UNIFORM DISTRIBUTION

Andrew Granville
Université de Montréal

Zeev Rudnick
Tel-Aviv University

1. Uniform distribution mod one

At primary school the first author was taught to estimate the area of a (convex) body by drawing it on a piece of graph paper, and then counting the number of (unit) squares inside. There is obviously a little ambiguity in deciding how to count the squares which straddle the boundary. Whatever the protocol, if the boundary is more-or-less smooth then the number of squares in question is proportional to the perimeter of the body, which will be small compared to the area (if the body is big enough). At secondary school the first author learnt that there are other methods to determine areas, sometimes more precise. As an undergraduate he learned that counting lattice points is often a difficult question (and that counting unit squares is "equivalent" to counting the lattice points in their bottom left-hand corner). Then, as a graduate student, he learnt that the primary school method could be turned around to provide a good tool for estimating the number of lattice points inside a convex body! In the specific case of a right-angled triangle we fix the slope $-\alpha$ of the hypotenuse and ask for the number of lattice points

$$A_\alpha(N) := \#\{(x, y) \in \mathbb{Z}^2 : x, y \geq 0 \text{ and } y + \alpha x \leq N\}.$$

For fixed α the primary school method yields

$$A_\alpha(N) = \frac{N^2}{2\alpha} + O_\alpha(N). \tag{1}$$

Can we improve on the error term $O_\alpha(N)$? For integer m we have

$$\left(A_{-1}(m) - \frac{m^2}{2}\right) - \left(A_{-1}(m - \frac{1}{m}) - \frac{(m - \frac{1}{m})^2}{2}\right)$$
$$= A_{-1}(m) - A_{-1}(m-1) + 1 - \frac{1}{2m^2} = \binom{m+1}{2} - \binom{m}{2} + O(1) = m + O(1);$$

thus we cannot replace the "$O_{-1}(N)$" term in (1) by "$o_{-1}(N)$." Moreover a similar argument works whenever $\alpha \in \mathbb{Q}$. It is unclear whether (1) can be improved when $\alpha \notin \mathbb{Q}$ so we now examine this case in more detail:

For each integer $x \geq 0$ the number of integers $y \geq 0$ for which $y + \alpha x \leq N$ is simply $\max\{0, 1 + [N - \alpha x]\}$, where $[t]$ denotes the largest integer $\leq t$. Whenever $x \leq N/\alpha$ we can write $1 + [N - \alpha x] = 1 + N - \alpha x - \{N - \alpha x\}$, where $\{t\} = t - [t]$. Therefore

$$\begin{aligned} A_\alpha(N) &= \sum_{x=0}^{[N/\alpha]} (1 + N - \alpha x - \{N - \alpha x\}) \\ &= \frac{N^2}{2\alpha} + \frac{1}{2}\left(N + \frac{N}{\alpha}\right) + O(1) - \sum_{x=0}^{[N/\alpha]} (\{N - \alpha x\} - \frac{1}{2}). \end{aligned} \tag{2}$$

The first term is indeed the area of our triangle. The second two terms account for half the length of the perimeter of our triangle. So, to able to prove that

$$A_\alpha(N) = \text{Area} + \frac{\text{Perimeter}}{2} + o_\alpha(N),$$

we need to establish that the mean value of $\{N - \alpha x\}$ is $\frac{1}{2}$ when α is irrational, as one might guess. Actually we will prove something much stronger. We will prove that these values, in fact any set of values $\{\alpha n + \beta : \ 1 \leq n \leq N\}$ with α irrational, are "uniformly distributed mod one," so that their average is $\frac{1}{2}$:

DEFINITION. . A sequence of real numbers $a_1, a_2, \ldots$ is *uniformly distributed mod one* if, for all $0 \leq b < c \leq 1$ we have

$$\#\{n \leq N : \ b < \{a_n\} \leq c\} \sim (c - b)N \quad \text{as } N \to \infty.$$

Note that the values $a_n = np/q + \beta$, $1 \leq n \leq N$ (here $\alpha = p/q \in \mathbb{Q}$) are evidently *not* uniformly distributed mod one.

