

Jonathan P. Sorenson

Office: Department of Computer Science and Software Engineering Phone: (317) 940-9765
Butler University Fax: (317) 940-9014
4600 Sunset Avenue E-mail: sorenson@butler.edu
Indianapolis, IN 46208 URL: <http://www.butler.edu/~sorenson/>

Education

University of Wisconsin-Madison, Fall 1986–Summer 1991:

Ph. D. in Computer Sciences with a Minor in Mathematics, August 1991.

Advisor: Eric Bach. Thesis Title: *Algorithms in Number Theory*.

Qualifiers passed: Operating Systems, Database, Theory.

M. A. in Mathematics, May 1989.

M. S. in Computer Sciences, December 1987.

Valparaiso University (Indiana), Fall 1982–Spring 1986:

B. S. in Computer Science with a Minor in Physics, May 1986.

B. S. in Mathematics, May 1986.

Experience

Head, Computer Science and Software Engineering, Butler University. Fall 2005–Present.

Professor, Computer Science and Software Engineering, Butler University. Spring 2004–Present.

Interim Head, Mathematics and Actuarial Science, Butler University. Fall 2006–Summer 2007.

Associate Professor, Computer Science and Software Engineering, Butler University. Fall 1999–Spring 2004.

Associate Professor, Mathematics and Computer Science, Butler University. Spring 1997–Fall 1999.

Assistant Professor, Mathematics and Computer Science, Butler University. Fall 1991–Spring 1997.

Visiting Scholar, Computer Science, Purdue University. Fall 1998.

Grants and Awards

External Grants

NSF Conference Travel Grant with Joshua Holden, May 2008. \$10,600.

NSA Conference Travel Grant, May 2008. \$10,500.

NSA Conference Travel Grant, May 2003. \$10,000.

NSF CSEMS Grant DUE-0123109, with Z.-H. Chen, P. Henderson, and P. Linos,
September 2001–July 2005. \$199,500.

NSF RUI Grant CCR-9626877, October 1996–September 1998. \$59,150.

NSF RUI Grant CCR-9204414, August 1992–July 1994. \$49,352.

Teaching Incentive Grant, General Electric Foundation, 1990. \$5,000.

Internal Grants and Awards

Butler University Research Grant, June 2009–May 2010. \$9,000.

Butler University Research Grant with Ankur Gupta, June 2008–May 2009. \$9,200.

Butler University Fellowship, June 2007–May 2008. \$3,000.

LAS Natural Sciences Faculty Member of the Year Award, Spring 2007.

Butler University Fellowship, June 2006–May 2007. \$3,200.

Butler University Research Grant with Scott Parsell, June 2005–May 2006. \$9,870.

Butler University Fellowship, June 2004–May 2005. \$3,480.

Butler University Fellowship, June 2001–May 2002. \$3,150.

Butler University Fellowship, June 2000–December 2000. \$2,750.

Butler University Fellowship, June 1999–May 2000. \$3,500.

HRI Faculty Grant, June 1998–May 1999, \$13,713.

Butler University Fellowship, June 1996–May 1997. \$2,750.

HRI Faculty Grant, June 1996–May 1997. \$4,600.

Butler University Fellowship, June 1995–May 1996. \$3,500.

HRI Faculty Grant with Amos Carpenter and Zhi-Hong Chen, September 1993–May 1994. \$20,000.

Butler University Fellowship, June 1992–May 1993. \$2,200.
Wisconsin Alumni Research Foundation Fellowship, Fall 1986–Summer 1987.
Outstanding Student Award, Computer Sciences Department, Fall 1986, Spring 1987. \$2,000.

Professional Organizations

Association for Computing Machinery
ACM SIGACT (Special Interest Group on Algorithms and Computation Theory)
ACM SIGCSE (Special Interest Group on Computer Science Education)
ACM SIGSAM (Special Interest Group on Symbolic and Algebraic Manipulation)
American Mathematical Society
Consortium for Computing in Small Colleges
Kappa Mu Epsilon

Committee Service

University Level:

Faculty Senate, Fall 2008–Present.
Student Conduct Board, Fall 2009–Present.
University Core Curriculum: Area 1, Fall 2009–Present.
Butler Brown Bag Seminar Series Organizer, Fall 2005–Present.
Science, Technology, and Society Committee, Fall 2005–Present.
Science Initiative Group, Summer 2003.
J. James Woods Lectures Committee, Fall 2001–Present.
Mathematics and Actuarial Science Search Committee, Fall 2002–Spring 2003.
Holcomb Awards Committee, Fall 1999–Spring 2004 (served as chair).
Faculty Assembly Executive Committee, Fall 1995–Spring 1997, Fall 2006–Spring 2008.
Writing Council, Fall 1994–Spring 2007.
Information Technology Planning Committee, Fall 1994–Spring 1995.
Information Resources Search Committee Chair, Fall 1993–Spring 1994.
College of Education Search Committee (for Math/Science faculty), Fall 1993–Spring 1994.
Computer Advisory Board Committee, Fall 1992–Spring 1994.

