Bibliography

John Abbott. Sparse squares of polynomials. *Math. Comp.*, 71(237):407–413, 2002. ISSN 0025-5718.
doi: 10.1090/S0025-5718-00-01294-1. Referenced on pages 106 and 112.

John Abbott and Anna Maria Bigatti. CoCoALib: a C++ library for doing computations in commutative algebra. Online, February 2011.
URL http://cocoa.dima.unige.it/cocoalib. Version 0.9942. Referenced on page 22.

Karl Abrahamson. Time-space tradeoffs for branching programs contrasted with those for straight-line programs. In *Foundations of Computer Science, 1986., 27th Annual Symposium on*, pages 402–409, October 1986.
doi: 10.1109/SFCS.1986.58. Referenced on page 57.

Alok Aggarwal and Jeffrey Scott Vitter. The input/output complexity of sorting and related problems. *Commun. ACM*, 31:1116–1127, September 1988. ISSN 0001-0782.
doi: 10.1145/48529.48535. Referenced on page 11.

D. Angluin and L. G. Valiant. Fast probabilistic algorithms for hamiltonian circuits and matchings. *Journal of Computer and System Sciences*, 18(2):155 – 193, 1979. ISSN 0022-0000.
doi: 10.1016/0022-0000(79)90045-X. Referenced on pages 10, 11 and 14.

V. L. Arlazarov, E. A. Dinic, M. A. Kronrod, and I. A. Faradžev. The economical construction of the transitive closure of an oriented graph. *Dokl. Akad. Nauk SSSR*, 194:487–488, 1970. ISSN 0002-3264. Referenced on page 17.

Martín Avendaño, Teresa Krick, and Ariel Pacetti. Newton-Hensel interpolation lifting. *Found. Comput. Math.*, 6(1):81–120, 2006. ISSN 1615-3375.
doi: 10.1007/s10208-005-0172-3. Referenced on pages 121 and 146.

Eric Bach. Number-theoretic algorithms. *Annual Review of Computer Science*, 4(1):119–172, 1990.
doi: 10.1146/annurev.cs.04.060190.001003. Referenced on page 150.

Eric Bach and Jeffrey Shallit. *Algorithmic number theory. Vol. 1.* Foundations of Computing Series. MIT Press, Cambridge, MA, 1996. ISBN 0-262-02405-5. Referenced on pages 10 and 127.

Eric Bach and Jonathan Sorenson. Sieve algorithms for perfect power testing. *Algorithmica*, 9:313–328, 1993. ISSN 0178-4617.
doi: 10.1007/BF01228507. Referenced on page 95.

David H. Bailey. FFTs in external or hierarchical memory. *The Journal of Supercomputing*, 4: 23–35, 1990. ISSN 0920-8542.
doi: 10.1007/BF00162341. Referenced on page 37.

R. C. Baker and G. Harman. The Brun-Titchmarsh theorem on average. In *Analytic number theory, Vol. 1 (Allerton Park, IL, 1995)*, volume 138 of *Progr. Math.*, pages 39–103. Birkhäuser Boston, Boston, MA, 1996. Referenced on page 155.

Paul Barrett. Implementing the Rivest Shamir and Adleman public key encryption algorithm on a standard digital signal processor. In Andrew Odlyzko, editor, *Advances in Cryptology âĂŤ CRYPTOâĂŹ 86*, volume 263 of *Lecture Notes in Computer Science*, pages 311–323. Springer Berlin / Heidelberg, 1987.
doi: 10.1007/3-540-47721-7_24. Referenced on page 29.

Walter Baur and Volker Strassen. The complexity of partial derivatives. *Theoretical Computer Science*, 22(3):317 – 330, 1983. ISSN 0304-3975.
doi: 10.1016/0304-3975(83)90110-X. Referenced on page 5.

Michael Ben-Or and Prasoon Tiwari. A deterministic algorithm for sparse multivariate polynomial interpolation. In *Proceedings of the twentieth annual ACM symposium on Theory of computing*, STOC '88, pages 301–309, New York, NY, USA, 1988. ACM. ISBN 0-89791-264-0.
doi: 10.1145/62212.62241. Referenced on pages 24, 119 and 122.

E. R. Berlekamp. Factoring polynomials over finite fields. *Bell System Tech. J.*, 46:1853–1859, 1967. ISSN 0005-8580. Referenced on page 7.

Daniel J. Bernstein. Detecting perfect powers in essentially linear time. *Math. Comp.*, 67(223): 1253–1283, 1998. ISSN 0025-5718.
doi: 10.1090/S0025-5718-98-00952-1. Referenced on pages 95 and 114.

Markus Bläser, Moritz Hardt, Richard J. Lipton, and Nisheeth K. Vishnoi. Deterministically testing sparse polynomial identities of unbounded degree. *Information Processing Letters*, 109(3):187 – 192, 2009. ISSN 0020-0190.
doi: 10.1016/j.ipl.2008.09.029. Referenced on pages 126, 139 and 145.

A. Borodin and S. Cook. A time-space tradeoff for sorting on a general sequential model of computation. In *Proceedings of the twelfth annual ACM symposium on Theory of computing*, STOC '80, pages 294–301, New York, NY, USA, 1980. ACM. ISBN 0-89791-017-6.
doi: 10.1145/800141.804677. Referenced on page 11.

A. Borodin and I. Munro. *The computational complexity of algebraic and numeric problems.* Number 1 in Elsevier Computer Science Library; Theory of Computation Series. American Elsevier Pub. Co., New York, 1975. ISBN 0444001689 0444001565. Referenced on page 141.

Allan Borodin and Prasoon Tiwari. On the decidability of sparse univariate polynomial interpolation. *Computational Complexity*, 1:67–90, 1991. ISSN 1016-3328. doi: 10.1007/BF01200058. Referenced on page 138.

Robert S. Boyer and J. Strother Moore. MJRTY — a fast majority vote algorithm. In Robert S. Boyer, editor, *Automated Reasoning: Essays in Honor of Woody Bledsoe*, Automated Reasoning, pages 105–117. Kluwer Academic Publishers, Dordrecht, The Netherlands, 1991. URL http://www.cs.utexas.edu/~moore/best-ideas/mjrty/index.html. Referenced on page 86.

