EQUIDISTRIBUTION IN NUMBER THEORY

PLAN OF LECTURES

1. Uniform distribution - Granville (1 lecture), Rudnick (1 lecture).

2. Exponential Sums and cryptography - Friedlander (2 lectures) Granville (1 lecture).

3. Spectral Theory - Venkatesh (3 lectures).

4. Hyperbolic geometry, Ergodic theory and Ratner's theorem - Marklof (1 lecture), Lindenstrauss (2 lectures), Venkatesh (1 lecture).

5. Quantum equidistribution- de Bievre (4 lectures), Lindenstrauss (2 lectures), Rudnick (2 lectures), Venkatesh (1 lecture).

6. Distribution of integers and uncertainty principles - Soundararajan (3 lectures), Granville (1 lecture).

7. Distribution of rational points on varieties - Heath-Brown (4 lectures), Tschinkel (3 lectures).

8. Distribution of “special” points - Bilu (3 lectures), Duke (4 lectures), Ullmo (3 lectures).

9. Spacing statistics - Marklof (3 lectures).

10. Invited student lectures on relevant subjects (2 lectures of 1 hour each).

1. Tutorial Uniform distribution

Lecturers: Granville (1 lecture), Rudnick (1 lecture), week 1.

- Uniform distribution modulo 1, Weyl's criterion,
- Examples - irrational rotation, Kronecker's theorem on (unique) ergodicity for tori.
- Fractional parts of xn^2.
- Metric theorems, normal numbers.

Background reading[1]:

L. Kuipers and H. Niederreiter, *Uniform distribution of sequences*, New York: John Wiley & Sons, 1974.

2. Distribution of integers and uncertainty principles

Lecturers: Granville (1 lecture, week 1), Soundararajan (3 lectures, week 2)

- Basics of probabilistic number theory, including Erdos-Kac Theorem.

[1] Bibliographic references will be made available at the library.

- Distribution of primes via prime k-tuples conjecture and perhaps via n-level correlations of zeros.
- Distribution of arithmetic sequences in arithmetic progressions:Siegel-Walfisz and Bombieri-Vinogradov in some generality. Uncertainty principle for such distributions.

Bibliography:

P.X. Gallagher, "On the distribution of primes in short intervals", *Mathematika* **23** (1976), pp. 4-9.

E. Bombieri, "Le Grand Crible dans la theorie analytique des nombres", *Astérisqu*e **18** (1987), 103 p.

H.L. Montgomery and K. Soundararajan, "Primes in short intervals", *Communications in Math. Physics* **252** (2004), pp. 589-617.

H. Maier, "Primes in short intervals", *Michigan Math. J.* **32** (1985) pp.221-225.

A. Granville and K. Soundararajan, "An uncertainty principle for arithmetic sequences", preprint available at www.arxiv.org.

3. Exponential Sums and cryptography

- Estimates for exponential sums, Gauss sums, Kloosterman sums, and their uses. Statistical attacks on the Diffie-Hellmann protocol.

Lecturer: Friedlander, 2 lectures, week 2.

- The Bourgain and Bourgain-Konyagin theorems.

Lecturer: Granville, 1 lecture. week 2.

Bibliography:

W.D. Banks, J.B. Friedlander, S.V. Konyagin, and I.E. Shparlinski, "Incomplete exponential sums and Diffie--Hellman triples'", *Math. Proc. Cambridge Phil. Soc.,* to appear.

J. Bourgain, Estimates on exponential sums related to Diffie-Hellman distributions', *Comptes Rendus Mathematique*, **338** (2004), pp. 825-830.

R. Canetti, J. B. Friedlander, S.Konyagin, M.Larsen, D.Lieman and I.E.Shparlinski, "On the statistical properties of Diffie–Hellman distributions", *Israel J. Math*., **120** (2000), pp. 23-46.

J. B. Friedlander, S. V. Konyagin and I.E.Shparlinski, "Some doubly exponential sums over Z_m", *Acta Arith.* **105** (2002), pp. 349-370.

J. B. Friedlander, C.Pomerance and I.E.Shparlinski,"Period of the power generator and small values of Carmichael's function", *Math. Comp.* **70** (2001), pp. 1591-1605 (see also **71** (2002), pp. 1803-1806).

J. B. Friedlander and I.E.Shparlinski, "On the distribution of the power generator", *Math. Comp.* **70**, (2001), pp. 1575-1589.

M. Z. Garaev, "Double exponential sums related to Diffie–Hellman distributions", Preprint, 2004.

4. Tutorial: Spectral theory of automorphic forms

Lecturer: Venkatesh, 3 lectures, week 1.

