Curriculum Vitae: Jill C. Pipher

ACADEMIC DEGREES

B.A. in Mathematics, UCLA, 1979

PhD. in Mathematics, UCLA, 1985, Harmonic Analysis

PROFESSIONAL EXPERIENCE

2017 - present, Vice President for Research, Brown University

2019 - 2021, President, American Mathematical Society

2013 - present, Elisha Benjamin Andrews Professor, Mathematics, Brown University

2011-2013, President, Association for Women in Mathematics

2010 - 2016, Founding Director, NSF Institute for Computational and Experimental Research in Mathematics, Brown University

1999, Co-founder, Ntru Inc.

1994-2013, Professor of Mathematics, Brown University

1989-1994, Associate Professor of Mathematics, Brown University

1987-1990, Assistant Professor, Mathematics, University of Chicago

1985-1987, L. E. Dickson Instructor, University of Chicago

AWARDS AND HONORS

Fellow of the Society for Industrial and Applied Mathematicians, 2019

Eisenbud Professor at Mathematical Sciences Research Institute, 2017

Elected Fellow of the American Academy of Arts and Sciences, 2015

Invited speaker, International Congress of Mathematicians, Seoul 2014

Elected Fellow of the American Mathematical Society, Inaugural class, 2012

NSF Mathematics Institute Awards, 2010, 2015

Research Professor, Mathematical Sciences Research Institute, 1997

Presidential Young Investigator Award, 1990-95

Alfred P. Sloan Foundation Fellowship, 1989-93

NSF Postdoctoral Fellowship, 1987-90

RECENT GRANTS and RESEARCH AWARDS

NSF DMS-1929284: 2020 - 2025; Institute for Computational and Experimental Research in Mathematics (Co-PI)

NSF DMS-1439786: 2015-2020; Institute for Computational and Experimental Research in Mathematics, $17.550,000 (PI)

Australia Research Council Grant, Discovery Project DP160100153, with X. Duong (MacQuarie University), M. Lacey (Georgia Tech), J. Li and L. Ward (University of South Australia), 2015-2018, $363,100 (Administered by: Macquarie University, Australia)

NSF DMS-0931908 Institute for Computational and Experimental Research in Mathematics, 2010-2015: $15,500,000 (PI)

PATENTS

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

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

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

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

SELECTED INVITED LECTURES 2006-present

AMS Congressional Briefing, Quantum Science and Cryptography, Washington DC, December 2019

Transatlantic University Forum for Women, Fondation L'Oréal Women in Science Panelist, Boston, September 2019

Invited speaker, Complex Analysis and its applications, Seattle, August 2019

Invited speaker, International Conference in Harmonic Analysis and PDE, Helsinki, June 2019

UConn Mathematics Distinguished Lecture, April 2019

The Dean's Lecture, Temple University, March 2019

Invited Speaker, Conference in Analysis and PDE, Instituto de Ciencias Matemticas, June 2018

Invited Colloquium Speaker, Institute for Advanced Study Women in Mathematics Conference, Princeton, May 2018

Stelson Lecture, Georgia Inst. of Technology, February, 2018

Plenary speaker, 20th anniversary Nebraska Conference for Undergraduate Women in Mathematics, January 2018

AWM-AMS Noether Lecture; Joint Mathematics Meeting, January 2018

Clanton Lecture, Furman University, November 2017

Invited Speaker, The AMSI/AustMS 2017 Workshop in Harmonic Analysis and PDE, July 2017

Zhu Kezhen Distinguished Lectures: Zhejiang University, Hangzhou, China, June 2017

Mathematical Association of American, Golden Section Invited Speaker, March 2017

Mathematical Sciences Research Institute Connections for Women Workshop, January 2017

Excelsior Lectures, Rochester University, September 2016

Invited Mini-Course and Conference Speaker, Centre de Recerca Matimatica, Barcelona, Spain, June 2016

Presidential Award Lecture at Brown University, April 2016

Annual Sampson Lectures, Bates College, March 2016

Science Sundays, Public Lecture at Ohio State University, February 2016

Plenary Speaker, AMS Eastern Sectional Meeting, Rutgers, NJ, November 2015

Invited Speaker, International Conference in Harmonic Analysis and Partial Differential Equations, ICMS, Edinburgh, July 2015

Annual Maheshwari Colloquium Address, University of Albany, April 2015

Distinguished Colloquium, University of British Columbia - Pacific Institute Mathematical Sciences, March 2015

AWM Research Symposium Plenary Speaker, University of Maryland, March 2015

Plenary Speaker, ANZIAM2014: Joint Meeting of Australia and New Zealand Math Societies, Melbourne, December 2014.

Invited Speaker, Conference in Harmonic Analysis and PDE in Honor of C. Kenig, Chicago, September 2014

Invited Speaker, Analysis Section, International Congress of Math. Seoul, Korea. August 2014

Invited Speaker, Conference in Harmonic Analysis and PDE, Sydney, Australia, July 2014

The Hayden-Howard Lecture, Mathematics, U. of Kentucky, April 2014

MAA Invited Address, Joint Mathematics Meeting, Baltimore, MD, January 2014

Plenary Speaker, Korean Women in Mathematical Sciences International Conference, KIAS, Korea, June 2013

The Gentry Lectures, Wake Forest University, April 2013

Keynote Speaker, Career Options for Women Workshop, IMA, March 2013

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

Class of 1960 Speaker and William Oliver lecturer, Williams College, September 2012.