Richard Brent and Paul Zimmermann. *Modern Computer Arithmetic*. Number 18 in Cambridge Monographs on Applied and Computational Mathematics. Cambridge Univ. Press, November 2010. Referenced on pages 28 and 55.

Peter Bürgisser and Martin Lotz. Lower bounds on the bounded coefficient complexity of bilinear maps. *J. ACM*, 51:464–482, May 2004. ISSN 0004-5411. doi: 10.1145/990308.990311. Referenced on page 56.

John F. Canny, Erich Kaltofen, and Lakshman Yagati. Solving systems of nonlinear polynomial equations faster. In *Proceedings of the ACM-SIGSAM 1989 international symposium on Symbolic and algebraic computation*, ISSAC '89, pages 121–128, New York, NY, USA, 1989. ACM. ISBN 0-89791-325-6. doi: 10.1145/74540.74556. Referenced on page 118.

David G. Cantor and Erich Kaltofen. On fast multiplication of polynomials over arbitrary algebras. *Acta Informatica*, 28:693–701, 1991. ISSN 0001-5903. doi: 10.1007/BF01178683. Referenced on pages 7, 20, 56 and 70.

David G. Cantor and Hans Zassenhaus. A new algorithm for factoring polynomials over finite fields. *Math. Comp.*, 36(154):587–592, 1981. ISSN 0025-5718. doi: 10.2307/2007663. Referenced on page 7.

Bernard Chazelle. A spectral approach to lower bounds with applications to geometric searching. *SIAM Journal on Computing*, 27(2):545–556, 1998. doi: 10.1137/S0097539794275665. Referenced on page 11.

Michael Clausen, Andreas Dress, Johannes Grabmeier, and Marek Karpinski. On zero-testing and interpolation of k-sparse multivariate polynomials over finite fields. *Theoretical Computer Science*, 84(2):151–164, 1991. ISSN 0304-3975. doi: 10.1016/0304-3975(91)90157-W. Referenced on page 118.

Stephen A. Cook and Robert A. Reckhow. Time bounded random access machines. *Journal of Computer and System Sciences*, 7(4):354–375, 1973. ISSN 0022-0000. doi: 10.1016/S0022-0000(73)80029-7. Referenced on page 10.

Stephen Arthur Cook. *On the minimum computation time of functions*. PhD thesis, Harvard University, 1966. Referenced on pages 17, 68 and 70.

James W. Cooley and John W. Tukey. An algorithm for the machine calculation of complex Fourier series. *Mathematics of Computation*, 19(90):297–301, 1965.
doi: 10.1090/S0025-5718-1965-0178586-1. Referenced on page 36.

Don Coppersmith and James Davenport. Polynomials whose powers are sparse. *Acta Arith*, 58:79–87, 1991. Referenced on page 106.

Thomas H. Cormen, Charles E. Leiserson, Ronald L. Rivest, and Clifford Stein. *Introduction to Algorithms*. The MIT Press, second edition, September 2001. ISBN 0262032937. Referenced on page 31.

Richard E. Crandall. *Topics in advanced scientific computation*. Springer-Verlag New York, Inc., Secaucus, NJ, USA, 1996. ISBN 0-387-94473-7. Referenced on pages 35 and 39.

Felipe Cucker, Pascal Koiran, and Steve Smale. A polynomial time algorithm for Diophantine equations in one variable. *J. Symbolic Comput.*, 27(1):21–29, 1999. ISSN 0747-7171.
doi: 10.1006/jsco.1998.0242. Referenced on page 95.

Annie Cuyt and Wen-shin Lee. A new algorithm for sparse interpolation of multivariate polynomials. *Theoretical Computer Science*, 409(2):180–185, 2008. ISSN 0304-3975.
doi: 10.1016/j.tcs.2008.09.002. Symbolic-Numerical Computations. Referenced on page 122.

James H. Davenport and Jacques Carette. The sparsity challenges. In *Symbolic and Numeric Algorithms for Scientific Computing (SYNASC), 2009 11th International Symposium on*, pages 3 –7, September 2009.
doi: 10.1109/SYNASC.2009.62. Referenced on page 7.

Anindya De, Piyush P. Kurur, Chandan Saha, and Ramprasad Saptharishi. Fast integer multiplication using modular arithmetic. In *STOC '08: Proceedings of the 40th annual ACM symposium on Theory of computing*, pages 499–506, New York, NY, USA, 2008. ACM. ISBN 978-1-60558-047-0.
doi: 10.1145/1374376.1374447. Referenced on page 56.

W. Decker, G.-M. Greuel, G. Pfister, and H. Schönemann. SINGULAR 3-1-2 — A computer algebra system for polynomial computations. Online, 2010.
URL http://www.singular.uni-kl.de. Referenced on page 22.

Richard A. Demillo and Richard J. Lipton. A probabilistic remark on algebraic program testing. *Information Processing Letters*, 7(4):193–195, 1978. ISSN 0020-0190.
doi: 10.1016/0020-0190(78)90067-4. Referenced on pages 105 and 118.

Angel Díaz and Erich Kaltofen. On computing greatest common divisors with polynomials given by black boxes for their evaluations. In *Proceedings of the 1995 international symposium on Symbolic and algebraic computation*, ISSAC '95, pages 232–239, New York, NY, USA, 1995. ACM. ISBN 0-89791-699-9.
doi: 10.1145/220346.220375. Referenced on page 118.

Angel Díaz and Erich Kaltofen. FOXBOX: a system for manipulating symbolic objects in black box representation. In *Proceedings of the 1998 international symposium on Symbolic and algebraic computation*, ISSAC '98, pages 30–37, New York, NY, USA, 1998. ACM. ISBN 1-58113-002-3.
doi: 10.1145/281508.281538. Referenced on pages 23 and 118.

