

Curriculum Vitae  
**Harald HELFGOTT**

*Adresse professionnelle :*

Harald Helfgott  
ENS-DMA  
45 rue d'Ulm  
F-75230 Paris  
France

*Adresse personnelle :*

H. A. Helfgott  
13 avenue Reille  
Paris 75014  
France

*Tél :* +33 (0)1.44.32.37.85

*Mail :* [harald.helfgott@dma.fr](mailto:harald.helfgott@dma.fr)

*Web :* [www.math.ens.fr/~helfgott](http://www.math.ens.fr/~helfgott)

## Données personnelles

Nom : Harald Andrés HELFGOTT  
Date de naissance : 25 nov. 1977 à Lima (Pérou)  
État civil : célibataire  
Nationalité : péruvienne  
Titre : Philosophiae doctor (PhD) en mathématiques  
Qualifié en section 25 aux fonctions de professeur des universités  
Habilitation à diriger des recherches (Paris-Sud)

## Formation

2003 Doctorat de Mathématiques, Princeton University, sous la direction de H. Iwaniec.  
Jury : H. Iwaniec, N. Katz, P. Sarnak, A. Wiles. Thèse :

*Root numbers and the parity problem*

1998 Bachelor of Arts summa cum laude, Brandeis University ; mention très honorable en mathématiques ; mention très honorable en informatique. Mémoire :

*Edge effects on local statistics in lattice dimers :  
a study of the Aztec diamond (finite case)*

## Activité professionnelle

2014– Directeur de Recherche 2ème classe, CNRS, Université de Paris VI/VII  
2010–2014 Chargé de Recherche 1ère classe, CNRS, École Normale Supérieure  
2009–2011 Reader, University of Bristol (en congé 2010-2011)  
2006–2009 Lecturer, puis Senior Lecturer (2008–2009), University of Bristol  
2004–2006 Chercheur post-doctoral, CRM-ISM-Université de Montréal  
Research Assistant Professor, Concordia University  
2003–2004 Gibbs Assistant Professor, Yale University  
1998–2003 Assistant de recherche et enseignement, Princeton University  
1995–1997 Assistant d'enseignement, Brandeis University

## Sujets de recherche

Théorie analytique des nombres, Théorie des groupes, Combinatoire additive, Géométrie diophantienne, Théorie probabiliste des nombres.

## Prix

2014 Chaire Gabriel Lamé (France/Russie : Université de l'État de Saint Pétersbourg)  
2013 Professeur honoraire (Universidad Nacional Mayor de San Marcos, Lima, Pérou, et Universidad Nacional San Antonio Abad, Cusco, Pérou)  
2011 Prix Adams (Cambridge)  
2010 Prix Whitehead (London Mathematical Society)  
2008 Prix Philip Leverhulme  
2007 Advanced Research Fellowship (Engineering and Physical Sciences Research Council)

## Cours enseignés

oct–nov 2012	Teoría de grupos	3ème cycle	UAM (Madrid)
fev 2012	Leçons d'arithmétique	M1	ENS
nov–déc 2009	Galois theory	1er cycle	Bristol
août–déc 2006	Group theory	1er cycle	Bristol
août–déc 2005	Ordinary differential equations	1er cycle	Concordia
août–déc 2004	Ordinary differential equations	1er cycle	Concordia
jan–mai 2004	Arithmetic	3ème cycle	Yale
août–déc 2003	Introduction to number theory	1er cycle	Yale
août–déc 2003	Multivariable calculus	1er cycle	Yale
jan–mai 2003	Multivariable calculus	1er cycle	Princeton

