Qualifying Examination Topics August 2007
Computer Algebra (MA 522-MA792K)

Erich Kaltofen
Department of Mathematics
North Carolina State University
Raleigh, North Carolina 27695-8205, USA
kaltofen@math.ncsu.edu

May 18, 2007

Number Arithmetic

- Repeated squaring [von zur Gathen and Gerhard 1999, §4.3]
- The extended Euclidean algorithm [von zur Gathen and Gerhard 1999, §3+§4.1–6]
- The Chinese remainder algorithm [von zur Gathen and Gerhard 1999, §5.4]
- Use of the birthday paradox for integer factoring [von zur Gathen and Gerhard 1999, Theorem 19.5+19.9]

Polynomial Arithmetic

- the Sylvester resultant [von zur Gathen and Gerhard 1999, Corollary 6.15]
- Subresultants; fundamental theorem (without proof) [von zur Gathen and Gerhard 1999, §11.2], [Brown and Traub 1971]
- Construction of a splitting field via factorization over algebraic extensions; definition of the Galois group; inseparable algebraic extensions; norm and trace [Notes by Kaltofen 1987].
- Finite fields: existence, primitive roots, Galois group; [von zur Gathen and Gerhard 1999, §25.4]
- The Berlekamp factoring algorithm for $\mathbb{Z}_p[x]$ [von zur Gathen and Gerhard 1999, §14.8]

Linear Algebra

- Analysis of Strassen's matrix multiplication algorithm [von zur Gathen and Gerhard 1999, §12.1]
- Dixon's lifting algorithm [Dixon 1982]

- The Berlekamp-Massey algorithm [Kaltofen and Lee 2003, Section 2.2]
- The Wiedemann black box linear system solver [von zur Gathen and Gerhard 1999, §12.4]

Abstract Domains

- Gauss's lemma and applications [von zur Gathen and Gerhard 1999, §6.2]
- The Schwartz-Zippel lemma [von zur Gathen and Gerhard 1999, §6.9]
- The definition of a differential field [von zur Gathen and Gerhard 1999, §22.1]
- Integration of algebraic functions in $\mathbb{C}(x)$ [von zur Gathen and Gerhard 1999, §22.2], [Kaltofen 1984, Section 1]

Gröbner Bases [von zur Gathen and Gerhard 1999, §21.1–5]

- Generalized division
- Definition of a Gröbner basis
- Buchberger's algorithm

Real Roots

- Cauchy's root bound (with proof)
- Sturm's theorem (see [Gantmacher 1960]—was handed out)

References

Brown, W. S. and Traub, J. F. On Euclid's algorithm and the theory of subresultants. *J. ACM*, 18:505–514, 1971.

Dixon, J. Exact solution of linear equations using p-adic expansions. *Numer. Math.*, 40(1): 137–141, 1982.

Gantmacher, F. R. *The Theory of Matrices*, volume 2. Chelsea Publ. Co., New York, N. Y., 1960.

von zur Gathen, Joachim and Gerhard, J. *Modern Computer Algebra*. Cambridge University Press, Cambridge, New York, Melbourne, 1999. ISBN 0-521-64176-4. Second edition 2003.

Kaltofen, E. The algebraic theory of integration. Lect. Notes, Rensselaer Polytechnic Instit., Dept. Comput. Sci., Troy, New York, 1984.

Kaltofen, Erich and Lee, Wen-shin. Early termination in sparse interpolation algorithms. *J. Symbolic Comput.*, 36(3–4):365–400, 2003. Special issue Internat. Symp. Symbolic Algebraic Comput. (ISSAC 2002). Guest editors: M. Giusti & L. M. Pardo.