Mathematics 207

Mathematics in Industry*

Richard Brent

October–November 1997

Course Description

A selection of mathematical topics with applications in science, engineering and commerce. Fast Fourier and related transforms, aspects of cryptography and secure communication, integer factorization algorithms, applications of elliptic curves over finite fields. Fast algorithms for computation of elementary functions using the arithmetic-geometric mean. Fast and stable solution of Toeplitz and related linear systems. The hope is to show that some real-world problems lead to beautiful mathematics.

Contact Information

Lectures: MWF 2–4, Science Center 304
Office: Science Center 435
Office hours: MW 4–5
Phone: 4954744
e-mail: `rpb@math.harvard.edu` or `Richard.Brent@anu.edu.au`
ftp: `ftp://ftp.das.harvard.edu/pub/rpb/math207` or `ftp://nimbus.anu.edu.au/pub/Brent`
url: `http://cslab.anu.edu.au/~rpb/` or
`ftp://ftp.das.harvard.edu/pub/rpb/math207/math207.html`

Course Outline

The material to be covered will depend on your interests and background, and on the time available. Following is an outline of some possibilities. The annotated bibliography should be useful as a starting point if you want to investigate any particular topics in more depth than we have time for in the course. There is no textbook. The books by Riesel [106], Schneier [111], Schroeder [112] and Van Loan [131] are recommended reading.

1 Preliminaries

Upper and lower resource bounds using "O" and "Ω" notation [74], the classes P and NP, basics of computer arithmetic and algorithms, Kronecker products. See Aho *et al* [3], Garey and Johnson [56], Goldwasser and Bellare [61, Appendices], Knuth [75] and Van Loan [131].

2 DFT, FFT and related transforms

The discrete Fourier transform (DFT) is a matrix-vector product which at first sight appears to require $\Omega(n^2)$ arithmetic operations. The fast Fourier transform (FFT) implements the DFT in $O(n \log n)$ arithmetic operations. There are many variants of the FFT, depending on the size n (and its prime factorization), whether recursion is implicit or explicit, whether symmetries in the data are exploited, etc. See Briggs [39] for the DFT, some history, applications, and an introduction to the FFT. Van Loan [131] has much more on the FFT. If you prefer an approach based on polynomials rather than linear algebra, then see Aho, Hopcroft and Ullman [3, Ch. 7]. Crandall [48, 49] covers related number-theoretic transformations and their applications.

3 Aspects of cryptography and secure communications

Cryptography is a topic of growing importance as the Internet becomes used more and more for mail, commerce and financial transactions. Cryptographic techniques are necessary to ensure privacy and authenticity of electronic messages. We shall look at some aspects of cryptography which have an interesting mathematical foundation, e.g. "public-key" cryptosystems such as the RSA system [107]. See Schneier [111] for a comprehensive survey and large bibliography. Seberry and Pieprzyk [114] is a less exhaustive alternative. The mathematics of public-key cryptography is covered in Brickell and Odlyzko [38], Goldwasser and Bellare [61], Riesel [106], Schroeder [112] and Stinson [124]. For practical and political aspects, see Schneier [110, 111] and Zimmermann [137].

4 Integer factorization and primality testing algorithms

> "The problem of distinguishing prime numbers from composites; and of resolving composite numbers into their prime factors, is one of the most important and useful in all of arithmetic ... The dignity of science seems to demand that every aid to the solution of such an elegant and celebrated problem be zealously cultivated."
>
> – C. F. Gauss, *Disquisitiones Arithmeticæ,* Art. 329 (1801).

Integer factorization and primality testing algorithms are of practical interest because they are needed in cryptographic algorithms such as RSA. We will consider various algorithms such as the elliptic curve method (ECM), the quadratic sieve (QS), and the number field sieve (NFS). For a brief survey and historical introduction, see [40]. A more comprehensive introduction is Riesel [106].

ECM was introduced by Hendrik Lenstra [81], and practical improvements were suggested and implemented by several people [23, 86]. The "state of the art" is summarized in [30, 31].

The quadratic sieve was popularized by Carl Pomerance, although it is based on earlier ideas of Fermat, Kraitchik, Brillhart, Morrison and others, and improvements have been contributed by Davis, Montgomery, Silverman and others [40]. The best current version is the "two large primes" multiple-polynomial quadratic sieve (MPQS). A good introduction is [99].

NFS is based on an idea of John Pollard, and is described in [79]. For recent developments, see [55, 91, 98, 99].