Dirichlet proved that for any integer $M \geq 1$ there exists integer m, $1 \leq m \leq M$ such that $\|m\alpha\| < 1/M$ (where $\|t\|$ denotes the distance from t to the nearest integer). To prove this note that there are $M + 1$ numbers $\{0 \cdot \alpha\}, \{1 \cdot \alpha\}, \ldots, \{M \cdot \alpha\}$ so, by the pigeonhole principle two, say $\{i \cdot \alpha\}$ and $\{j \cdot \alpha\}$ with $0 \leq i < j \leq M$, must belong to the same interval $[k/M, (k + 1)/M)$ and so the result follows with $m = j - i$.

For $\alpha \notin \mathbb{Q}$ we have $\delta := \|m\alpha\| > 0$. We will show that for each i, $1 \leq i \leq m$ the set of values $\{\alpha n + \beta : 1 \leq n \leq N, \ n \equiv i \pmod m\}$ is well-distributed mod one, and so the union of these sets is. This set of values is $\{j(m\alpha)+(i\alpha+\beta)\} : \ 1 \leq j \leq J_i\}$ where $J_i = N/m + O(1)$. We can rewrite this as $\{\delta j + \gamma \pmod 1 : 1 \leq j \leq J\}$

where $\gamma \equiv i\alpha + \beta \pmod 1$ if $\delta = \{m\alpha\}$, and $\gamma \equiv i\alpha + \beta - \delta(J+1) \pmod 1$ if $1 - \delta = \{m\alpha\}$, by replacing j with $J + 1 - j$. Now, for $0 \le \gamma < 1$ and $K = [\delta J + \gamma]$

$$\begin{aligned}\#\{j \le J : \{\delta j + \gamma\} \in [b, c)\} &= \sum_{k=0}^{K} \#\{j \le J : \delta j + \gamma \in [k + b, k + c)\} \\ &= (K + O(1))\left(\frac{c-b}{\delta} + O(1)\right) \\ &= (c-b)J + O\left(\frac{c-b}{\delta} + \delta J + 1\right).\end{aligned}$$

So fix $\epsilon > 0$ and let $M > 1/\epsilon$ so that $\delta < 1/M < \epsilon$. We have just shown that

$$\#\{n \le N : \{\alpha n + \beta \in [b, c)\}\} = (c-b)N + O\left(\frac{m}{\delta} + \delta N\right).$$

Selecting $N > m/\delta^2$ this is $(c - b + O(\epsilon))N$. Letting $\epsilon \to 0$ we deduce that the sequence $\{\alpha n + \beta : n \ge 1\}$ is uniformly distributed mod one.

The above argument works for linear polynomials in α but it is hard to see how it can be modified for more general sequences. However to determine whether a sequence of real numbers is uniformly distributed we have the following extraordinary, and widely applicable, criterion:

WEYL'S CRITERION. *(*Weyl, 1914*) A sequence of real numbers $a_1, a_2, \dots$ is uniformly distributed mod one* if and only if *for every integer $b \ne 0$ we have*

$$\left|\sum_{n \le N} e(ba_n)\right| = o_b(N) \quad \text{as } N \to \infty. \tag{3}$$

In other words $\limsup_{N\to\infty} \frac{1}{N}|\sum_{n\le N} e(ba_n)| = 0$.

(Here, and throughout, $e(t) := e^{2i\pi t}$.) In particular if $a_n = \alpha n + \beta$ then

$$\sum_{n \le N} e(ba_n) = e(b\beta) \sum_{n \le N} e(b\alpha n) = e(b(\alpha + \beta)) \cdot \frac{e(b\alpha N) - 1}{e(b\alpha) - 1},$$

the sum of a geometric progression, provided $b\alpha$ is not an integer, so that

$$\left|\sum_{n \le N} e(ba_n)\right| \le \frac{2}{|e(b\alpha) - 1|} \asymp \frac{1}{\|b\alpha\|} \ll_b 1 = o_b(N), \tag{4}$$

as $|e(t) - 1| \asymp \|t\|$. Since $b\alpha$ is never an integer when $\alpha \notin \mathbb{Q}$ we deduce, from Weyl's criterion, that the sequence $\{\alpha n + \beta : n \ge 1\}$ with α irrational, is uniformly distributed mod one.

REMARK. We immediately deduce from Weyl's criterion that if $a_1, a_2, \dots$ is uniformly distributed mod one then so is $ka_1, ka_2, \dots$ for any non-zero integer k. Actually this can be deduced from the definition of uniform distribution mod one.

Proof. We recall that $|\sin t| \le \|t\|$ so that $|e(t) - 1| \le \pi\|t\|$.

