + z + z^2 + \cdots + z^{a-1})$$

has positive coefficients, is of degree $\leqslant (3/8)(m^2 - 1)$, and is divisible by the polynomial $g_m(z)$ of Theorem 3′.

[Recall that, since our polynomials have a zeroth term, the number n of coefficients is one more than the degree. Thus to deduce Theorems 3 and 3a from 3′ and 3a′ requires a little attention to detail. For Theorems 3 and 3′, the formulas (*) and (**) match because the product in (**) starts with $a = 2$.

In Theorem 3a, the term "-1" could be dropped, giving the simpler relation $m \leqslant (8n/3)^{1/2}$, by making a careful enumeration of cases (m even/m odd) and by considering the greatest integer in the square root. Since Theorem 3a (unlike Theorem 3) is not best possible, there seems to be no point in pursuing the matter.]

Proof of Theorem 1′. We begin with the familiar θ-function identity $\sum_{k=-\infty}^{\infty} e^{-\pi x k^2} e^{2\pi i k t} = x^{-1/2} \sum_{\nu=-\infty}^{\infty} e^{-(\pi/x)(\nu+t)^2}$ where we will suppose $0 < x \leqslant 1$ and $-\frac{1}{2} < t \leqslant \frac{1}{2}$.

We obtain an approximate equality from this by truncating the left side past the terms $-n/2 < k \leqslant n/2$ while at the same time truncating the right side past the single term $\nu = 0$ (and later on setting $x = 2/mn$). Thus we obtain

$$\sum_{-n/2<k\leqslant n/2} e^{-\pi x k^2} e^{2\pi i k t} = \frac{1}{x^{1/2}} e^{-(\pi/x)t^2} + E,$$

where

$$|E| \leqslant 2 \sum_{k \geqslant n/2} e^{-\pi x k^2} + \frac{2}{x^{1/2}} \sum_{v=1}^{\infty} e^{-(\pi/x)(v-1/2)^2}.$$

Now we have

$$\sum_{k\geqslant n/2} e^{-\pi x k^2} \leqslant \sum_{j\geqslant 0} e^{-\pi x(n^2/4+j^2)} < e^{-\pi x(n^2/4)} \left(1 + \int_0^{\infty} e^{-\pi x u^2}\, du\right)$$

$$= e^{-\pi x(n^2/4)} \left(1 + \frac{1}{2x^{1/2}}\right) < \frac{3}{x^{1/2}} e^{-\pi x(n^2/4)}$$

while

$$\sum_{v=1}^{\infty} e^{-(\pi/x)(v-1/2)^2} \leqslant e^{-\pi/4x}(1 + e^{-\pi/x} + e^{-2\pi/x} + \cdots)$$

$$= \frac{e^{-\pi/4x}}{1 - e^{-\pi/x}} < \frac{3}{2} e^{-\pi/4x}$$

and so $|E| \leqslant (3/x^{1/2})(e^{-\pi x(n^2/4)} + e^{-\pi/4x})$.

Now we shall think of these series as functions of t (or more properly of $e^{2\pi i t}$), and let σ be the value corresponding to $t = 0$. We find:

$$\sigma = \sum_{-n/2<k\leqslant n/2} e^{-\pi x k^2} = \frac{1}{x^{1/2}} + E',$$

where E' satisfies the same inequality as E above.

Let us now define the desired function φ:

$$\varphi(e^{2\pi i t}) = \frac{e^{2\pi i [n/2] t}}{\sigma} \sum_{-n/2<k\leqslant n/2} e^{-\pi x k^2} e^{2\pi i k t}.$$

For $e^{2\pi it} \in W - \{1\}$ we have $|t| \geqslant 1/m$ and so we may estimate this φ by

$$\frac{x^{-1/2}e^{-\pi/xm^2} + E}{x^{-1/2} + E'} \leqslant \frac{e^{-\pi/xm^2} + 3(e^{-\pi x(n^2/4)} + e^{-\pi/4x})}{1 - 3(e^{-\pi x(n^2/4)} + e^{-\pi/4x})},$$

and if we finally choose $x = 2/mn$ we obtain the bound

$$\frac{7e^{-(\pi/2)(n/m)}}{1 - 6e^{-(\pi/2)(n/m)}} \leqslant 10e^{-(\pi/2)(n/m)}$$

as required.

