Conversations between ergodic theory and number theory

What are the links, and what would a more
effective formulation on either side mean/require?

Tom Ward (UEA) 30/10/09, QMUL

- ergodic theorems I $\leftrightarrow$ normality
- ergodic theorems II $\leftrightarrow$ equidistribution
- recurrence $\leftrightarrow$ Szemerédi
- mixing $\leftrightarrow$ unit theorems
- rigidity $\leftrightarrow$ Littlewood
- growth problems $\leftrightarrow$ Lehmer, Mersenne,...
- UBC $\leftrightarrow$?

Setting:

Ergodic theory studies measurable maps $T : X \to X$ preserving a probability measure; write (and fix) $(X, \mathcal{A}, \mu, T)$.

Often X or T has additional structure (homogeneous space, compact group, metric space, Cantor set, continuous map, group rotation,...) and there are distinguished measures (uniquely invariant, maximizing, algebraic, absolutely continuous,...).

ergodic theorems I $\leftrightarrow$ normality:

Theorem 1 (Birkhoff 1931): Assume that T is ergodic (has no non-trivial measurable invariant sets). Then, given any representative f of an element of L^1_μ, there is a null set $N(f)$ for which

$$\frac{1}{N}\sum_{n=1}^{N-1} f(T^n x) \longrightarrow \int f \,\mathrm{d}\mu$$

for all $x \notin N(f)$.

Theorem 2 (Borel 1909): Lebesgue almost-every $x \in [0,1]$ is *normal* (blocks of j digits appear with frequency b^{-j}) for every base $b \geq 2$.

Th.1 $\Rightarrow$ Th.2 via the fact that $x \mapsto bx$ (mod 1) preserves Lebesgue measure and is ergodic.

- The last statement might be attributed to van Vleck (1908).

- Borel's 1909 paper is "characterized by convenient neglect of error terms in asymptotics, incorrect reasoning, and correct results" (Doob)

ergodic theorems II $\leftrightarrow$ equidistribution:

Theorem 3 (Weyl 1910/Bohl 1909/Sierpiński 1910): Every orbit under the map $x \mapsto x + t$ (mod 1) on $[0, 1)$ is *equidistributed* (asymptotic proportion of time in (a, b) equal to $b - a$) if $t \notin \mathbb{Q}$.

Theorem 4 (Weyl 1916): If p is a polynomial with at least one irrational coefficient, then $\{p(n) \mid n \in \mathbb{N}\}$ is equidistributed modulo 1.

Theorem 5 (old; in Oxtoby 1952): If T is continuous, X a compact metric space, then T has only one invariant Borel probability measure if and only if

$$\frac{1}{N} \sum_{n=1}^{N-1} f(T^n x) \to C(f)$$

for any $f \in C(X)$ and *every* $x \in X$.

Th.5 $\Rightarrow$ Th.3 as it is easy to check that Lebesgue measure is uniquely invariant. Th.4 looks more subtle, but turns out to be a consequence of the same phenomena.

Theorem 6 (Furstenberg 1961): If $T : X \to X$ is uniquely ergodic and $c : X \to G$ is continuous (G a compact group), then for the skew-product map

$$(x, g) \mapsto (Tx, c(x)g),$$

ergodicity implies unique ergodicity.

Th.6 ⇒ Th.4 by expressing 4 as one factor in a uniquely ergodic map on a high-dimensional torus.

- Th. 6 is a consequence of making the right definition of "generic point": $x \in X$ is generic for T and μ if the orbit of x is equidistributed with respect to μ. Lemma: for a continuous map T on a compact metric space, μ-a.e. point is generic for T and μ.

recurrence $\leftrightarrow$ Szemerédi:

Theorem 7 (Szemerédi 1975): A subset S of $\mathbb{N}$ with positive upper Banach density,

$$\limsup_{N-M\to\infty} \frac{|S \cap [M,N]|}{N-M} > 0,$$

contains arithmetic progressions of arbitrary finite length.

Theorem 8 (Furstenberg 1977): If $\mu(A) > 0$ then for any $k \geq 1$ there is some n for which

$$\mu\left(A \cap T^{-n}A \cap T^{-2n}A \cap \cdots \cap T^{-kn}A\right) > 0.$$

Th.8 $\Leftrightarrow$ Th.7, giving a new proof and starting a new field. The connection between them is easy, but both proofs lie quite deep.