We begin by assuming that $a_1, a_2, \dots$ is uniformly distributed mod one. Fix integer b and then fix integer $M > b$. Since the sequence is uniformly distributed mod one we know that for each m, $0 \le m \le M-1$, there are $N/M + o(N)$ values of $n \le N$ with $m/M \le a_n < (m+1)/M$; moreover, for such n, we have $|e(ba_n) - e(bm/M)| \le \pi\|b/M\|$. Therefore

$$\sum_{n\le N} e(ba_n) = \sum_{m=0}^{M-1} \left(\frac{N}{M} + o(N)\right)\left(e\left(\frac{bm}{M}\right) + O_b\left(\frac{1}{M}\right)\right) = O_b\left(\frac{N}{M}\right) + o(MN).$$

Now letting M get increasingly large we deduce that our sum is indeed $o_b(N)$.

On the other hand, assume that (1) holds and define the characteristic function $\chi_{(b,c]}$ by $\chi_{(b,c]}(t) = 1$ if $\{t\} \in (b,c]$, and $= 0$ otherwise. A well-known result from Fourier analysis tells us that one can approximate any "reasonable" function arbitrarily well using polynomials. That is, for any $\epsilon > 0$ there exists integer d and coefficients c_j, $-d \le j \le d$, such that $\left|\chi(t) - f(e(t))\right| \le \epsilon$ for all $t \in [0,1)$ where $f(x) = \sum_{j:|j|\le d} c_j x^j$. Therefore

$$\begin{aligned}\#\{n \le N : b < \{a_n\} \le c\} &= \sum_{n\le N} \chi_{(b,c]}(a_n) = \sum_{n\le N} \Big(f(e(a_n)) + O(\epsilon)\Big)\\ &= \sum_{j:|j|\le d} c_j \sum_{n\le N} e(ja_n) + O(N\epsilon) = c_0 N + o(N) + O(N\epsilon)\end{aligned}$$

by (4). Now

$$c - b = \int_0^1 \chi_{(b,c]}(t)dt = \sum_{j:|j|\le d} c_j \int_0^1 e(jt)\,dt + O(\epsilon) = c_0 + O(\epsilon)$$

and so, by combining the last two equations and letting $\epsilon \to 0$, we have shown that the sequence is uniformly distributed mod one.

One can deduce that $a_1, a_2, \dots$ is uniformly distributed mod one if and only if, for every continuous function $f\colon [0,1) \to \mathbb{R}$, we have

$$\lim_{N\to\infty} \frac{1}{N} \sum_{n\le N} f(\{a_n\}) = \int_0^1 f(x)\,dx.$$

To prove this note that the functions $e(bx)$, $b \in \mathbb{Z}_{\ge 0}$ form an appropriate (Fourier) basis for the continuous functions on $[0,1)$.

An explicit version of Weyl's result, which is useful for many applications, was given by Erdős and Turán (Erdős and Turán, 1948): For any sequence of real numbers, and any $0 \le b < c \le 1$ we have

$$\left|\frac{1}{N}\#\{n \le N : \ b < \{a_n\} \le c\} - (c-b)\right| \le \frac{6}{m+1} + \frac{4}{\pi}\sum_{b=1}^{m}\frac{1}{b}\left|\frac{1}{N}\sum_{n\le N} e(ba_n)\right|.$$

There is a nice application of Weyl's theorem in the theory of elliptic curves: Let E be an elliptic curve defined over $\mathbb{Q}$ and suppose that E has infinitely many rational points. Poincaré showed that the rational points form an additive group, and Mordell proved Poincaré's conjecture that this group has finite rank; in other words $E(\mathbb{Q})$ is an additive group of the form $\mathbb{Z}^r \bigoplus T$ where the torsion subgroup T (that is, the subgroup of points of finite order) and r are finite. Let us suppose that $P_1, \dots, P_r$ form a basis for the $\mathbb{Z}^r$ part of $E(\mathbb{Q})$: For any given arc A on $E(\mathbb{R})$ we can ask what proportion of the points $\{n_1P_1 + n_2P_2 + \dots + n_rP_r + t : 0 \le n_1, \dots, n_r \le N-1, \ t \in T\}$ lie on A, as $N \to \infty$? The connection with our work above lies in the Weierstrass parameterization of E: There exists an isomorphism $\wp\colon \mathbb{C}/(\mathbb{Z}+\mathbb{Z}i) \to E$; that is $\wp(v+w) = \wp(v) + \wp(w)$ for all $v, w \in \mathbb{C}$. So select $z_1, \dots, z_r \in \mathbb{C}$ such that $\wp(z_j) = P_j$ and τ such that $\wp(\tau) = t$. The above question then becomes to determine the proportion of the points

