CURRICULUM VITAE

Lawrence C. Washington
Born 1951 in Vermont, US citizen

Department of Mathematics
University of Maryland
College Park, Maryland 20742

e-mail: lcw@umd.edu

Education

Johns Hopkins University	B.A.	1968-1971
Johns Hopkins University	M.A.	1971
Princeton University	Ph.D.	1971-1974

Professional Experience

Stanford University	Assistant Professor	1974-1977
University of Maryland	Visiting Asst. Prof.	1977-1978
University of Maryland	Assistant Professor	1978-1981
University of Maryland	Associate Professor	1981-1986
University of Maryland	Professor	1986-present
University of Maryland	Associate Chair for Graduate Studies	2011-2016
University of Maryland	Distinguished Scholar-Teacher	2011-present
University of Maryland	Associate Chair for Undergraduate Studies	2021-present

Visiting Positions

Institut des Hautes Études Scientifiques	1980-1981
Max-Planck-Institut, Bonn	Summer 1984
Mathematical Sciences Research Institute, Berkeley	1986-1987
Univ. Campinas, Brazil	August 1988
Nankai Institute, Tianjin, China	May 1990
Institute for Advanced Study	Spring, Summer 1996
Center for Computing Sciences	Summers 1999-2000
C.E.M., Perugia, Italy	August 2004
Center for Communications Research, Princeton	July 2017

Publications

Research Articles

1. Class numbers and $\mathbb{Z}_p$-extensions, Math. Ann. 214 (1975), 177-193.
2. Class numbers of elliptic function fields and the distribution of prime numbers, Acta Arith. 28 (1975), 111-114.
3. A note on p-adic L-functions, J. Number Theory 8 (1976), 245-250.
4. Relative integral bases, Proc. Amer. Math. Soc. 56 (1976), 93-94; 70 (1978), 92.
5. The class number of the field of 5^n-th roots of unity, Proc. Amer. Math. Soc. 61 (1976), 205-208.
6. On Fermat's Last Theorem, J. reine angew. Math. 289 (1977), 115-117.

7. The calculation of $L_p(1,\chi)$, J. Number Theory 9 (1977), 175-178.

8. Units of irregular cyclotomic fields, Illinois J. Math. 23 (1979), 1-8.

9. Euler factors for p-adic L-functions, Mathematika 25 (1978), 68-75.

10. Kummer's calculation of $L_p(1,\chi)$, J. reine angew. Math. 305 (1979), 1-8.

11. (with B. Ferrero) The Iwasawa invariant μ_p vanishes for abelian number fields, Annals of Math. 109 (1979), 377-395.

12. The non-p-part of the class number in a cyclotomic $\mathbb{Z}_p$-extension, Inventiones Math. 49 (1978), 87-97.

13. The derivative of p-adic L-functions, Acta Arith. 40 (1980), 109-115.

14. P-adic L-functions at $s = 0$ and $s = 1$, Analytic Number Theory (Grosswald Conference) Springer Lecture Notes in Math., vol. 899, Springer-Verlag, New York, 1981, 166-170.

15. Zeroes of p-adic L-functions, Séminaire de Théorie des Nombres, Paris, 1980-81 (Sém. Delange-Pisot-Poitou), Birkhäuser, Boston, 1982, 337-357.

16. (with G. Cornell) Class numbers of cyclotomic fields, J. Number Theory 21 (1985), 260-274.

17. (with E. Seah and H. Williams) The calculation of a large cubic class number with an application to real cyclotomic fields, Math. Comp. 41 (1983), 303-305.

18. (with R. Vohra) Counting spanning trees in the graphs of Kleitman and Golden and a generalization, J. Franklin Institute 318 (1984), 349-355.

19. On some cyclotomic congruences of F. Thaine, Proc. Amer. Math. Soc. 93 (1985), 10-14.

20. Some remarks on Cohen-Lenstra heuristics, Math. Comp. 47 (1986), 741-747.

21. Class numbers of the simplest cubic fields, Math. Comp. 48 (1987), 371-384.

22. (with K. H. Dovermann) Relations between cyclotomic units and Smith equivalence of representations, Topology 28 (1989), 81-89.

23. (with R. Schoof) Quintic polynomials and real cyclotomic fields with large class numbers, Math. Comp. 50 (1988), 543-556.