College Level (Liberal Arts and Sciences):

LAS Development Committee, Fall 2009–Present.
External member, Psychology Promotion and Tenure Committee, Fall 2009.
LAS Honors Board, Fall 2001–Spring 2003 (chair for 2002–2003).
LAS Professional Standards Committee, Fall 2001–Spring 2003, Fall 2005–Spring 2009 (chair).
LAS Scholarship Committee, Spring 2001, Spring 2002.
LAS Committee on Academic Change and Improvement, Fall 1997–Spring 1999.
LAS Curriculum Committee, Fall 1991–Spring 1994.

Professional Activities

PhD Thesis Committee for Nichole Pitcher, University of Illinois at Chicago, Fall 2008–Spring 2009.
Program Chair, Math and CS Division, Butler Undergraduate Research Conference, 1992–2000.
Faculty Advisor for the Computer Science Club/ACM Student Chapter, Fall 1991–Present.
Academic advisor for 25–30 students.
Science Olympiad event coordinator, Spring 1994, 1996, 1997, 1999, 2000, 2002, 2006, 2009, and 2010.
Organized the following meetings/conferences:
Organizing committee member and poster session chair, *ANTS VIII*, Banff, Alberta Canada, May 2008.
(with Scott Parsel) *Number Theory and Cryptography*,
AMS Sectional Meeting, Notre Dame University, April 8–9, 2006.
Program committee member, *ANTS VI*, University of Vermont, June 2004.
(with Michael Jacobson, Jr., Renate Scheidler, Andreas Stein, and Gary Walsh)
Conference on Number Theory in Celebration of the 60th Birthday of Hugh C. Williams,
Banff, Alberta, Canada, May 23–28, 2003.

(with Joshua Holden, Jon Rickert, and Andreas Stein) *Computational and Algorithmic Number Theory and Cryptography*,

AMS Sectional Meeting, Indiana University, April 4-6 2003.

(with Eric Bach) *Computational and Algorithmic Number Theory and Cryptography*,

AMS Sectional Meeting, Ohio State University, September 21-23, 2001.

(with Eric Bach) *Number Theory, Algorithms, and Cryptography*,

AMS Sectional Meeting, Notre Dame, April 8-9, 2000.

30th Midwest Theory Day, Butler University, April 23rd, 1994.

Referee for the following journals:

The Computer Journal; *Designs, Codes, and Cryptography*; *Discrete and Applied Mathematics*; *Finite Fields and Their Applications*; *Information Processing Letters*; *Information and Computation*; *IEEE Transactions on Information Theory*; *J. Algorithms*; *J. Number Theory*; *Mathematics of Computation*.

Referee for the following conferences:

The Midwest Conference of the *Consortium for Computing in Small Colleges*, *ACM SIGCSE Technical Symposium*, *ANTS*, *ISSAC*, *STACS*.

Reviewed grant proposals for the National Science Foundation.

Reviewer for *Zentralblatt für Mathematik* and *Mathematical Reviews*.

Reviewed the *CRC Handbook of Applied Cryptography*.

External Program Reviewer for Computer Science at Xavier University, 1999.

Presentations at Meetings and Conferences

“Fast Bounds on the Distribution of Smooth Numbers,”

7th Algorithmic Number Theory Symposium, Berlin, Germany, July 23–28, 2006.

“The Pseudosquares Prime Sieve,”

7th Algorithmic Number Theory Symposium, Berlin, Germany, July 23–28, 2006.

“Computing Prime Harmonic Sums” (poster),

7th Algorithmic Number Theory Symposium, Berlin, Germany, July 23–28, 2006.

“Lehmer’s Algorithm for Very Large Numbers” (poster),

6th Algorithmic Number Theory Symposium,

University of Vermont, June 13-18, 2004. (*SIGSAM Bulletin*, 38(3) 2004.)

“An Analysis of the Generalized Binary GCD Algorithm,”

Conference in Number Theory in Honour of H.C. Williams (invited),

The Banff Center, Banff, Alberta Canada, May 29, 2003.