$$\{n_1z_1 + n_2z_2 + \cdots + n_rz_r + \tau \pmod{\mathbb{Z}+\mathbb{Z}i} : 0 \le n_1, \dots, n_r \le N-1, \ \tau \in \wp^{-1}(T)\}$$

that lie on $\wp^{-1}(A)$, a two-dimensional uniform distribution question. Like this the proportion can be shown to be

$$\int_{(x,y)\in A}\frac{dx}{y}\Big/\int_{(x,y)\in E(\mathbb{R})}\frac{dx}{y}.$$

(For more background on elliptic curves see (Silverman and Tate, 1992)).

For given $v = (a_1, \dots, a_k) \in \mathbb{R}^k$ define $v \pmod 1$ to be the vector $(a_1 \pmod 1, \dots, a_k \pmod 1)$. We say that the sequence of vectors $v_1, v_2, \dots \in \mathbb{R}^k$ is *uniformly distributed mod one* if for any $0 \le b_j < c_j < 1$ for $j = 1, 2, \dots, k$, we have

$$\#\left\{n \le N : a_n \pmod 1 \in \bigoplus_{j=1}^{k}[b_j, c_j)\right\} \sim \prod_{j=1}^{k}(c_j - b_j)\cdot N \quad \text{as } N \to \infty.$$

WEYL'S CRITERION IN K DIMENSIONS. *A sequence of vectors $v_1, v_2, \dots \in \mathbb{R}^k$ is uniformly distributed mod one* if and only if *for every $b \in \mathbb{Z}^k$, $b \ne 0$ we have*

$$\left|\sum_{n\le N} e(b.v_n)\right| = o_b(N) \quad \text{as } N \to \infty. \tag{5}$$

We can deduce Kronecker's famous result that if $1, \alpha_1, \alpha_2, \dots, \alpha_k$ are linearly independent over $\mathbb{Q}$ then the vectors $\{(n\alpha_1, n\alpha_2, \dots, n\alpha_k) : n \geq 1\}$ are uniformly distributed mod one.

A final remark on $\{\alpha n + \beta\}_{n\geq 1}$: Let $a_n = \alpha n + \beta \pmod 1$ for all $n \geq 1$. The transformation $T_\alpha : x \to x + \alpha$ gives $T : a_n \to a_{n+1}$. We want to define a measure μ on $\mathbb{R}/\mathbb{Z}$ such that, for any "sensible" set A we have $\mu(A) = \mu(T_\alpha^{-1}A)$. In fact, when $\alpha \notin \mathbb{Q}$, the only invariant such measure, μ, is the Lebesgue measure, and thus the values a_n are distributed according to this measure, that is they are uniformly distributed mod one. See Section 2.4 of Lindenstrauss's paper in this volume (Lindenstrauss, 2006) for more details of this kind of ergodic theoretic proof.

2. Fractional Parts of αn^2

We have seen, in the last section, that any sequence $\{\alpha n + \beta : n \geq 1\}$, with α irrational, is uniformly distributed mod one. One might ask about higher degree polynomials in n. Our goal in this section is to prove the following celebrated theorem of H. Weyl:

THEOREM 2.1. *For any irrational real number α, the sequence $\{\alpha n^2 : n \geq 1\}$ is uniformly distributed mod one.*

For a streamlined proof, see the book (Kuipers and Niederreiter, 1974). Here we will give an argument close to the original:

By Weyl's criterion, we need to show that for fixed integer $b \neq 0$, the "Weyl sum"

$$S_\beta(N) = \sum_{n=1}^{N} e(\beta n^2)$$

is $o_\beta(N)$, where $\beta = b\alpha$. Note that β is also irrational.