5 Some other applications of number theory

> "Anyone who considers arithmetical methods of producing random digits is, of course, in a state of sin."
>
> – John von Neumann, 1951

Pseudo-random number generators are used in simulation, randomized algorithms [27] and cryptography [111]. However, it is surprisingly difficult to generate "good" pseudo-random numbers. We will consider some generators with long periods and good statistical properties [24, 26, 75]. The analysis of these generators involves some number theory. For a wide variety of other interesting applications of number theory, see Schroeder [112].

6 Fast computation of elementary functions

Brent [20, 21] and Salamin [108] gave quadratically convergent algorithms for the computation of elementary functions and constants such as π. Their work inspired the book by Borwein and Borwein [17]. These algorithms have mainly been used for very high precision computations, but they have other possible applications.

7 Fast and stable solution of structured linear systems

Toeplitz matrices have a special structure which can be exploited to solve Toeplitz linear systems quickly [5]. There are many interesting connections with the theory of Padé approximation, continued fractions, orthogonal polynomials, and the Schur algorithm [113]. Much can be generalized to "low displacement rank" systems [72]. Unfortunately, the numerical instability of many of the fast algorithms makes them useless in practice. Recently there has been an upsurge of interest in fast algorithms which have desirable stability properties [29], and we may look at the ideas behind some of these algorithms.

Annotated Bibliography

The following bibliography lists some relevant books and papers. See particularly those marked "$\Rightarrow$" and (to a lesser extent) "$\rightarrow$". Several of the books and papers have extensive bibliographies so I have not attempted to give a complete list of papers here.

References

[1] Leonard M. Adleman, *On distinguishing prime numbers from composite numbers (extended abstract)*, Proc. IEEE Symp. Found. Comp. Sci. **21** (1980), 387–406. Shows that there is a deterministic algorithm to settle primality of n in $O((\log n)^{c\log\log\log n})$ steps, where c is an effectively computable constant. Thus primality testing is "almost" in P.

[2] Leonard M. Adleman and M. A. Huang, *Recognizing primes in random polynomial time*, Proc. Nineteenth Annual ACM Symposium on the Theory of Computing, ACM, New York, 1987, 462–469. Gives a guaranteed correct algorithm which *usually* runs in polynomial time. Compare the Rabin-Miller algorithm [103], which runs in polynomial time but has a small probability of error.

[3] $\rightarrow$ Alfred V. Aho, John E. Hopcroft and Jeffrey D. Ullman, *The Design and Analysis of Computer Algorithms*, Addison-Wesley, 1974. Chapter 7 gives a different approach to the FFT from Van Loan [131].

[4] Miklós Ajtai and Cynthia Dwork, *A public-key cryptosystem with worst-case/average-case equivalence*, Proc. 29th Annual ACM Symposium on the Theory of Computing (STOC'97), ACM, 1997, 284–293. Most public-key cryptosystems depend for their security on the supposed difficulty of solving the integer factorization problem or a closely related problem. This paper gives a cryptosystem which depends on the difficulty of finding the shortest nonzero vector in a certain n-dimensional lattice. It is shown that random instances are (almost) as hard to solve as worst-case instances. Unfortunately, an implementation of the cryptosystem would be very slow because only one bit is determined by each lattice problem.

[5] Gregory S. Ammar and William B. Gragg, *Superfast solution of real positive definite Toeplitz systems*, SIAM J. Matrix Anal. Appl. **9** (1988), 61–76. Discusses "superfast" algorithms for Toeplitz systems. This means algorithms with time bound $O(n(\log n)^2)$, for example see [33, 12, 69, 92]. Merely "fast" algorithms have time bound $O(n^2)$ but in practice may be better than "superfast" algorithms for moderate values of n.

[6] A. O. L. Atkin and François Morain, *Elliptic curves and primality proving,* Math. Comp. **61** (1993), 29–68. Programs available from `ftp://ftp.inria.fr/INRIA/ecpp.V3.4.1.tar.Z`. Describes the ECPP primality test, which is useful for proving primality of numbers of several hundred decimal digits (see [30] for examples).

[7] Eric Bach, *Analytic Methods in the Analysis and Design of Number-Theoretic Algorithms*, MIT Press, 1985. Gives a version of Miller's polynomial-time primality test [84] with explicit (small) constants, assuming the Extended Riemann Hypothesis (ERH). [ERH is the extension of the Riemann hypothesis to all Dirichlet L-functions.]

