Polynomial Factorization: a Success Story*

[Plenary Lecture]†

Erich Kaltofen

Department of Mathematics, North Carolina State University
Raleigh, North Carolina 27695-8205 USA
kaltofen@math.ncsu.edu; http://www.kaltofen.us

ABSTRACT

The problem of factoring a polynomial in a single or several variables over a finite field, the rational numbers or the complex numbers is one of the success stories in the discipline of symbolic computation. In the early 1960s implementors investigated the constructive methods known from classical algebra books, but—with the exception of Gauss's distinct degree factorization algorithm—found the algorithms quite inefficient in practice [16]. The contributions in algorithmic techniques that have been made over the next 40 years are truly a hallmark of symbolic computation research.

The early pioneers, Berlekamp, Musser, Wang, Weinberger, Zassenhaus and others applied new ideas like randomization, that even before the now famous algorithms for primality testing by Rabin and Strassen, and like generic programming with coefficient domains as abstract data classes, and they introduced the powerful Hensel lifting lemma to computer algebra. We note that while de-randomization for integer primality testing has been accomplished recently [1], the same remains open for the problem of computing a root of a polynomial modulo a large prime [12, Research Problem 14.48].

Polynomial-time complexity for rational coefficients was established in the early 1980s by the now-famous lattice basis reduction algorithm of A. Lenstra, H. W. Lenstra, Jr., and L. Lovász. The case of many variables first became an application of the DeMillo and Lipton/Schwartz/Zippel lemma [30] and then triggered a fundamental generalization from the standard sparse (distributed) representation of polynomials to the one by straight line and black box programs [11, 17, 19]. Effective versions of the Hilbert irreducibility theorem are needed for the probabilistic analysis, which serendipitously later have also played a role in the PCP characterization of $\mathcal{NP}$ [2]. Unlike many other problems in commutative algebra and algebraic geometry, such as algebraic system solving, the polynomial factoring problem is of probabilistic polynomial-time complexity in the number of variables.

Complex coefficients in multivariate factors can be represented either by exact algebraic numbers or by imprecise floating point numbers. The latter formulation is a cornerstone in the new computer algebra subject of SNAP (Symbolic-Numeric Algorithms for Polynomials) (see, e.g., [4]). The approaches for both exact and imprecise coefficients are manifold, including Ruppert's partial differential equations [26, 27, 6, 10] and Gao's and Lauder's far-reaching generalization of Eisenstein's criterion in the multivariate case to Newton polytope decomposition [8, 9]. The currently best algorithms were all discovered recently within the past ten years.

The baby steps/giant steps technique and fast distinct and equal degree factorization implementations have, at last, yielded in the mid 1990s theoretical and practical improvements over the original univariate Berlekamp algorithm for coefficients in finite fields [13, 29, 18, 3]. The average time analysis for selected algorithms is also completed [5]. For bivariate polynomials over finite fields, surprisingly Gröbner basis techniques are useful in practice [23].

New polynomial-time complexity results are the computation of low degree factors of very high degree sparse (lacunary) polynomials by H. W. Lenstra, Jr. [20, 21], and the deterministic distinct degree factorization for multivariate polynomials over large finite fields [7]. However, many problems with high degree polynomials over large finite fields in sparse or straight line program representations, such as computing a root modulo a large prime, are not known to be in random polynomial time or NP-hard (cf. [24, 25, 15]).

Finally, in 2000 Mark van Hoeij [14] reintroduced lattice basis reduction, now in the Berlekamp-Zassenhaus algorithm, to conquer the hard-to-factor Swinnerton-Dyer polynomials in practice. Sasaki in 1993 had already hinted of the used approach [28].

In my talk I will discuss a selection of the highlights, state remaining open problems, and give some applications including an unusual one due to Moni Naor [22].

Categories and Subject Descriptors

F.2.1 [**Analysis of Algorithms and Problem Complexity**]: Computations on polynomials; I.1.2 [**Symbolic and Algebraic Manipulation**]: Algebraic algorithms

*This material is based on work supported in part by the National Science Foundation under Grants Nos. CCR-9988177 and ITR/ASC-0113121.

†The transparencies of this lecture can be found at http://www.kaltofen.us/bibliography/lectures/.

ISSAC'03, August 3–6, 2003, Philadelphia, Pennsylvania, USA.

General Terms

algorithms

Keywords

polynomial factorization,randomized algorithm,straight line program,black box polynomial,lattice basis reduction,symbolic/numeric hybrid method

REFERENCES

Kaltofen's papers are available at http://www.kaltofen.us.

[1] M. Agrawal, N. Kayal, and N. Saxena. PRIMES is in P. Manuscript, 2002. Available from http://www.cse.iitk.ac.in/news/primality.pdf.

[2] S. Arora and M. Sudan. Improved low degree testing and its applications. In *Proc. 29th Annual ACM Symp. Theory Comput.*, pages 485–495, New York, N.Y., 1997. ACM Press. Full version available from http://theory.lcs.mit.edu/~madhu/papers.html.

[3] O. Bonorden, J. von zur Gathen, J. Gerhard, O. Müller, and M. Nöcker. Factoring a binary polynomial of degree over one million. *SIGSAM Bulletin*, 35(1):16–18, 2001.