24. On Sinnott's proof of the vanishing of the Iwasawa invariant μ_p, Algebraic Number Theory – in honor of K. Iwasawa, Advanced Studies in Pure Mathematics, vol. 17, Academic Press, Boston, 1990 and Kinokuniya, Tokyo, 1989, 457-462.

25. Stickelberger's theorem for cyclotomic fields, in the spirit of Kummer and Thaine, Number Theory: Proceedings of the International Number Theory Conf. (Laval, 1987), ed. by J-M. De Koninck and C. Levesque, Walter de Gruyter, Berlin, 1989, 990-993.

26. (with E. Friedman) On the distribution of divisor class groups of curves over a finite field, Number Theory: Proceedings of the International Number Theory Conf. (Laval, 1987), ed. by J-M. De Koninck and C. Levesque, Walter de Gruyter, Berlin, 1989, 227-239.

27. (with P. Bremser and P. Schumer) A note on the incongruence of consecutive integers to a fixed power, J. Number Theory, 35 (1990), 105-108.

28. A family of cyclic quartic fields arising from modular curves, Math. Comp. 57 (1991), 763-775.

29. Kummer's lemma for prime-power cyclotomic fields, J. Number Theory 40 (1992), 165-173.

30. (with Allan Adler) p-adic L-functions and higher dimensional magic cubes, J. Number Theory 52 (1995), 179-197.

31. (with Y.-Y. Shen) A family of real 2^n-tic fields, Trans. A.M.S. 345 (1994), 413-434.

32. Appendix to "On the ℓ-adic Iwasawa λ-invariant in a p-extension" by E. Friedman and J. Sands, Math. Comp. 64 (1995), 1659-1674 (appendix: 1669-1673).

33. Siegel zeros for 2-adic L-functions, Canadian Mathematical Society, Conference Proceedings Series 15 (1995), 393-396.

34. (with Y.-Y. Shen) A family of real p^n-tic fields, Canadian J. Math. 47 (1995), 655-672.

35. (with Boyd Roberts) The modularity of some $\mathbb{Q}$-curves, Compositio Math. 111 (1998), 35-49.

36. A family of cubic fields and zeros of 3-adic L-functions, J. Number Theory, 63 (1997), 408-417.

37. p-adic L-functions and sums of powers, J. Number Theory 69 (1998), 50-61.

38. (with Xianke Zhang) Ideal class groups and their subgroups of real quadratic fields, Science in China (=Scientia Sinica), series A 40(1997),No.9, 909-916 (Chinese version: Vol.27 (1997), No.6, 522-528).

39. (with Xianke Zhang) Heuristics and related results on class groups of real quadratic fields, Science in China(=Scientia Sinica) 41 (1998), no. 4, 365-370.

40. (with Xianke Zhang) Modification of Cohen-Lenstra Heuristics for ideal class groups of certain real quadratic fields, Chinese Science Bulletin, 42(1997), No.23, 1959-1962 (Chinese version: Kexue Tongbao, Vol.42(1997),No.19, 2053-2056).

41. (with D. Shanks and P. Sime) Zeros of 2-adic L-functions and congruences for class numbers and fundamental units, Math. Comp. 68 (1999), 1243-1255.

42. Some remarks on Fibonacci matrices, Fibonacci Quart. 37 (1999), 333-341.

43. (with M. Goresky and A. Klapper) Fourier transforms and the 2-adic span of periodic binary sequences, IEEE Trans. Inform. Theory 46 (2000), 687-691.

44. (with C. Helou and R. Roll) Power residue character of rational primes, J. Ramanujan Math. Soc. 16 (2001), 19–37.

45. (with J. Kraft) Heuristics for class numbers and λ-invariants, Math. of Computation 76 (2007), 1005-1023.

46. (with D. Hubbard) Kummer generators and lambda invariants, J. Number Theory 130 (2010), 61-81; also available on arXiv:0810.1691.

47. Computing roots of unity: Appendix to "On taking square roots without quadratic nonresidues over finite fields" by Tsz-Wo Sze, Math. Comp. 80 (2011), 1797-1811; appendix: 1806-1809; also available on arXiv:0812.2591v2.