- Th. 8 has no hypotheses beyond the setting.
- Effective versions exist, due to Gowers, Tao, and others.
- Th. 8 involves an approach to decomposing measure-preserving maps, and a correspondence principle to translate between ergodic theory and infinite combinatorics.

mixing $\leftrightarrow$ unit theorems:

Theorem 9 (Schlickewei 1990/van der Poorten & Schlickewei 1991): Let K be a field of characteristic zero, $G \subset K \setminus \{0\}$ a finitely-generated multiplicative subgroup, and $a_1, \dots, a_n \in K \setminus \{0\}$. Then

$$a_1 x_1 + \cdots + a_n x_n = 1$$

has only finitely many solutions $(x_1, \dots, x_n) \in G^n$ for which no proper subsum vanishes.

Theorem 10 (Schmidt & Ward 1993): Mixing implies mixing of all orders for $\mathbb{Z}^d$-actions by automorphisms of compact connected abelian groups.

Th.9 $\Leftrightarrow$ Th.10 via Fourier analysis; the connection is easy. Th. 9 is a deep result, and Th. 10 has no other proof.

- Th. 9 has quantitative versions but not effective ones (that is, there are bounds on the number of solutions in terms of K, n, and rank(G) but no bounds on the height of solutions.

- Th. 10 should have various strengthenings in terms of rate of mixing, directional uniformity etc.

- There is an analogous correspondence between mixing on disconnected groups and unit theorems in positive characteristic, due to Masser (2004) but it is different: in particular Th. 10 is false on disconnected groups.

rigidity $\leftrightarrow$ Littlewood:

Let $\langle t\rangle$ denote the distance from $t \in \mathbb{R}$ to the nearest integer.

Conjecture 11 (Littlewood 1930s): $\liminf_{n\to\infty} n\langle nx\rangle\langle ny\rangle = 0$ for every $x, y \in \mathbb{R}$.

The continued fraction expansion of x or y shows this is no more than $\frac{1}{2}$; the point is whether one can do a little better for two different numbers simultaneously.

Conjecture 12 (Margulis, special case): Let A be the group of positive diagonal matrices in $\mathrm{SL}_k(\mathbb{R})$, $k \geq 3$, acting on the space $\mathrm{SL}_k(\mathbb{R})/\mathrm{SL}_k(\mathbb{Z})$. If μ is an A-invariant ergodic probability measure on this space, is there a closed connected group $L > A$ for which μ is the unique L-invariant measure on a single closed L-orbit (that is, is μ automatically algebraic)?

Conj.12 $\Rightarrow$ Conj.11, but more importantly a partial version of Conj. 12 gives a partial Conj. 11.

Theorem 13 (Einsiedler–Katok–Lindenstrauss 2006): Conjecture 12 holds under the additional hypothesis that μ gives positive entropy to some one-parameter subgroup of A. Hence, the set of counterexamples to Conjecture 11 lies inside a countable union of sets of box dimension zero.

This is an instance of "abelian" measure rigidity, in contrast to the rigidity associated to Raghunathan's conjecture, in which individual elements of the action exhibit rigidity.

growth problems ↔ Lehmer, Mersenne,...:

Theorem 14: The set of topological entropies of group automorphisms is the closure of $\{m(f) \mid f \in \mathbb{Z}[x]\}$, where $m(f) = \int_0^1 \log|f(\mathrm{e}^{2\pi\mathrm{i}s})|\,\mathrm{d}s$ and $m(0) := \infty$.

Conjecture 15 (Lehmer 1933): $\inf\{m(f) \mid f \in \mathbb{Z}[x], m(f) > 0\} > 0$.

If Lehmer's conjecture is false, then the set of entropies is $[0, \infty]$; if it is true, then the set of entropies is countable.

- Under a weak hypothesis (ergodic, or mixing, which in this setting really means not having a periodic part) any compact group automorphism is measurably isomorphic to an iid process. Thus we do not know if all iid processes have models as group automorphisms.

- Lehmer's problem has been solved for "non-reciprocal" polynomials and for bounded degree, but remains open.

(Nonsensical) Question: what are the dynamical properties of a “typical” compact group automorphism?

Sample subquestion: Choose a subset S of the primes by throwing a fair coin. What is

$$\limsup_{n\to\infty}\frac{1}{n}\log(2^n-1)\prod_{p\in S}|2^n-1|_p?$$

Easy arguments say this is $\geqslant \frac{1}{2}\log 2$ (Ward 1998) – but it clearly should be $\log 2$ almost surely.

UBC:

Unlike the others, this is simply a conjecture that is simultaneously arithmetical and dynamical.

Uniform Boundedness Conjecture (Morton–Silverman 1994): Given $d \geq 2$, $N \geq 1$, $D \geq 1$ there is a constant $C(d, N, D)$ such that for any number field K with $[K : \mathbb{Q}] \leq D$ and any (finite) morphism $\phi : \mathbb{P}^N \to \mathbb{P}^N$ of degree d defined over K, the number of pre-periodic points of ϕ in $\mathbb{P}^N(K)$ is bounded above by $C(d, N, D)$.