“A Fast Algorithm for Approximately Counting Smooth Numbers,”

2001 Illinois Number Theory Conference,

University of Illinois at Urbana-Champaign, May 18, 2001.

“A Fast Algorithm for Approximately Counting Smooth Numbers,”

4th Algorithmic Number Theory Symposium,

University of Leiden, The Netherlands, July 5, 2000.

“A Fast Algorithm for Approximately Counting Smooth Numbers,”

Math 2000, Cryptography and Number Theory Symposium (invited),

McMaster University, Hamilton Ontario, Canada, June 11, 2000.

“A Sublinear-Time Algorithm for Integer Modular Exponentiation,”

Conference on the Mathematics of Public-Key Cryptography,

Fields Institute, Toronto Ontario, Canada, June 12, 1999.

“Trading Time for Space in Prime Number Sieves,” 3rd Algorithmic Number Theory Symposium,

Reed College, Portland Oregon, June 21, 1998.

“Trading Time for Space in Prime Number Sieves,” Midwest Theory Day,

University of Kentucky, April 4, 1998.

“Trading Time for Space in Prime Number Sieves,” AMS Regional Meeting,

University of Wisconsin-Milwaukee, October 25, 1997. (927-68-24)

“Genetic Algorithms for the Extended GCD Problem” (poster), ISSAC’97,

Maui, Hawaii, July 21, 1997. (*SIGSAM Bulletin*, 31(3):34–35, 1997.)

“A Genetic Algorithm for the Extended GCD Problem,” Midwest Theory Day,
Indiana University, April 19, 1997.

- “Efficient Algorithms for Computing the Jacobi Symbol,”
2nd Algorithmic Number Theory Symposium,
University of Bordeaux, France, May 19, 1996.
- “Efficient Algorithms for Computing the Jacobi Symbol,” AMS Regional Meeting,
Kent State University, November 3, 1995.
- “An Analysis of Lehmer’s Euclidean GCD Algorithm,”
1995 International Symposium on Symbolic and Algebraic Computation,
Concordia University, Montreal, August 12th, 1995.
- “Some Recent Results in Prime Number Sieves,” Midwest Theory Day,
University of Chicago, December 3, 1994.
- “Analysis of a left-shift Binary GCD Algorithm,” Algorithmic Number Theory Symposium,
Cornell University, Ithaca, New York, May 1994.
- “Explicit Bounds for Primes in Residue Classes,”
Lehmer minisymposium of the 50th Anniversary Meeting of *Mathematics of Computation*,
University of British Columbia at Vancouver, August 13th, 1993.
- “An Analysis of Pollard’s $p - 1$ Integer Factoring Algorithm,” Midwest Theory Colloquium,
Indiana University, April 11th, 1992.
- “The k -ary GCD Algorithm,” 23rd Midwest Theory Consortium,
Northwestern University, December 1st, 1990.

Invited Hour-Long Presentations

- Three one-hour lectures as part of the summer school on
Computational Number Theory and Applications to Cryptography,
University of Wyoming, June 19-23, 2006.
- “Fast algorithms for bounding the distribution of smooth integers,”
Number Theory Inspired by Cryptography workshop,
Banff International Research Station, Alberta Canada, November 6, 2005.
- “The Pseudosquares Prime Number Sieve,”
Computer Sciences Seminar,
University of Wisconsin-Madison, May 23, 2005.
- “The Pseudosquares Prime Number Sieve,”
Center for Information Security and Cryptography Seminar,
University of Calgary, Alberta Canada, March 18, 2005.
- “Algorithms for Computing the Greatest Common Divisor,”
Center for Information Security and Cryptography Seminar,
University of Calgary, Alberta Canada, October 17, 2003.
- “Algorithms for Computing the Greatest Common Divisor,” Information Protection Seminar,
University of Illinois at Urbana-Champaign, October 17, 2001.
- “Introduction to Cryptology,” Mathematics/Physics Colloquium,
Miami University of Ohio, January 28, 1998.
- “Genetic Algorithms and the Extended GCD Problem,” Mathematics Colloquium,
Wabash College, October 7, 1997.
- “Introduction to Cryptology,” Mathematics/Physics Colloquium,
Western Illinois University, October 28th, 1996.
- “Some Recent Results in Prime Number Sieves,” Discrete Mathematics Colloquium,
Auburn University, May 3, 1996.
- “Some Recent Results in Prime Number Sieves,” Computer Science Colloquium,
Indiana University, January 27, 1995.
- “Some Recent Results in Prime Number Sieves,” Theoretical Computer Science Seminar,
University of Cincinnati, October 26, 1994.
- “Explicit Bounds for Primes in Residue Classes,” Mathematics Colloquium,
CWI, Amsterdam, June 29th, 1993.
- “GCD Algorithms,” Computer Science Colloquium, University of Waterloo, July 27th, 1992.
- “GCD Algorithms,” Computer Science Colloquium, Purdue University, November 25th, 1991.
- “The k -ary GCD Algorithm,” Parallel Computing Research Colloquium,
Valparaiso University, October 1990.

