CURRICULUM VITAE: JILL PIPHER

EDUCATION

B.A. in Mathematics, UCLA, 1979
PhD. in Mathematics, UCLA, 1985, Harmonic Analysis

PROFESSIONAL EXPERIENCE

2011-2013 President, Association for Women in Mathematics
2010 - present, Director, Institute for Computational and Experimental Research in Mathematics, Brown University
1994 - present, Professor, Brown University
1989-1994, Associate Professor, Brown University
1987-1990, Assistant Professor, University of Chicago
1985-1987, L. E. Dickson Instructor, University of Chicago

AWARDS AND HONORS

Elected Fellow of the American Mathematical Association, Inaugural class
NSF Mathematics Institute Award, 2010
NSF Postdoctoral Fellowship, 1987-90
Alfred P. Sloan Foundation Fellowship, 1989-93
Presidential Young Investigator Award, 1990-95
Mathematical Sciences Research Inst. Research Professor, 1997

GRANTS

1. Sloan Foundation B2012-38, Blackwell-Tapia Conference grant, $30.000, (Administered by: Brown U.)
2. American Institute of Mathematics, Research grant SQuaREs program: 2011-2014, three funded research meetings at AIM.
3. Australia Research Council Grant, Discovery Project DP120100399, with X. Duong (MacQuarie University, M. Lacey (Georgia Tech), and L. Ward (University of South Australia), 2012-2014, $270,000 (Administered by: U. of South Australia)
5. NSF DMS-091153249 Virtual Institute: Mathematical and Statistical Sciences, 2011-2013, Science Across Virtual Institutes pilot program, $420,664, (Administered by: Brown U.).
6. NSF DMS-0931908 Institute award, 2010-2015: $15,500,000 (Administered by: Brown U.)

7. National Security Agency: AWM Workshops and Their Impact, 2011-2013, $81,000, (Administered by: AWM)

8. NSF DMS-0901139 Research Grant, 2009-2013, $435,307 (Administered by: Brown U.)

9. US Department of Energy: Recognition of and activities for women in the mathematical sciences, 2011-2014, $120,000, (Administered by: AWM)

PATENTS

1. 6,081,597 Hoffstein , Pipher, Silverman: Public key cryptosystem method and apparatus, awarded June 27, 2000

2. 6,298,137 Hoffstein, Pipher, Silverman: Ring-based public key cryptosystem method, awarded October 2, 2001

3. 7,308,097 Hoffstein, Howgrave-Graham, Pipher, Silverman, Whyte: Digital signature and authentication method and apparatus, awarded December 11, 2007

4. 7,913,088 Hoffstein, Howgrave-Graham, Pipher, Silverman, Whyte: Digital signature and authentication method and apparatus, awarded March 22, 2011

RESEARCH AND PUBLICATIONS

1.Bounded double square functions, Ann. Inst. Fourier 2, (1986), p. 69-82.

2. Journe's covering lemma and its extension to higher dimensions, Duke J. Math. 53 (3) (1986), p. 683-690

3. Hardy spaces and the Dirichlet problem on Lipschitz domains, with C. Kenig, Revista Iberoamericana 3 (2) (1987), p. 191-247

4. Oblique derivative problems on Lipshitz domains with L^p data, with C. Kenig, Amer. J. Math. 110 (4) (1988), p. 715-738

5. Oblique derivative problems for the Laplacian in Lipschitz domains, Revista Iberoamericana 3 (3) (1988), p.455-471

6. The h-path distribution of the lifetime of conditioned Brownian motion for non-smooth domains, with C. Kenig, Probab. Th. Rel. Fields 82 (1989), p. 615-623

7. Area integral estimates for biharmonic functions, with G. Verchota, TAMS 327 (2) (1991), p. 903-918

8. The theory of weights and the Dirichlet problem for elliptic equations, with R. Fefferman and C. Kenig, Annals of Math. 134 (1991)p. 65-124

9. The Dirichlet problem in L^p for biharmonic functions on Lipschitz domains, with G. Verchota, Amer. J. Math. 114 (1992), p. 923-972

10. The maximum principle for biharmonic functions, with G. Verchota, Comm. Math. Helv. 68 (1993), p. 385-414

11. Co-editor, Partial Differential Equations with Minimal smoothness and Applications, IMA Vol 42, Springer-Verlag, 1992

12. A martingale inequality related to exponential square integrability, PAMS 118 (2) (1993)

13. Maximum principles for polyharmonic functions in Lipschitz and C^1 domains, with G. Verchota, J. Potential Analysis 4 (1995), p. 615-636

14. The Neumann problem for elliptic equations with non-smooth coefficients, with C. Kenig, Inventiones Math. 113 (1995), p.447-509

15. Boundary value problems for higher order operators, Fourier Analysis and Partial Differential Equations: Proceedings of the El Escorial Conference, edited by J. Garcia-Cuerva et al, Chapter 20 (1995), CRC Press.

