

CURRICULUM VITAE (SEPTEMBER 2008 – 10 PAGES)

WILLIAM D. BANKS

Department of Mathematics, University of Missouri
202 Mathematical Sciences Building, Columbia, MO 65211 USA
(1-573) 882-4305 • e-mail: bbanks@math.missouri.edu

Education

- 1982–1986 B.S. Mathematics, California Institute of Technology, Pasadena, CA
Undergraduate advisor: Tom Apostol
- 1989–1994 Ph.D. Mathematics, Stanford University, Stanford, CA
Dissertation: “Exceptional representations on the metaplectic group”
Graduate advisor: Daniel Bump

Academic Appointments

- 1994–1996 Centre Interuniversitaire en Calcul Mathématique Algébrique,
Montréal, QC Canada (on leave Spring 1995)
Postdoctoral Fellow
- Spring 1995 Mathematical Sciences Research Institute, Berkeley, CA
Postdoctoral Fellow
- 1996–1998 Oklahoma State University, Stillwater, OK
Postdoctoral Fellow
- 1998–Present University of Missouri, Columbia, MO
Postdoctoral Fellow, 1998
Assistant Professor, 2000
Associate Professor, 2003
Professor, 2007

Research Interests

Analytic and algebraic number theory, representation theory, cryptography.

Additional Work Experience

- 1986–1987 Computer Programmer, AeroVironment, Inc., Monrovia, CA
1987–1989 Computer Programmer, Sungene Technologies, Milpitas, CA

RESEARCH

Publications

- (1) “The Casselman-Shalika formula for a distinguished model,” *Proc. Amer. Math. Soc.* **123** (1995), no. 3, 681–692.
- (2) “Twisted symmetric-square L-functions and the nonexistence of Siegel zeros on $GL(3)$,” *Duke Math. J.* **87** (1997), no. 2, 343–353.
- (3) “Heredity of Whittaker models on the metaplectic group,” *Pacific J. Math.* **185** (1998), no. 1, 89–96.
- (4) “A corollary to Bernstein’s theorem and Whittaker functionals on the metaplectic group,” *Math. Res. Lett.* **5** (1998), 781–790.
- (5) with J. Levy and M. Sepanski, “Block-compatible metaplectic cocycles,” *J. Reine Angew. Math.* **507** (1999), 131–163.
- (6) with D. Lieman and I. Shparlinski, “An identification scheme based on sparse polynomials,” in *Public Key Cryptography, Third International Workshop on Practice and Theory in Public Key Cryptography, PKC2000 (Melbourne)*, Lecture Notes in Comput. Sci. **1751**, Springer-Verlag, Berlin (2000).
- (7) with F. Griffin, D. Lieman and I. Shparlinski, “Nonlinear complexity of the Naor-Reingold pseudo-random function,” in *Proceedings of ICISC’99 (Seoul)*, Lecture Notes in Comput. Sci. **1787**, Springer-Verlag, Berlin (2000).
- (8) with D. Lieman and I. Shparlinski, “An extremely small and efficient identification scheme,” in *Proceedings of ACISP2000 (Brisbane)*, Lecture Notes in Comput. Sci. **1841**, Springer-Verlag, Berlin (2000).
- (9) with D. Lieman, I. Shparlinski, and V. To, “Cryptographic applications of sparse polynomials over finite rings,” in *Proceedings of ICISC2000 (Seoul)*, Lecture Notes in Comput. Sci. **2015**, Springer-Verlag, Berlin (2001).
- (10) with D. Bump and D. Lieman, “On the dimension of the Jacquet module of a certain induced representation,” in *Ideal Theoretic Methods in Commutative Algebra*, Lecture Notes in Pure and Applied Math. **220**, Marcel Dekker, Inc., New York (2001).
- (11) “Some unusual identities for special values of the Riemann zeta function,” *Ramanujan J.* **5** (2001), no. 2, 153–157.
- (12) with I. Shparlinski, “Distribution of inverses in polynomial rings,” *Indag. Math. (N.S.)* **12** (2001), no. 3, 303–315.
- (13) with I. Shparlinski, “On the number of sparse RSA Exponents,” *J. Number Theory* **95** (2002), no. 2, 340–350.