[8] E. H. Bareiss, *Numerical solution of linear equations with Toeplitz and vector Toeplitz matrices*, Numerische Mathematik **13** (1969), 404–424. Gives an $O(n^2)$ algorithm for the solution of Toeplitz systems; in the symmetric case this is essentially Schur's algorithm. The numerical properties are similar to those of Gaussian elimination *without* pivoting [15].

[9] M. Beeler, R. W. Gosper and R. Schroeppel, *Hakmem*, Memo No. **239**, MIT AI Lab, 1972. An obscure report containing some gems. Several algorithms which were rediscovered later can be found here. On pp. 70–71 there is a fast algorithm (attributed to Salamin) for evaluating $\log(x)$.

[10] Charles H. Bennett, F. Bessette, Giles Brassard, L. Salvail and J. Smolin, *Experimental quantum cryptography*, J. of Cryptography **5** (1992), 3–28. A good place to start on quantum cryptography. Available on the web from Brassard's on-line bibliography [19].

[11] M. Ben-Or, *Probabilistic algorithms in finite fields*, Proc. 22nd IEEE Symposium on Foundations of Computer Science, 1981, 394–398. Shows how to find a zero of a polynomial of degree n over $GF(p)$ in $O(n \log n \mathrm{loglog} n \log p)$ operations. See also Rabin [104].

[12] Robert R. Bitmead and Brian D. O. Anderson, *Asymptotically fast solution of Toeplitz and related systems of equations*, Linear Algebra Appl. **34** (1980), 103–116. An early "superfast", i.e. $O(n(\log n)^2)$ algorithm, using the concept of displacement rank. It is practical because the constants are too large [5].

[13] Henk Boender and Herman J. J. te Riele, *Factoring integers with large prime variations of the quadratic sieve,* Experimental Mathematics, **5** (1996), 101–117. Also Report NM-R9513, Department of Numerical Mathematics, Centrum voor Wiskunde en Informatica, Amsterdam, July 1995. `ftp://ftp.cwi.nl/pub/CWIreports/NW/NM-R9513.ps.Z`.

[14] Adam W. Bojanczyk, Richard P. Brent and Frank R. de Hoog, *Stability analysis of a general Toeplitz system solver*, Numerical Algorithms **10** (1995), 225–244. `ftp://nimbus.anu.edu.au/pub/Brent/rpb143.dvi.gz`.

[15] Adam W. Bojanczyk, Richard P. Brent, Frank R. de Hoog and Douglas R. Sweet, *On the stability of the Bareiss and related Toeplitz factorization algorithms*, SIAM J. Matrix Anal. Appl. **16** (1995), 40–57. `ftp://nimbus.anu.edu.au/pub/Brent/rpb144.dvi.gz`. Bareiss [8] gives an $O(n^2)$ algorithm for the solution of Toeplitz systems; in the symmetric case this is essentially Schur's algorithm. This paper shows that the numerical properties of the Bareiss algorithm are similar to

those of Gaussian elimination *without* pivoting. Thus, it is stable in the positive-definite symmetric case. For generalizations, see [43, 123].

[16] A. Borodin and I. Munro, *The Computational Complexity of Algebraic and Numeric Problems*, American Elsevier, New York, 1975. A good summary of results on fast polynomial evaluation and interpolation.

[17] → Jonathan M. Borwein and Peter B. Borwein, *Pi and the AGM*, John Wiley and Sons, New York, 1987. Describes the quadratically convergent algorithms of Brent [20, 21] and Salamin [108] for the computation of elementary functions and constants such as π. Chapter 6 has a brief description of the FFT in terms of fast polynomial evaluation and interpolation.

[18] Giles Brassard, *A note on the complexity of cryptography*, IEEE Trans. on Information Theory **IT-25** (1979), 232–233. Shows that if the problem of breaking a cryptosystem is NP-hard, then NP = CoNP (which is considered very unlikely). See also Selman [115] and Taylor [127].

[19] Giles Brassard, *A Bibliography of Quantum Cryptography*, `http://www.iro.umontreal.ca/~crepeau/Biblio-QC.html`. Earlier version published in SIGACT News **24**, 3 (1993), 16–20. A comprehensive bibliography of the field of Quantum Cryptography (which we do not attempt to cover in this bibliography). Has links to online versions of many of the papers. The field was started by Wiesner [134]. A good place to start is the paper by Bennett *et al* [10].

