Joint work with Jaroslav Hančl and Jean-Louis Verger-Gaugry

On Polynomials in Primes, Ergodic Averages and Monogenic Groups

Speaker: Radhakrishnan Nair

University of Liverpool

7th June 2024

Kronecker's Theorem

For a real number y, let $\{y\}$ denote its fractional part. Also suppose α is an irrational number. Then the sequence $(\{n\alpha\})_{n\geq 1}$ is dense in $[0, 1)$. L. Kronecker 1884.

Nicolai Oresme 1320–1382

One of the theorems of Nicolai Oresme is that for two points moving uniformly and incommensurably along a circle, "no sector of the circle is so small that two such mobiles could not conjunct in it at some point in the future and could not have conjuncted in it at some time in the past." A detailed study of this and related theorems show that he was in pocession of the arguments needed for the proof to be conclusive.

Jan Van Plato, academy of Finland 1993

Uniform Distribution on [0.1)

We say sequence a sequence $x_1, \ldots, x_N, \ldots$ is uniformly distributed modulo one if

$$\lim_{N\to\infty} \frac{1}{N} \#\{1 \le n \le N : \{x_n\} \in I\} = |I|$$

for every interval $I \subseteq [0, 1)$. Here $|I|$ denotes the length of I.

Uniform Distribution on [0.1)

We say sequence a sequence $x_1, \ldots, x_N, \ldots$ is uniformly distributed modulo one if

$$\lim_{N\to\infty} \frac{1}{N} \#\{1 \le n \le N : \{x_n\} \in I\} = |I|$$

for every interval $I \subseteq [0,1)$. Here $|I|$ denotes the length of I. Equivalently:

$$\lim_{N\to\infty} \frac{1}{N} \sum_{n=1}^{N} e^{2\pi i h x_n} = 0,$$

for every $h \in \mathbb{Z}\backslash\{0\}$. (Weyl's Criterion 1916)

Uniform Distribution of Polynomials

Let $\psi(x) = \alpha_0 + \alpha_1 x + \alpha_2 x^2 + \ldots + \alpha_k x^l$, with at least one of the numbers $\alpha_1, \ldots, \alpha_l$ irrational.

Uniform Distribution of Polynomials

Let $\psi(x) = \alpha_0 + \alpha_1 x + \alpha_2 x^2 + \ldots + \alpha_k x^l$, with at least one of the numbers $\alpha_1, \ldots, \alpha_l$ irrational.

Then the sequence $(\psi(n))_{n \geq 1}$ is uniform distribution modulo one. (H. Weyl 1916). (Following earlier independent work of P. Bohl, W. Sierpiński and H. Weyl.)

Uniform Distribution of Polynomials

Let $\psi(x) = \alpha_0 + \alpha_1 x + \alpha_2 x^2 + \ldots + \alpha_k x^l$, with at least one of the numbers $\alpha_1, \ldots, \alpha_l$ irrational.

Then the sequence $(\psi(n))_{n\geq 1}$ is uniform distribution modulo one. (H. Weyl 1916). (Following earlier work and work of P. Bohl, W. Sierpiński and H. Weyl.)

If $(p_n)_{n\geq 1}$ is the sequence of rational primes then $(\psi(p_n))_{n\geq 1}$ is u.d. modulo 1. (I.M. Vinogradov 1937, G. Rhin 1974).

Applying Birkhoff's Theorem

Suppose $\alpha \notin \mathbb{Q}$ and if $f \in L^1([0,1))$. Then

$$\lim_{N\to\infty} \frac{1}{N} \sum_{n=0}^{N-1} f(\{x + n\alpha)\}) = \int_0^1 f(t)dt$$

for almost all x with respect to Lebesgue measure on $[0,1)$.

J.F Koksma, R. Salem 1949

If ψ is as in Weyl's theorem and $f \in L^2([0,1))$ with $f(u) \sim \sum_{n\in\mathbb{Z}} c_n e^{nu}$ and $\sum_{|n|\geq K} |c_n| = O((\log K)^{-\gamma})$ (†) for some $\gamma > 0$. Then

$$\lim_{N\to\infty} \frac{1}{N} \sum_{n=0}^{N-1} f(\{x + \psi(n)\}) = \int_0^1 f(t)dt$$

for almost all x with respect to Lebesgue measure on $[0,1)$.

Can (†) be weakened? R. C. Baker 1983, M. Weber1996. Yes. using Bouragin's ergodic theorem (proof corrected by me) Nair 1996.