Jack Dongarra and Francis Sullivan. Guest editors' introduction to the top 10 algorithms. *Computing in Science Engineering*, 2(1):22–23, January/February 2000. ISSN 1521-9615.
doi: 10.1109/MCISE.2000.814652. Referenced on page 36.

J.-G. Dumas, T. Gautier, M. Giesbrecht, P. Giorgi, B. Hovinen, E. Kaltofen, B. D. Saunders, W. J. Turner, and G. Villard. LINBOX: A generic library for exact linear algebra. In Arjeh M Cohen, Xiao-Shan Gao, and Nobuki Takayama, editors, *Mathematical software*, Proc. First International Congress of Mathematical Software, pages 40–50. World Scientific, 2002.
doi: 10.1142/9789812777171_0005. Referenced on page 24.

Jean-Guillaume Dumas, Pascal Giorgi, and Clément Pernet. Dense linear algebra over word-size prime fields: the FFLAS and FFPACK packages. *ACM Trans. Math. Softw.*, 35:19:1–19:42, October 2008. ISSN 0098-3500.
doi: 10.1145/1391989.1391992. Referenced on page 29.

Ahmet Duran, B. David Saunders, and Zhendong Wan. Hybrid algorithms for rank of sparse matrices. In *Proc. SIAM Conf. on Appl. Linear Algebra*, 2003. Referenced on page 71.

Mark J. Encarnación. Black-box polynomial resultants. *Information Processing Letters*, 61(4): 201–204, 1997. ISSN 0020-0190.
doi: 10.1016/S0020-0190(97)00016-1. Referenced on page 5.

P. Erdös. On the number of terms of the square of a polynomial. *Nieuw Arch. Wiskunde (2)*, 23:63–65, 1949. Referenced on page 106.

Paul Erdös, Carl Pomerance, and Eric Schmutz. Carmichael's lambda function. *Acta Arith.*, 58 (4):363–385, 1991. ISSN 0065-1036. Referenced on page 151.

Richard Fateman. Draft: Comparing the speed of programs for sparse polynomial multiplication. Online, July 2002.
URL http://www.cs.berkeley.edu/~fateman/algebra.html. Referenced on page 6.

Richard Fateman. Draft: What's it worth to write a short program for polynomial multiplication? Online, December 2008.
URL http://www.cs.berkeley.edu/~fateman/papers/shortprog.pdf. Referenced on page 71.

Michael Filaseta, Andrew Granville, and Andrzej Schinzel. Irreducibility and greatest common divisor algorithms for sparse polynomials. In *Number theory and polynomials*, volume 352 of *London Math. Soc. Lecture Note Ser.*, pages 155–176. Cambridge Univ. Press, Cambridge, 2008.
doi: 10.1017/CBO9780511721274.012. Referenced on page 8.

M. J. Fischer and S. L. Salzberg. Finding a majority among n votes: Solution to problem 81-5. *Journal of Algorithms*, 3(4):376–379, 1982. ISSN 0196-6774.
doi: 10.1016/0196-6774(82)90031-1. Referenced on page 86.

Timothy S. Freeman, Gregory M. Imirzian, Erich Kaltofen, and Lakshman Yagati. Dagwood: A system for manipulating polynomials given by straight-line programs. *ACM Trans. Math. Softw.*, 14:218–240, September 1988. ISSN 0098-3500.
doi: 10.1145/44128.214376. Referenced on pages 5 and 23.

Matteo Frigo and Steven G. Johnson. The design and implementation of FFTW3. *Proceedings of the IEEE*, 93(2):216–231, 2005. Special issue on "Program Generation, Optimization, and Platform Adaptation". Referenced on page 135.

Matteo Frigo, Charles E. Leiserson, Harald Prokop, and Sridhar Ramachandran. Cache-oblivious algorithms. In *Foundations of Computer Science, 1999. 40th Annual Symposium on*, pages 285–297, 1999.
doi: 10.1109/SFFCS.1999.814600. Referenced on page 11.

Martin Fürer. Faster integer multiplication. In *Proceedings of the thirty-ninth annual ACM symposium on Theory of computing*, STOC '07, pages 57–66, New York, NY, USA, 2007. ACM. ISBN 978-1-59593-631-8.
doi: 10.1145/1250790.1250800. Referenced on pages 17 and 56.

Sanchit Garg and Éric Schost. Interpolation of polynomials given by straight-line programs. *Theoretical Computer Science*, 410(27-29):2659–2662, 2009. ISSN 0304-3975.
doi: 10.1016/j.tcs.2009.03.030. Referenced on pages 3, 108, 117, 119, 122, 123, 127, 132, 133, 135 and 146.

Mickaël Gastineau and Jacques Laskar. TRIP: A computer algebra system dedicated to celestial mechanics and perturbation series. *SIGSAM Bull.*, 44:194–197, January 2011. ISSN 0163-5824.
doi: 10.1145/1940475.1940518. Referenced on page 22.

Joachim von zur Gathen and Jürgen Gerhard. *Modern Computer Algebra*. Cambridge University Press, Cambridge, second edition, 2003. ISBN 0521826462. Referenced on pages 17, 100, 101, 119 and 154.

Joachim von zur Gathen, Marek Karpinski, and Igor Shparlinski. Counting curves and their projections. *Computational Complexity*, 6:64–99, 1996. ISSN 1016-3328.
doi: 10.1007/BF01202042. Referenced on page 94.

Mark Giesbrecht and Daniel Roche. Interpolation of shifted-lacunary polynomials. *Computational Complexity*, 19:333–354, 2010. ISSN 1016-3328.
doi: 10.1007/s00037-010-0294-0. Referenced on page 137.

Mark Giesbrecht and Daniel S. Roche. Interpolation of shifted-lacunary polynomials [extended abstract]. In *Proc. Mathematical Aspects of Computer and Information Sciences (MACIS) 2007*, 2007. Referenced on pages 137 and 145.

Mark Giesbrecht and Daniel S. Roche. On lacunary polynomial perfect powers. In *ISSAC '08: Proceedings of the twenty-first international symposium on Symbolic and algebraic computation*, pages 103–110, New York, NY, USA, 2008. ACM. ISBN 978-1-59593-904-3. doi: 10.1145/1390768.1390785. Referenced on pages 94 and 115.