Publications

Co-authors that were Butler undergraduates at time of submission are in boldface.

Refereed Journal and Conference Research Papers

1. A. Gupta, **A. Kispert**, and J. Sorenson, Online Sorting via Searching and Selection, submitted. Available from ArXiv.org.
2. J. Sorenson, A Sublinear Time Randomized Parallel GCD Algorithm for the EREW PRAM, submitted. Available from ArXiv.org.
3. E. Bach, D. Klyve, and J. Sorenson, Computing Prime Harmonic Sums, *Mathematics of Computation* 78:2283-2305, 2009.
4. D. J. Bernstein and J. Sorenson, Modular Exponentiation via the Explicit Chinese Remainder Theorem, *Mathematics of Computation* 76,257:443-454, 2007.
5. S. Parsell and J. Sorenson, Fast Bounds on the Distribution of Smooth Numbers, *Proceedings of the 7th International Symposium on Algorithmic Number Theory (ANTS-VII)*, Florian Hess, Sebastian Pauli, and Michael Pohst eds., Berlin, Germany, pages 168-181, 2006. LNCS 4076, ISBN 3-540-36075-1.
6. J. Sorenson, The Pseudosquares Prime Sieve, *Proceedings of the 7th International Symposium on Algorithmic Number Theory (ANTS-VII)*, Florian Hess, Sebastian Pauli, and Michael Pohst eds., Berlin, Germany, pages 193-207, 2006. LNCS 4076, ISBN 3-540-36075-1.
7. J. Sorenson, An Analysis of the Generalized Binary GCD Algorithm, *High Primes and Misdemeanors: Lectures in Honour of the 60th Birthday of Hugh Cowie Williams*, Alf van der Poorten and Andreas Stein eds., Banff, Alberta, Canada, 2004. (MR 2005h:11279)
8. J. Sorenson, A fast algorithm for approximately counting smooth numbers, *Proceedings of the Fourth International Symposium on Algorithmic Number Theory (ANTS-IV)*, W. Bosma ed., Leiden, The Netherlands, July 2000, Springer-Verlag LNCS 1838.
9. **S. Meyer Eikenberry** and J. Sorenson, Efficient algorithms for computing the Jacobi symbol, *Journal of Symbolic Computation* 26(4):509–523, 1998. (MR 99h:11146)
Extended abstract appeared in the *Proceedings of the Second International Symposium on Algorithmic Number Theory (ANTS-II)*, H. Cohen ed., Bordeaux, France, May 1996. Springer-Verlag LNCS 1122. (MR 97m:11157)
10. J. Sorenson, Trading time for space in prime number sieves, *Proceedings of the Third International Symposium on Algorithmic Number Theory (ANTS-III)*, J. Buhler ed., Portland, Oregon, June 1998, pages 179–195. Spring-Verlag LNCS 1423.
11. **S. Hunter** and J. Sorenson, Approximating the number of integers with small prime factors. *Mathematics of Computation* 66:1729–1741, 1997. (MR 98c:11093)
12. E. Bach and J. Sorenson, Explicit Bounds for Primes in Residue Classes. *Mathematics of Computation* 65(216):1717–1735, 1996. (MR 97a:11143)
Preliminary version appeared in the proceedings of *Mathematics of Computation 1943–1993: A Half-Century of Computational Mathematics. Mathematics of Computation 50th Anniversary Symposium*, W. Gautschi, ed., Vancouver, British Columbia, Canada, August 9–13, 1993. Published in *AMS Proceedings of Symposia in Applied Mathematics*, 48:535–539, 1994. (MR 96e:11152)
13. **B. Dunten**, **J. Jones**, and J. Sorenson, A space-efficient fast prime number sieve. *Information Processing Letters* 59:79–84, 1996. (MR 97g:11141)
14. C. Pomerance and J. Sorenson, Counting the Integers Factorable via Cyclotomic Methods. *Journal of Algorithms* 19:250–265, 1995. (MR 96e:11163)
This work is an improvement and extension of: J. Sorenson, *Counting the Integers Cyclotomic Methods Can Factor*, Computer Sciences Technical Report #919, University of Wisconsin-Madison, March 1990.

