30. Januar 2002. U. Schoenwaelder; *http://www.math.rwth-aachen.de/∼Ulrich.Schoenwaelder*
HB = Hochschulbibl. RWTH, HBZ = *http://www.hbz-nrw.de/* (HBZ-CD-ROM Online), MB = Mathematikbibl., DB = Didaktikbibl. (Winter), FH = Bibl. Fachhochschule Aachen, FL = Fernleihe, IB Nr. Institutsbibliothek Nr., LB = HB–Lehrbuchsammlung, LS = HB–Lesesaal

Literatur über die Faktorisierung ganzer Zahlen

[1] E. Bach. Toward a theory of Pollard's rho method. *Inform. and Comput.*, 90:139–155, 1991.

[2] Eric Bach and Jeffrey Shallit. Factoring with cyclotomic polynomials. *Math. Computation*, 52(185):201–219, 1989.

[3] Eric Bach and Jeffrey Shallit. *Algorithmic Number Theory, Vol I: Efficient Algorithms*. Foundations of Computing. MIT Press, 1996. ISBN 0-262-02405-5. MB. HBZ.

[4] R. Bach. Number–theoretic algorithms. *Ann.Rev. Comput. Sci.*, 4:119–172, 1990.

[5] E. Behrends. $N = NP$? Oder, anders gefragt: Ist Glück in der Mathematik entbehrlich? *DIE ZEIT*, 1999(10, 4. März):43, 1999. RSA-Verfahren.

[6] Michael N. Bleicher. The Search for Perfect Numbers. In Anatole Beck, sMichael N. Bleicher, and Donald W. Crowe, editors, *Excursions into Mathematics*, chapter 2, pages 79–143. A K Peters, millenium ed. 2000 edition, 2000. FL: SUB Göttingen. S. 110–124: Faktorisierung.

[7] D. Boneh. Twenty years of attacks on the RSA cryptosystem. *Notices Amer. Math. Soc.*, 46:203–213, 1999.

[8] W. Bosma and A. K. Lenstra. An implementation of the elliptic curve integer factorization method. In W. Bosma and A. van der Poorten, editors, *Computational Algebra and Number Theory*, pages 119–136. Kluwer, 1995.

[9] R. Brent. Factorization of the tenth Fermat number. *Math. Comp.*, 68:429–451, 1999.

[10] R. P. Brent. An improved Monte Carlo factorization algorithm. *BIT*, 20:176–184, 1980.

[11] R. P. Brent and J. M. Pollard. Factorization of the eigth Fermat number. *Math. Computation*, 36:627–630, 1981.

[12] D. Bressoud and S. Wagon. *A Course in Computational Number Theory*. Emeryville, CA: Key College Publishing, 2000. ISBN 1-930190-10-7. HBZ.

[13] David M. Bressoud. *Factorization and Primality Testing*. UTM. Springer–Verlag, 1989. HB: Bb1761. Lst.-B. ISBN 0-387-97040-1.

[14] J. Brillhart, D. H. Lehmer, J. L. Selfridge, B. Tuckerman, and jr. S. S. Wagstaff. *Factorizations of* $b^n \pm 1$, $b = 2, 3, 5, 6, 7, 10, 11, 12$ *up to high powers*. Contemporary Mathematics 22. AMS, 1983. Einführung, Übersicht, großes Literaturverzeichnis.

[15] Stefania Cavallar et al. Factorization of a 512-bit RSA modulus. In B. Preneel, editor, *Advances in Cryptology – EUROCRYPT 2000 (Intern. Conf. .., Bruges, Belgium, May 2000)*, number 1807 in LNCS, page 1 ff. Springer–Verlag, 2000. http://link.springer.de/ see Books/Book Series.

[16] H. Cohen. *A Course in Computational Algebraic Number Theory*. GTM 138. Springer–Verlag, 1993. Ch. 8: Factoring in the dark ages; Ch. 10: Modern factoring methods.

[17] Richard Crandall and Carl Pomerance. *Prime Numbers: A Computational Perspective*. New York: Springer, 2001. ISBN 0-387-94777-9. MB: 19315.
1 Primes! 1.1 Problems and progress; 1.2 Celebrated conjectures and curiosities; 1.3 Primes of special form; 1.4 Analytic number theory. 2 Number-theoretical tools 2.1 Modular arithmetic; 2.2 Polynomial arithmetic; 2.3 Squares and roots. 3 Recognizing primes and composites 3.1 Trial division; 3.2 Sieving; 3.3 Pseudoprimes; 3.4 Probable primes and witnesses; 3.5 Lucas pseudoprimes; 3.6 Counting primes. 4 Primality proving 4.1 The $n-1$ test; 4.2 The $n+1$ test; 4.3 The finite field primality test; 4.4 Gauss and Jacobi sums. 5 Exponential factoring algorithms 5.1 Squares; 5.2 Monte Carlo methods; 5.3 Baby-steps, giant-steps; 5.4 Pollard $p-1$ method; 5.5 Binary quadratic forms. 6 Subexponential factoring algorithms 6.1 The quadratic sieve factoring algorithm; 6.2 Number field sieve; 6.3 Rigorous factoring; 6.4 Index-calculus method for discrete logarithms. 7 Elliptic curve arithmetic. 8 The ubiquity of prime numbers 8.1 Crytography .. 9 Fast algorithms for large-integer arithmetic. S. 501–525: References.