Nair 1996

If ψ is as in Weyl's theorem and $f \in L^p([0,1))$ for $p > 1$. Then

$$\lim_{N\to\infty} \frac{1}{N} \sum_{n=0}^{N-1} f(\{x + \psi(n)\}) = \int_0^1 f(t)dt$$

for almost all x with respect to Lebesgue measure on $[0,1)$.

Hančl, Nair, Verger-Gaugry 2024

Using the polynomial in prime ergodic theorem, Wierdl 89, Bourgain 1990, Nair 90,92, Trojan 2019 as follows :

If ψ is as in Weyl's theorem, $(p_n)_{n\geq 1}$ is the sequences of rational primes, and $f \in L^p([0,1))$ for $p > 1$. Then

$$\lim_{N\to\infty} \frac{1}{N} \sum_{n=0}^{N-1} f(\{x + \psi(p_n)\}) = \int_0^1 f(t)dt,$$

for almost all x with respect to Lebesgue measure on $[0,1)$.

p-adic numbers

Let p be a prime. Any nonzero rational number a can be written in the form $a = p^{\alpha}(r/s)$ where $\alpha \in \mathbb{Z}, r, s \in \mathbb{Z}$ and $p \nmid r, p \nmid s$.

Definition

The p-**adic absolute value** of $a \in \mathbb{Q}$ is defined by

$$|a|_p = p^{-\alpha} \quad \text{and} \quad |0|_p = 0.$$

p-adic numbers

Let p be a prime. Any nonzero rational number a can be written in the form $a = p^{\alpha}(r/s)$ where $\alpha \in \mathbb{Z}, r, s \in \mathbb{Z}$ and $p \nmid r, p \nmid s$.

Definition

The p-**adic absolute value** of $a \in \mathbb{Q}$ is defined by

$$|a|_p = p^{-\alpha} \quad \text{and} \quad |0|_p = 0.$$

The p-adic field $\mathbb{Q}_p$ is constructed by completing $\mathbb{Q}$ w.r.t. p-adic absolute value.

p-adic numbers

Let p be a prime. Any nonzero rational number a can be written in the form $a = p^{\alpha}(r/s)$ where $\alpha \in \mathbb{Z}, r, s \in \mathbb{Z}$ and $p \nmid r, p \nmid s$.

Definition

The p-**adic absolute value** of $a \in \mathbb{Q}$ is defined by

$$|a|_p = p^{-\alpha} \quad \text{and} \quad |0|_p = 0.$$

The p-adic field $\mathbb{Q}_p$ is constructed by completing $\mathbb{Q}$ w.r.t. p-adic absolute value.

The p-adic absolute value $|.|_p$ satisfies the following **properties**:

1. $|a|_p = 0$ if and only if $a = 0$,
2. $|ab|_p = |a|_p|b|_p$ for all $a, b \in \mathbb{Q}_p$,
3. $|a + b|_p \leq |a|_p + |b|_p$ for all $a, b \in \mathbb{Q}_p$,
4. $|a + b|_p \leq \max\{|a|_p, |b|_p\}$ for all $a, b \in \mathbb{Q}_p$.

The p-adic absolute value is *non-archimedian*.

The topology of $\mathbb{Q}_p$

Let $a \in \mathbb{Q}_p$ and $r \geq 0$ be a real number.
The **open ball** of radius r and center a is the set

$$\overline{B}(a, r) = \{x \in \mathbb{Q}_p : |x - a|_p < r\}.$$

The **ring of p-adic integers** is the closed set

$$\mathbb{Z}_p = \{x \in \mathbb{Q}_p : |x|_p \leq 1\}.$$

Open sets are also closed and vice versa on the p-adic numbers.

The p-adic integers I

If $\alpha, \beta \in \mathbb{Z}_p$, then $|\alpha|_p \leq 1$ and $|\beta|_p \leq 1$, so we obtain

$$|\alpha\beta|_p = |\alpha|_p |\beta|_p \leq 1 \cdot 1 = 1,$$

and therefore $\alpha\beta \in \mathbb{Z}_p$. Also, we have

$$|\alpha + \beta|_p \leq \max\left(|\alpha|_p, |\beta|_p\right) \leq \max\left(1, 1\right) = 1,$$

so $\alpha + \beta \in \mathbb{Z}_p$. Now we see $\mathbb{Z}_p$ is a commutative ring.