[20] Richard P. Brent, *Multiple-precision zero-finding methods and the complexity of elementary function evaluation*, in [129], 151–176. Abstract: `ftp://nimbus.anu.edu.au/pub/Brent/rpb028a.dvi.gz`. Gives an elegant, quadratically convergent algorithm for the computation of π; see also [21, 108]. Also gives quadratically convergent algorithms for elementary functions using the AGM. Some of the ideas can be found in [9].

[21] Richard P. Brent, *Fast multiple-precision evaluation of elementary functions*, J. ACM **23** (1976), 242–251. Also appeared as Report TR STAN-CS-75-515, DCS, Stanford (August 1975). Abstract: `ftp://nimbus.anu.edu.au/pub/Brent/rpb034a.dvi.gz`. Gives an elegant, quadratically convergent algorithm for the computation of π; see also [20, 108]. Also gives quadratically convergent algorithms for elementary functions using Landen transformations.

[22] Richard P. Brent, *An improved Monte Carlo factorization algorithm,* BIT **20** (1980), 176–184. Abstract: `ftp://nimbus.anu.edu.au/pub/Brent/rpb051a.dvi.gz`. Gives a practical improvement of Pollard's rho method [97].

[23] Richard P. Brent, *Some integer factorization algorithms using elliptic curves,* Australian Computer Science Communications **8** (1986), 149–163. Also Report CMA-R32-85, Centre for Mathematical Analysis, Australian National University, Canberra, Sept. 1985, 20 pp. Abstract: `ftp://nimbus.anu.edu.au/pub/Brent/rpb097a.dvi.gz`. A description of the first program implementing Lenstra's ECM algorithm [81] with a "birthday paradox" second phase. Includes a heuristic analysis of the second phase. For more recent results, see [30].

[24] Richard P. Brent, *Uniform random number generators for supercomputers*, Proc. Fifth Australian Supercomputer Conference, Melbourne, December 1992, 95-104. `ftp://nimbus.anu.edu.au/pub/Brent/rpb132.dvi.gz`. A survey of good (and some bad) methods for uniform random number generation.

[25] Richard P. Brent, *On computing factors of cyclotomic polynomials,* Math. Comp. **61** (1993), 131–149. `ftp://nimbus.anu.edu.au/pub/Brent/rpb135.dvi.gz`. Gives a practical algorithm for computing Aurifeuillian factorizations.

[26] Richard P. Brent, *On the periods of generalized Fibonacci recurrences*, Math. Comp. **63** (1994), 389-401. `ftp://nimbus.anu.edu.au/pub/Brent/rpb133.dvi.gz`. Shows how to get periodic sequences with extremely long periods using the theory of irreducible polynomials over GF(2).

[27] Richard P. Brent, *Uses of randomness in computation*, Tech. Report TR-CS-94-06, CS Lab, ANU, June 1994 (invited talk presented at Theory Day, University of NSW, April 1994). `ftp://nimbus.anu.edu.au/pub/Brent/rpb147.dvi.gz`. A quick introduction to randomized algorithms. For more, see Motwani and Raghavan [90].

[28] Richard P. Brent, *Large factors found by ECM,* Computer Sciences Laboratory, Australian National University, Dec. 1995 (and more recent updates). `ftp://nimbus.anu.edu.au/pub/Brent/champs.ecm`. A collection of all known prime factors of at least 40 decimal digits found by ECM, with information on parameters used, number of curves, group orders etc. The largest factor found so far (as at September 1997) has 49 decimal digits [30].

[29] Richard P. Brent *Stability of fast algorithms for structured linear systems,* Tech. Report TR-CS-97-18, CS Lab, ANU, September 1997. `ftp://nimbus.anu.edu.au/pub/Brent/rpb177tr.dvi.gz`. A recent survey paper, to appear as a chapter in *Stability of fast methods for linear systems with structure* (editors, Ali H. Sayed and Thomas Kailath), to be published by SIAM.

[30] Richard P. Brent, *Factorization of the tenth Fermat number*, Math. Comp., 1998, to appear. `ftp://nimbus.anu.edu.au/pub/Brent/rpb161.dvi.gz`. The title says it. Describes some of the details of ECM implementations and gives some heuristic asymptotic analysis of ECM. Also includes a brief history of attempts to factor Fermat numbers.

[31] Richard P. Brent, *Factorization of the tenth and eleventh Fermat numbers,* Report TR-CS-96-02, Computer Sciences Laboratory, Australian National Univ., Canberra, Feb. 1996. `ftp://nimbus.anu.edu.au/pub/Brent/rpb161tr.dvi.gz`. A preliminary version of [30], including more detail on different implementations of ECM.