## Cours extrascolaires enseignés

juillet 2014	Growth in groups and applications	IHÉS (Bures-sur-Yvette)
avr 2012	Crecimiento y diámetro en los grupos finitos	USACH (Santiago, Chili)
mar 2012	Téoría analítica de números	IMPA (Lima, Pérou)
jan 2011	La croissance dans les groupes	EPFL (Lausanne, Suisse)
oct 2010	Ideas analíticas en la teoría de números	UNMSM (Lima, Pérou)
sep 2010	Ideas analíticas en la teoría de números	UMSA (La Paz, Bolivie)
août 2010	Growth in linear algebraic groups	TIFR (Mumbai, Inde)
mars–avr 2008	A brief course in arithmetic combinatorics	IMSc (Chennai, India)
sep 2007	Azar y aritmética. Combinatoria aditiva	U. de Huamanga (Pérou)
été 2007	Azar y aritmética	UNMSM (Lima, Pérou)
fev 2007	Probabilidades e Teoria dos Números	IMPA (Brésil)
juin 2005	Normas, desigualdades y dualidad	U. de la Habana (Cuba)
mars 2004	Ideas geométricas en la teoría de números	IMCA (Lima, Pérou)

## Articles

### *Mathématiques pures*

28. On the dimension of additive sets (avec P. CANDELA), prépublication.
27. Random generators of the symmetric group : diameter, mixing time and spectral gap (avec Á. Seress et A. Zuk), à paraître à *J. of Algebra*.
26. The ternary Goldbach conjecture is true, prépublication.
25. Major arcs for Goldbach's problem, prépublication.
24. Numerical verification of the ternary Goldbach conjecture up to  $8.875e30$  (avec D. Platt), à paraître à *Experiment. Math.*
23. Growth in groups : ideas and perspectives, à paraître à *Bull. of the Am. Math. Soc.*
22. On growth in an abstract plane (avec N. GILL et M. RUDNEV), à paraître à *Proc. of the Am. Math. Soc.*
21. Minor arcs for Goldbach's problem, prépublication.
20. Bounds on the diameter of Cayley graphs of the symmetric group (avec J. BAMBERG, N. GILL, T. HAYES, Á. SERESS, P. SPIGA), *J. Algebraic Combin.* 40 (2014), no. 1, 1–22.
- Th3. Groupes, courbes et croissance, mémoire d'habilitation, Paris-Sud (Orsay).
19. Square-free values of  $f(p)$ ,  $f$  cubic, à paraître à *Acta Math.*
18. On the diameter of permutation groups (avec Á. SERESS), à paraître à *Annals of Math.*
17. Deterministic methods to find primes (comme *D. H. J. Polymath*, avec T. TAO et E. CROOT), *Math. Comp.* 81 (2012), no. 278, 1233–1246.
16. Growth in solvable subgroups of  $GL_r(\mathbb{Z}/p\mathbb{Z})$  (avec N. GILL), à paraître à *Math. Annalen*. 15. Growth of small generating sets in  $SL_n(\mathbb{Z}/p\mathbb{Z})$  (avec N. GILL), *Int. Math. Res. Notices*, Vol. 2011, 4226–4251.
14. An explicit incidence theorem in  $\mathbb{F}_p$  (avec M. RUDNEV), *Mathematika*, 57 (2011), no. 1, 135–145.
13. Improving Roth's theorem in the primes (avec A. de ROTON), *Int. Math. Res. Notices*, Vol. 2011, 767–783.
12. Growth in  $SL_3(\mathbb{Z}/p\mathbb{Z})$ , *J. Eur. Math. Soc. (JEMS)*, vol. 13, no. 3, pp. 651–851.