Publications (cont'd)

- (14) with I. Shparlinski, “Average normalisations of elliptic curves,” *Bull. Austral. Math. Soc.* **66** (2002), 353–358.
- (15) with A. Conflitti and I. Shparlinski, “Character sums over integers with restricted g -ary digits,” *Illinois J. Math.* **46** (2002), no. 3, 819–836.
- (16) with D. Bump and D. Lieman, “Whittaker-Fourier coefficients of metaplectic Eisenstein series,” *Compositio Math.* **135** (2003), no. 2, 153–178.
- (17) with A. Harcharras, S. Neuwirth and E. Ricard, “Matrix inequalities with applications to the theory of iterated kernels,” *Linear Algebra Appl.* **362** (2003), 275–286.
- (18) with I. Shparlinski, “A variant of NTRU with non-invertible polynomials,” in *Progress in Cryptology – Indocrypt 2002*, Lecture Notes in Comput. Sci. **2551**, Springer-Verlag, Berlin (2003).
- (19) with A. Harcharras and I. Shparlinski, “Short Kloosterman sums for polynomials over finite fields,” *Canad. J. Math.* **55** (2003), 225–246.
- (20) with A. Harcharras, “New examples of noncommutative $\Lambda(p)$ sets,” *Illinois J. Math.* **47** (2003), 1063–1078.
- (21) with A. Conflitti, J. Friedlander and I. Shparlinski, “Exponential sums over Mersenne numbers,” *Compositio Math.* **140** (2004), 15–30.
- (22) with A. Conflitti and I. Shparlinski, “Number theoretic designs for directed regular graphs of small diameter,” *SIAM J. Discrete Math.* **17** (2004), no. 3, 377–383.
- (23) with A. van der Poorten, “Squares from products of integers,” *Austral. Math. Soc. Gaz.* **31** (2004), no. 1, 40–42.
- (24) with I. Shparlinski, “Congruences and exponential sums with the Euler function,” in *High primes and misdemeanours: lectures in honour of the 60th birthday of Hugh Cowie Williams*, 49–59, Fields Inst. Commun. **41**, Amer. Math. Soc., Providence, RI, 2004.
- (25) with J. Friedlander, C. Pomerance and I. Shparlinski, “Multiplicative structure of values of the Euler function,” in *High primes and misdemeanours: lectures in honour of the 60th birthday of Hugh Cowie Williams*, 29–47, Fields Inst. Commun. **41**, Amer. Math. Soc., Providence, RI, 2004.
- (26) with I. Shparlinski, “Arithmetic properties of numbers with restricted digits,” *Acta Arith.* **112** (2004), no. 4, 313–332.
- (27) with A. Harcharras, “On the norm of an idempotent Schur multiplier on the Schatten class,” *Proc. Amer. Math. Soc.* **132** (2004), no. 7, 2121–2125.

Publications (cont'd)

- (28) with A. Harcharras and I. Shparlinski, “Smooth values of shifted primes in arithmetic progressions,” *Michigan Math. J.* **52** (2004), no. 3, 603–618.
- (29) with D. Hart and M. Sakata, “Almost all palindromes are composite,” *Math. Res. Lett.* **11** (2004) nos. 5-6, 853–868.
- (30) with R. Heath-Brown and I. Shparlinski, “On the average value of divisor sums in arithmetic progressions,” *Int. Math. Res. Not.* **2005**, no. 1, 1–25.
- (31) with F. Luca, “Concatenations with binary recurrent sequences,” *J. Integer Seq.* **8** (2005), no. 1, Article 05.1.3, 18 pp. (electronic)
- (32) with F. Luca, I. Shparlinski and H. Stichtenoth, “On the value set of $n!$ modulo a prime,” *Turkish J. Math.* **29** (2005), 169–174.
- (33) with F. Luca and I. Shparlinski, “Irrationality of power series for various number theoretic functions,” *Manuscripta Math.* **117** (2005), no. 2, 183–197.
- (34) with F. Luca, F. Saidak and I. Shparlinski, “Values of arithmetical functions equal to a sum of two squares,” *Quart. J. Math. Oxford Ser.* **56** (2005), 123–139.
- (35) with F. Luca, “Nonaliquots and Robbins numbers,” *Colloq. Math.* **103** (2005), 27–32.
- (36) with K. Ford, F. Luca, F. Pappalardi and I. Shparlinski, “Values of the Euler function in various sequences,” *Monatsh. Math.* **146** (2005), 1–19.
- (37) with F. Luca, F. Saidak and P. Stănică, “Compositions with the Euler and Carmichael functions,” *Abh. Math. Sem. Hamburg* **75** (2005), 215–243.
- (38) with M. Garaev, F. Luca and I. Shparlinski, “Uniform distribution of the fractional part of the average prime divisor,” *Forum Math.* **17** (2005), no. 6, 885–901.
- (39) “Towards faster cryptosystems, II,” in *Public Key Cryptography*, Proceedings of Symposia in Pure Mathematics, **62**, American Mathematical Society, 2005.
- (40) with F. Luca, “Roughly squarefree values of the Euler and Carmichael functions,” *Acta Arith.* **120** (2005), 211–230.
- (41) with I. Shparlinski, “Prime divisors of palindromes,” *Period. Math. Hungar.* **51** (2005), 1–10.
- (42) with F. Luca and I. Shparlinski, “Some divisibility properties of the Euler function,” *Glasgow Math. J.* **47** (2005), no. 3, 517–528.
- (43) with G. Harman and I. Shparlinski, “Distributional properties of the largest prime factor,” *Michigan Math. J.* **53** (2005), 665–681.
- (44) with F. Luca and I. Shparlinski, “On certain sums related to multiple divisibility by the largest prime factor,” *Ann. Sci. Math. Québec* **29** (2005), no. 2, 131–145.