Mark Giesbrecht and Daniel S. Roche. Detecting lacunary perfect powers and computing their roots. *Journal of Symbolic Computation*, to appear, 2011. URL http://arxiv.org/abs/0901.1848. Referenced on page 94.

Mark Giesbrecht, Erich Kaltofen, and Wen-shin Lee. Algorithms for computing sparsest shifts of polynomials in power, chebyshev, and pochhammer bases. *Journal of Symbolic Computation*, 36(3-4):401 – 424, 2003. ISSN 0747-7171. doi: 10.1016/S0747-7171(03)00087-7. ISSAC 2002. Referenced on pages 138, 141, 142, 143, 144, 153 and 155.

Mark Giesbrecht, George Labahn, and Wen-shin Lee. Symbolic-numeric sparse interpolation of multivariate polynomials. *Journal of Symbolic Computation*, 44(8):943 – 959, 2009. ISSN 0747-7171. doi: 10.1016/j.jsc.2008.11.003. Referenced on page 122.

Etienne Grandjean and J. Robson. RAM with compact memory: a realistic and robust model of computation. In E. Börger, H. Büning, M. Richter, and W. Schönfeld, editors, *Computer Science Logic*, volume 533 of *Lecture Notes in Computer Science*, pages 195–233. Springer Berlin / Heidelberg, 1991. doi: 10.1007/3-540-54487-9_60. Referenced on page 10.

Torbjörn Granlund et al. *GNU Multiple Precision Arithmetic Library, The*. Free Software Foundation, Inc., 4.3.2 edition, January 2010. URL http://gmplib.org/. Referenced on pages 22, 68 and 133.

Andrew Granville and Carl Pomerance. On the least prime in certain arithmetic progressions. *Journal of the London Mathematical Society*, s2-41(2):193–200, April 1990. doi: 10.1112/jlms/s2-41.2.193. Referenced on page 150.

Dima Grigoriev and Marek Karpinski. A zero-test and an interpolation algorithm for the shifted sparse polynomials. In Gérard Cohen, Teo Mora, and Oscar Moreno, editors, *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes*, volume 673 of *Lecture Notes in Computer Science*, pages 162–169. Springer Berlin / Heidelberg, 1993. doi: 10.1007/3-540-56686-4_41. Referenced on page 138.

Dima Grigoriev, Marek Karpinski, and Andrew M. Odlyzko. Short proofs for nondivisibility of sparse polynomials under the extended Riemann hypothesis. *Fundam. Inf.*, 28(3-4):297–301, 1996. ISSN 0169-2968. Referenced on page 94.

Dima Yu. Grigoriev and Marek Karpinski. The matching problem for bipartite graphs with polynomially bounded permanents is in NC. In *Foundations of Computer Science, 1987., 28th Annual Symposium on*, pages 166–172, October 1987. doi: 10.1109/SFCS.1987.56. Referenced on pages 108 and 146.

Dima Yu. Grigoriev and Y. N. Lakshman. Algorithms for computing sparse shifts for multivariate polynomials. *Applicable Algebra in Engineering, Communication and Computing*, 11:43–67, 2000. ISSN 0938-1279.
doi: 10.1007/s002000050004. Referenced on page 155.

Dima Yu. Grigoriev, Marek Karpinski, and Michael F. Singer. Fast parallel algorithms for sparse multivariate polynomial interpolation over finite fields. *SIAM Journal on Computing*, 19(6): 1059–1063, 1990.
doi: 10.1137/0219073. Referenced on page 121.

Darrel Hankerson, Alfred Menezes, and Scott Vanstone. *Guide to elliptic curve cryptography*, chapter 2: Finite Field Arithmetic, pages 25–74. Springer Professional Computing. Springer-Verlag, New York, 2004. Referenced on page 28.

William Hart, Fredrick Johansson, and Sebastian Pancratz. *FLINT: Fast Library for Number Theory*, version 2.0.0 edition, January 2011.
URL http://www.flintlib.org/. Referenced on page 22.

David Harvey. zn_poly: a C library for polynomial arithmetic in $\mathbb{Z}/n\mathbb{Z}[x]$. Online, October 2008.
URL http://cims.nyu.edu/~harvey/code/zn_poly/. Version 0.9. Referenced on pages 22 and 66.

David Harvey. A cache-friendly truncated FFT. *Theoretical Computer Science*, 410(27–29): 2649–2658, 2009a. ISSN 0304-3975.
doi: 10.1016/j.tcs.2009.03.014. Referenced on pages 37 and 40.

David Harvey. Faster polynomial multiplication via multipoint Kronecker substitution. *Journal of Symbolic Computation*, 44(10):1502–1510, 2009b. ISSN 0747-7171.
doi: 10.1016/j.jsc.2009.05.004. Referenced on page 9.

David Harvey and Daniel S. Roche. An in-place truncated Fourier transform and applications to polynomial multiplication. In *ISSAC '10: Proceedings of the 2010 International Symposium on Symbolic and Algebraic Computation*, pages 325–329, New York, NY, USA, 2010. ACM. ISBN 978-1-4503-0150-3.
doi: 10.1145/1837934.1837996. Referenced on pages 35 and 53.

D. R. Heath-Brown. Almost-primes in arithmetic progressions and short intervals. *Mathematical Proceedings of the Cambridge Philosophical Society*, 83(03):357–375, 1978.
doi: 10.1017/S0305004100054657. Referenced on page 150.

D. R. Heath-Brown. Zero-free regions for Dirichlet L-functions, and the least prime in an arithmetic progression. *Proc. London Math. Soc.*, s3-64(2):265–338, March 1992.
doi: 10.1112/plms/s3-64.2.265. Referenced on pages 18 and 150.

Michael T. Heideman, Don H. Johnson, and C. Sidney Burrus. Gauss and the history of the fast Fourier transform. *ASSP Magazine, IEEE*, 1(4):14–21, October 1984. ISSN 0740-7467.
doi: 10.1109/MASSP.1984.1162257. Referenced on page 36.