- Northcott gives a non-uniform bound.

- Restricting to $N = 1$, $D = 1$ and degree 4 implies Mazur's theorem (1978) uniformly bounding the size of the torsion subgroup of the $\mathbb{Q}$-points of elliptic curves defined over $\mathbb{Q}$.

- For $N = 1$ and degree 4, it implies Merel's theorem (1996) that the size of the torsion subgroup of an elliptic curve over a number field is bounded in terms of the degree of number field only.

- Fakhruddin (2001) showed that UBC implies there is a constant $C(N, D)$ so that if $[K : \mathbb{Q}] \leqslant D$ and A is an abelian variety defined over K of dimension N, then $|A(K)_{\text{tors}}| \leqslant C(N, D)$.

- If UBC holds for $\mathbb{Q}$, then it holds for number fields.

References:

G. D. Birkhoff, Proof of the ergodic theorem, *Proc. Nat. Acad. Sci. U.S.A.* **17** (1931), 656-660.

P. Bohl, ‘Über ein in der Theorie der säkularen Störungen vorkommendes Problem’, *J. für Math.* **135** (1909), 189–283.

É. Borel, Les probabilités dénombrables et leurs applications arithmétiques, *Rend. Circ. Mat. Palermo* **27** (1909), 247-271.

M. Einsiedler, A. Katok, and E. Lindenstrauss, ‘Invariant measures and the set of exceptions to Littlewood’s conjecture’, *Ann. of Math. (2)* **164** (2006), no. 2, 513–560.

M. Einsiedler and T. Ward, *Ergodic Theory: with a view towards Number Theory*, Springer GTM (to appear), 2010.

N. Fakhruddin, ‘Boundedness results for periodic points on algebraic varieties’, *Proc. Indian Math. Soc.* **111**(2) (2001), 173–178.

H. Furstenberg, ‘Strict ergodicity and transformation of the torus’, *Amer. J. Math.* **83** (1961), 573–601.

H. Furstenberg, ‘Ergodic behavior of diagonal measures and a theorem of Szemerédi on arithmetic progressions’, *J. Analyse Math.* **31** (1977), 204–256.

D. H. Lehmer, ‘Factorization of cyclotomic polynomials’ *Ann. Math.* **34** (1933), 461–479.

D. W. Masser, ‘Mixing and linear equations over groups in positive characteristic’, *Israel J. Math.* **142** (2004), 189–204.

B. Mazur, ‘Modular curves and the Eisenstein ideal’, *IHES Publ. Math.* **47** (1978), 33–186.

L. Merel, ‘Bornes pour la torsion des courbes elliptiques sur les corps de nombres’, *Invent. Math.* **124** (1996), 437–449.

P. Morton and J. H. Silverman, ‘Rational periodic points of rational functions’, *Int. Math. Res. Notices* (2) (1994), 97–110.

D. G. Northcott, ‘Periodic points on an algebraic variety’, *Ann. of Math. (2)* **51** (1950), 167–177.

J. C. Oxtoby, ‘Ergodic sets’ *Bull. Amer. Math. Soc.* **58**, (1952), 116–136.

A. J. v. d. Poorten and H. P. Schlickewei, ‘Additive relations in fields’, *J. Austral. Math. Soc. Ser. A* **51** (1991), no. 1, 154–170.

H. P. Schlickewei, ‘S-unit equations over number fields’, *Invent. Math.* **102** (1990), no. 1, 95–107.

K. Schmidt and T. Ward, ‘Mixing automorphisms of compact groups and a theorem of Schlickewei’, *Invent. Math.* **111** (1993), no. 1, 69–76.

W. Sierpiński, ‘Sur la valeur asymptotique d’une certaine somme’, *Bull Intl. Acad. Polonmaise des Sci. et des Lettres (Cracovie)* (1910), 9–11.

E. Szemerédi, ‘On sets of integers containing no k elements in arithmetic progression’, *Acta Arith.* **27** (1975), 199–245.

E. B. v. Vleck, On non-measurable sets of points, with an example, *Trans. Amer. Math. Soc.* **9** (1908), no. 2, 237-244.

T. Ward, ‘Almost all S-integer dynamical systems have many periodic points’, *Ergodic Th. Dynam. Sys.* **18** (1998), 471–486.

H. Weyl, ‘Über die *Gibbs*sche Erscheinung und verwandte Konvergenzphänomene’, *Rendiconti del Circolo Matematico di Palermo* **30** (1910), 377–407.

H. Weyl, ‘Uber die Gleichverteilung von Zahlen mod Eins’, *Math. Ann.* **77** (1916), 313–352.