Publications (cont'd)

- (45) with F. Luca and I. Shparlinski, “Arithmetic properties of $\varphi(n)/\lambda(n)$ and the structure of the multiplicative group modulo n ,” *Comment. Math. Helv.* **81** (2006), no. 1, 1–22.
- (46) with J. Friedlander, S. Konyagin and I. Shparlinski, “Incomplete character sums and Diffie–Hellman triples,” *Math. Proc. Cambridge Philos. Soc.* **140** (2006), 193–206.
- (47) with J. Friedlander, F. Luca, F. Pappalardi and I. Shparlinski, “Coincidences in the values of the Euler and Carmichael functions,” *Acta Arith.* **122** (2006), no. 3, 207–234.
- (48) with I. Shparlinski, “Non-residues and primitive roots in Beatty sequences,” *Bull. Austral. Math. Soc.* **73** (2006), 433–443.
- (49) with F. Luca, “On integers with a special divisibility property,” *Arch. Math. (Brno)* **42** (2006), 31–42.
- (50) with I. Shparlinski, “Multiplicative character sums with the g -ary sum of digits function,” *Ramanujan J.* **11** (2006), no. 2, 215–219.
- (51) with J. Friedlander, M. Garaev and I. Shparlinski, “Double character sums over elliptic curves and finite fields,” *Pure Appl. Math. Q.* **2** (2006), no. 1, 179–197.
- (52) with I. Shparlinski, “Short character sums with Beatty sequences,” *Math. Res. Lett.* **13** (2006), 539–547.
- (53) with J. Friedlander, M. Garaev and I. Shparlinski, “Character sums with exponential functions over smooth numbers,” *Indag. Math. (N.S.)* **17** (2006), no. 2, 157–168.
- (54) with F. Pappalardi, “Values of the Euler function free of k -th powers,” *J. Number Theory* **120** (2006), no. 2, 326–348.
- (55) with I. Shparlinski, “Congruences and rational exponential sums with the Euler function,” *Rocky Mountain J. Math.* **36** (2006), 1415–1426.
- (56) with F. Luca and I. Shparlinski, “Common divisors of the Euler function at related arguments,” *Acta Sci. Math. (Szeged)* **72** (2006), no. 3-4, 525–536.
- (57) with I. Shparlinski, “Average value of the Euler function on binary palindromes,” *Bull. Pol. Acad. Sci. Math.* **54** (2006), no. 2, 95–101.
- (58) with I. Shparlinski, “Prime divisors of Beatty sequences,” *J. Number Theory* **123** (2007), no. 2, 413–425.
- (59) with F. Luca and I. Shparlinski, “On rough and smooth neighbours,” *Rev. Mat. Complut.* **20** (2007), no. 1, 109–118.
- (60) with I. Shparlinski, “On values taken by the largest prime factor of shifted primes,” *J. Aust. Math. Soc.* **82** (2007), 133–147.

Publications (cont'd)

- (61) with I. Shparlinski, “Integers with a large smooth divisor,” *Integers* **7** (2007), A17, 11 pp. (electronic)
- (62) with F. Luca, “Sums of prime divisors and Mersenne numbers,” *Houston J. Math.* **33** (2007), no. 2, 403–413 (electronic).
- (63) with F. Luca, “When the sum of aliquots divides the totient,” *Proc. Edinb. Math. Soc.* **50** (2007), 563–569.
- (64) with F. Luca, “Composite integers n for which $\varphi(n) \mid n - 1$,” *Acta Math. Sinica, English Series* **23** (2007), no. 10, 1915–1918.
- (65) with M. Sakata and F. Saidak, “Kloosterman sums for modified van der Corput sequences,” *Uniform Distribution Theory 2* (2007), no. 1, 39–52.
- (66) with F. Luca and I. Shparlinski, “Estimates for Wieferich numbers,” *Ramanujan J.* **14** (2007), no. 3, 361–378.
- (67) with A. Güloğlu and W. Nevans, “Representations of integers as sums of primes from a Beatty sequence,” *Acta Arith.* 130 (2007), no. 3, 255–275.
- (68) with I. Shparlinski, “Exponential sums with polynomial values of the discrete logarithm,” *Uniform Distribution Theory 2* (2007), no. 2, 67–72.
- (69) with M. Garaev, R. Heath-Brown and I. Shparlinski, “Density of non-residues in Burgess-type intervals and applications,” *Bull. London Math. Soc.* 40 (2008), 88–96.