We turn to Theorem 2': Now the points of W break the unit circle into arcs (the so-called Farey arcs); if the arc A has for endpoints a primitive a_1th root of 1 and a primitive a_2th root of 1 then we say it is of type (a_1, a_2) and we write $r(A) = \min(a_1, a_2)$. We also write $l(A)$ for the length of A.

Some simple facts in the elementary theory of Farey arcs are that

(1) If A is of type (a_1, a_2) then $l(A) = 2\pi/a_1a_2$.

(2) If (a_1, a_2) is a type of some A then $a_1 + a_2 > m$, and a simple consequence of these is that

(3) $l(A) \leqslant 4\pi/m \cdot r(A)$.

Let us fix a number j and agree to call an arc a *major arc* if $r(A) < j$ and a *minor arc* if $r(A) \geqslant j \in \mathbb{N}$. We also introduce the set S consisting of all the midpoints (on the circle) of pairs of points each from a major arc, and we proceed to estimate the measure of this set S. If we fix on two (not necessarily distinct) major arcs A_1 and A_2, then the set of midpoints between the points from A_1 and the points from A_2 consists of two arcs each of length $\frac{1}{2}(l(A_1) + l(A_2))$. Altogether then, we have

$$\begin{aligned} |S| &\leqslant \sum_{A_1, A_2 \text{ major}} l(A_1) + l(A_2) = 2 \sum_{A \text{ major}} l(A) \cdot \sum_{A \text{ major}} 1 \\ &= 2 \sum_{r<j} \sum_{r(A)=r} l(A) \cdot \sum_{r<j} \sum_{r(A)=r} 1, \end{aligned}$$

and from (3) and the fact that the number of arcs with $r(A) = r$ is $2\varphi(r) \leqslant 2r$, this is in turn bounded by

$$2 \cdot \sum_{r<j} \frac{8\pi}{m} \sum_{r<j} 2r < 2 \cdot \frac{8\pi}{m} j \cdot j^2,$$

and so we obtain

(4) $|S| < (16\pi/m)j^3$.

For convenience at this point we introduce the norm $\|f(z)\| = \sup_{|z|=1} |f(z)|$ (on functions, f, which need not necessarily be analytic).

We now prove

LEMMA 1. *Let $P(z)$ be a polynomial of degree $\leqslant mj/4\pi$ such that $|P(z)| \leqslant 1$ throughout $W - \{1\}$.*

Then, except on the set S, $|P(z)| \leqslant (2\|P\|)^{1/2}$.

Proof. Fix $z \notin S$ and form the trigometric polynomial $T(\zeta) = P(\zeta)P(z^2/\zeta)$. For each ζ either ζ or z^2/ζ lies on a minor arc (or else z, their midpoint, would belong to S). Suppose w.l.o.g. that ζ lies on a minor arc, B, and let ω be the nearer endpoint of B to ζ; note that $\omega \neq 1$, so that $|T(\omega)| = |P(\omega)| \cdot |P(z^2/\omega)| \leqslant 1 \cdot \|P\|$.

Now, by Bernstein's theorem we have $\|T'\| \leqslant mj/4\pi \|T\|$, and so $|T(\zeta)| = |T(\omega) + \int_\omega^\zeta T'(s)\,ds| \leqslant \|P\| + mj/4\pi \|T\| \cdot \frac{1}{2}l(B)$ so that, by (3), $|T(\zeta)| \leqslant \|P\| + \frac{1}{2}\|T\|$. Varying ζ gives $\|T\| \leqslant \|P\| + \frac{1}{2}\|T\|$ and we obtain $\|T\| \leqslant 2\|P\|$. Finally, setting $\zeta = z$ in the definition of T, we obtain $T(z) = P^2(z)$ which gives us $|P^2(z)| \leqslant 2\|P\|$ as required.