Wassily Hoeffding. Probability inequalities for sums of bounded random variables. *J. Amer. Statist. Assoc.*, 58:13–30, 1963. ISSN 0162-1459.
URL http://www.jstor.org/stable/2282952. Referenced on page 125.

Joris van der Hoeven. The truncated Fourier transform and applications. In *Proceedings of the 2004 international symposium on Symbolic and algebraic computation*, ISSAC '04, pages 290–296, New York, NY, USA, 2004. ACM. ISBN 1-58113-827-X.
doi: 10.1145/1005285.1005327. Referenced on pages 2, 40, 47 and 50.

Joris van der Hoeven. Notes on the truncated Fourier transform. Technical Report 2005-5, Université Paris-Sud, Orsay, France, 2005.
URL http://www.texmacs.org/joris/tft/tft-abs.html. Referenced on page 40.

Gerhard Jaeschke. On strong pseudoprimes to several bases. *Math. Comp.*, 61(204):915–926, 1993.
doi: 10.1090/S0025-5718-1993-1192971-8. Referenced on page 151.

Seyed Mohammad Mahdi Javadi and Michael Monagan. A sparse modular GCD algorithm for polynomials over algebraic function fields. In *Proceedings of the 2007 international symposium on Symbolic and algebraic computation*, ISSAC '07, pages 187–194, New York, NY, USA, 2007. ACM. ISBN 978-1-59593-743-8.
doi: 10.1145/1277548.1277575. Referenced on page 118.

Seyed Mohammad Mahdi Javadi and Michael Monagan. On factorization of multivariate polynomials over algebraic number and function fields. In *Proceedings of the 2009 international symposium on Symbolic and algebraic computation*, ISSAC '09, pages 199–206, New York, NY, USA, 2009. ACM. ISBN 978-1-60558-609-0.
doi: 10.1145/1576702.1576731. Referenced on page 118.

Seyed Mohammad Mahdi Javadi and Michael Monagan. Parallel sparse polynomial interpolation over finite fields. In *Proceedings of the 4th International Workshop on Parallel and Symbolic Computation*, PASCO '10, pages 160–168, New York, NY, USA, 2010. ACM. ISBN 978-1-4503-0067-4.
doi: 10.1145/1837210.1837233. Referenced on page 121.

Stephen C. Johnson. Sparse polynomial arithmetic. *SIGSAM Bull.*, 8:63–71, August 1974. ISSN 0163-5824.
doi: 10.1145/1086837.1086847. Referenced on pages 7, 31 and 70.

Valentine Kabanets and Russell Impagliazzo. Derandomizing polynomial identity tests means proving circuit lower bounds. *Computational Complexity*, 13:1–46, 2004. ISSN 1016-3328.
doi: 10.1007/s00037-004-0182-6. 10.1007/s00037-004-0182-6. Referenced on page 118.

E. Kaltofen. Single-factor Hensel lifting and its application to the straight-line complexity of certain polynomials. In *Proceedings of the nineteenth annual ACM symposium on Theory of computing*, STOC '87, pages 443–452, New York, NY, USA, 1987. ACM. ISBN 0-89791-221-7.
doi: 10.1145/28395.28443. Referenced on page 95.

Erich Kaltofen. Notes on polynomial and rational function interpolation. Unpublished manuscript, 1988. Referenced on page 146.

Erich Kaltofen. Factorization of polynomials given by straight-line programs. In *Randomness and Computation*, pages 375–412. JAI Press, 1989. Referenced on page 5.

Erich Kaltofen and Pascal Koiran. On the complexity of factoring bivariate supersparse (lacunary) polynomials. In *ISSAC '05: Proceedings of the 2005 international symposium on Symbolic and algebraic computation*, pages 208–215, New York, NY, USA, 2005. ACM. ISBN 1-59593-095-7.
doi: 10.1145/1073884.1073914. Referenced on pages 7, 34 and 95.

Erich Kaltofen and Pascal Koiran. Finding small degree factors of multivariate supersparse (lacunary) polynomials over algebraic number fields. In *ISSAC '06: Proceedings of the 2006 international symposium on Symbolic and algebraic computation*, pages 162–168, New York, NY, USA, 2006. ACM. ISBN 1-59593-276-3.
doi: 10.1145/1145768.1145798. Referenced on pages 34, 95 and 116.

Erich Kaltofen and Wen-shin Lee. Early termination in sparse interpolation algorithms. *Journal of Symbolic Computation*, 36(3-4):365–400, 2003. ISSN 0747-7171.
doi: 10.1016/S0747-7171(03)00088-9. ISSAC 2002. Referenced on pages 71, 121 and 138.

Erich Kaltofen and Barry M. Trager. Computing with polynomials given by black boxes for their evaluations: Greatest common divisors, factorization, separation of numerators and denominators. *Journal of Symbolic Computation*, 9(3):301–320, 1990. ISSN 0747-7171.
doi: 10.1016/S0747-7171(08)80015-6. Computational algebraic complexity editorial. Referenced on pages 5, 7 and 118.

Erich Kaltofen and Lakshman Yagati. Improved sparse multivariate polynomial interpolation algorithms. In P. Gianni, editor, *Symbolic and Algebraic Computation*, volume 358 of *Lecture Notes in Computer Science*, pages 467–474. Springer Berlin / Heidelberg, 1989.
doi: 10.1007/3-540-51084-2_44. Referenced on pages 119 and 121.

Erich Kaltofen and Zhengfeng Yang. On exact and approximate interpolation of sparse rational functions. In *Proceedings of the 2007 international symposium on Symbolic and algebraic computation*, ISSAC '07, pages 203–210, New York, NY, USA, 2007. ACM. ISBN 978-1-59593-743-8.
doi: 10.1145/1277548.1277577. Referenced on page 122.

Erich Kaltofen, Y. N. Lakshman, and John-Michael Wiley. Modular rational sparse multivariate polynomial interpolation. In *Proceedings of the international symposium on Symbolic and algebraic computation*, ISSAC '90, pages 135–139, New York, NY, USA, 1990. ACM. ISBN 0-201-54892-5.
doi: 10.1145/96877.96912. Referenced on pages 121 and 146.