11. Power-free values, repulsion between points, different beliefs and the existence of error, *Anatomy of Integers*<sup>1</sup>, 81–88, Amer. Math. Soc., Providence, RI, 2008.
10. How small must ill-distributed sets be? A two-dimensional large sieve (with A. VENKATESH), *Analytic number theory : essays in honor of Klaus Roth*, 224–234, Cambridge U. Press, 2009.
9. Growth and generation in  $SL_2(\mathbb{Z}/p\mathbb{Z})$ , *Ann. of Math.* **167** (2008), no. 2, 601–623.
8. Power-free values, large deviations and integer points on irrational curves, *J. Théor. Nombres Bordeaux* **19** (2007), 433–472.
7. The parity problem for irreducible polynomials, soumis, 11 pages.
6. The parity problem for reducible polynomials, *J. London Math. Soc. (2)* **73** (2006), no. 2, 415–435.
5. Integral points on elliptic curves and 3-torsion in class groups (avec A. VENKATESH), *J. Amer. Math. Soc.* **19** (2006), no. 3, 527–550.
4. Root numbers and ranks over global function fields (avec B. CONRAD et K. CONRAD), *Adv. Math.* **198** (2005), 684–731.
3. On the square-free sieve, *Acta Arith.* **115** (2004), 349–402.
2. On the behaviour of root numbers in families of elliptic curves, soumis, 65 pages.
0. Root numbers and the parity problem, thèse de doctorat, Princeton University, juin 2003.
1. Enumeration of tilings of diamonds and hexagons with defects (avec I. M. GESSEL), *Electron. J. Combin.* **6** (1999), no. 1, R16, 26 pp.
00. Edge effects on local statistics in lattice dimers : a study of the Aztec diamond (finite case), mémoire, Brandeis University, mai 1998.

#### *Monographies – mathématiques pures*

M1. *Azar y aritmética*, *Monografías del Instituto de Matemática y Ciencias Afines*, 50. Instituto de Matemáticas y Ciencias Afines (IMCA), Lima, Pérou, 2010.

#### *Pédagogie et histoire*

- PH3. A modern vision of the work of Cardano and Ferrari on quartics, *CONVERGENCE* (avec M. HELFGOTT), an online journal of the Mathematical Association of America, July 2009.
- PH2. A noncalculus proof that Fermat’s principle of least time implies the law of refraction (avec M. HELFGOTT), *Am. J. Phys.* **70** (2002), no. 12, 1224–1225.
- PH1. Maxima and minima before Calculus (avec M. HELFGOTT), *Pro Mathematica* XII (1998), nos. 23–24, 135–158.

#### *Informatique*

- I3. Lossless image compression by block matching (avec J. A. STORER), *Comput. J.* **40** (1997), no. 2/3, 137–145.
- I2. Asymmetry in Ziv/Lempel ’78 Parsing (avec M. COHN), 320–328, en *Compression and complexity of sequences : proceedings, 1997*, IEEE, Los Alamitos, CA, IEEE Computer Society Press, 1997.
- I1. On Maximal Parsings of Strings (avec M. COHN), 291–299, en *Proceedings DCC ’1997 : Data Compression Conference* IEEE, Los Alamitos, CA, 1997.

#### **Exposés pléniers et autres conférences choisies**

- |         |   |
|---------|---|
| 8/2014  | The ternary Goldbach problem, exposé invité, ICM 2014, Séoul, Corée.  |
| 8/2014  | The ternary Goldbach problem, Eleventh Algorithmic Number Theory Symposium ANTS-XI, Gyeongju, Corée (exposé plénier).           |
| 6/2014  | Conjecture de Goldbach, Colloque Jeunes Chercheurs, Université de Bordeaux 1 (trois exposés ; conférencier plénier).            |
| 5/2014  | The ternary Goldbach problem, CANT (Combinatorial and Analytic Number Theory) 2014, New York, USA. Série plénière de 4 exposés. |
| 4/2014  | The ternary Goldbach conjecture, British Mathematical Colloquium 2014, Queen Mary University London ( <i>morning talk</i> ).    |
| 05/2013 | The ternary Goldbach conjecture, Mathematische Arbeitstagung 2013, Max Planck Institute for Mathematics, Bonn, Allemagne.       |
| 4/2010  | Growth in linear algebraic groups, Analytic Number Theory, Göttingen, Allemagne (trois exposés ; conférencier plénier).         |