- The modular group, congruence groups, unit groups of quaternion algebras. Hecke operators.
- Spectral theory: compact quotients, The Laplacian and its spectral resolution. Eisenstein series. Maass waveforms and their L-functions. Weyl's law.
- Trace formulae: Selberg and Kuznetsov (as required for applications).
- A survey of higher rank generalizations - the Hilbert modular group, Siegel upper half-space, GL(n).

Bibliography:

Henryk Iwaniec and Emmanuel Kowalski, *Analytic number theory*, American Mathematical Society: Providence (RI), 2004.

Henryk Iwaniec, *Spectral methods of automorphic forms*, (2nd ed.), American Mathematical Society: Providence (RI), *Revista Matemática Iberoamericana*, Madrid, 2002.

Peter Sarnak, *Some applications of modular forms,* Cambridge Tracts in Mathematics 99. Cambridge University Press: Cambridge, 1990.

5. Ergodic theory and Ratner's theorem

Lecturers: Marklof, Venkatesh, Lindenstrauss.

- Basics of hyperbolic geometry: The hyperbolic metric, rigid motions, discrete groups,geodesics and horocycles.Representation of the geodesic and horocycle flows in terms of right translation on $\Gamma\backslash PSL(2,\mathbf R)$.

  Lecturer: Marklof, 1 lecture, week 1 (day 1).

- Mixing of the geodesic and horocycle flows.

  Lecturer: Venkatesh, 1 lecture, (end of) week 1.

- Basics on ergodic theorems, shearing properties, Ratner theorem statement in general, proof in basic case of $SL(2,\mathbf R)$.

  Lecturer: Lindenstrauss, 2 lectures, week 2.

Bibliography:

S. V. Fomin, I. P. Kornfeld and I. Grigorevich Sinai, *Ergodic Theory*, New York: Springer Verlag, (1982).

6. Quantum equidistribution

This topic has its roots in the physicists' studies on ``quantum chaos'', in particular on the statistical properties of high-energy stationary states of simple quantum mechanical systems whose classical counterpart is chaotic. The corresponding mathematical theory is difficult and general results are largely lacking, with the notable exception of the quantum ergodicity theorem, first formulated by A. Schnirelman in the early 1970's. Of special interest to us is the notion that in a chaotic system, quantum particles should be equidistributed in a suitable sense. Special models with underlying arithmetic structure have recently been studied,

giving rise to various problems of interest to number theorists. Among these are the Quantum Unique Ergodicity conjecture for negatively curved manifolds (Rudnick and Sarnak) and analogues for quantum maps. Special cases of these conjectures have been proved, for the cat map by Kurlberg and Rudnick and for compact congruence surfaces by Lindenstrauss.

6.1 Classical and quantum mechanics, quantum ergodicity

Lecturer: de Bievre, 4 lectures, week 1.

- General background on classical mechanics.
- Quantum mechanics.
- Statement of Egorov's theorem and the quantum ergodicity theorem.
- Quantum maps: Background, proof of Egorov, quantum ergodicity.

Bibliography:

S. De Bievre, “Quantum chaos: a brief first visit, course notes for a Course taught at the Cuernavaca Summer School in Harmonic Analysis and Mathematical Physics, June 2000, *Contemporary Mathematics* **289**, pp. 161-218 (2001).

M. Degli Esposti and S. Graffi (Eds.), *The Mathematical Aspects of Quantum Maps*, Springer Lecture Notes in Physics 618, New York : Springer, (2003), pp. 91-144.

6.2 Quantum Unique Ergodicity for congruence surfaces

Lecturers: Lindenstrauss and Venkatesh, 3 lectures, week 2.

- The quantum unique ergodicity conjecture. An overview of the proof.

  Lecturer: Lindenstrauss, 1 lecture.

- Arithmetic quantum limits have positive entropy,

  Lecturer: Venkatesh, 1 lecture.

- Cartan actions and how ergodic theory can bootstrap the positive entropy into equidistribution.

  Lecturer: Lindenstrauss, 1 lecture.

6.3 The arithmetic theory of quantum maps

Lecturer: Rudnick, 2 lectures, week 2.

Quantum maps are popular model for studying the problems of quantum chaos. An exceptionally tractable case is that of linear toral automorphisms (``cat maps''), which is that of a hyperbolic element of the modular group acting on the torus. A quantum analogue of this system was proposed by Hannay and Berry in 1980. Kurlberg and Rudnick found that this quantum system admits many hidden symmetries, closely analogous to the Hecke operators in the theory of modular forms. For the desymmetrized system, they were able to prove quantum unique ergodicity in 2000. Remarkably it was later discovered (by Faure, Nonnenmacher and de Bievere 2003) that without taking into account the Hecke operators we can get ``scars'', that is counter examples to QUE. This model continues to provide new opportunities for number theorists to provide insight into the problems of quantum chaos.