48. (with R. Schoof) Visibility of ideal classes, J. Number Theory 130 (2010), 2715-2731; also available on arXiv:0809.5209

49. (with J. Hirsh) p-adic continued fractions, Ramanujan J. 25 (2011), 389-403.

50. (with C. Panraksa) Arithmetic dynamics and dynamical units, East-West J. of Mathematics 14 (2012), 201-207.

51. (with C. Panraksa) Real algebraic curves of constant width, Periodica Math. Hungarica 74 (2017), 235-244. (doi:10.1007/s10998-016-0149-9).

52. (with J. Gerard) Sums of powers of primes, Ramanujan J. 45 (2018), 171-180.

53. (with D. Hubbard) Iwasawa invariants of some non-cyclotomic $\mathbb{Z}_p$-extensions, J. Number Theory 188 (2018), 18-47 (also available on arxiv:1703.06550).

54. (with S. Balady) A family of cyclic quartic fields with explicit fundamental units, Acta Arithmetica 187 (2019), 43-57 (available on arxiv.org/abs/1708.07184).

55. (with W. Gasarch and S. Zbarsky) The coefficient-choosing game, J. Combinatorics and Number Theory 10 (2018), 1-17 (earlier version: arxiv.org/abs/1707.04793).

56. (with D. Hubbard and R. Bröker) Explicit Computations in Iwasawa theory, Proceedings of the Thirteenth Algorithmic Number Theory Symposium, edited by Renate Scheidler and Jonathan Sorenson, Open Book Series 2, Mathematical Sciences Publishers, Berkeley, 2019, pp. 137-153. DOI 10.2140/obs.2019.2.137,

57. (with A. Yang) Analogues of the Robin-Lagarias Criteria for the Riemann Hypothesis, Int. J. Number Theory 17, No. 4 (2021), 843–870 (also available on arxiv.org/pdf/2008.04787.pdf).

58. (with M. Mishra and R. Schoof) Class groups of real cyclotomic fields, Monatsh. Math. 195 (2021), no. 3, 489-496. (also available on arxiv.org/pdf/2011.07409.pdf).

59. (with H. Knopfe) Dirichlet series expansions of p-adic L-functions, Abh. Math. Semin. Univ. Hamburg 91 (2021), no. 2, 325-334. (also available on arxiv.org/pdf/2102.02851.pdf).

60. (with S. Jin) An elliptic curve analogue of Pillai's lower bound on primitive roots, Canad. Math. Bull. 65 (2022), no. 2, 496–505. (also available on arxiv.org/abs/2104.13256.pdf).

61. (with D. Pincus) Relative ideal classes of arbitrary order, Ramanujan J. 62 (2023), 819–842 (also available on arxiv.org/pdf/2206.12313.pdf).

62. (with D. Kundu) Heuristics for anticyclotomic $\mathbb{Z}_p$-extensions, to appear in Experimental Mathematics, 23 pp. (Published online: 15 Jun 2023; also available on arxiv.org/pdf/2207.13199.pdf).

63. Sums of powers of primes II, Ramanujan Journal, 65 (2024), 783–795.

64. (with D. Pincus) On the field isomorphism problem for the family of simplest quartic fields, to appear in Acta Arithmetica; (available on https://arxiv.org/abs/2406.10414)

Research Articles not yet published

1. (with J. Hirsh) Polynomials with equal images over number fields. 25 pp. (to be submitted soon).

2. (with D. Kundu) The first layer of a cyclotomic $\mathbb{Z}_p$-extension and related heuristics. 20 pp. (submitted).

Monographs

1a. Introduction to Cyclotomic Fields, Graduate Texts in Math., Springer-Verlag, New York, 1982 (389 pp.).

1b. Introduction to Cyclotomic Fields, 2nd edition (corrected and expanded), Graduate Texts in Math., Springer-Verlag, New York, 1996 (487 pp.).

2a. Introduction to Cryptography with Coding Theory (with Wade Trappe), Prentice Hall, 2002 (490 pp.) Plus: unpublished Solutions Manual (available from Prentice Hall) (129 pp.).

2b. Introduction to Cryptography with Coding Theory, 2nd edition (with Wade Trappe), Prentice Hall, 2005 (577 pp.). Plus: unpublished Solutions Manual (available from Prentice Hall) (174 pp.).