---

1. Actes de congrès.

## Autres exposés à des conférences et colloques

- 7/2014 The ternary Goldbach problem, First Joint International Meeting RSME-SCM-SEMA-SIMAI-UMI, Bilbao, Espagne.
- 6/2014 Growth in groups : ideas and perspectives, Mathematics Colloquium, Göttingen, Allemagne.
- 6/2014 Die schwache Goldbachsche Vermutung, Marburg-Gießen Kolloquium, Marburg, Allemagne.
- 5/2014 Random generators of the symmetric group : diameter, mixing time and spectral gap, Workshop : Finding Algebraic Structures in Extremal Combinatorial Configurations, IMPA, UCLA, États-Unis.
- 5/2014 Growth in groups : ideas and perspectives, MSRI, Berkeley, États-Unis.
- 5/2014 The ternary Goldbach conjecture, Helvetic Algebraic Geometry, Château Mercier, Sierre, Suisse.
- 2/2014 La conjetura débil de Goldbach, ICMAT, Madrid, Espagne.
- 2/2014 The ternary Goldbach problem, Automorphic forms and arithmetic, Göttingen, Allemagne.
- 10/2013 The ternary Goldbach problem, Analytic number theory, MFO (Mathematisches Forschungsinstitut Oberwolfach), Oberwolfach, Allemagne.
- 08/2013 The ternary Goldbach problem, Workshop on Combinatorics, Number Theory and Dynamical Systems, IMPA (Instituto Nacional de Matemática Pura e Aplicada), Rio de Janeiro, Brésil.
- 06/2013 La conjecture ternaire de Goldbach, Etienne Fouvry 60th birthday conference, CIRM, Luminy.
- 11/2012 Towards the ternary Goldbach conjecture, Conference on Zeta functions, Université Indépendante de Moscou.
- 11/2012 Hacia la conjetura ternaria de Goldbach, Coloquio de matemáticas, Universidad Autónoma de Madrid, Espagne.
- 10/2012 Higher-dimensional sieves, Arithmetic Geometry, Centro di Ricerca Matematica Ennio de Giorgi, Scuola Normale Superiore, Pisa, Italie.
- 7/2012 On the diameter of permutation groups, Additive Combinatorics in Paris, Institut Henri Poincaré, Paris.
- 6/2012 Minor arcs for Goldbach's problem, Analytic methods for diophantine problems, Mathematisches Institut, Göttingen, Allemagne.
- 6/2012 Minor arcs for Goldbach's problem, Annual Meeting of the Canadian Number Theory Association, Lethbridge, AB, Canada.
- 3/2012 The diameter of permutation groups, International Number Theory Conference in Memory of Alf van der Poorten, Newcastle, Australia.
- 12/2011 Growth in permutation groups, International Meeting on Number Theory, Harish-Chandra Research Institute, Allahabad.
- 12/2011 Grupos y diámetros : ideas y perspectivas, Séminario IMPA/CNRS, IMPA, Rio de Janeiro, Brésil.
- 6/2011 Growth in groups : an overview, Young workshop in arithmetics and combinatorics, Madrid, Espagne.
- 5/2011 Growth in solvable groups, Resonances in mathematical physics, Peyresq, France.
- 3/2011 Finding primes deterministically, Discrete analysis, Newton Institute, Cambridge, Royaume-Uni.
- 3/2011 Finding primes deterministically, Colloquium, Durham University, Royaume-Uni.
- 2/2011 Growth in solvable groups, Group Actions in Analytic Number Theory, Lausanne, Suisse.
- 1/2011 Growth and expansion in groups, Group Actions in Analytic Number Theory, Lausanne, Suisse (trois exposés).
- 12/2010 Comment améliorer le théorème de Roth sur les nombres premiers, Arithmétique Lille-Litoral 2010, Lille, France.
- 8/2010 Improving Roth's theorem in the primes, ICM-Zeta satellite conference, IMSc, Chennai.
- 6/2010 Growth in solvable groups, Conference on Zeta functions, Université Indépendante de Moscou.