Mathematics Association of America Distinguished Lecture, Carriage House, Washington D.C., April 2012.

National Science Foundation-Mathematics and Physical Sciences Distinguished Lecture, April 2011.

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

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

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

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

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

Invited Lecture, European Mathematics Institute Conference, Barcelona, June 2009.

Coxeter Lectures at the Fields Institute, Toronto, February, 2008.

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

Jean Ryan Memorial Lecture, Purdue University, October 2008.

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

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

Invited Speaker, International Conference in Analysis and Partial Differential Equations, Beijing, June 2007

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

Invited Lecture Series, University of Virginia, 2006

SELECTED PROFESSIONAL SERVICE

Member, Board on Mathematics Sciences and Analytics (BMSA), National Academies of Sciences, Engineering, Medicine, 2018-2021

Member, Science Advisory Board, Mathematics and Physical Sciences, Simons Foundation, 2016-2019

Subcommittee Chair, NSF-Division of Mathematical Sciences Committee of Visitors, September, 2016

Member, Mathematics Research Communities Advisory Board for the American Mathematical Society, 2017 - 2019

Member, American Mathematical Society Committee on National Awards and Public Representation, 2016-2018

Chair, Departmental Review Committee, Mathematics, U. of Maryland, April 2016

Member, Science Advisory Board, Institute for Mathematical Sciences, National University of Singapore, 2016-2018.

Member, Mathematical Association of America, Committee on Prizes and Awards, 2015-2018

Member, External Review Committee for the Simons Institute for Theory of Computing, November, 2015

Member, Departmental Review Committee, Mathematical Sciences, Cornell University, October 2015

Member, American Mathematical Society Committee on Committees, 2014-2016

Member, MAA Search Committee for Editor of Mathematics Monthly, 2014-2015

Member, Selection Committee, National Science Foundation Alan Waterman Award, 2014-2017

Member, Selection Committee, American Mathematical Society Fellows Program, 2014-2017

Member, Society for Industrial and Applied Mathematics Committee on Science Policy, 2014 - 2020

Member, DIMACS (Discrete Mathematics and Computer Science) Advisory Board, 2014-2016

US Delegate-at-large to the International Mathematical Union General Assembly, Korea, 2014

Member, Springer Advisory Board, Undergraduate and Graduate Texts in Mathematics Series, 2012 - 2018

President, Association for Women in Mathematics, 2011 - 2013

Organizer, Association for Women in Mathematics Research Symposium, Santa Clara University, NSA and NSF funded, March 2013

Organizer, Association for Women in Mathematics: *40 years and counting* Conference at Brown University, NSF funded, Sept. 2011

Organizer, Geometry Discrepancy 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

Member, External Review Committee, Mathematics Department, Wellesley U. 2007

Panelist, National Science Foundation, Individual Research Grants and Focused Research Grants, multiple years

SELECTED BROWN UNIVERSITY SERVICE , 2000-present

Member, Executive Director Corporate Relations Search Committee, 2017

Member, Dean of the Graduate School Search Committee, 2016

Member, Provost's Rapid Planning Group: Data Sciences Initiative, 2015

Member, Watson Institute Brazil Collaborative Research Fund selection committee, 2013-2016

Member, Vice President for Research Search Committee, 2013

Member, President's Lectures Advisory Committee, Brown University, 2013

Speaker, Brown Commencement Forum: with J. Hoffstein, D. Mumford, and B. Sandstede, May 2011

Member, Undergraduate Task Force, Fall 2007

Member, Dean of the College Search Committee, spring 2005

Member, Academic Priorities Committee , 2003-2004

WISE faculty advisor/mentor, 2000-present

Member, University Nominations Committee, 2001

Organizer and Speaker, Inaugural Committee - Faculty forums, Inaugural Weekend, 2001

Member, Provost Search Committee, Fall 2000

SELECTED DEPARTMENTAL SERVICE

Member, Hiring Committee, 2018-2019

Member, Senior Search Hiring Committee, 2014-2015

Brown *Symposium for Undergraduate Mathematical Sciences* faculty coordinator 2002-2012.

Colloquium Chair, 2010

Department Chair, January 2005 - June 2008

Mathematics-Applied Mathematics WISE affinity group faculty advisor, 2000-2012

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

TRAINING OF STUDENTS

PhD Students:

Nancy Lim (1993), Sanja Hukovic (1998), Danielle Jamison (1999), Camil Muscalu (2000), Xiao Xiao (2011), Xaiomin Ma (2011), Theresa Anderson (2015), Yumeng Ou (2016). Alex Barron (2019), Linhan Li (2019)

Undergraduate Honors Supervision: 4

Thesis reading committee memberships (not including Ph.D. students): 21

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

19. 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 Nick Howgrave-Graham, Jeffrey Hoffstein, and William Whyte. IACR Cryptology ePrint Archive (2005)

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, first edition 2008, second edition 2015.

