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 zu Primzahltests

[1] W. Adams and D. Shanks. Strong primality tests that are not sufficient. *Math. Comp.*, 39:255–300, 1982.

[2] L. M. Adleman and M.-D. A. Huasy. *Primality Testing and Abelian Varieties over Finite Fields.* LMN 1512. Springer–Verlag, 1992. MB: 16263.

[3] P. Alfeld. Why are there infinitely many prime numbers? http://www.math.utah.edu/ alfeld/math//q2.html, 16-Aug-1996. With examples where $prime \times prime.. + 1$ is not prime.

[4] W. Alford, A. Granville, and C. Pomerance. There are infinitely many Carmichael numbers. *Annals of Mathematics*, 139:703–722, 1994. MB: Z 18.

[5] R. Balasubramanian and S. Nagara. Density of Carmichael numbers with three prime factors. *Math. Comp.*, 66:1705–1708, 1997.

[6] A. Bartholomé, J. Rung, and H. Kern. *Zahlentheorie für Einsteiger (mit einem Geleitwort von Jürgen Neukirch).* Vieweg, 1995. Euklidischer Algorithmus, kleiner Fermat, Pseudoprimzahlen. Ziel ist das Verständnis eines wichtigen Primzahltests.

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

[8] J. W. Bruce, P. J. Giblin, and P. J. Rippon. *Microcomputers and Mathematics.* Cambridge Univ. Press, 1990. HB: Bm 2340. Euklidischer Algorithmus, Kettenbrüche, Fibonacci-Folge, Eulers Phi–Funktion, Legendre–Symbol, Primzahlen, Primzahltests, π, e (ist irrational: S. 278), Differentialgleichungssysteme.

[9] Chris K. Caldwell. The prime pages: prime number research, records, and resources. http://www.utm.edu/ research/primes/, 1999. University of Tennessee at Martin.

[10] J. H. Conway and R. K. Guy. *The Book of Numbers.* Springer–Verlag, 1996. MB: 17923. S. 17: How numbers are written; S. 30: Square numbers; S. 33: Triangular numbers; polygonal numbers; tetrahedral numbers; sums of cubes; S. 68: Pascal's triangle; S. 91: Bell numbers, Stirling numbers, Catalan numbers, Bernoulli numbers, Fibonacci numbers (sunflower) [see also S. 202]; S. 127: Primes; S. 146: Sums of two squares; S. 152: Farey fractions and Ford circles; S. 157: Fractions cycle into decimals; S. 171: Pythagorean fractions; S. 176: Continued fractions; S. 181: Geometric problems and algebraic numbers; S. 211: Complex numbers; Gaussian primes; Eisenstein primes; S. 230: Hamilton's quaternions; S. 237: Some transcendental numbers: π, Liouville's number, e, ...; S. 265: Infinite and infinitesimal numbers; S. 283: Surreal numbers; games.

[11] D. A. Cox. *Primes of the form* $x^2 + ny^2$. Wiley, 1989. MB: 15156. §14.D: Elliptic curve primality tests.

[12] 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 allgorithms for large-integer arithmetic. S. 501–525: References.

[13] H. Davenport. *The Higher Arithmetic. An Introduction to the Theory of Numbers.* Hutchinson & Co. Ltd.; Cambridge Univ. Press, 1952, ^{6}1992. MB: 16723. 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 (2. Testing for primality, 7. The RSA cryptographic method).

[14] K. Devlin. There are infinitely many Carmichael numbers. *Focus*, 12(4):1–2, 1992.

[15] Stefanie Krivsky et al. MathePrisma. http://www.MathePrisma.uni-wuppertal.de, Gesehen Oktober 2001. Interview in DIE ZEIT Nr. 41, 4. Oktober 2001, Seite 80 Chancen. Enthält den Modul „Primzahlgeheimnisse“ mit Sieb des Erastosthenes, Primzahlzwillingen, geraden Zahlen als Summe zweier Primzahlen, Primzahlen zwischen zwei Quadratzahlen, Fermat- und Mersennezahlen.

[16] Gerd Faltings, editor. *Primzahlen im Schnelltest (Spektrum der Wissenschaft, Februar 1983)*, Verständliche Forschung. Heidelberg: Spektrum Akdem. Verlag, 1996. HB: Bb2020.

[17] O. Forster. *Algorithmische Zahlentheorie (mit Diskette).* Vieweg, 1996. Lst. A f. Math.

[18] A. Granville. Primality testing and Carmichael numbers. *Notices AMS*, 39(7):696–700, 1992.

[19] (Cray Research). New Mersenne prime discovered. *Focus*, 12(3):3, 1992. $2^{756839} - 1$.

[20] P. Ribenboim. Prime number records. *College Mathematics Journal*, 25:280–290, 1994. George Pólya Award for paper: see Notices AMS 42:7 (1994), 1295–1296.

[21] P. Ribenboim. *The New Book of Prime Number Records.* Springer–Verlag, 1996. Primality testing; historical presentation of the main problems about prime numbers.

[22] I. Richards. The invisible prime factor. *American Scientist*, 70:176–179, 1982. The author explains how elementary number theory such as Euclid's Lemma and modular arithmetic can be used to test wether an integer is prime. He then discusses how prime numbers can be used to create secret codes that are extremely difficult to break.

[23] H. Riesel. *Prime Numbers and Computer Methods for Factorization*. Birkhäuser, 1985, ^{2}1994. MB: 12884.

[24] M. I. Rosen. A proof of the Lucas-Lehmer-Test. *Amer. Math. Monthly*, 95:855–856, 1988. MB: Z 42.

[25] Hugh C. Williams. *Édouard Lucas and Primality Testing*. Canadian Mathematical Society series of monographs and advanced texts 22. Wiley-Interscience, 1998. ISBN 0-471-14852-0 (hbk). HBZ.