Papers Accepted

- (70) “Carmichael numbers with a square totient,” to appear in *Canad. Math. Bull.*
- (71) with M. Garaev, F. Luca and I. Shparlinski, “Uniform distribution of fractional parts related to pseudoprimes,” to appear in *Canad. J. Math.*
- (72) with F. Luca and J. Friedlander, “Integers without divisors from a fixed arithmetic progression,” to appear in *Forum Math.*
- (73) with A. Güloğlu, W. Nevans and F. Saidak, “Descartes numbers,” to appear in the *Anatomy of Integers* conference proceedings
- (74) with S. Balasuriya and I. Shparlinski, “Congruences and exponential sums with the sum of aliquot divisors function,” to appear in *Int. J. Number Theory*
- (75) with I. Shparlinski, “Character sums with Beatty sequences on Burgess-type intervals,” to appear in the *Klaus Roth Festschrift*
- (76) with I. Shparlinski, “Sato–Tate, cyclicity, and divisibility statistics on average for elliptic curves of small height,” to appear in *Israel J. Math.*

Papers Accepted (cont'd)

- (77) with D. Hart, P. Moree and W. Nevans, “The Nicolas and Robin inequalities with sums of two squares,” to appear in *Monatsh. Math.*
- (78) with A. Güloğlu, “Values of the Carmichael function equal to a sum of two squares,” to appear in *Turkish J. Math.*
- (79) with I. Shparlinski, “Multiplicative character sums with twice-differentiable functions,” to appear in *Quart. J. Math. Oxford Ser.*

Submitted Manuscripts

- (80) with F. Luca and L. Szalay, “A variant on the notion of Diophantine s -tuples,” submitted to *Glasgow Math. J.*
- (81) with A. Güloğlu and W. Nevans, “On the congruence $n \equiv a \pmod{\varphi(n)}$,” submitted to *Integers*
- (82) with A. Abercrombie and I. Shparlinski, “Arithmetic functions on Beatty sequences,” submitted to *Acta Arith.*
- (83) with I. Shparlinski, “Prime numbers with Beatty sequences,” submitted to *Colloq. Math.*
- (84) with A. Güloğlu and W. Nevans, “On primitive Dirichlet characters and the Riemann hypothesis,” submitted to *J. Number Theory*

PROFESSIONAL ACTIVITIES

Teaching Experience

Stanford University, Stanford, CA
Single and Multivariable Calculus
Linear Algebra

Concordia University, Montréal, QC (Canada)
Linear Algebra
Differential Equations

Oklahoma State University, Stillwater, OK
Single and Multivariable Calculus
Applications of Modern Mathematics

University of Missouri, Columbia, MO
Finite Mathematics
Introduction to Calculus (Primary Instructor/Course Coordinator)
Advanced Calculus
Multivariable Calculus
Linear Algebra
Introduction to Cryptography
Introduction to Analytic Number Theory
Advanced Analytic Number Theory (Graduate Seminar)
Advanced Algebraic Number Theory (Graduate Seminar)
Representation Theory (Graduate Seminar)
Automorphic Forms (Graduate Seminar)

Teaching Award

Provost Outstanding Junior Faculty Teaching Award, 2003.

Advising and Mentoring

Undergraduate
Dylan Cooper, 2002.
Benjamin Schulz, 2002.
Michael Deutsch, 2003.
Sheraun Howard, 2003.

Graduate
Mark Budden, 2000–2003.
Larry Ellis, 2000–2001.
Stephen Boul, 2000.
Steven Shattuck, 2000.
Derrick Hart, 2002.
Adriano Marzullo, 2004–2006.
Valeria D’Orazio, 2004–2006.
Wesley Nevans, 2005–present.

Postdoctoral
Mayumi Sakata, 2001–2004.
Filip Saidak, 2003–2005.
Ahmet Güloğlu, 2005–present.

