

## CURRICULUM VITAE

Lawrence C. Washington  
Born 1951 in Vermont, U. S. citizen

Department of Mathematics  
University of Maryland  
College Park, Maryland 20742  
e-mail: lcw@math.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

### 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
C.E.M., Perugia, Italy	August 2004

### 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.

Typeset by  $\mathcal{A}\mathcal{M}\mathcal{S}$ -TEX

10. Kummer's calculation of  $L_p(1, \chi)$ , *J. reine angew. Math.* 305 (1979), 1-8.
11. (with B. Ferrero) The Iwasawa invariant  $\mu_p$  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  $\mu_p$ , *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  $\ell$ -adic Iwasawa  $\lambda$ -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) (these originally were one paper, but it had to be split into three parts)
  - (a) 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).
  - (b) Heuristics and related results on class groups of real quadratic fields, Science in China(=Scientia Sinica) 41 (1998), no. 4, 365-370.
  - (c) 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).
39. (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.
40. Some remarks on Fibonacci matrices, Fibonacci Quarterly 37 (1999), 333-341.
41. (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.
42. (with C. Helou and R. Roll) Power residue character of rational primes, J. Ramanujan Math. Soc. 16 (2001), 19-37.
43. (with J. Kraft) Heuristics for class numbers and  $\lambda$ -invariants, Mathematics of Computation 76 (2007), 1005-1023.

#### Research Articles not yet accepted for publication

1. (with R. Schoof) Visibility of ideal classes, preprint, 14 pp. (to be submitted soon)
2. Computing roots of unity: Appendix to "On Taking Square Roots and Finding Quadratic Nonresidues in Finite Fields" by Tsz-Wo Sze (2007).
3. (with D. Hubbard) Kummer generators and lambda invariants, about 10pp. (2008).

#### 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.).
- 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.).

#### 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 Quarterly 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 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 (to appear; 20 pp.).
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 (to appear, 2008; 3 pp.).

#### Membership in Honorary or Professional Societies

American Mathematical Society  
Phi Beta Kappa

Mathematical Association of America

### Recent Service to the Department

Honors Committee Chair  
 High School Mathematics Competition Chair  
 Algebra/Number Theory Field Committee Chair  
 Graduate Committee  
 Algebra Exam Writer and Grader  
 Salary Committee (2005)  
 Priorities Committee (2005, 2006)  
 Committee to Choose Undergrad. Advisor (2006)  
 Elementary School Mathematics Committee (2007-8)  
 Secondary School Mathematics Committee (2007-8)

### Service to the Mathematical Community

Reviewer for Mathematical Reviews and Zentralblatt  
 Referee for several journals and NSF, NSA, NSERC, ...  
 Evaluator for Westinghouse/Intel Competition: 1982-85, 1988-present  
 Judge for Westinghouse Competition: 1998  
 Question writer for Montgomery County Math. League, 1987, 1998, 2000-present  
 Grader for Montgomery County Math. League 1988-90, 1998-present  
 Research Mentor for Senior Projects, Blair H. S. 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)  
 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  
 NSA Mathematics Oversight Panel, 2001-present  
 External reviewer for Dept. of Math., Loyola College, 2003  
 Judge, Junior Science and Humanities Symposium, 2005, 2006  
 External thesis examiner, Queen's University (Kingston, Ontario), 2007  
 Coach, Tilden Middle School Math Team, 2008

### 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  
 NSF/NSA contracts, summers, 1975-1992, 1994-1997, 1999, 2000 (because of certain consulting, I stopped applying for grants in 1999)  
 MSRI Mid-Career Sabbatical Award, 1986-87  
 Mentor for 8 Westinghouse 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, 1991, 1994, 1997, 1999

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

Quoted in National Enquirer, 1989

Track: Age Group All-American: 1500m (2006), mile (2002, 2006, 2007, 2008), 3000m (2001, 2002); 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	Ph.D.	Aug. 2007

	fields with applications to cryptanalysis		
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	Number theoretic algorithms for elliptic curves	Ph.D.	Aug. 2008

*Current Ph.D. students and projected finishing dates:* Thomas Draper (2008), Enver Ozdemir (2009), Eleni Agathocleous (2009),

*Current M.A./M.S. thesis students and projected finishing dates:* Les Kartchner (2008), Haejun Park (2008).

### Invited Talks

Around 120 talks in 13 countries

5/5/2008