The p-adic integers I

If $\alpha, \beta \in \mathbb{Z}_p$, then $|\alpha|_p \leq 1$ and $|\beta|_p \leq 1$, so we obtain

$$|\alpha\beta|_p = |\alpha|_p |\beta|_p \leq 1 \cdot 1 = 1,$$

and therefore $\alpha\beta \in \mathbb{Z}_p$. Also, we have

$$|\alpha + \beta|_p \leq \max\left(|\alpha|_p, |\beta|_p\right) \leq \max\left(1, 1\right) = 1,$$

so $\alpha + \beta \in \mathbb{Z}_p$. Now we can see that $\mathbb{Z}_p$ is a commutative ring. Furthermore, $|1|_p = 1$. Now if $n \in \mathbb{N}$, then $n = \underbrace{1 + \cdots + 1}_{n \text{ times}}$, so we have

$$|n|_p = |1 + \cdots + 1|_p \leq \max\left(|1|_p, \ldots, |1|_p\right) = 1,$$

and hence $n \in \mathbb{Z}_p$.

The p-adic integers I

Consider the set $\mathbb{Z}_p = \{x \in \mathbb{Q}_p \mid |x|_p \leq 1\}$. We call $\mathbb{Z}_p$ the *p-adic integers*. If $\alpha, \beta \in \mathbb{Z}_p$, then $|\alpha|_p \leq 1$ and $|\beta|_p \leq 1$, so we obtain

$$|\alpha\beta|_p = |\alpha|_p |\beta|_p \leq 1 \cdot 1 = 1,$$

and therefore $\alpha\beta \in \mathbb{Z}_p$. Also, we have

$$|\alpha + \beta|_p \leq \max(|\alpha|_p, |\beta|_p) \leq \max(1, 1) = 1,$$

so $\alpha + \beta \in \mathbb{Z}_p$. Now we can see that $\mathbb{Z}_p$ is a commutative ring. Furthermore, $|1|_p = 1$. Now if $n \in \mathbb{N}$, then $n = \underbrace{1 + \cdots + 1}_{n \text{ times}}$, so we have

$$|n|_p = |1 + \cdots + 1|_p \leq \max(|1|_p, \ldots, |1|_p) = 1,$$

and hence $n \in \mathbb{Z}_p$. We note also that $|-n|_p = |n|_p \leq 1$, so $-n \in \mathbb{Z}_p$. Moreover, $|0|_p = 0 \leq 1$, so $0 \in \mathbb{Z}_p$. We have shown that $\mathbb{Z} \subseteq \mathbb{Z}_p$.

The p-adic integers I

Consider the set $\mathbb{Z}_p = \{x \in \mathbb{Q}_p \mid |x|_p \leq 1\}$. We call $\mathbb{Z}_p$ the *p-adic integers*. If $\alpha, \beta \in \mathbb{Z}_p$, then $|\alpha|_p \leq 1$ and $|\beta|_p \leq 1$, so we obtain

$$|\alpha\beta|_p = |\alpha|_p |\beta|_p \leq 1 \cdot 1 = 1,$$

and therefore $\alpha\beta \in \mathbb{Z}_p$. Also, we have

$$|\alpha + \beta|_p \leq \max(|\alpha|_p, |\beta|_p) \leq \max(1, 1) = 1,$$

so $\alpha + \beta \in \mathbb{Z}_p$. Now we can see that $\mathbb{Z}_p$ is a commutative ring. Furthermore, $|1|_p = 1$. Now if $n \in \mathbb{N}$, then $n = \underbrace{1 + \cdots + 1}_{n \text{ times}}$, so we have

$$|n|_p = |1 + \cdots + 1|_p \leq \max(|1|_p, \ldots, |1|_p) = 1,$$

and hence $n \in \mathbb{Z}_p$. We note also that $|-n|_p = |n|_p \leq 1$, so $-n \in \mathbb{Z}_p$. Moreover, $|0|_p = 0 \leq 1$, so $0 \in \mathbb{Z}_p$. We have shown that $\mathbb{Z} \subseteq \mathbb{Z}_p$.

The p-adic integers II

Every element $\alpha \in \mathbb{Z}_p$ can be expressed as the sum

$$\alpha = \sum_{n=0}^{\infty} a_n p^n,$$

where $a_n \in \{0, 1, \ldots, p-1\}$, and where the sequence (a_n) is uniquely determined by α.
Note this immediately imples $\overline{\mathbb{Z}} = \mathbb{Z}_p$.