2c. Introduction to Cryptography with Coding Theory, 3rd edition (with Wade Trappe), Prentice Hall, 2020 (718 pp.) (in production). Plus: unpublished Solutions Manual (available from Prentice Hall).

3a. Elliptic Curves: Number Theory and Cryptography, CRC Press, 2003 (428 pp.).

3b. Elliptic Curves: Number Theory and Cryptography, 2nd edition CRC Press, 2008 (513 pp.).

4a. An Introduction to Number Theory with Cryptography (with James S. Kraft), CRC Press, 2014 (554 pp.). Plus: unpublished Solutions Manual (available from CRC) (133 pages).

4b. An Introduction to Number Theory with Cryptography, 2nd edition (with James S. Kraft), CRC Press, 2018 (578 pp.). Plus: unpublished Solutions Manual (available from CRC) (149 pages).

5. Elementary Number Theory (with James S. Kraft), CRC Press, 2015 (393 pp.) (a scaled-down and revised version of #4) Plus: unpublished Solutions Manual (available from CRC) (84 pages).

6. Elementary Calculus, Ming Press, 2019 (about 200pp.); online text and exercises for Math 120.

Other Articles, etc.

1. On the self-duality of $\mathbb{Q}_p$, Amer. Math. Monthly 81 (1974), 369-371.

2. (with E. Griffin) Disproof of a conjecture on biconcatenated primes, J. Recreational Math. 9 (1976), 104-105.

3. (with M. Hellman et al.) Results of an initial attempt to cryptanalyze the NBS encryption standard, Stanford University Center for Systems Research, Technical Report SEL 76-042, 1976.

4. Class numbers and $\mathbb{Z}_p$-extensions, Queen's Number Theory Conference, Queen's Papers in Pure and Applied Mathematics, no. 54 (1980), 119-127.

5. Probabilities, Appendix to Cyclotomic Fields II by S. Lang, Springer-Verlag, New York, 1980, 18-22.

6. Benford's law for Fibonacci and Lucas numbers, Fibonacci Quart. 19 (1981), 175-177.

7. Zeros of p-adic L-functions, Séminaire de Théorie des Nombres, Bordeaux, 1980-1981, exp. 25, 4 pp. (exposition based on #15 above).

8. Recent results on cyclotomic fields, Semin. Notes, Inst. Math., Univ. Aarhus 1 (1982), 120-128.

9. Thaine's results on cyclotomic fields (informally circulated manuscript, 1986; it now is a section of Chapter 15 of the second edition of my cyclotomic fields book).

10. Unique factorization, Fermat's Last Theorem, and quintic polynomials, Proceedings of the Kandy Colloquium on Number Theory (Dec. 1987), 6 pp. (exposition based on #23 above; I do not know whether this article actually appeared).

11. Number fields and elliptic curves, Number Theory and Applications, ed. by R. Mollin, (Proceedings of the NATO Advanced Study Institute, Banff Centre, Canada, 1988), NATO ASI series, Kluwer Academic Publishers, Dordrecht-Boston-London, 1989; pp. 245-278.

12. Abelian number fields of small degree, Algebra and topology 1990 (Taejon, 1990), Proc. KAIST Math. Workshop, 5, Korea Adv. Inst. Sci. Tech., Taejon, 1990, pp. 63-78.

13. Introduction to Iwasawa theory, Topics in Algebra (ed. by Myung-Hwan Kim), Proceedings of Workshops in Pure Mathematics, vol. 10, part I, Korean Academic Council, 1990, pp. 90-95.

14. (with J.-F. Mestre, R. Schoof, D. Zagier) Quotients homophones des groupes libres /Homophonic quotients of free groups, Experim. Math. 2 (1994), 153-155.

15. Wiles' Strategy, Proceedings of "400 años de matemáticas en torno al teorema de Fermat," El Escorial, Spain, 1994.

16. Galois cohomology, in: Modular Forms and Fermat's Last Theorem (ed. by Cornell, Silverman, and Stevens), Springer-Verlag, 1997, pp. 101-120.

17. Cubic fields and zeros of 3-adic L-functions, Proceedings of the Waseda Conference on Number Theory, 1997, 72-77.

18. Review of *Handbook of Elliptic and Hyperelliptic Curve Cryptography* (ed. by H. Cohen and G. Frey), SIGACT NEWS 41, no. 4 (2010).