[18] H. Davenport. *The Higher Arithmetic. An Introduction to the Theory of Numbers*. Hutchinson & Co. Ltd.; Cambridge Univ. Press, 1952, ^{6}1992. MB: 16 723. Inhalt: I Factorization and primes. II Congruences. III Quadratic residues. IV Continued fractions. V Sums of squares. VI Quadratic forms. VII Some Diophantine equations. VIII Computers and the theory of numbers (4. Pollard's factoring method. 5. Factoring large numbers. 7. The RSA cryptographic method).

[19] K. Devlin. *Sternstunden der modernen Mathematik. Berühmte Probleme und neue Lösungen*. Birkhäuser, 1990. MB: 15864. Die Originalausgabeerschien 1988 unter dem Titel „Mathematics: The New Golden Age“ bei Penguin Books Ltd. §1: Primzahlen, Faktorzerlegung und Geheimcodes.

[20] J. D. Dixon. Factorization and primality tests. *Amer. Math. Monthly*, 91(6):333–352, 1984. MB.

[21] jr. H. W. Lenstra. Factoring integers with elliptic curves. *Annals of Math.*, 126:649–673, 1987.

[22] H. Kleiner. Das RSA–Verfahren. *Praxis der Mathematik*, 26(5):133–140, 1984. HB: Z1757-26. MB: Z 101.

[23] N. Koblitz. *A Course in Number Theory and Cryptography*. GTM 114. Springer–Verlag, 1987. HB: 114 Bb 1244. Ch. I: Some topics in elementary number theory; §1: Time estimates for doing arithmetic, §2: Divisibility and the Euclidean algorithm, §3: Congruences (Fermat's Little Theorem, Chinese Remainder Theorem), §4: Some applications to factoring. Ch. II: Finite fields and quadratic residues. Ch. III: Cryptography. Ch. IV: Public Key. Ch. V: Primality and Factoring. Ch. VI: Elliptic Curves (cryptosystems, factorization).

[24] D. H. Lehmer. Factorization then and now. In D. V. Chudnovsky and R. D. Jenks, editors, *Computers in Mathematics*, LNPAM 125. Dekker, 1990.

[25] A. K. Lenstra and H. W. Lenstra, jr. Algorithms in number theory. In J. van Leeuwen, editor, *Handbook of Theoretical Computer Science, Vol. A*, pages 673–715. Elsevier, Amsterdam, 1990.
[26] A. K. Lenstra, H. W. Lenstra, jr., M. S. Manasse, and S. M. Pollard. The factorization of the ninth Fermat number. Preprint, 1991.
[27] A. K. Lenstra and H. W. Lenstra, editors. *The Development of the Number Field Sieve*, LNM 1554. Springer–Verlag, 1993. Six research papers on the number field sieve for factoring large integers. A variant applies in general.
[28] H. W. Lenstra and C. Pomerance. A rigorous time bound for factoring integers. *Journal of the AMS*, 5:483–516, 1992. MR 92m: 11145.
[29] P. L. Montgomery. Speeding the Pollard and elliptic curve methods of factorization. *Math. Computation*, 48(177):243–264, 1987.
[30] M. A. Morrison and J. Brillhart. A method of factoring and the factorization of F_7. *Math. Computation*, 29(129):183–205, 1975.
[31] Cornelia Niederdrenk-Felgner. Das RSA-Verschlüsselungssystem – Ein Thema für die Schule? *Beiträge zum Mathemsatikunterricht*, 1989:274–277, 1989. HB: Bb1256-1989.
[32] J. M. Pollard. Theorems on factorization and primality testing. *Proc. Camb. Philos. Soc.*, 76:521–528, 1974.
[33] C. Pomerance. Analysis and comparison of some integer factoring algorithms. In H. Lenstra and R. Tijdeman, editors, *Computational Methods in Number Theory*, pages 89–141. 1982.
[34] C. Pomerance. Implementation of the continued fraction integer factoring algorithm. *Congress. Numer.*, 37:99–118, 1983.
[35] C. Pomerance. The quadratic sieve factoring algorithm. In T. Beth, N. Cot, and I. Ingemanson, editors, *Advances in Cryptology*, LNCS 209, pages 169–182. Springer–Verlag, 1985.
[36] C. Pomerance. Factoring. In C. Pomerance, editor, *Cryptology and Computational Number Theory*, Proc. of Symposia in Appl. Math. 42, pages 27–47. AMS, 1990.
[37] H. I. Riesel. *Prime Numbers and Computer Methods of Factorization*. PM 126. Birkhäuser, 1985, ^{2}1994. MB: 12884.
[38] R. Rumely. Recent advances in primality testing. *Notices AMS*, 30(5):475–477, 1985. Übersichtsartikel zu Primzahltests und Faktorisierung.
[39] S. S. Wagstaff, jr. and J. W. Smith. Methods of factoring large integers. In D. V. Chudnovsky, G. V. Chudnovsky, H. Cohn, and M. B. Nathanson, editors, *Number Theory (New York, 1984-1985)*, LNM 1240, pages 281–303. Springer–Verlag, 1987. Übersichtsartikel.
[40] R. D. Silverman. The multiple polynomial quadratic sieve. *Math. Computation*, 48(177):329–339, 1987.
[41] M. C. Wunderlich. Implementing the continued fraction factoring algorithm on parallel machines. *Math. of Computation*, 44(169):251–260, 1985.