LEMMA 2. *If $P(z)$ is an nth degree polynomial such that $|P(z)| \leqslant 1$ on $|z| = 1$ except for a set, T, of measure $\alpha \leqslant 1$, then $\|P\| \leqslant e^{2\alpha n}$. (Here the measure of the circle is taken to be 2π.)*

[This is not the best possible result, such being that $\|P\| \leqslant T_n(\sec \alpha/4)$ whether or not $\alpha \leqslant 1$; the proof is essentially contained in [2]. The weak version above is all that we require and so we include the simple proof.]

Proof. By Jensen's formula we have, for $r < 1$,

$$\log |P(re^{i\theta})| \leqslant \frac{1 - r^2}{2\pi} \int_{-\pi}^{\pi} \frac{\log |P(e^{it})|\,dt}{1 - 2r\cos(\theta - t) + r^2}$$

$$\leqslant \frac{1 - r^2}{2\pi} \int_T \frac{\log |P(e^{it})|}{(1 - r)^2}\,dt \leqslant \frac{1 - r^2}{2\pi} \cdot \frac{\log \|P\|}{(1 - r)^2} \cdot \alpha,$$

and so

$$\log \frac{|P(re^{i\theta})|}{r^n} \leqslant \frac{1 + r}{1 - r} \frac{\alpha}{2\pi} \log \|P\| + n \log \frac{1}{r}.$$

The maximum, over θ, of $|P(re^{i\theta})|/r^n$ is the maximum modulus of $P(z)/z^n$ on $|z| = r$ and, by the maximum modulus theorem (applied to the function $P(z)/z^n$ in a "disk about the point at infinity"), this bounds the maximum modulus of $P(z)/z^n$ on $|z| = 1$, i.e., $\|P\|$.

Thus we obtain

$$\log \|P\| \leqslant \frac{\alpha}{2\pi} \frac{1 + r}{1 - r} \log \|P\| + n \log \frac{1}{r}.$$

Setting $r = e^{-\alpha}$ and observing that

$$\alpha \frac{1 + e^{-\alpha}}{1 - e^{-\alpha}} \leqslant \frac{1 + e^{-1}}{1 - e^{-1}} < \pi$$

this gives $\log \| P \| \leqslant \frac{1}{2} \log \| P \| + n\alpha$, the desired result.

Combining (4) and our two lemmas we easily obtain the following:

LEMMA 3. *Let $P(z)$ be a polynomial of degree $\leqslant mj/4\pi$ and suppose that $16\pi j^3/m \leqslant 1$. If $|P(z)| \leqslant 1$ throughout $W - \{1\}$ then $\| P \| \leqslant 2e^{16j^4}$.*

Proof. Lemma 1 gives $|P(z)| \leqslant (2 \| P \|)^{1/2}$ except on S, which by (4) has measure $\leqslant 16\pi j^3/m \leqslant 1$. Lemma 2 is therefore applicable to $P(z)/(2 \| P \|)^{1/2}$ and it gives $\| P \|/(2 \| P \|)^{1/2} \leqslant e^{(2 \cdot 16\pi j^3/m)(mj/4\pi)} = e^{8j^4}$, as required.

Theorem 2′ can now be read off from this lemma. Simply choose j as the first integer above $4\pi(n/m)$. Then surely $\varphi(z)$ does have degree $n \leqslant mj/4\pi$ and we do have $16\pi j^3/m < (16\pi/m)(4\pi(n/m) + 1)^3 < 10^5(n^3/m^4) < 1$, since $m > 20n^{3/4}$.

Lemma 3 applied to $P(z) = e^{10^6(n/m)^4} \cdot \varphi(z)$ then gives $e^{10^6(n/m)^4} \| \varphi \| \leqslant 2e^{16(4\pi(n/m)+1)^4}$ which easily implies $\| \varphi \| < \frac{1}{2}$ as required. Theorem 2′ is proved.