19. Algebraic Number Theory, in: Handbook of Discrete and Combinatorial Mathematics, 2nd edition, CRC Press (to appear), 9pp.

20. Elliptic Curves, in: Handbook of Discrete and Combinatorial Mathematics, 2nd edition, CRC Press (to appear), 9pp.

21. (with Matthew Yu) Primality Tests Inspired by the Lucas-Lehmer Test, 11pp.

Membership in Honorary or Professional Societies

American Mathematical Society
Phi Beta Kappa
Mathematical Association of America

Recent Service to the Department and University

Mathematics Undergraduate Director (2021 - present)
Mathematics Graduate Director (2011-2016)
Honors Committee Chair (ca. 1988-present)
High School Mathematics Competition Chair (2004-2010), Committee member (1979-present)
Algebra/Number Theory Field Committee Chair
Graduate Committee (ca. 1990-present)
Algebra Exam Writer and Grader (ca. 1990-present)
Salary Committee (2005)
Policy Committee 2012-2013, 2016-2017, 2020-2021
Hiring Committee 2016-2019
Committee to Choose Graduate Coordinator 2017
Priorities Committee (2005, 2006)
Committee to Choose Undergrad. Advisor (2006)
Elementary School Mathematics Committee (2007-8)
Secondary School Mathematics Committee (2007-8)
French and German exams writer/grader (2008-2019)
Maryland Mathematics Institute (2008-2014, 2016-2019)
Banneker-Key Scholarship Selection Committee (2009-2012, 2014-2017, 2023)
CMPS/CMNS APT Committee (2009-2011)
Kirwan Undergraduate Education Award Committee, 2014
TLTC Elevate Fellows participant, 2015
Colloquium Room Committee, 2015-2016
Graduate Council, 2018-2021
Graduate PCC Committee, 2019-2021
English Proficiency Review Committee, 2019
Graduate Research Appreciation Day, Judge, 2019
Maryland Summer Scholars, Reviewer, 2018, 2019, 2020
Committee to redesign Math for Life Sciences, 2018
UK Fellowships STEM Sub-Committee, 2021, 2022, 2023
Goldwater Nomination Committee, 2021, 2022, 2023, 2024
Maryland Day, planner and exhibitor, 2022, 2023, 2024, 2025
Math Success Committee, 2023- present
Math Dept Climate Committee, 2024
UMD Calculus Project Steering Committee, 2022-present
Committee to Review Math Chair Levy, 2023
Search Committee for Math Graduate Coordinator, 2023
Co-PI: Teaching and Learning Innovation Grant, Refining Mathematics Instruction through Student Feedback (with M. Brodsky and D. Chazan), 2024

Co-Director, Brin Mathematics Summer Camp, 2024, 2025
Co-organizer, Vistas in Number Theory conference, Brin Math. Research Center, Univ. Md., June 2024
Co-organizer, MASON VII Conference (Mid-Atlantic Seminar on Numbers), Brin Center, March 2025.