40. Iterated Riesz Commutators: a simple proof of boundedness, with M. Lacey, S. Petermichl, B. Wick, Proceedings of Analysis at El Escorial 2008, (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, , Proc. Amer. Math. Soc. 139 (2011), 1445-1454

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, Bulletin of the London Mathematical Society, 43(6), 1151-1166..

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, J. Geometric Analysis, (2013), 23, 2091-2157.

48. Dyadic structure of multiparameter function spaces, with Ji Li and L. Ward, Revista Mat. Iberoamericana, Vol 31, Issue 3, (2015), 767-797.

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, J. Amer. Math. Soc. 28 (2015), 483-529

50. Perturbations of elliptic operators in chord arc domains, with E. Milakis and T. Toro, Contemporary Math.,AMS, Vol 612, (2014), 143-163.

51. Boundary value problems for elliptic operators satisfying a Carleson condition, with M. Dindos and D. Rule, Comm. Pure and Appl. Math. Vol. 70, Issue 7 (2017), 13161365

52. The regularity problem for second order elliptic operators with complex-valued bounded measurable coefficients, with S. Hofmann, C. Kenig, and S. Mayboroda, Mathematische Annalen, 361(3-4), (2015), 863-907.

53. Diophantine approximation and directional discrepancy of rotated lattices, with D. Bilyk, X. Ma, and C. Spencer, Trans. of Amer. Math. Soc., http://dx.doi.org/10.1090/tran/6492, September 2015

54. Practical Signatures from the partial Fourier recovery problem, with J. Hoffstein, J. Schank, J. Silverman, and W. Whyte, International Conference on Applied Cryptography and Network Security ACNS 2014: Applied Cryptography and Network Security, 476-493

55. Carleson Measures and Boundary Value Problems, Proceedings of the International Congress of Mathematicians, Seoul, 2014

56. Transcript secure signatures based on modular lattices, with J. Hoffstein, J. Schanck, W. Whyte, PQCrypto 2014, Waterloo, ON, Canada, October 1-3, 2014. Proceedings, Lecture Notes in Computer Science Volume 8772 2014

57. Square functions and the A_∞ property of elliptic measures with C. Kenig, B. Kirchheim, and T. Toro, J. Geom. Anal. Volume 26, Issue 3, (2016) 2383-2410.

58. BMO Solvability and the A_∞ condition for second order parabolic operators, with M. Dindos and S. Petermichl, Annales de l'Institut Henri Poincare (C) Non Linear Analysis, 13.10. (2016)

59. Fully Homomorphic Encryption from the Finite Field Isomorphism Problem, with Y. Doroz, J. Hoffstein, J. Pipher, J. Silverman, B Sunar, W. Whyte, Z. Zhang, to appear in Proceedings of PKC 2018, the 21st edition of the International Conference on Practice and Theory of Public Key Cryptography, published by Springer in their Lecture Notes in Computer Science series.

60. Regularity of solutions to divergence form elliptic equations with complex coefficients, with M. Dindos, to appear in Advances in Math.

61. Perturbation of p-elliptic complex coefficient operators, with M. Dindos, Acta Math. Sinica, English series, April 2019.

62. Choosing Parameters for NTRUEncrypt, with J. Hoffstein, J. Schanck, J. Silverman, W. Whyte, Z. Zhang Topics in Cryptology –CT-RSA 2017: The Cryptographers' Track at the RSA Conference 2017 Springer LNCS 10159

63.A signature scheme from Learning with Truncation, with J. Hoffstein, W. Whyte, and Z. Zhang, preprint.

64. Boundary behavior of solutions of elliptic operators in divergence form with a BMO anti-symmetric part, with L. Li, Communications in PDE, Vol. 44, No. 2 (2019), 156-204

65. Commutators of multi-parameter flag singular integrals and applications, with X. Duong, J. Li, Y. Ou, and B. Wick, Analysis and PDE, Vol. 12, No. 5 (2019), 1357-1396

66. Boundary value problems for second order elliptic operators with complex coefficients, with M. Dindos, accepted by APDE (Analysis and Partial Differential Equations), August 2019.

67. Weighted Estimates of Singular Integrals and Commutators in the Zygmund Dilation Setting, with S. Duong, J. Li, Y. Ou, and B.Wick, submitted

68. L^p theory for the square roots and square functions of elliptic operators having a BMO anti-symmetric part, with S. Hofmann, L. Li, S. Mayboroda, submitted

69. The Dirichlet problem for elliptic operators having a BMO anti-symmetric part, with S. Hofmann, L. Li, S. Mayboroda, submitted

70. Extrapolation of the Dirichlet problem for elliptic equations with complex coefficients, with M. Dindos. J.Functional Analysis, Volume 279, Issue 7, 15 October 2020,

71. Weighted estimates of singular integrals and commutators in the Zygmund dilation setting, with X. Duong, J. Li, Y. Ou, and B. Wick, submitted.

72. The p-ellipticity condition for second order elliptic systems and applications to the Lamé and homogenization problems, with M. Dindos, J. Li, submitted.