Proof of Theorems 3′ *and* 3a′. This is almost trivial. For Theorem 3′: We know from our general "characteristic function" argument that a polynomial

$$\varphi(z) = \mu_0 + \mu_1 z + \cdots + \mu_{n-1} z^{n-1}$$

gives exact equidistribution of mass on $\{0, 1, \ldots, n - 1\}$ for all congruence classes (mod a) for any particular a if and only if $\varphi(z)$ vanishes at all ath roots of unity other than 1. In other words, we have:

LEMMA. *The sequence of numbers $\mu_0, \mu_1, \ldots, \mu_{n-1}$ gives the same total mass to each congruence class* (mod a) *on $\{0, 1, \ldots, n - 1\}$ if and only if the polynomial $\varphi(z)$ is divisible by*

$$1 + z + z^2 + \cdots + z^{a-1} = \prod_{\substack{d \mid a \\ d \neq 1}} \Phi_d(z) \qquad (\textit{where } \Phi_d = \textit{the } d\textit{th cyclotomic polynomial}).$$

Note. The above lemma means that the measure $\mu_0, \mu_1, \ldots, \mu_{n-1}$ is a convolution product of some measure $\{\nu_k\}$ with the measure $\{1, 1, 1, \ldots, 1, 0, 0, 0, \ldots\}$ consisting of a "1's" followed by an infinite string of "0's."

The lemma can be proved purely combinatorially, and then using it, Theorems 3 and 3a can be proved algebraically without invoking Fourier analysis. We doubt, however, whether the same thing is true for Theorems 1 and 2.

Theorems 3′ and 3a′ are immediate consequences of the lemma. We conclude with two "complements" to Theorem 3 which were observed by Thomas Vehka.

The first is that, if we take the measure $\{\mu_k\}$ determined by the polynomial

$$g_m(z) = \prod_{a=2}^{m} \Phi_a(z)$$

(so that $g_m(z) = \mu_0 + \mu_1 z + \cdots + \mu_{n-1} z^{n-1}$), then each value μ_k is an *integer*, and the total mass of the interval $\{0, 1, \ldots, n-1\}$ is equal to the least common multiple of all the numbers $\leqslant m$.

To see this, just note that the total mass $= g_m(1)$, and that each $\Phi_a(1) =$ either p or 1, depending on whether a is a prime power p^k or not.

[Since each μ_k is an integer, the "equipartition" (mod a) for all $a \leqslant m$ trivially implies that the total mass would have to be a common multiple of all the numbers $a \leqslant m$. What is remarkable is that it is always the *least* common multiple.]

The second observation is that the measures determined by the polynomials $g_m(z)$ are not necessarily positive. Thus let $\mu_{k,m}$ = the coefficient of z^k in $g_m(z)$ = the mass at the integer k corresponding to $g_m(z)$. Then there are infinitely many values of m for which $\mu_{1,m}$ is negative. For, remembering that

$$g_m(z) = \prod_{a=2}^{m} \Phi_a(z),$$

and using the standard formula for the cyclotomic polynomial Φ_a, we obtain

$$\mu_{1,m} = -\sum_{a=2}^{m} \mu(a) \qquad \text{(where } \mu(a) \text{ is the Möbius function).}$$

Finally, it is well known[1] that the series $\sum \mu(a)$ oscillates between $+\infty$ and $-\infty$; in other words, the numbers $\mu_{1,m}$ oscillate in sign, assuming both positive and negative values of arbitrarily large magnitude.[2]

[1] The oscillation of $\sum \mu(a)$ follows, via a standard Tauberian theorem of analytic number theory, from the fact that the function $1/\zeta(s)$ has no singularities on the real axis.

[2] The first value of m for which $\mu_{1,m} < 0$ is $m = 95$. We do not know whether there is any smaller value of m for which some other coefficient $\mu_{k,m}$, $k \neq 1$, is negative.

REFERENCES

1. H. HALBERSTAM AND H.-E. RICHERT, "Sieve Methods," Academic Press, London, 1974.
2. REMEŹ, Sur une propiété des Polynomes de Tebebychev, *Comm. Inst. Sci. Kharkov* **13** (1936), 93–95.