Service to the Mathematical Community

Reviewer for Mathematical Reviews and Zentralblatt
Referee for several journals and NSF, NSA, NSERC, ...
Evaluator for Westinghouse/Intel/Regeneron Competition: 1982-85, 1988-2013, 2016
Judge for Westinghouse Competition: 1998
Question writer for Montgomery County Math. League, 1987, 1998, 2000-2020
Grader for Montgomery County Math. League 1988-90, 1998-2020
Research Mentor for K-12 students: Blair HS Magnet Program: 1989-90 (3 students), 1992-3 (2 students), 1994-5 (2 students), 1997-8 (3 students), 1998-99 (1 student), 1999-2000 (1 student), 2009-2010 (1 student), 2012-2013 (1 student), 2014 (1 student), 2015 (1 student), 2016-2017 (1 student), 2018 -2019 (2 students), 2019-2020 (1 student), 2020-2021 (1 student), 2023 (1 student); Baltimore Poly: 2008-2009 (1 student), 2011-2012 (1 student), 2012-2013 (1 student), 2014-2015 (1 student); homeschooled: 2012 - present (1 student); Feynman School/Takoma Park MS: 2019-present (1 student); Atholton HS: 2019-2020 (1 student); Poolesville HS: 2023 (1 student)
MAA Program Committee (Baltimore meeting), 1992
Expert witness for France Télécom vs. RSA, 2004
Expert witness for Cylink vs. RSA, 1995-1996
NSF Number Theory Advisory Panel, 1996
Contributor to Comprehensive Dictionary of Mathematics, CRC Press, 1997
External reviewer for Dept. of Math., Rutgers Univ., Newark, 1996
NSF Panel for NATO Postdoctoral Fellowships, 1999
External reviewer for Dept. of Math., Loyola College, 2003
Judge, Junior Science and Humanities Symposium, 2005, 2006
Judge, Farmland Elementary School Science Fair, 2004-2010
External thesis examiner, Queen's University (Kingston, Ontario), 2007
Coach, Tilden Middle School Math Team, 2008, 2009
Judge, Society for Science - Middle School Program, 2008
Five lectures at Elliptic Curve Cryptography Workshop, Calgary, 2009
Exhibitor, Howard County Math Fair, 2014, 2015, Howard County STEM Festival 2017
Work on CUPM Curriculum Guide for Majors in the Mathematical Sciences, 2014
Program Committee, BalkanCrypt 2014
Science Fair mentor and judge, SEED School, Spring 2014
Cambridge University Press Textbook Advisor, 2014-present
Judge, William Beanes Elementary School Science Fair, 2015, 2017
Grader, Putnam Exam, 2017, 2019, 2020, 2021
Editorial Board, Ramanujan Journal (2018 - present)
Exhibitor, Girl Scout Council of the Nation's Capital Expo, 2019
Exhibitor, Spooky Mad Science Expo for K to 12, Alexandria, VA, 2023, 2024
Collaborating Editor, American Math. Monthly Problems Section (2019-present)
Associate Editor of the MAA's Problem Books Series (2022 -)
Question writer, Montgomery Middle School Math League, 2022 - present
Statewide Math Group committee, 2024-present
Maryland Applied Calculus Working Group, 2024-present

Grants, Awards, Honors

Séminaire Bourbaki talk on my work (#11 and #12 above) by J. Oesterlé ("Travaux de Ferrero et Washington sur le nombre de classes d'idéaux des corps cyclotomiques"), 1978
Alfred P. Sloan Research Fellow, 1979-1981
John M. Smith Award for Distinguished College or University Teaching (Math. Assoc. of America), 2009
University of Maryland Distinguished Scholar-Teacher, 2011

Fellow of the American Mathematical Society, 2023
NSF/NSA contracts, summers, 1975-1992, 1994-1997, 1999-2000 (because of certain consulting, I stopped applying for grants after 1999)
MSRI Mid-Career Sabbatical Award, 1986-87
Mentor for 8 Westinghouse/Intel Science Talent Search Winners: #1 (1989), #2 (1989), #5(1990) (this one also won the Grand Prize in the 1990 International Science Fair), Top 40 (1992), #8 (1993), #4 (1995), Top 40 (1999), Top 40 (2004).
Certificate of Teaching Excellence/ Merrill Scholar Mentor: 1991, 1994, 1997, 1999, 2008, 2011
Nominee for Outstanding Teacher Award, Panhellenic Assoc. and Interfraternity Council, 1997
Nominee for Teacher of the Year, U.Md. Parents' Assoc., 2001
Dean's Award for Excellence in Teaching, 2003, 2021
Quoted in National Enquirer (2/27/1990)
Track: Age Group All-American: 800m (2016, 2018), 1500m (2006, 2016, 2018), mile (2002, 2006-2018, 2020, 2021, 2022, 2023, 2024), 3000m (2001, 2002, 2007, 2014, 2018); 3rd place in 1500m in National Age Group Track Championships (2006)