Weyl's idea was to *square* the sum and notice that the resulting sum is essentially that of a polynomial one degree lower, that is a linear polynomial. Indeed,

$$|S_\beta(N)|^2 = \sum_{x,y\leq N} e(\beta(x^2 - y^2)) = N + 2\Re \sum_{y>x} e(\beta(y^2 - x^2))$$

Writing $y = x+h$, with $h = 1, \dots, N-1$, $x = 1, \dots, N-h$ we have $y^2 - x^2 = 2hx + h^2$ which is *linear* in x. Thus we find

$$|S_\beta(N)|^2 \;=\; N + 2\Re \sum_{h=1}^{N-1} e(\beta h^2) \sum_{x=1}^{N-h} e(2\beta h \cdot x)$$

$$\leq N + 2\sum_{h=1}^{N-1}\left|\sum_{x=1}^{N-h} e(2\beta h\cdot x)\right|$$
$$\ll N + \sum_{h=1}^{N-1}\min\left\{N, \frac{1}{||2\beta h||}\right\}, \tag{6}$$

proceeding as in (4).

We again use Dirichlet's observation that there exists $q \leq N$ with $||q(2\beta)|| < 1/N$. Let a be the integer nearest $q(2\beta)$; we may assume that $(a, q) = 1$. If $h = H + j$, $1 \leq j \leq q$ then $||2\beta h|| = ||2\beta H + aj/q|| + O(1/N)$; so as j runs from 1 to q the values $||2\beta h||$ (where $h = H + j$) run through the values $||\gamma + i/q||$ for $0 \leq i \leq q - 1$, with error no more than $O(1/N)$, where $|\gamma| \leq 1/2q$. Thus,

$$\sum_{h=H+1}^{H+q}\min\left\{N, \frac{1}{||2\beta h||}\right\} \ll N + \sum_{i=1}^{q/2}\frac{q}{i} \ll N + q\log q.$$

Partitioning the integers up to $N - 1$ into at most $N/q + 1 \leq 2N/q$ intervals of length q or less, we thus deduce, from (6), that

$$\left|\frac{1}{N}S_\beta(N)\right|^2 \ll \frac{1}{q} + \frac{\log q}{N}. \tag{7}$$

Now $q = q_N \to \infty$ as $N \to \infty$ so (7) is $o(1)$ and we are done. To see that $q_N \to \infty$ as $N \to \infty$, suppose not so that $||q(2\beta)|| < \frac{1}{N}$ for infinitely many integers N and thus $||q(2\beta)|| = 0$. But then β can be written as a rational number with denominator $2q$, contradicting hypothesis.

This result is widely applicable and this proof is easily modified to fit a given situation. For example see the proof of Lemma 3.2 in Heath-Brown's paper (Heath-Brown, 2006) in this volume.

A rather elegant ergodic theoretic proof of Theorem 2.1 is given in Section 3 of Lindenstrauss's paper in this volume (Lindenstrauss, 2006).

Theorem 2.1 is a special case of

THEOREM 2.2. *Let $P(x) = a_d x^d + a_{d-1}x^{d-1} + \cdots + a_1 x + a_0$ be a polynomial with at least one of the coefficients $a_1, \ldots a_d$ irrational. Then the sequence $\{P(n) : n \geq 1\}$ is uniformly distributed modulo* 1.

This can be proved along the same lines as Theorem 2.1 (the special case of the polynomial $P(x) = \alpha x^2$) except that a single squaring operation will now produce a polynomial of one degree less, not a linear one. One then iterates this procedure to get back to the case of linear polynomials, see, e.g., (Davenport, 2005) for details.

One can deduce from Weyl's criterion in n-dimension and Theorem 2.2 that the vectors $\{(n\alpha, n^2\alpha, \dots, n^k\alpha)\colon n \geq 1\}$ are uniformly distributed mod one if α is not rational (see also Lindenstrauss's article (Lindenstrauss, 2006) in this volume).

3. Uniform distribution mod N

For a given set A define $A(x) = 1$ if $x \in A$, and $A(x) = 0$ otherwise. Also define the *Fourier transform of* A to be

$$\hat{A}(b) := \sum_n A(n)e(bn) = \sum_{n\in A} e(bn).$$

Writing $A_N = \{a_j : 1 \leq j \leq N\}$ the Weyl criterion becomes that $a_1, a_2, \dots$ is uniformly distributed mod one if and only if $\hat{A}_N(b) = o_b(N)$ for every non-zero integer b.