Erich Kaltofen, Zhengfeng Yang, and Lihong Zhi. On probabilistic analysis of randomization in hybrid symbolic-numeric algorithms. In *Proceedings of the 2007 international workshop*

on Symbolic-numeric computation, SNC '07, pages 11–17, New York, NY, USA, 2007. ACM. ISBN 978-1-59593-744-5.
doi: 10.1145/1277500.1277503. Referenced on page 122.

Erich Kaltofen, John P. May, Zhengfeng Yang, and Lihong Zhi. Approximate factorization of multivariate polynomials using singular value decomposition. *Journal of Symbolic Computation*, 43(5):359–376, 2008. ISSN 0747-7171.
doi: 10.1016/j.jsc.2007.11.005. Referenced on page 118.

Erich L. Kaltofen. The "seven dwarfs" of symbolic computation. Manuscript prepared for the final report of the 1998-2008 Austrian research project SFB F013 "Numerical and Symbolic Scientific Computing," Peter Paule, director, April 2010a.
URL http://www.math.ncsu.edu/~kaltofen/bibliography/10/Ka10_7dwarfs.pdf. Referenced on page 2.

Erich L. Kaltofen. Fifteen years after DSC and WLSS2: What parallel computations I do today [invited lecture at PASCO 2010]. In *Proceedings of the 4th International Workshop on Parallel and Symbolic Computation*, PASCO '10, pages 10–17, New York, NY, USA, 2010b. ACM. ISBN 978-1-4503-0067-4.
doi: 10.1145/1837210.1837213. Referenced on pages 119 and 120.

A. A. Karatsuba and Yu. Ofman. Multiplication of multidigit numbers on automata. *Doklady Akademii Nauk SSSR*, 7:595–596, 1963. Referenced on pages 7, 17, 54 and 70.

Marek Karpinski and Igor Shparlinski. On the computational hardness of testing square-freeness of sparse polynomials. In Marc Fossorier, Hideki Imai, Shu Lin, and Alain Poli, editors, *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes*, volume 1719 of *Lecture Notes in Computer Science*, pages 731–731. Springer Berlin / Heidelberg, 1999.
doi: 10.1007/3-540-46796-3_47. 10.1007/3-540-46796-3_47. Referenced on page 95.

Donald E. Knuth. *The art of computer programming, Volume 2: seminumerical algorithms*. Addison-Wesley, Boston, MA, 1981. ISBN 0-201-89684-2. Referenced on pages 8, 17 and 150.

A. N. Kolmogorov and V. A. Uspenskiĭ. On the definition of an algorithm. *Uspehi Mat. Nauk*, 13(4(82)):3–28, 1958. ISSN 0042-1316.
URL http://mi.mathnet.ru/eng/umn7453. Referenced on page 10.

Leopold Kronecker. Grundzüge einer arithmetischen Theorie der algebraischen Grössen. *Journal Für die reine und angewandte Mathematik*, 92:1–122, 1882. Referenced on page 8.

Y. N. Lakshman and B. David Saunders. Sparse shifts for univariate polynomials. *Applicable Algebra in Engineering, Communication and Computing*, 7:351–364, 1996. ISSN 0938-1279.
doi: 10.1007/BF01293594. Referenced on pages 138 and 141.

Susan Landau. Factoring polynomials over algebraic number fields. *SIAM Journal on Computing*, 14(1):184–195, 1985.
doi: 10.1137/0214015. Referenced on page 110.

H. W. Lenstra, Jr. Finding small degree factors of lacunary polynomials. In *Number theory in progress, Vol. 1 (Zakopane-Kościelisko, 1997)*, pages 267–276. de Gruyter, Berlin, 1999. Referenced on pages 7, 24, 34, 95 and 116.

Xin Li, Marc Moreno Maza, Raqeeb Rasheed, and Éric Schost. The modpn library: Bringing fast polynomial arithmetic into MAPLE. *ACM Commun. Comput. Algebra*, 42:172–174, February 2009a. ISSN 1932-2240.
doi: 10.1145/1504347.1504374. Referenced on page 23.

Xin Li, Marc Moreno Maza, and Éric Schost. Fast arithmetic for triangular sets: From theory to practice. *Journal of Symbolic Computation*, 44(7):891–907, 2009b. ISSN 0747-7171.
doi: 10.1016/j.jsc.2008.04.019. International Symposium on Symbolic and Algebraic Computation. Referenced on pages 30, 40 and 51.

Rudolf Lidl and Harald Niederreiter. *Finite fields*, volume 20 of *Encyclopedia of Mathematics and its Applications*. Addison-Wesley Publishing Company Advanced Book Program, Reading, MA, 1983. ISBN 0-201-13519-1. Referenced on pages 97 and 98.

U. V. Linnik. On the least prime in an arithmetic progression. II. The Deuring-Heilbronn phenomenon. *Rec. Math. [Mat. Sbornik] N.S.*, 15(57):347–368, 1944. Referenced on page 18.

Roman Maeder. Storage allocation for the Karatsuba integer multiplication algorithm. In Alfonso Miola, editor, *Design and Implementation of Symbolic Computation Systems*, volume 722 of *Lecture Notes in Computer Science*, pages 59–65. Springer Berlin / Heidelberg, 1993.
doi: 10.1007/BFb0013168. Referenced on page 55.

Yishay Mansour. Randomized interpolation and approximation of sparse polynomials. *SIAM Journal on Computing*, 24(2):357–368, 1995.
doi: 10.1137/S0097539792239291. Referenced on page 122.

John D. Markel. FFT pruning. *Audio and Electroacoustics, IEEE Transactions on*, 19(4):305–311, December 1971. ISSN 0018-9278.
doi: 10.1109/TAU.1971.1162205. Referenced on page 40.

M. Mignotte. An inequality about factors of polynomials. *Math. Comp.*, 28:1153–1157, 1974. ISSN 0025-5718. Referenced on page 101.