[32] Richard P. Brent, Richard E. Crandall and Karl H. Dilcher, *Two new factors of Fermat numbers,* Tech. Report TR-CS-97-11, CSL, ANU, May 1997. `ftp://nimbus.anu.edu.au/pub/Brent/rpb175tr.dvi.gz`. Has new factors of F_{13} and F_{16} found by ECM. Since the Tech. Report came out, the number of authors and the number of factors have both increased by one: see R. P. Brent, R. E. Crandall, K. Dilcher and Chris Van Halewyn, *Three new factors of Fermat numbers*, submitted for publication.

[33] Richard P. Brent, Fred G. Gustavson and David Y. Y. Yun, *Fast solution of Toeplitz systems of equations and computation of Padé approximants*, J. Algorithms **1** (1980), 259–295. Abstract: `ftp://nimbus.anu.edu.au/pub/Brent/rpb059a.dvi.gz`. Gives the first "superfast", i.e. $O(n(\log n)^2)$, algorithm for Toeplitz systems, exploiting their connection with Padé approximants. Not practical because of numerical stability problems, but later "lookahead" methods were invented to overcome these problems.

[34] Richard P. Brent, Peter L. Montgomery and Herman J. J. te Riele, *Factorizations of $a^n \pm 1$, $13 \le a < 100$: Update 2,* Report NM-R9609, CWI, Amsterdam, March 1996. `ftp://nimbus.anu.edu.au/pub/Brent/rpb134u2.*.gz`. The second update to an extension of the Cunningham tables [40]. Illustrates the "state of the art" of integer factorization algorithms.

[35] Richard P. Brent and John M. Pollard, *Factorization of the eighth Fermat number,* Math. Comp. **36** (1981), 627–630. Abstract: `ftp://nimbus.anu.edu.au/pub/Brent/rpb061a.dvi.gz`. An early success for a modified version of Pollard's "rho" algorithm [97]. Pollard contributed the epigram *"I am now entirely persuaded to employ the method, a handy trick, on gigantic composite numbers"*, which is useful if you want to remember the smaller factor 1238926361552897 of $F_8 = 2^{2^8} + 1$ (a good party trick). Open problem: find epigrams for other factors of Fermat numbers.

[36] Ernest F. Brickell, *Solving low density knapsacks,* Advances in Cryptology – Proc. Crypto '83, Plenum Press, New York, 1984, 25–37. One of the papers which showed that many cryptosystems based on the knapsack problem could be broken. See also [37, 38, 52, 95].

[37] Ernest F. Brickell, *The cryptanalysis of knapsack cryptosystems*, in Applications of Discrete Mathematics (R. D. Ringeisen and F. Roberts, eds.), SIAM, Philadelphia, 1988, 3–23. Another paper which showed that many cryptosystems based on the knapsack problem could be broken. See also [36, 38, 52, 95].

[38] → Ernest F. Brickell and Andrew M. Odlyzko, *Cryptanalysis: a survey of recent results,* in Contemporary Cryptology (G. J. Simmons, ed.), IEEE Press, 1991, 501–540. Preliminary version in *Proc. IEEE* **76**, 1988, 578–593. An excellent survey up to 1991. Available from `http://www.research.att.com/~amo/doc/complete.html`.

[39] → William L. Briggs and Van Emden Henson, *The DFT: An Owner's Manual for the Discrete Fourier Transform*, SIAM, Philadelphia, 1995. As the title says, this book covers the *discrete* Fourier transform (DFT), not just the *fast* Fourier transform (FFT). Includes some history, applications, a chapter on the FFT, and a chapter on related transforms. Easier reading than Van Loan [131].

[40] John Brillhart, Derrick H. Lehmer, John L. Selfridge, Bryant Tuckerman, and Samuel S. Wagstaff, Jr., *Factorizations of* $b^n \pm 1$, $b = 2, 3, 5, 6, 7, 10, 11, 12$ *up to high powers*, 2nd ed., Amer. Math. Soc., Providence, RI, 1988. The "Cunningham" project. As well as tables, has a good survey and historical introduction.

[41] James R. Bunch, *Stability of methods for solving Toeplitz systems of equations*, SIAM J. Sci. Statist. Comput. **6** (1985), 349–364.