When A is a subset of the residues mod N we define

$$\hat{A}(b) := \sum_n A(n)e\left(\frac{bn}{N}\right) = \sum_{n\in A} e\left(\frac{bn}{N}\right).$$

Let A be a set of integers, and let $(t)_N$ denote the least non-negative residue of t (mod N) (so that $(t)_N = N\{t/N\}$). The idea of uniform distribution mod N is surely something like: For all $0 \leq b < c \leq 1$ and all $m \not\equiv 0 \pmod N$ we have

$$\#\{a \in A :\ bN < (ma)_N \leq cN\} \sim (c-b)|A|. \tag{8}$$

One can only make such a definition if $|A| \to \infty$ (since this is an asymptotic formula) but we are often interested in smaller sets A, indeed that are a subset of $\{1, 2, \dots, N\}$; so we will work with something motivated by, but different from, (8). Let us see how far we can go to proving the analogy to Weyl's criterion. Fix $\epsilon > 0$:

Define

$$\mathrm{Error}(A;k) := \max_{\substack{0\leq x\leq N\\ m\not\equiv 0 \pmod N}} \left|\#\left\{a \in A : x < (ma)_N \leq x + \frac{N}{k}\right\} - \frac{|A|}{k}\right|.$$

Suppose that $\mathrm{Error}(A;k) \leq \epsilon|A|/k$ for some $k > 1/\epsilon$ We proceed much as in the proof of Weyl's criterion above: Subdivide our interval $(0, N]$ into subintervals $I_j := (jN/k, (j+1)N/k]$, so that if $(ma)_N \in I_j$ then $e(ma/N) = e(j/k) + O(1/k)$. Therefore

$$\begin{aligned}\hat{A}(m) &= \sum_{j=0}^{k-1} \sum_{\substack{a\in A\\ (ma)_N\in I_j}} e(ma/N) = \sum_{j=0}^{k-1} e(j/k) \sum_{\substack{a\in A\\ (ma)_N\in I_j}} 1 + O(|A|/k)\\ &\ll k\,\mathrm{Error}(A;k) + \frac{|A|}{k} \ll \epsilon|A|.\end{aligned}$$

In the other direction our proof is somewhat different from that for Weyl's criterion: We begin by supposing that $|\hat{A}(b)| \le \epsilon^2|A|$ for all $b \not\equiv 0 \pmod N$. For $J = [\delta N]$

$$\sum_{\substack{a\in A\\ 1\le (ma)_N\le J}} 1 = \sum_{j=1}^{J}\sum_{a\in A}\frac{1}{N}\sum_r e\left(r\left(\frac{ma-j}{N}\right)\right) = \frac{J}{N}|A| + \frac{1}{N}\sum_{r\neq 0}\hat{A}(rm)\sum_{j=1}^{J} e\left(\frac{-rj}{N}\right).$$

If r runs through the non-zero integers in $(-N/2, N/2]$ then $|\sum_{j=1}^{J} e(-rj/N)| \ll N/|r|$. Thus the second term here is, for $R \approx N/(\epsilon^2|A|)$

$$\begin{aligned}
&\ll \sum_{r\neq 0}\frac{|\hat{A}(rm)|}{r} \le \sum_{0\le|r|\le R}\frac{|\hat{A}(rm)|}{r} + \sum_{R<|r|\le N/2}\frac{|\hat{A}(rm)|}{r}\\
&\le (\log R)\max_{s\neq 0}|\hat{A}(s)| + \left(\sum_r |\hat{A}(rm)|^2\right)^{1/2}\left(\sum_{R<|r|} 1/r^2\right)^{1/2}\\
&\le (\log R)\epsilon^2|A| + (|A|N/R)^{1/2} \ll \epsilon|A|
\end{aligned}$$

provided $\epsilon \ll 1/\log(N/|A|)$.

One can thus formulate an appropriate analogy to Weyl's criterion along the lines: The Fourier transforms of A are all small if and only if A and all its dilates are "uniformly distributed." (A *dilate* of A is the set $\{ma : a \in A\}$ for some $m \not\equiv 0 \pmod N$.) This result is central to the spectacular recent progress in harmonic analysis by Gowers et. al, (see (Granville et al., 2006)).

To give one example of how such a notion can be used, we ask whether a given set A of residues mod N contains a non-trivial 3-term arithmetic progression? In other words we wish to find solutions to $a + b = 2c$ with $a, b, c \in A$ where $a \neq b$.