Hiroshi Mikawa. On primes in arithmetic progressions. *Tsukuba Journal of Mathematics*, 25 (1):121–153, June 2001.
URL http://hdl.handle.net/2241/100471. Referenced on pages 149 and 150.

Michael Monagan. In-place arithmetic for polynomials over z_n. In John Fitch, editor, *Design and Implementation of Symbolic Computation Systems*, volume 721 of *Lecture Notes in Computer Science*, pages 22–34. Springer Berlin / Heidelberg, 1993.
doi: 10.1007/3-540-57272-4_21. Referenced on page 28.

Michael Monagan and Roman Pearce. Polynomial division using dynamic arrays, heaps, and packed exponent vectors. In Victor Ganzha, Ernst Mayr, and Evgenii Vorozhtsov, editors,

Computer Algebra in Scientific Computing, volume 4770 of *Lecture Notes in Computer Science*, pages 295–315. Springer Berlin / Heidelberg, 2007.
doi: 10.1007/978-3-540-75187-8_23. Referenced on pages 31, 70 and 72.

Michael Monagan and Roman Pearce. Parallel sparse polynomial multiplication using heaps. In *Proceedings of the 2009 international symposium on Symbolic and algebraic computation*, ISSAC '09, pages 263–270, New York, NY, USA, 2009. ACM. ISBN 978-1-60558-609-0.
doi: 10.1145/1576702.1576739. Referenced on pages 23 and 31.

Michael Monagan and Roman Pearce. Sparse polynomial division using a heap. *Journal of Symbolic Computation*, In Press, Corrected Proof, 2010a. ISSN 0747-7171.
doi: 10.1016/j.jsc.2010.08.014. Referenced on page 23.

Michael Monagan and Roman Pearce. Parallel sparse polynomial division using heaps. In *Proceedings of the 4th International Workshop on Parallel and Symbolic Computation*, PASCO '10, pages 105–111, New York, NY, USA, 2010b. ACM. ISBN 978-1-4503-0067-4.
doi: 10.1145/1837210.1837227. Referenced on page 23.

Peter L. Montgomery. Modular multiplication without trial division. *Math. Comp.*, 44(170): 519–521, 1985.
doi: 10.2307/2007970. Referenced on page 29.

PARI/GP, version 2.3.5. The PARI Group, Bordeaux, February 2010.
URL http://pari.math.u-bordeaux.fr/. Referenced on page 22.

Philippe Pébay, J. Maurice Rojas, and David C. Thompson. Optimizing n-variate $(n+k)$-nomials for small k. *Theoretical Computer Science*, In Press, Corrected Proof, 2010. ISSN 0304-3975.
doi: 10.1016/j.tcs.2010.11.053. Referenced on page 8.

Ola Petersson and Alistair Moffat. A framework for adaptive sorting. *Discrete Applied Mathematics*, 59(2):153–179, 1995. ISSN 0166-218X.
doi: 10.1016/0166-218X(93)E0160-Z. Referenced on page 70.

David A. Plaisted. New NP-hard and NP-complete polynomial and integer divisibility problems. *Theoret. Comput. Sci.*, 31(1-2):125–138, 1984. ISSN 0304-3975.
doi: 10.1016/0304-3975(84)90130-0. Referenced on page 94.

David Alan Plaisted. Sparse complex polynomials and polynomial reducibility. *J. Comput. System Sci.*, 14(2):210–221, 1977. ISSN 0022-0000. Referenced on page 94.

J. M. Pollard. Monte Carlo methods for index computation (mod p). *Math. Comp.*, 32(143): 918–924, 1978. ISSN 0025-5718.
doi: 10.1090/S0025-5718-1978-0491431-9. Referenced on page 119.

J. M. Pollard. Kangaroos, monopoly and discrete logarithms. *Journal of Cryptology*, 13:437–447, 2000. ISSN 0933-2790.
doi: 10.1007/s001450010010. Referenced on page 119.

Andrew Quick. Some GCD and divisibility problems for sparse polynomials. Master's thesis, University of Toronto, 1986. Referenced on page 94.

Daniel S. Roche. Adaptive polynomial multiplication. In *Proc. Milestones in Computer Algebra (MICA)*, pages 65–72, 2008. Referenced on page 69.

Daniel S. Roche. Space- and time-efficient polynomial multiplication. In *ISSAC '09: Proceedings of the 2009 international symposium on Symbolic and algebraic computation*, pages 295–302, New York, NY, USA, 2009. ACM. ISBN 978-1-60558-609-0.
doi: 10.1145/1576702.1576743. Referenced on page 53.

Daniel S. Roche. Chunky and equal-spaced polynomial multiplication. *Journal of Symbolic Computation*, In Press, Accepted Manuscript:–, 2010. ISSN 0747-7171.
doi: 10.1016/j.jsc.2010.08.013. Referenced on page 69.

J. Barkley Rosser and Lowell Schoenfeld. Approximate formulas for some functions of prime numbers. *Ill. J. Math.*, 6:64–94, 1962.
URL http://projecteuclid.org/euclid.ijm/1255631807. Referenced on pages 101, 110, 123 and 149.

John Savage and Sowmitri Swamy. Space-time tradeoffs for oblivious integer multiplication. In Hermann Maurer, editor, *Automata, Languages and Programming*, volume 71 of *Lecture Notes in Computer Science*, pages 498–504. Springer Berlin / Heidelberg, 1979.
doi: 10.1007/3-540-09510-1_40. Referenced on page 56.

Nitin Saxena. Progress on polynomial identity testing. *Bull. EATCS*, 99:49–79, 2009. Referenced on pages 5 and 118.

A. Schinzel. On the number of terms of a power of a polynomial. *Acta Arith.*, 49(1):55–70, 1987. ISSN 0065-1036. Referenced on pages 103 and 106.

A. Schönhage. Storage modification machines. *SIAM Journal on Computing*, 9(3):490–508, 1980.
doi: 10.1137/0209036. Referenced on pages 10, 17 and 20.