The p-adic integers II

Every element $\alpha \in \mathbb{Z}_p$ can be expressed as the sum

$$\alpha = \sum_{n=0}^{\infty} a_n p^n,$$

where $a_n \in \{0, 1, \ldots, p-1\}$, and where the sequence (a_n) is uniquely determined by α.
Note this immediately imples $\overline{\mathbb{Z}} = \mathbb{Z}_p$.
Set theoretically we may write $\mathbb{Z}_p = \Pi_{n=1}^{\infty} X_n$ with $X_n = \{0, 1, \ldots, p-1\}$ for each n.

The p-adic integers II

Every element $\alpha \in \mathbb{Z}_p$ can be expressed as the sum

$$\alpha = \sum_{n=0}^{\infty} a_n p^n,$$

where $a_n \in \{0, 1, \ldots, p-1\}$, and where the sequence (a_n) is uniquely determined by α.
Note this immediately imples $\overline{\mathbb{Z}} = \mathbb{Z}_p$.
Set theoretically we may write $\mathbb{Z}_p = \Pi_{n=1}^{\infty} X_n$ with $X_n = \{0, 1, \ldots, p-1\}$ for each n.
Also $\mathbb{Z}_p$ is a compact topological group under the operation of addition. The set $\mathbb{Z}_p$ being a topological group means the two maps $(x, y) \to x + y$ and $x \to x^{-1}$ for $x, y \in \mathbb{Z}_p$ are continuous in all variables.

Haar measure and characters on the p-adic numbers

For each non-negative integer n and a finite set $A \subseteq \{1, 2, \ldots, a_n\}$, let $\lambda_n(A)$ denote the measure on $\{0, 1, \cdots, a_n - 1\}$ with $a_n = p$ given by $\lambda_n(A) = card(A)/a_n$. Haar measure is the corresponding product measure on $\mathbb{Z}_p$.
The dual group of $\mathbb{Z}_p$, which we denote $\hat{\mathbb{Z}}_p$ consists of all rationals $t = \frac{\ell}{p^r}$ for some non-negative integer r. To evaluate a character χ_t at $x = \sum_{n \geq 0} x_n p^n$ in $\mathbb{Z}_p$ we write

$$\chi_t(x) = e(\frac{\ell}{p^r}(x_0 + px_1 + \cdots + p^{r-1}x_r)),$$

where as usual, for a real number x, $e(x)$ denotes $e^{2\pi ix}$.

Uniform Distribution/Weyl's Criteria on G

Suppose G is a compact topological group with Haar measure λ. We say sequence a sequence $x_1, \ldots, x_N, \ldots$ is uniformly distributed on G if given $f \in C(G)$, we have

$$\lim_{N\to\infty} \frac{1}{N} \sum_{n=0}^{N-1} f(x_n) = \int_G f d\lambda.$$

Equivalently: For every $\chi \neq \chi_0$ in $\hat{G}$ (the dual group of G)

$$\lim_{N\to\infty} \frac{1}{N} \sum_{n=0}^{N-1} \chi(x_n) = 0.$$

In the sequel, we specialize to $G = \mathbb{Z}_p$.

What about the squares in $\mathbb{Z}_p$?

Suppose $N = kp^r + s$ where $s \in [0, p^r - 1] \cap \mathbb{Z}$. Here $k = [\frac{N}{p^r}]$.

$$\sum_{n=1}^{N} \chi_t(n^2) = k \sum_{u=1}^{p^r} e^{2\pi i \frac{l}{p^l} u^2} + \sum_{n=kp^r+1}^{s} \chi_t(n^2).$$

Thus

$$\lim_{N\to\infty} \frac{1}{N} \sum_{n=0}^{N-1} \chi(n^2) = \frac{1}{p^r} \sum_{u=1}^{p^r} e^{2\pi i \frac{l}{p^r} u^2}.$$

What about the squares

Suppose $N = kp^r + s$ where $s \in [0, p^r - 1] \cap \mathbb{Z}$. Here $k = [\frac{N}{p^r}]$.

$$\sum_{n=1}^{N} \chi_t(n^2) = k \sum_{u=1}^{p^r} e^{2\pi i \frac{l}{p^r} u^2} + \sum_{n=kp^l+1}^{s} \chi_t(n^2).$$

Thus

$$\lim_{N\to\infty} \frac{1}{N} \sum_{n=0}^{N-1} \chi(n^2) = \frac{1}{p^r} \sum_{u=1}^{p^r} e^{2\pi i \frac{lu^2}{p^r}}.$$

Set $\frac{l}{p^l}$ to be $\frac{1}{p}$ say. Then a classical identity of C. F. Gauss for 'Gauss sums' says

$$\left| \frac{1}{p} \sum_{u=1}^{p} e^{2\pi i \frac{u^2}{p}} \right|^2 = p.$$

So in particular it is not zero and hence $(n^2)_{n\geq 1}$ can't be uniformly distributed on $\mathbb{Z}_p$. This arguement isn't available for cubes Proving non-uniformity of distribution for higher degree polynomials and much more general totally disconnected groups, is currently open.