PROPOSITION 3.1. *If A is a subset of the residues $\pmod N$ where N is odd, for which $|\hat{A}(m)| < |A|^2/N - 1$ whenever $m \not\equiv 0 \pmod N$ then A contains non-trivial 3-term arithmetic progressions.*

Proof. Since $(1/N)\sum_r e(rt/N) = 0$ unless t is divisible by N, whence it equals 1, we have that the number of 3-term arithmetic progressions in A is

$$\sum_{a,b,c\in A}\frac{1}{N}\sum_r e\left(\frac{r(a+b-2c)}{N}\right) = \frac{1}{N}\sum_r \hat{A}(r)^2\hat{A}(-2r).$$

The $r = 0$ term gives $|A|^3/N$. We regard the remaining terms as error terms, and bound them by their absolute values, giving a contribution (taking $m \equiv -2r \pmod N$)

$$\le \frac{1}{N}\sum_r |\hat{A}(r)|^2 \cdot \max_{m\neq 0}|\hat{A}(m)| = |A|\max_{m\neq 0}|\hat{A}(m)|.$$

There are $|A|$ trivial 3-term arithmetic progressions (of the form a, a, a) so we have established that A has non-trivial 3-term arithmetic progressions when

$$|A|^3/N - |A| \max_{m\neq 0} |\hat{A}(m)| > |A|,$$

yielding the result.

Let us apply Proposition 3.1 to the sets

$$A_\delta := \left\{ n \pmod N : \left\| \frac{n^2}{N} \right\| < \frac{\delta}{2} \right\}$$

for N prime with $0 < \delta < 1$. For $J = [\delta N/2]$ we have

$$\hat{A}_\delta(m) = \sum_n e\left(\frac{mn}{N}\right) \sum_{-J\le j\le J} \frac{1}{N} \sum_r e\left(r\frac{(j-n^2)}{N}\right)$$

so that

$$|\hat{A}_\delta(m)| \le \frac{1}{N} \sum_r \left| \sum_{-J\le j\le J} e\left(\frac{rj}{N}\right) \right| \left| \sum_n e\left(\frac{mn-rn^2}{N}\right) \right|.$$

Now $\sum_n e(mn/N) = 0$ if $m \neq 0$, and $= N$ if $m = 0$. If $r \neq 0$ then $\sum_n e((mn-rn^2)/N)$ is a Gauss sum and so has absolute value $\sqrt{N}$. Moreover $|\sum_{-J\le j\le J} e(rj/N)| \ll N/r$ for $1 \le r \le N/2$. Inputting all this above we obtain $|\hat{A}_\delta(m)| \ll \sqrt{N}\log N$ for each $m \not\equiv 0 \pmod N$ and $\#A_\delta = |\hat{A}_\delta(0)| = \delta N + O(\sqrt{N}\log N)$. Now, for fixed $\delta > 0$ we have proved that each $|\hat{A}_\delta(m)| = o(\delta^2 N)$, and so Proposition 3.1 implies that A_δ contains non-trivial 3-term arithmetic progressions. In fact the proof of Proposition 3.1 yields that A_δ has $\sim \delta^3 N^2$ 3-term arithmetic progressions $a, a+d, a+2d$.

The previous result is in fact a special case of Roth's (Roth, 1953) theorem, which states that for any $\delta > 0$ if N is sufficiently large then any subset A of $\{1, \dots, N\}$ with more than δN elements contains a non-trivial 3-term arithmetic progression. His proof is a little too complicated to discuss in detail here but we will outline the main ideas. If $\delta > \frac{2}{3}$ then A must contain three consecutive integers, so the result follows. Otherwise we proceed by a form of induction, showing that if there exists $A \subset \{1, \dots, N\}$, with $\#A \sim \delta N$, which contains no non-trivial 3-term arithmetic progression then there exists $A' \subset \{1, \dots, N'\}$, with $\#A' \sim \delta' N'$, which contains no non-trivial 3-term arithmetic progression, where $\delta' = (1 + c\delta)\delta$ and $N' = [N^{1/3}]$. The induction then yields Roth's theorem for any $\delta \gg 1/\log\log N$. To prove the induction step we begin by increasing N by a negligible amount so that it is prime, and then considering A as a set of residues mod N. By a slight modification of the proof of Proposition 3.1 one can show that if A does not contain a non-trivial 3-term arithmetic progression then A is not

uniformly distributed mod N. By the definition of uniformly distributed mod N, this implies that there is some dilate of A, say $mA \pmod N$ and some segment $[bN, cN]$ which contains rather more or rather less elements than expected; one can show that, in fact, there must be some segments with rather more, and some segments with rather less. Taking one of these segments with rather more elements than expected, in fact containing $1+c\delta$ times as many elements as expected, we can identify a segment of an arithmetic progression (of length N') within $\{1, \dots, N\}$ which contains $\sim \delta' N'$ elements of A, and from this we construct A' (integer $j \in A'$ if and only if the jth term of the arithmetic progression is in A).