15. J. Sorenson, Analysis of Lehmer's Euclidean GCD algorithm. Proceedings of the 1995 ACM International Symposium on Symbolic and Algebraic Computation (ISSAC'95), pages 254–258.
16. J. Shallit and J. Sorenson, Analysis of the left-shift binary GCD algorithm. *Journal of Symbolic Computation* 17:473–486, 1994. (MR 95g:68057, 96f:11168)
Preliminary version appeared in the *Proceedings of the First International Symposium on Algorithmic Number Theory* (ANTS-I), L. M. Adleman and M.-D. Huang eds., Ithaca, NY, May 1994, pp. 169–183. Springer-Verlag LNCS 877.
17. J. Sorenson and I. Parberry, Two Fast Parallel Prime Number Sieves, *Information and Computation* 114(1):115–130, 1994. (MR 95h:11097)
A preliminary version appeared as Technical Report CRPDC-91-8, Center for Research in Parallel and Distributed Computing, Department of Computer Sciences, University of North Texas, July 1991.
18. J. Sorenson, Polylog Depth Circuits for Integer Factoring and Discrete Logarithms, *Information and Computation* 110(1):1–18, 1994. (MR 95j:11120)
A preliminary version appeared as Computer Sciences Technical Report #872, University of Wisconsin-Madison, August 1989.
19. J. Sorenson, Two Fast GCD Algorithms. *Journal of Algorithms* 16:110–144, 1994. (MR 94k:11135)
A preliminary version appeared as Computer Sciences Technical Report #979, University of Wisconsin-Madison, November 1990.
20. E. Bach and J. Sorenson, Sieve Algorithms for Perfect Power Testing, *Algorithmica* 9:313–328, 1993. (MR 94d:11103)
Appeared previously as Computer Sciences Technical Report #852, University of Wisconsin-Madison, June 1989.

Non-Refereed Papers and Tech Reports (not mentioned previously)

1. J. Sorenson, A sublinear-time parallel algorithm for integer modular exponentiation, *Proceedings of the Conference on The Mathematics of Public Key Cryptography*, The Fields Institute, University of Toronto, Ontario Canada, June 12-17, 1999.
2. J. Shallit and J. Sorenson, A Binary Algorithm for the Jacobi Symbol, *SIGSAM Bulletin*, 27(1):4–11, January 1993.
3. J. Sorenson, *An Analysis of Two Prime Number Sieves*, Computer Sciences Technical Report #1028, University of Wisconsin-Madison, June 1991.
4. J. Sorenson, *Algorithms in Number Theory*, PhD Thesis, Computer Sciences Technical Report #1027, University of Wisconsin-Madison, June 1991.
5. J. Sorenson, *An Introduction to Prime Number Sieves*, Computer Sciences Technical Report #909, University of Wisconsin-Madison, January 1990.

Teaching-Related Publications (Refereed)

1. J. Sorenson and P. K. Linos, EPICS: A Service Learning Program at Butler University, *Proceedings of the 35th Annual IEEE Frontiers in Education Conference*, Indianapolis, Indiana USA, pages F2F-21–F2F-25, 2005. ISBN 0-7803-9077-6.
2. J. Sorenson, An honors course on Alan M. Turing, *SIGCSE Bulletin Inroads* 37,4:103-106, 2005.
3. J. Sorenson, Experiences with Writing Assignments in Upper-Division Computer Science Courses, Chapter 4 in *Teaching in the 21st Century: Adapting Writing Pedagogies to the College Curriculum*. Alice Robertson and Barbara Smith, eds., Falmer Press, New York, 1999.

Other Stuff

1. J. Sorenson, Poster Abstracts ANTS-8, *SIGSAM Bulletin* 164(2):48–66, 2008.

2. J. Sorenson, Lehmer's algorithm for very large numbers (poster abstract), in I. Kotsireas and E. Volcheck, ANTS VI Poster Abstracts, *SIGSAM Bulletin* 38,3:102-104, 2004. (Refereed)
3. **V. Piehl**, J. Sorenson, and **N. Tiedeman**, Genetic algorithms for the extended GCD problem, Accepted to the *Journal of Symbolic Computation* but never printed.
Posters presented at the *1997 CUR Poster Session on Capitol Hill*, and at ISSAC'97, which appeared on pp. 34–35, in M. J. Encarnación, ISSAC'97 Poster Abstracts, *SIGSAM Bulletin* 31(3):29–61, 1997. (Refereed)
4. J. Sorenson, 30th Midwest Theory Day (Conference Report), *SIGACT News* 25(3):97–101, 1994.