Theses Directed

James Kraft	Iwasawa invariants of CM-fields	Ph.D.	May 1987
Yuan-Yuan Shen	Units of Real Cyclic Octic Fields	Ph.D.	Dec. 1988
Mary Conrad	Computing the number of points on an elliptic curve over a finite field	M.A.	May 1990
Patrick Sime	On the ideal class group of real biquadratic fields	Ph.D.	May 1992
Eric Liverance (joint with D. Zagier)	Heights of Heegner Points in a family of elliptic curves	Ph.D.	May 1993
Bruce Lancaster	Estimates of coefficients of Dirichlet series	M.A.	May 1993
Terri Marquiss	Sphere packing densities of lattices arising in number theory	M.A.	Aug. 1993
Boyd Roberts	Q-curves over quadratic fields	Ph.D.	Aug. 1995
Alan Laing	On higher level singular moduli	Ph.D.	Jan. 1996
Mark Morgan	Computing the degree of modular parameterizations of Q-curves	Ph.D.	May 1999
William McGraw (joint with S. Kudla)	Arithmetic properties of modular forms and the Weil representation	Ph.D.	May 2001
Mu-Ling Chang	On the monogenesis of rings of integers in certain sextic fields	Ph.D.	May 2001
Laura Corcoran	Developments in elliptic curve computational techniques	M.A.	Dec. 2002
Edward Eikenberg	Rational points on some families of elliptic curves	Ph.D.	May 2004
Victoria Checa	Investigation into solvable quintics	M.A.	Dec. 2004
Justina Horvath	An investigation of Alexander polynomials	M.A.	Dec. 2005
Prathap Sridharan	A survey of the attack on MD5	M.S.	May 2006
Aliza Steurer	On the Galois groups of the 2-class field towers of some imaginary quadratic fields	Ph.D.	Aug. 2006
Angela Hennessy	Gröbner bases with applications in graph theory	M.A.	Dec. 2006
John Vogler	Linear forms in logarithms and integer points on genus-two curves	Ph.D.	Dec. 2006
Susan Schmoyer	Triviality and non-triviality of Tate-Lichtenbaum self pairings	Ph.D.	May 2007

Gregory Bard	Algorithms for solving linear and polynomial systems of equations over finite fields with applications to cryptanalysis	Ph.D.	Aug. 2007
Kathryn Truman	Analysis and extension of non-commutative NTRU	Ph.D.	Aug. 2007
Tsz Wo (Nicholas) Sze	On solving univariate polynomial equations over finite fields and some related problems	Ph.D.	Dec. 2007
Juliana Belding (joint with R. Bröker)	Number theoretic algorithms for elliptic curves	Ph.D.	Aug. 2008
Haejun Park	Various aspects of digital cash	M.A.	Aug. 2008
Thomas Draper	Nonlinear complexity of Boolean permutations	Ph.D.	May 2009
Enver Ozdemir	Curves and their applications to factoring polynomials	Ph.D.	Aug. 2009
Eleni Agathocleous	Class numbers of real cyclotomic fields of conductor pq	Ph.D.	Aug. 2009
Michael Goldman	Fast hashing into elliptic and hyperelliptic curves	M.A.	Aug. 2011
Chatchawan Panraksa	Arithmetic dynamics of quadratic polynomials and dynatomic units	Ph.D.	Aug. 2011
Jeremy Bradford	Commutative endomorphism rings of simple abelian varieties over finite fields	Ph.D.	Dec. 2012
David Blagg	Unramified extensions of the cyclotomic $\mathbb{Z}_2$-extension of $\mathbb{Q}(\sqrt{d}, i)$	Ph.D.	May 2014
Clarice Dziak Glowacki	Timing attacks on cryptosystems: 18 years later	M.A.	Aug. 2014
Angela Hennessy	An algorithmic approach to invariant rational functions	Ph.D.	Dec. 2014
Morgan Stern	Investigations of highly irregular primes and associated ray class fields	Ph.D.	Dec. 2014
Stephen Balady	Families of cyclic cubic fields	Ph.D.	Aug. 2017
Samuel Bloom	Lang-Trotter questions on the reductions of abelian varieties	Ph.D.	May 2018
Daniel Plummer	Bitcoin, blockchain technology, and secure hash algorithms	M.S. (Howard Univ.)	May 2019
Arijit Sehanobish	Universal deformations and p-adic L-functions	Ph.D.	Aug. 2019
Ariella Kirsch	Ranks of p-class groups in cyclic p-extensions of anti-cyclotomic $\mathbb{Z}_2$-extensions	Ph.D.	Aug. 2019
Steven Reich	Class groups of characteristic-p function field analogues of $\mathbb{Q}(n^{1/p})$	Ph.D.	May 2021
David Pincus	On the divisibility of class numbers in families of number fields	Ph.D.	Dec. 2021
Jermain McDermott	Eventually stable quadratic polynomials over $\mathbb{Q}(i)$	Ph.D.	Aug. 2024
Jordan Hirsh	Polynomials with equal images over number fields	Ph.D.	Aug. 2024