4. Normal Numbers

Are there any patterns in the digits of π? Science fiction writers (Sagan, 1985) would have us believe that secret messages are encoded far off in the tail of π but computational evidence so far suggests the contrary, that there are no patterns, indeed that every sequence of digits appears about as often as in a random sequence. If the digits are written in base 10 then this question is equivalent to asking whether the sequence $\{10^n\pi : n \geq 1\}$ is uniformly distributed mod one? If so we say that π *is normal in base* 10. In general we say that real number α *is normal in base* b if the sequence $\{b^n\alpha : n \geq 1\}$ is uniformly distributed mod one; and that α *is normal*, if it is normal in base b for every integer $b \geq 2$.

In general very little is known about normality. A few specific numbers of very special form can be shown to be normal to certain bases. The one thing that we can show is that almost all numbers are normal, with a proof that fails to identify any such number!

THEOREM 4.1. *Almost all* $x \in [0, 1)$ *are normal.*

(By "almost all" we mean that the set of such x has measure 1.) Theorem 4.1 follows from:

THEOREM 4.2. *For any increasing sequence of integers* $a_1, a_2, \dots$, *the sequence* $\{a_n x : n \geq 1\}$ *is uniformly distributed mod one for almost all* $x \in [0, 1)$.

Deduction of Theorem 4.1. Taking $a_j = b^j$ for each j we see that almost all $x \in [0, 1)$ are normal in base b. Theorem 4.1 follows since the exceptional set has measure 0 as it is a countable union of measure 0 sets.

Proof of Theorem 4.2. We begin by noting that

$$\int_0^1 \left| \frac{1}{N} \sum_{n \leq N} e(ba_n x) \right|^2 dx = \frac{1}{N^2} \sum_{m,n \leq N} \int_0^1 e(bx(a_m - a_n))\, dx = \frac{1}{N};$$

so that

$$\int_0^1 \sum_{m\ge 1}\left|\frac{1}{m^2}\sum_{n\le m^2} e(ba_nx)\right|^2 dx = \sum_{m\ge 1}\frac{1}{m^2} = \frac{\pi^2}{6}.$$

Therefore (in a step that takes some thinking about)

$$\sum_{m\ge 1}\left|\frac{1}{m^2}\sum_{n\le m^2} e(ba_nx)\right|^2 < \infty$$

for almost all x, and so

$$\lim_{m\to\infty}\left|\frac{1}{m^2}\sum_{n\le m^2} e(ba_nx)\right| = 0.$$

Now if $m^2 \le N < (m+1)^2$ then $\sum_{n\le N} e(ba_nx) = \sum_{n\le m^2} e(ba_nx) + O(m)$ and the result follows.

References

Davenport, H. (2005) *Analytic methods for Diophantine equations and Diophantine inequalities*, Cambridge, Cambridge University Press.

Erdős, P. and Turán, P. (1948) On a problem in the theory of uniform distribution I, II, *Indag. Math.* **10**, 370–378, 406–413.

Granville, A., Nathanson, M., and Solymosi, J. (eds.) (2006) *Additive Combinatorics, a school and workshop*, Providence, RI, Amer. Math. Soc., to appear.

Heath-Brown, D. R. (2006) Analytic methods for the distribution of rational points on algebraic varieties, in this volume.

Kuipers, L. and Niederreiter, H. (1974) *Uniform distribution of sequences*, Pure and Applied Mathematics, New York–London–Sydney, Wiley-Interscience.

Lindenstrauss, E. (2006) Three examples of how to use measure classification in number theory, in this volume.

Roth, K. F. (1953) On certain sets of integers, *J. London Math. Soc.* **28**, 104–109.

Sagan, C. (1985) *Contact: A Novel*, New York, Simon and Schuster.

Silverman, J. and Tate, J. (1992) *Introduction to elliptic curves*, New York, Springer-Verlag.

Weyl, H. (1914) Über ein Problem aus dem Gebeit der diophantischen Approximationen, *Nachr. Ges. Wiss. Göttingen (math.-phys. Kl.)* pp. 234–244.

INDEX