## Exposés à des conférences et colloques (cont.)

- 5/2010 Growth and expansion : an overview, Expansion in Groups, Imperial College, Londres, Royaume-Uni.
- 4/2010 Growth in finite simple groups, Number theory days, ETHZ, Zurich, Suisse.
- 3/2010 Growth in simple groups of Lie type, Conference in honor of Laci Babai's 60th Birthday, OSU, Columbus, Ohio, États-Unis.
- 3/2010 Growth in simple groups of Lie type, Workshop on graphs and arithmetic, CRM, Montréal, QC, Canada.
- 11/2009 Growth of small subsets in  $SL_n(\mathbb{F}_p)$ , Géométrie, dynamique et représentations des groupes, CIRM, Luminy, France.
- 7/2009 Exponential sums and the large sieve, Activités analytiques et additives à Lille, U. de Lille 1, France.
- 11/2008 Growth in  $SL_3(\mathbb{F}_p)$ , Discrete rigidity phenomena in additive combinatorics, MSRI, Berkeley, CA, États-Unis.
- 4/2008 Growth in  $SL_3(\mathbb{F}_p)$ , Groups and geometries, Oberwolfach, Allemagne.
- 4/2008 Growth in  $SL_3(\mathbb{F}_p)$ , Clay-Fields conference on additive combinatorics, number theory and harmonic analysis, Fields Institute, Toronto, ON, Canada.
- 4/2008 Growth in  $SL_3(\mathbb{F}_p)$ , Analytic number theory, Oberwolfach, Allemagne.
- 2/2008 Growth in linear algebraic groups : an approach via incidence, Expanders in pure and applied mathematics, Institute for Pure and Applied Mathematics, UCLA, Los Angeles, CA, États-Unis.
- 7/2007  $p^3 + 2$  is square-free infinitely often, Diophantine equations via analytic number theory, University of Bristol, Royaume-Uni.
- 5/2007  $p^3 + 2$  is square-free infinitely often, School and conference on analytic number theory, International Centre for Theoretical Physics, Trieste, Italy.
- 9/2006  $p^3 + 2$  is square-free infinitely often, India-UK number theory conference, Institute of Mathematical Sciences, Chennai (Madras), India.
- 4/2006 Growth and generation in  $SL_2(\mathbb{Z}/p\mathbb{Z})$ , Workshop on additive combinatorics, CRM (Centre de Recherches Mathématiques), Montréal, QC, Canada.
- 3/2006 Power-free values, points on curves, large deviations and modularity, Anatomy of Integers, CRM (Centre de Recherches Mathématiques), Montréal, QC, Canada.
- 12/2005 Larger and better sieves?, Workshop on gaps between primes, AIM, Palo Alto, CA, États-Unis.
- 11/2005 Growth and generation in  $SL_2(\mathbb{Z}/p\mathbb{Z})$ , Workshop on Lie groups, representations and discrete mathematics, Institute for Advanced Studies, Princeton, NJ, États-Unis.
- 10/2005 Growth and generation in  $SL_2(\mathbb{Z}/p\mathbb{Z})$ , Colloque en l'honneur d'Henryk Iwaniec, Bordeaux, France.
- 7/2005 Growth and generation in  $SL_2(\mathbb{Z}/p\mathbb{Z})$ , Journées arithmétiques, Marseille, France.
- 6/2005 Growth and generation in  $SL_2(\mathbb{Z}/p\mathbb{Z})$ , Canadian Mathematical Society summer meeting, Waterloo, ON, Canada.
- 5/2005 Growth and generation in  $SL_2(\mathbb{Z}/p\mathbb{Z})$ , Conférence en théorie analytique des nombres, Université Laval, QC, Canada.
- 4/2005 Growth and generation in  $SL_2(\mathbb{Z}/p\mathbb{Z})$ , Conference in Honor of Paul Monsky, Brandeis, Waltham, MA, États-Unis.
- 12/2004 Power-free values of polynomials with prime arguments, CMS winter meeting, Montréal, QC, Canada.
- 11/2004 Power-free values of polynomials and integer points on irrational curves, Diophantine approximation and analytic number theory, Banff International Research Station, Banff, AB, Canada.
- 4/2004 Integral points on elliptic curves and 3-torsion in class groups, AMS sectional meeting, Lawrenceville, NJ, États-Unis.
- 4/2004 On the behavior of root numbers in families of elliptic curves, Atelier sur la théorie spectrale et les formes automorphes, Montréal, QC, Canada.
- 12/2003 Elliptic curves, square-free numbers and class groups, Brandeis-Harvard-MIT-Northeastern joint mathematics colloquium, Brandeis U., Waltham, MA, États-Unis.