A. Schönhage and V. Strassen. Schnelle Multiplikation großer Zahlen. *Computing*, 7:281–292, 1971. ISSN 0010-485X.
doi: 10.1007/BF02242355. Referenced on pages 7, 17, 56 and 70.

Arnold Schönhage. Schnelle Multiplikation von Polynomen über Körpern der Charakteristik 2. *Acta Informatica*, 7:395–398, 1977. ISSN 0001-5903.
doi: 10.1007/BF00289470. Referenced on pages 56 and 70.

Arnold Schönhage, Andreas F. W. Grotefeld, and Ekkehart Vetter. *Fast algorithms*. Bibliographisches Institut, Mannheim, 1994. ISBN 3-411-16891-9. A multitape Turing machine implementation. Referenced on page 10.

J. T. Schwartz. Fast probabilistic algorithms for verification of polynomial identities. *J. ACM*, 27:701–717, October 1980. ISSN 0004-5411.
doi: 10.1145/322217.322225. Referenced on pages 106 and 118.

Victor Shoup. Fast construction of irreducible polynomials over finite fields. *Journal of Symbolic Computation*, 17(5):371–391, 1994. ISSN 0747-7171.
doi: 10.1006/jsco.1994.1025. Referenced on pages 99 and 100.

Victor Shoup. NTL: A Library for doing Number Theory. Online, August 2009.
URL http://www.shop.net/ntl/. Version 5.5.2. Referenced on pages 22, 66, 115 and 133.

Igor E. Shparlinski. Computing Jacobi symbols modulo sparse integers and polynomials and some applications. *Journal of Algorithms*, 36(2):241–252, 2000. ISSN 0196-6774.
doi: 10.1006/jagm.2000.1091. Referenced on page 95.

Amir Shpilka and Amir Yehudayoff. Arithmetic circuits: A survey of recent results and open questions. *Foundations and Trends in Theoretical Computer Science*, 5(3-4):207–388, 2010. Referenced on page 118.

A. J. Sommese and C. W. Wampler. *Numerical solution of polynomial systems arising in engineering and science*. World Scientific, Singapore, 2005. Referenced on page 118.

Andrew J. Sommese, Jan Verschelde, and Charles W. Wampler. Numerical decomposition of the solution sets of polynomial systems into irreducible components. *SIAM Journal on Numerical Analysis*, 38(6):2022–2046, 2001.
doi: 10.1137/S0036142900372549. Referenced on page 118.

Andrew J. Sommese, Jan Verschelde, and Charles W. Wampler. Numerical factorization of multivariate complex polynomials. *Theoretical Computer Science*, 315(2-3):651–669, 2004. ISSN 0304-3975.
doi: 10.1016/j.tcs.2004.01.011. Referenced on page 118.

Henrik V. Sorensen and C. Sidney Burrus. Efficient computation of the DFT with only a subset of input or output points. *Signal Processing, IEEE Transactions on*, 41(3):1184–1200, March 1993. ISSN 1053-587X.
doi: 10.1109/78.205723. Referenced on page 40.

Hans J. Stetter. *Numerical Polynomial Algebra*. Society for Industrial and Applied Mathematics, Philadelphia, PA, USA, 2004. ISBN 0898715571. Referenced on page 118.

David R. Stoutemyer. Which polynomial representation is best? Surprises abound! In *Proc. 1984 Macsyma users' conference*, pages 221–243, Schenectady, New York, 1984. Referenced on page 6.

Emmanuel Thomé. Karatsuba multiplication with temporary space of size $\leq n$. Online, September 2002.
URL http://www.loria.fr/~thome/publis/. Referenced on page 55.

A. L. Toom. The complexity of a scheme of functional elements simulating the multiplication of integers. *Doklady Akademii Nauk SSSR*, 150:496–498, 1963. ISSN 0002-3264. Referenced on pages 17, 68 and 70.

A. M. Turing. On computable numbers, with an application to the Entscheidungsproblem. *Proc. London Math. Soc.*, s2-42(1):230–265, 1937.
doi: 10.1112/plms/s2-42.1.230. Referenced on page 10.

Jr. Wagstaff, Samuel S. Greatest of the least primes in arithmetic progressions having a given modulus. *Math. Comp.*, 33:1073–1080, 1979.
doi: 10.1090/S0025-5718-1979-0528061-7. Referenced on page 151.

André Weil. On some exponential sums. *Proc. Nat. Acad. Sci. U. S. A.*, 34:204–207, 1948. ISSN 0027-8424. Referenced on page 98.

Triantafyllos Xylouris. On Linnik's constant. Technical report, arXiv:0906.2749v1 [math.NT], 2009.
URL http://arxiv.org/abs/0906.2749. Referenced on pages 18 and 150.

Thomas Yan. The geobucket data structure for polynomials. *Journal of Symbolic Computation*, 25(3):285–293, 1998. ISSN 0747-7171.
doi: 10.1006/jsco.1997.0176. Referenced on pages 31 and 70.

David Y. Y. Yun. On square-free decomposition algorithms. In *Proceedings of the third ACM symposium on Symbolic and algebraic computation*, SYMSAC '76, pages 26–35, New York, NY, USA, 1976. ACM.
doi: 10.1145/800205.806320. Referenced on page 95.

Umberto Zannier. On the number of terms of a composite polynomial. *Acta Arith*, 127(2): 157–167, 2007.
doi: 10.4064/aa127-2-5. Referenced on page 106.

Richard Zippel. Probabilistic algorithms for sparse polynomials. In Edward Ng, editor, *Symbolic and Algebraic Computation*, volume 72 of *Lecture Notes in Computer Science*, pages 216–226. Springer Berlin / Heidelberg, 1979.
doi: 10.1007/3-540-09519-5_73. Referenced on pages 7, 105 and 118.

Richard Zippel. Interpolating polynomials from their values. *Journal of Symbolic Computation*, 9(3):375–403, 1990. ISSN 0747-7171.
doi: 10.1016/S0747-7171(08)80018-1. Computational algebraic complexity editorial. Referenced on pages 7, 120 and 121.