Bibliography:

M. Degli Esposti and S. Graffi (Eds.), *The Mathematical Aspects of Quantum Maps*, Springer Lecture Notes in Physics 618, New York : Springer, (2003).

7. DISTRIBUTION OF RATIONAL POINTS ON VARIETIES

Lecturers: Heath-Brown, Tschinkel, week 2.

The topic is a very old one in number theory: Given a system of Diophantine equations which has infinitely many solutions (rational or integer), to find the asymptotic number of solutions of bounded ``height''. About 15 years ago, some conjectures of Manin created a new wave of interest in this issue.

In addition to the question of the asymptotic count of the number of solutions, an interesting question is to study their distribution, for instance when and where do the solutions become equidistributed.

7.1 Tutorial: The circle method

Lecturer: Roger Heath-Brown, 3 lectures, week 1.

An exposition of the circle method and applications, with sketches of the proofs. No prerequisites will be assumed in the lectures. For instance, will show how to count number of points of bounded height on hypersurface - one equation in many variables.

Suggested reading:

R.C. Vaughan, *The Hardy-Littlewood Method*, Cambridge Tracts in Mathematics no. 125,Cambridge: Cambridge University Press, (1997).

H. Davenport, Edited and prepared for publication by T.D. Browning, *Analytic Methods for Diophantine Equations and Diophantine Inequalities* (2^{nd} Ed.),Cambridge: Cambridge University Press, 2005.

7.2 Algebro-geometric setting

Lecturer: Yuri Tschinkel, 2 lectures, week 2.

- Classification of varieties, rational varieties, canonical versus anti-canonical, Fano varieties, Naive theory of heights, statement of Manin's conjectures.

  1 lecture

- Relatively self-contained examples using algebro-geometric tools, maybe del-Pezzo surfaces ?

  1 lecture

Bibliography:

Marc Hindry and Joseph H. Silverman, *Diophantine geometry*, New York: Springer-Verlag,(2000).

Miles Reid, “Complex algebraic geometry”, *Chapters on algebraic surfaces,* Park City (UT): Amer. Math. Soc., 1997.

Robin Hartshorne, *Algebraic geometry*, New York: Springer-Verlag, 1977.

Yu. I. Manin, *Cubic forms*, Amsterdam: North-Holland Publishing Co., 1986.

Serge Lang, *Number theory III: Diophantine geometry,* Berlin: Springer-Verlag, 1991.

7.3 Combinations of analytic and algebro-geometric methods

Examples in which success has required a combination of methods from Analytic Number Theory and Diophantine Geometry.

Lecture: Heath-Brown, 1 lecture, week 2.

7.4 Homogeneous varieties via spectral theory and Ratner theory.

- Projective spaces and Grassmanians via Eisenstein series. Toric, additive or some spherical varieties using harmonic analysis techniques.

Lecturer: Tschinkel, 1 lecture, week 2.

8. Distribution of ``special'' points

Lecturers: Bilu, Duke, Ullmo, week 1.

This section addresses “special” points on varieties. Examples are: torsion points on group varieties, CM-points on modular varieties,Hecke orbits, Galois orbits. There are various results about finiteness properties and restrictions on the location of such points. For instance a paper of Lang from 1965 it is shown that an irreducible curve in the affine plane contains only finitely many torsion points, that is points whose coordinates are roots of unity, unless it is a (multiplicative) translate of a subgroup by torsion point, that is after translation it is of the form $x^m=y^n$ or $x^my^n=1$. The corresponding assertion in the context of on abelian varieties was related to the Mordell conjecture, subsequently proved by Faltings. Generalizations of this were formulated by Mumford, Bogomolov and recently by Andre and Oort in the context of Shimura varieties, partially motivated by results in transcendence theory such as the Siegel-Schneider theorem that the value of the j-function at an algebraic number are algebraic exclusively at CM-points.

In some cases, once the location of the special points (that is their Zariski closure) is determined, one knows that the points are equidistributed there, in a suitable sense. In the context of CM-points, the paradigm here is Duke's theorem.

The goal of this summer school is to make these results and conjectures comprehensible to an audience which does not have background in arithmetic algebraic geometry, complex multiplication/Shimura varieties, or the analytic theory of automorphic forms.

8.1 Small points and the Andre-Oort conjecture.

- The Siegel-Schneider theorem and the origins of the Andre-Oort conjecture in transcendence theory.

Overview and introduction to the Andre-Oort conjecture and CM-points, the Manin-Mumford conjectures and Bogomolov's conjecture.