## Exposés à des conférences et colloques (cont.)

- 5/2003 Root numbers, the square-free sieve and elliptic curves, Workshop on automorphic L-functions, Fields Institute, Toronto, ON, Canada.
- 6/2001 The average of the Moebius function on polynomials and the average root number of a family of elliptic curves, Premières journées du Nord sur les nombres premiers, Lille I, France.
- 5/2001 The average of  $\mu$  on integers represented by a polynomial of degree greater than two and its relation to the average root number in families of elliptic curves, Seaway number theory conference, Carleton University, Ottawa, ON, Canada.
- 7/2000 Curvas elípticas y números primos, XX Coloquio de la Sociedad Matemática Peruana, Lima, Perú.

Plus de 55 exposés invités à des séminaires.

## Encadrement d'étudiants doctoraux et post-docs

- 2010–2014 1 Postdoc (Pablo Candela), 1 étudiante doctorale (Alisa Sedunova), supervision d'étudiants de M1/M2, DMA, ENS, Paris, France
- 2006–2010 1 Postdoc (Nick Gill), 1 étudiant doctoral (Dave Mendes da Costa)  
Département de mathématiques, Université de Bristol, Royaume-Uni

## Organisation de conférences

- 2015 AGRA 2015 (Aritmética, grupos y análisis), école d'été, Cusco, Peru. Coorganisateurs (comité scientifique) : G. Tornaría, C. G. Moreira.
- 2015 Growth, symbolic dynamics and combinatorics of words in groups, conférence, ENS, Paris, France. Coorganisateurs : A. Erschler, K. Juschenko.
- 2014 Arithmetic and allied subjects on the banks of the Neva, Saint-Pétersbourg, Russie. Coorganisatrice (comité scientifique) : K. Juschenko.
- 2012 AGRA (Aritmética, grupos y análisis), école d'été, Santiago, Chili. Coorganisateurs : A. Navas, C. G. Moreira.
- 2010 AQUA (Analytic questions in arithmetic), école d'été, Tata Institute, Mumbai, Inde. Coorganisateurs : A. Gorodnik, J. Sengupta.

## Fonctions administratives et/ou responsabilités collectives

- 2013– Membre du comité éditorial de la *Revista Matemática Iberoamericana*
- 2013– Membre correspondant de l'*Academia Nacional de Ciencias del Perú*.
- 2012/13 Directeur du séminaire d'élèves de théorie analytique des nombres à l'ENS
- 2008/09 Coorganisateur de groupes de travail de théorie des nombres et théorie ergodique à Bristol
- 2005 Organisateur du séminaire de théorie combinatoire additive à Montréal
- 2005/06 Coorganisateur du séminaire de théorie analytique des nombres à Montréal
- 2004/05 Organisateur du séminaire de théorie des nombres à Yale University

Membre de juries de doctorat et d'habilitation. Rapporteur pour divers journaux mathématiques (dont *Ann. of Math.* et *Invent. Math.*), pour *Engineering and Physical Sciences Research Council (EPSRC)* (évaluation de projets) et pour *Mathematical reviews*.

## Connaissances en informatique

Programmation : C, Scheme.

Logiciels scientifiques : SAGE, PARI, Gnuplot, LaTeX.

## **Langues**

Espagnol : langue maternelle. Utilisée dans un cadre professionnel.

Anglais et français : lus, parlés et écrits couramment. Utilisés dans un cadre professionnel.

Allemand et espéranto : lus, parlés et écrits couramment.

Russe et grec ancien : Niveau intermédiaire.

Quechua, polonais : Notions de base.