[4] R. M. Corless, E. Kaltofen, and S. M. Watt. Section 2.12.3. Symbolic/Numeric Methods: Hybrid Methods. In J. Grabmeier, E. Kaltofen, and V. Weispfenning, editors, *Computer Algebra Handbook*, pages 112–125. Springer Verlag, Heidelberg, Germany, 2002.

[5] P. Flajolet, X. Gourdon, and D. Panario. The complete analysis of a polynomial factorization algorithm over finite fields. *J. Algorithms*, 40(1):37–81, 2001.

[6] S. Gao. Factoring multivariate polynomials via partial differential equations. *Math. Comput.*, 72:801–822, 2003.

[7] S. Gao, E. Kaltofen, and A. Lauder. Deterministic distinct degree factorization for polynomials over finite fields. Paper submitted, 10 pages, 2001.

[8] S. Gao and A. G. B. Lauder. Decomposition of polytopes and polynomials. *Discrete and Computational Geometry*, 26:89–104, 2001.

[9] S. Gao and A. G. B. Lauder. Hensel lifting and polynomial factorisation. *Math. Comput.*, 71:1663–1676, 2002.

[10] S. Gao and V. M. Rodrigues. Irreducibility of polynomials modulo p via Newton polytopes. Preprint, 13 pages. Available from http://www.math.clemson.edu/~sgao/pub.html. To appear *J. Number Theory*, 2003.

[11] J. von zur Gathen. Irreducibility of multivariate polynomials. *J. Comput. System Sci.*, 31:225–264, 1985.

[12] J. von zur Gathen and J. Gerhard. *Modern Computer Algebra*. Cambridge University Press, Cambridge, New York, Melbourne, 1999.

[13] J. von zur Gathen and V. Shoup. Computing Frobenius maps and factoring polynomials. *Comput. Complexity*, 2:187–224, 1992.

[14] M. van Hoeij. Factoring polynomials and the knapsack problem. *J. Number Theory*, 95:167–189, 2002. Implementation available at http://web.math.fsu.edu/~hoeij/.

[15] O. H. Ibarra, S. Moran, and L. E. Rosier. Probabilistic algorithms and straight-line programs for some rank decision problems. *Information Process. Lett.*, 12:227–232, 1981.

[16] S. C. Johnson. Tricks for improving Kronecker's method. Report, Bell Laboratories, 1966.

[17] E. Kaltofen. Factorization of polynomials given by straight-line programs. In S. Micali, editor, *Randomness and Computation*, volume 5 of *Advances in Computing Research*, pages 375–412. JAI Press Inc., Greenwhich, Connecticut, 1989.

[18] E. Kaltofen and V. Shoup. Subquadratic-time factoring of polynomials over finite fields. *Math. Comput.*, 67(223):1179–1197, July 1998.

[19] E. Kaltofen and B. Trager. Computing with polynomials given by black boxes for their evaluations: Greatest common divisors, factorization, separation of numerators and denominators. *J. Symbolic Comput.*, 9(3):301–320, 1990.

[20] H. W. Lenstra, Jr. Finding small degree factors of lacunary polynomials. In *Number Theory in Progress*, volume I, Diophantine Problems and Polynomials, pages 267–276. Walter de Gruyter, 1999. Proceedings of a meeting in honor of the 70th birthday of Andrzej Schinzel.

[21] H. W. Lenstra, Jr. On the factorization of lacunary polynomials. In *Number Theory in Progress*, volume I, Diophantine Problems and Polynomials, pages 277–291. Walter de Gruyter, 1999. Proceedings of a meeting in honor of the 70th birthday of Andrzej Schinzel.

[22] M. Naor. A protocol for spam prevention. Lecture at the "Complexity Theory" Meeting in Oberwolfach, Apr. 2003. To appear in Proc. CRYPTO 2003.

[23] M. Noro and K. Yokoyama. Yet another practical implementation of polynomial factorization over finite fields. In T. Mora, editor, *Proc. 2002 Internat. Symp. Symbolic Algebraic Comput. (ISSAC'02)*, pages 200–206, New York, N. Y., 2002. ACM Press.

[24] D. A. Plaisted. Sparse complex polynomials and polynomial reducibility. *J. Comput. System Sci.*, 14:210–221, 1977.

[25] D. A. Plaisted. Some polynomial and integer divisibility problems are NP-hard. *SIAM J. Comput.*, 7:458–464, 1978.

[26] W. M. Ruppert. Reduzibilität ebener Kurven. *J. reine angew. Math.*, 369:167–191, 1986.

[27] W. M. Ruppert. Reducibility of polynomials *f(x,y)* modulo *p*. *J. Number Theory*, 77:62–70, 1999.

[28] T. Sasaki and M. Sasaki. A unified method for multivariate polynomial factorization. *Japan J. of Industrial and Applied Mathem.*, 10(1):21–39, Feb. 1993.

[29] V. Shoup. A new polynomial factorization algorithm and its implementation. *J. Symbolic Comput.*, 20(4):363–397, 1995.

[30] R. Zippel. Newton's iteration and the sparse Hensel algorithm. In *Proc. 1981 ACM Symp. Symbolic and Algebraic Comput.*, pages 68–72. ACM, 1981.