What about $(\{n^2\alpha\})_{n\geq 1}$ on $[0,1)$?

$$\left|\sum_{n=1}^{N} e^{2\pi i h n^2 \alpha}\right|^2 = \left(\sum_{n=1}^{N} e^{2\pi i h n^2 \alpha}\right)\left(\overline{\sum_{m=1}^{N} e^{2\pi i h m^2 \alpha}}\right)$$

$$= \sum_{n,m=1}^{N} e^{2\pi i h (n^2-m^2)\alpha} \ll N + \left|\sum_{1\leq m<n\leq N} e^{2\pi i h (n^2-m^2)\alpha}\right|$$

$$\ll N + \left|\sum_{l=1}^{N}\sum_{m=l+1}^{N} e^{2\pi i h ((m+l)^2-m^2)\alpha}\right| = N + \left|\sum_{l=1}^{N}\sum_{m=l+1}^{N} e^{2\pi i h (2ml+l^2)\alpha}\right|$$

$$\ll N + \sum_{l=1}^{N} \frac{1}{|1-e^{2\pi i h l \alpha}|} \ll N + \sum_{l=1}^{N} \frac{1}{\|l\alpha\|} = o(N^2).$$

using diophantine properties of α. Hence $(n^2\alpha)_{n\geq 1}$ u.d. mod. 1.

This is the clue to the difference between connected groups like S^1 and totally disconnected groups likes the p-adic integers.

To sum up

We say $g \in \mathbb{Z}_p$ is a generator if $(ng)_{n\geq 1}$ is dense in $\mathbb{Z}_p$. Suppose one of $\{\alpha_1, \ldots, \alpha_k\} \subset \mathbb{Z}_p$ is a generator and let $\psi(x) = \alpha_0 + \alpha_1 x + \ldots + \alpha_k x^k$. Then if $f \in L^q(\mathbb{Z}_p)$ for $q > 1$ and

$$f(x) \sim \sum_{t \in \hat{\mathbb{Z}}_p} c_t \chi_t(x)$$

the limits,

$$Nf(x) = \lim_{N\to\infty} \frac{1}{N} \sum_{n=0}^{N-1} f(x + \psi(n))$$

and

$$\Pi f(x) = \lim_{N\to\infty} \frac{1}{N} \sum_{n=0}^{N-1} f(x + \psi(p_n))$$

exist almost every where with respect to Haar measure on $\mathbb{Z}_p$,

where

$$Nf(x) = \sum_{t \in \hat{\mathbb{Z}}_p} N_t c_t \chi_t(x),$$

and

$$\Pi f(x) = \sum_{t \in \hat{\mathbb{Z}}_p} \Pi_t c_t \chi_t(x).$$

(from earlier ergodic theorems).

When ψ is linear, then $N_1 = \int_{\mathbb{Z}_p} f dt$, and $N_t \equiv 0$ if $t \neq 0$ and N_t and Π_t are generalizations of Gauss sums.

We can also show that $Nf(x) = \int_{\mathbb{Z}_p} f dl$ and $\Pi f(x) = \int_{\mathbb{Z}_p} f dm$, by the Riesz-representation theorem (for continuous f), which can be shown to be continuous with respect to Haar measure on $\mathbb{Z}_p$. The measures are expected not to be Haar measure, except in special cases but the proofs seem difficult beyond squares.

References

[**AR**] Asmar, N. H. : Nair, Radhakrishnan Certain averages on the a-adic numbers. Proc. Amer. Math. Soc. 114 (1992), no. 1, 21–28.

[**B**] Trojan, B. : Variational estimates for discrete operators modeled on multi-dimensional polynomial subsets of primes. Math. Ann. 374 (2019), no. 3-4, 1597–1656

[**N1**] Nair, R. : On polynomials in primes and J. Bourgain's circle method approach to ergodic theorems. Ergodic Theory Dynam. Systems 11 (1991), no. 3, 485–499.

[**N2**] Nair, R. : On polynomials in primes and J. Bourgain's circle method approach to ergodic theorems. II. Studia Math. 105 (1993), no. 3, 207–233.

[**N3**] Nair, R. : On some arithmetic properties of Lp summable functions. Quart. J. Math. Oxford Ser. (2) 47 (1996), no. 185, 101–105.