Masters Committee Service

Mark Budden, 1999.
Larry Ellis, 1999.
Stephen Boul, 2001 (advisor).
Amy Ginn, 2001.
Angela Muenks, 2002.
Chris Thornhill, 2004.
Arpit Ghoting, 2005.
Mike Pemberton, 2007.
Daniel Sutantyo, 2007.
Valeria D’Orazio, 2008.

Ph.D. Committee Service

Mark Budden, 2003 (advisor).
Derrick Hart, 2008.

Miscellaneous Teaching Activities

Supervised undergraduate Putnam Exam workshop, 1998.
Undergraduate math club supervisor, 1999.
Coached undergraduate math team to state victory, 1999.
Coached undergraduate math team to state victory, 2000.

Grants and Fellowships

MSRI Postdoctoral Fellowship (5 months), 1995.
NSF Grant “Metaplectic Forms and Cryptography,” 2000–2004.

Proposal Review

National Science Foundation, 2001–2002.

Refereeing

International Mathematics Research Notices, 2002.
Mathematics of Computation, 2003.
American Mathematical Monthly, 2004.
Journal of Number Theory, 2005.
Proceedings of the AMS, 2005.
Experimental Mathematics, 2006.
Finite Fields and Their Applications, 2006.
International Journal of Number Theory, 2006.
Journal of Integer Sequences, 2006.
Journal of Number Theory, 2006.
London Mathematical Society, 2006.
Revista Colombiana De Matematicas, 2006.
Rocky Mountain Journal of Mathematics, 2006.

Memberships

American, Australian and Canadian Mathematical Societies.

Invited Lectures

- Fall 1993 Purdue University Colloquium
- Spring 1994 Texas Christian University Colloquium
- Fall 1994 Vermont-Québec Number Theory Seminar (Montréal)
- Spring 1995 Mathematical Sciences Research Institute
- Fall 1995 Vermont-Québec Number Theory Seminar (Montréal)
- Spring 1996 Université Laval Colloquium
- Spring 1996 AMS Meeting in Iowa City
- Spring 1996 University of Toronto Colloquium
- Fall 1996 Oklahoma State University Colloquium
- Fall 1997 Missouri Algebra Weekend
- Spring 1999 Arts and Sciences Week Special Lecture (UM-Columbia)
- Spring 1999 Vermont-Québec Number Theory Seminar (Montréal)
- Spring 1999 Automorphic Forms Workshop in Santa Barbara
- Summer 1999 Macquarie University Colloquium (Sydney)
- Summer 1999 Vermont-Québec Number Theory Seminar (Montréal)
- Fall 1999 Midwest Arithmetical Geometry in Cryptography Workshop
- Fall 1999 University of Iowa Colloquium
- Fall 1999 ICISC'99 Conference in Cryptography (Seoul)
- Spring 2000 Baylor University Colloquium
- Spring 2000 PKC2000 Conference in Cryptography (Melbourne)
- Spring 2000 Graduate Student Seminar (UM-Columbia)
- Spring 2000 AMS Meeting in Santa Barbara
- Summer 2000 ACISP2000 Conference in Cryptography (Brisbane)
- Fall 2000 ICISC2000 Conference in Cryptography (Seoul)
- Spring 2001 Automorphic Forms Workshop in Mountain View
- Fall 2001 Macquarie University Colloquium (Sydney)
- Fall 2001 Australian Mathematical Society Meeting (Canberra)
- Fall 2001 Georgia Institute of Technology Colloquium
- Fall 2002 Workshop on Algebraic and Complexity-Theoretical
Methods in Cryptology (Bochum)
- Spring 2003 AMS Short Course on Public Key Cryptography (Baltimore)
- Summer 2003 Number Theory Conference in Honour of Professor H.C. Williams (Banff)
- Fall 2003 36th National Congress of the Mexican Mathematical Society (Pachuca)
- Spring 2004 Universidad Nacional Autónoma de México Colloquium (Morelia)
- Spring 2004 Macquarie University Colloquium (Sydney)
- Fall 2004 37th National Congress of the Mexican Mathematical Society (Ensenada)
- Spring 2005 ArithmeTexas 2005 (College Station)
- Spring 2005 Universidad Nacional Autónoma de México Colloquium (Morelia)
- Fall 2005 Conférence de Théorie Analytique des Nombres (Québec)
- Spring 2006 Vermont-Québec Number Theory Seminar (Montréal)
- Spring 2006 Anatomy of Integers Conference (Montréal)
- Spring 2006 Italian-Polish Number Theory Days (Poznań)
- Fall 2007 INTEGERS Conference (Univ. of West Georgia)
- Spring 2008 Analytic Number Theory (Oberwolfach)