16. Review of: Harmonic Analysis Techniques in Second Order Elliptic PDE, by Carlos Kenig, Bulletin of the AMS 33 (2) (1996), p. 229-236

17. Dilation invariant estimates and a boundary Garding inequality, with G. Verchota, Annals of Math. 14 (1995), p. 1-38

18. The Neumann and regularity problem for second order divergence form equations, Part II, with C. Kenig, Duke J. Math. 81 (1) Special volume in honor of J. Nash (1995), p. 227-250

18. Area integral estimates for higher order elliptic equations and systems, with B. Dahlberg, C. Kenig and G. Verchota, Annals L'Inst. Fourier 47 (1997), p.1425-1461

20. A convexity property of eigenvalues and applications, with W. Beckner and C. Kenig, manuscript

21. Littlewood-Paley estimates: some applications to elliptic boundary value problems, CRM Proceedings and Lecture Notes 12 (1997), p. 221-238.

22. Vector potential theory on non-smooth domains in $\mathbf{R}^3$, and applications to electromagnetic scattering with D. Mitrea and M. Mitrea, J. Fourier Analysis and Appl. 3 (2) (1997), p. 131-192

23. Multiparameter operators and sharp weighted inequalities, with R. Fefferman, American J. Math. 119 (2) (1997), p. 337-370

24. The inhomogeneous Dirichlet problem for Δ^2 in Lipschitz domains, with V. Adolfsson, J. Funct. Anal. 159 (1998), p. 137-190

25. The absolute continuity of elliptic measure revisited, with C. Kenig, J. of Fourier Analysis and Applications (4) (1998), p. 463-468

26. NTRU: a ring based public key cryptosystem, with J. Hoffstein and J. Silverman, Algorithmic Number Theory (ANTS III), J. Buhler (ed.), Lecture Notes in Computer Science 1423, Springer-Verlag (1998), p. 267-288

27. A new approach to the absolute continuity of elliptic measure, with applications to nonsymmetric equations, with H. Koch, C. Kenig and T. Toro, Advances in Math. 153 (2000), p.231-298.

28. NSS: An NTRU lattice-based signature scheme, with J. Hoffstein and J. Silverman, Proceedings of Eurocrypt 2001.

29. The Dirichlet problem for elliptic equations with drift terms, with C. Kenig, Publicaciones Matematiques 45 (2001), 199-217.

30.Five lectures on NTRU encryption and digital signatures, L'Institut Fourier, Grenoble, 2002 Summer School in Cryptology

31. NTRUSign: Digital Signatures using the NTRU lattice, with N. Howgrave-Graham, J. Hoffstein, J. Silverman, W. Whyte, CT-RSA 2003 Proceedings.

31. Biparameter paraproducts, with C. Muscalu, T. Thiele, T. Tao, Acta Mathematica 193 (2004), p. 269-296.

32. Multiparameter paraproducts, with C. Musalu, T. Thiele, T. Tao, Rev. Mat. Iberoamericana Volume 22, Number 3 (2006), 963-976.

33. A covering lemma for rectangles in $\mathbb{R}^n$, with R. Fefferman, Proc. AMS 133, No.11 (2005), p.3235-3241.

34. Variations on the theme of Journe's lemma, with C. Cabrillo, M. Lacey, and U. Molter, Houston J. Math., Vol. 32 (3), (2006), p. 833-863

35. On estimating the lattice security of NTRU, with N. Howgrave-Graham and J. Hoffstein, submitted

36. BMO from Dyadic BMO on the bidisc, with L. Ward, Journal London Math. Soc., Vol. 77 No. 2, 2008, p. 524-544.

37. The L^p Dirichlet Problem for second order elliptic operators and a p-adapted square function, with M. Dindos and S. Petermichl, J. Funct. Anal. Vol. 249, issue 2, 2007. pl 372-392.

38. Multiparamater Riesz Commutators, with M. Lacey, S. Petermichl, and B. Wick, American Journal of Mathematics, Volume 131, Number 3, June 2009, pp. 731-769

39. Introduction to Mathematical Cryptography, by J. Hoffstein, J. Silverman, J. Pipher, Book, 500 pages, Springer Undergraduate Texts in Mathematics, August 2008.

40. Iterated Riesz Commutators: a simple proof of boundedness, with M. Lacey, S. Petermichl, B. Wick, Proceedings of Analysis at El Escorial 2008, published 2009.

41. Geometric-arithmetic averaging of dyadic weights with L. Ward and X. Xiao, Rev. Mat. Iberoamericana Volume 27, Number 3 (2011), 953-976.

42. Weak-star convergence in multiparameter Hardy spaces, with S. Treil, to appear in Proc. of Amer. Math. Soc.

43. BMO solvability and the A^∞ condition for elliptic operators, with M. Dindos, C. Kenig, Special Edition of J. Geometric Analysis, Volume 21, Number 1, January 2011 , pp. 78-95(18)

44. Directional discrepancy in two dimensions with D. Bilyk, X. Ma, and C. Spencer, to appear in Bulletin of the London Math. Society.

45. Practical Lattice-based cryptography: NTRUEncrypt and NTRUSign, w. J. Hoffstein, N. Howgrave-Graham, W. Whyte, Chapter 11 in The LLL Algorithm: Survey and Applications, p. 340-390, published by Springer, 2010.