Invited Talks

Around 160 talks in 13 countries

Recent Talks:

Elliptic Curves Course (5 lectures), ECC Conference, Calgary, August 2009
Churchill H.S., December 2009
Sage Conf. on p-adic L-functions and Iwasawa theory, Montréal, Feb. 2010
Math Awareness Day: Math in Sports, Howard Community College, April 2010
Pi Mu Epsilon Lecture, University of Maryland, May 2010
Colloquium, McMaster University, October 2010
Colloquium, Towson University, November 2010
Boston University Math Club, November 2010
Poolesville H.S., March 2011
Colloquium, Temple University, April 2011
SEED School (Washington, DC), April 2011
Conference in Number Theory, Carleton Univ., Ottawa, June 2011
REU (2 lectures), Boise State University, July 2011
Baltimore Math. Circle, October 2011
Colloquium, Morgan State, October 2011
Johns Hopkins Alumni Association, February 2012
Colloquium, Boise State, March 2012
Towson Undergrad. Research Conf., March 2012
Sherwood H.S., May 2012
Annual Meeting, Pacific Div. of AAAS (Boise, Idaho), June 2012
Poolesville H.S., November 2012
Colloquium, Montgomery College, April 2013
Colloquium, Howard University, September 2013
Number Theory Seminar, Arizona State, November 2013
Crypto Rally Talk, Arizona State, November 2013
SEED School (Washington, DC), November 2013
REU, Boise State University, July 2014
G. Milton Wing Lectures (3 lectures), University of Rochester, September/October 2014
Churchill H.S., October 2014
MAA Invited Lecture, Bowie, November 2014
Middlebury College, November 2014
Colloquium, Montgomery College, April 2015
SIAM Research Awareness Day, Old Dominion University, April 2015
STEM Night, Takoma Park Middle School, April 2015
Career Day, Quibbletown (N.J.) Middle School, June 2015
Wilde Lake H.S., October 2015
Georgetown University Math Club, February 2016
West Chester University, Colloquium, February 2016
STEM Night, Takoma Park Middle School, April 2016
REU, University of Maryland, July 2016
REU, Boise State University, July 2016
Montgomery Blair H.S. Math Club, October 2016
STEAM Night, Takoma Park Middle School, March 2017
Colloquium, University of Virginia, October 2017
Montgomery Blair H.S. Math Club, December 2017
STEAM Night, Takoma Park Middle School, April 2018
Georgetown University Math Club, November 2018
Helen Barton Lecture, UNC Greensboro, February 2019
Spring Colloquium, American University, April 2019
Gilman School, May 2019

C. E. Smith J. D. S., November 2019
Colloquium, Howard University, January 2020
AMS Meeting, Charlottesville, VA (45-minute lecture; canceled by COVID), March 2020
International Conference on Class Groups of Number Fields and Related Topics (ICCGNFRT 2021), October 2021
Iwasawa Theory Virtual Seminar, March 2022
AMS Special Session on Iwasawa Theory, Amherst, MA, October 2022
Seminar, Louisiana State Univ., October 2022
International Conference on Class Groups of Number Fields and Related Topics (ICCGNFRT 2022), Kozhikode, India, November 2022
International Conference on Special Functions and Applications (ICSFA-22), Mysore, India, November 2022
Seminar, Univ. Virginia, February 2023
Seminar, Univ. Georgia, April 2023
International Conference on Class Groups of Number Fields and Related Topics (ICCGNFRT 2023), Kozhikode, India, November 2023
AMS Special Session, Howard Univ., April 2024
International Conference on Class Groups of Number Fields and Related Topics (ICCGNFRT 2023), Berhampur, India, November 2024
International Conference on Diophantine Equations, Polynomials and Related Areas (ICDEPRA) -2024, New Delhi, India, November 2024

2/7/2025