Lecturer: Ullmo, 1 lecture, week 1.

- Lang's theorem on torsion/division points on curves (needs very little prerequisites).

Lecturer: Bilu, 1 lecture, week 1.

- The case of the multiplicative group: Galois orbits, Bilu's theorem. An overview of the case of abelian varieties.

  Lecturer: Bilu, two lectures, week 1.

- Generalizations - more advanced cases, the role of GRH, the use of Ratner theory. Andre-Oort for products of modular curves. Equidistribution of subgroups of group varieties

  Lecturer: Ullmo, 2 lectures, week 2.

Bibliography:

Yu Bilu, "Limit distribution of small points on algebraic tori", *Duke Math. J.* **89** (1997), 465-476.

L. Clozel, H. Oh and E. Ullmo, "Hecke operators and equidistribution of Hecke Points », *Invent. Math.* **144**, (2001), p. 327-351.

L. Clozel and E. Ullmo, "Equidistribution des points de Hecke, *Contributions to Automorphic Forms, Geometry and Arithmetic, A Volume in Honnor of Joseph Shalika*, H. Hida, D. Ramakrishnan and F. Shahidi (Eds.),Baltimore: Johns Hopkins University Press, 2004.

L. Clozel and L. Ullmo, "Equidistribution de sous-variétés spéciales », to appear in *Annals of Maths*.

L. Clozel and E. Ullmo, « Equidistribution de mesures algébriques », to appear in *Compositio*.

W. Duke, "Hyperbolic distribution problems and half integral weights Maass-forms", Invent. Math. **92**, no 1, (1988) p. 73-90.

B. Edixhoven and A. Yafaev, "Subvarieties of Shimura varieties", *Ann. Math*. **157** (2) (2003), p. 621-645.

M. Mignotte, « Sur un théorème de M. Langevin », *Acta Arith*. **54** (1989), p. 81-86.

Th. Ransford, *Potential Theory in the Complex Plane*, Cambridge: Cambridge University Press, 1995.

L. Szpiro, E. Ullmo and S. Zhang, "Equidistribution des petits points", *Inventiones* **127** (1997), p. 337-347.

E. Ullmo, Positivité et discrétion des points algébriques des courbes, *Annals of Maths* **147** (1998), 167–179.

E. Ullmo, Théorie Ergodique et Géométrie Algébrique. *Proceedings of the International Congress of Mathematicians*, Beijing 2002, Higher Education Press, Vol II, 197–206.

E. Ullmo, Equidistribution de sous-variétés spéciales II, preprint 2005.

D. Zagier, "Algebraic numbers close to both 0 and 1", *Math. Comp*. **61** (1993), 485-491.

S. Zhang, Equidistribution of small points on abelian varieties, *Annals of Maths* **147** (1998), 159–165.

8.2 Equidistribution of CM points - Duke's theorem

Lecturer: Duke, 4 lectures, week 1

Bibliography:

Henryk Iwaniec and Emmanuel Kowalski, *Analytic number theory*, American Mathematical Society: Providence (RI) 2004.

Henryk Iwaniec, *Spectral methods of automorphic forms* (2nd ed.), American Mathematical Society: Providence (RI), *Revista Matemática Iberoamericana*, Madrid, 2002.

Henryk Iwaniec, *Topics in classical automorphic forms,* American Mathematical Society: Providence (RI), 1997.

Sarnak, Peter *Some applications of modular forms*, Cambridge: Cambridge University Press, 1990.

9. SPACINGS AND LATTICE POINTS

Lecturer: Marklof, 3 lectures, week 2

- Spacing statistics: Definitions, spacing statistics in mathematical physics, conjectures about integrable systems, examples of Poisson statistics.
- Lattice points, Heath-Brown's theorem and Bleher's work, the Gaussian regime (Hughes-Rudnick).
- Pair correlation for tori: Sarnak, Eskin-Margulis-Mozes and Marklof.

10. INVITED LECTURES

Lecturers: Andrei Yafaev, Gergely Gharcos

10.2 Andre-Oort conjecture : Andre-Oort conjecture, different approaches to conjecture and results obtained so far

10.3 The subconvexity problem for Rankin-Selberg L-functions in the level aspect: I will sketch the proof of a general subconvex bound in the level aspect for Rankin-Selberg L-functions associated with two primitive holomorphic or Maass cusp forms on the upper half-plane. The proof was completed in joint work with Michel, based on earlier work of Kowalski-Michel-VanderKam and Michel. The result implies the equidistribution of incomplete Galois orbits of Heegner points on Shimura curves associated with indefinite quaternion algebras over Q.