46. Multiparameter Div-Curl identities, with M. Lacey, S. Petermichl, and B. Wick, Bull. London Math. Soc. (2012) 44 (6): 1123-1131

47. Harmonic Analysis on chord-arc domains, with E. Millakis and T. Toro, to appear J. Geometric Analysis.

48. One parameter and multi-parameter function classes are intersections of finitely many dyadic classes, with Ji Li and L. Ward, submitted for publication.

49. Square function/nontangential maximal function estimates, and the Dirichlet problem for second order non-symmetric elliptic equations, with S. Hofmann, C. Kenig, and S. Mayboroda, submitted for publication.

50. Perturbations of elliptic operators in chord arc domains, with T. Toro and E. Milakis, submitted for publication.

51. Boundary value problems for elliptic operators satisfying a Carleson condition, with M. Dindos and D. Rule, submitted.

SELECTED INVITED LECTURES 2002-present

Invited Speaker, Grenoble Summer School in Cryptology: 5 lectures on NTRU encryption and digital signatures, June 2002

Plenary Lecturer at NSF supported 6th annual New Mexico Analysis Conference, March 2003

Invited speaker, joint AMS-RSME meeting, Seville, Spain, June 2003

Invited Speaker, Fabes-Chiarenza International Conference, Siracusa, Italy, December 2003.

Invited Speaker, Fabes-Riviere International Conference, Minneapolis, Minnesota, April 2004

Invited Lecturer, Women's Program at IAS : 5 lectures on analysis for the graduate course, one research lecture, May 2004.

University of Edinburgh, The Maxwell Institute Analysis Seminar, October 2005.
Invited Lectures at University of Virginia, 2006

The Inaugural Virginia Chatelain Distinguished Lecture, Kansas State University, 2006.

Invited Speaker, Conference in Harmonic Analysis and PDE, Beijing, June 2007

Plenary Speaker, Lars Ahlfors Centenary Celebration, Helsinki, Finland, August 2007.

Special Colloquium, The Martha Davenport Heard Lecture at Wellesley College, October 2007.

Jean Ryan Memorial Lecture, Purdue University, October 2008.

Invited Lecturer, Nanyang Technical University, Singapore, December 2008.

Coxeter Lectures at the Fields Institute in Toronto, Feb. 2008.

CRM European Math Institute Conference Lecture, Barcelona, June 2009.

Women in Mathematics at MIT, Invited speaker, January 2010.

Invited Speaker, February Fourier Talks, Norber Wiener Institute, February 2010.

Invited Lecture, Harmonic Analysis Conference in Honor of R. Wheeden, Sevilla Spain, June 2010.

Invited Public Lecture, Institute for Mathematics and its Application (IMA), March 2011.

Invited Lecture, Mathematics Department, Zhongshan University, Guangzhou China, March 2011.

NSF-MPS Distinguished Lecture, April 2011.

MAA Distinguished Lecture, Carriage House, Washington D.C., April 2012.

Invited Lecture series, Institute for Mathematics for Industry, U. of Kyushu, Fukuoka, Japan, November 2012

SELECTED BROWN UNIVERSITY SERVICE 2000-2012

President's Lectures Advisory Committee, Brown University, 2013

Brown Commencement Forum: with Jeff Hoffstein, David Mumford, and Bjorn Sandstede, May 2011

Undergraduate Task Force, Fall 2007

Dean of the College Search Committee, spring 2005

Academic Priorities Committee , 2003-2004

WISE faculty advisor/mentor, 2000-present

University Nominations Committee, 2001

Inaugural Committee - Faculty forums, Inaugural Weekend, 2001

Provost Search Committee, fall 2000

RECENT PROFESSIONAL SERVICE

Springer Advisory Board, Undergraduate and Graduate Texts in Mathematics Series

President, Association for Women in Mathematics, Feb. 1, 2011 - Feb. 1, 2013

Organizer, AWM Research Symposium, Santa Clara University, March 2013, NSA and NSF funded

Organizer, AWM: 40 years and counting Conference at Brown University, NSF funded, 325 participants, Sept. 2011

Organizer, Geometry Discreptancy SQuares conference, American Institute of Mathematics, Palo Alto, CA, May 2010

Organizer, Workshop on Elliptic Boundary Value Problems, Banff International Research Station, April 2010

Associate Editor, Potential Analysis, 2010-2012

Organizer, Discrepancy Theory: Pure and Applied, American Inst. Mathematics Workshop, December 2008

NSF Panelist, Individual Research Grants in Harmonic Analysis, PDE, and Focused Research Grants.

SELECTED DEPARTMENTAL SERVICE 2000-2012

Brown SUMS faculty coordinator 2002-present.

Acting Department Graduate Advisor, Jan. 2009 - June 2009.

Mathematics-Applied Mathematics WISE affinity group faculty advisor

Department Chair, January 2005 - June 2008

PhD Students: Nancy Lim, Sanja Hukovic, Danielle Jamison, Camil Muscalu, Xiao Xiao, Xaiomin Ma, Theresa Anderson (current), Yumeng Ou (current).

Colloquium Chair, September 2010 - December 2010