[42] C. S. Burrus and T. W. Parks, *DFT/FFT and Convolution Algorithms*, John Wiley and Sons, New York, 1985. For the connection between the FFT and fast convolution. See also Nussbaumer [94] and Van Loan [131], Chapter 4.

[43] Shiv Chandrasekaran and Ali H. Sayed, *Stabilizing the generalized Schur algorithm*, SIAM J. Matrix Anal. Appl. **17** (1996), 950–983. Proves stability of a class of fast algorithms in the positive-definite case, generalizing the results of [15]. Similar results are given by Stewart and Van Dooren [123].

[44] B. Chor and Ronald L. Rivest, *A knapsack type public key cryptosystem based on arithmetic in finite fields*, IEEE Trans. Information Theory **34** (1988), 901–909. Perhaps the only knapsack-based cryptosystem which has stood the test of time – apparently it has not yet been broken. The reason may be that it does not attempt to hide an easy knapsack problem by modular multiplication. See also [38].

[45] David V. and Gregory V. Chudnovsky, *Sequences of numbers generated by addition in formal groups and new primality and factorization tests,* Adv. in Appl. Math. **7** (1986), 385–434. Gives many parameterizations of elliptic curves, including one (found independently by Montgomery [86]) which is probably the most efficient for use in ECM.

[46] Henri Cohen, *A course in computational algebraic number theory,* Graduate Texts in Mathematics **138**, Springer-Verlag, 1993. Excellent overall. Chapter 4 includes algorithms on algebraic numbers so is relevant to NFS.

[47] James Cooley and John Tukey, *An algorithm for the machine calculation of complex Fourier series*, Math. Comp. **19** (1965), 297–301. The paper which rediscovered and popularized the FFT. For history, see [39].

[48] → Richard E. Crandall, *Projects in Scientific Computation*, Springer-Verlag/Telos, 1994. Discusses some number-theoretic algorithms, the FFT and other transforms, and various applications in biology, physics, chemistry etc. Includes Mathematica programs.

[49] → Richard E. Crandall, *Topics in Advanced Scientific Computation*, Springer-Verlag/Telos, 1996. A sequel to *Projects* [48]. Includes chapters on integer factorization and transforms.

[50] Richard E. Crandall and Barry F. Fagin, *Discrete weighted transforms and large-integer arithmetic,* Math. Comp. **62** (1994), 305–324. For fast integer multiplication, especially mod $2^n \pm 1$.

[51] George Cybenko, *The numerical stability of the Levinson-Durbin algorithm for Toeplitz systems of equations*, SIAM J. Sci. Statist. Computing **1** (1980), 303–319. The first significant result on the stability of Levinson's algorithm, but the result only applies under rather strict conditions (the matrix must be positive definite with all reflection coefficients positive) so has to be interpreted with care. It has recently been recognized that the Schur/Bareiss algorithm is generally more stable than the Levinson-Durbin algorithm: see [15].

[52] Y. Desmedt, *What happened with knapsack cryptographic schemes*, in Performance Limits in Communication, Theory and Practice (J. K. Skwirzynski, ed.),Kluwer, 1988, 113–134. Discusses the demise of most proposed knapsack schemes. See also Brickell and Odlyzko [38]. An apparent exception is the scheme by Chor and Rivest [44].

[53] Whitfield Diffie and Martin E. Hellman, *New directions in cryptography*, IEEE Trans. on Information Theory, **IT-22**, 1976, 644–654. The paper which introduced the idea of "public-key" or "asymmetric" cryptography. The RSA paper [107] was a little later.

[54] J. Durbin, *The fitting of time-series models*, Rev. Int. Stat. Inst. **28** (1959), 229–249. Improved Levinson's algorithm [82] to give what is often called the Levinson-Durbin algorithm.

[55] Marije Elkenbracht-Huizing, *An implementation of the number field sieve,* Experimental Mathematics, **5** (1996), 231–253. Also Report NM-R9511, Department of Numerical Mathematics, Centrum voor Wiskunde en Informatica, Amsterdam, July 1995. `ftp://ftp.cwi.nl/pub/CWIreports/NW/NM-R9511.ps.Z`. Gives implementation details and timings for both the special number field sieve (SNFS) and the general number field sieve (GNFS).

[56] Michael Garey and David Johnson, *Computers and Intractability: A Guide to the Theory of NP-Completeness*, W. H. Freeman, San Francisco, 1979. The "bible" on NP-completeness, with many examples.

[57] Simson Garfinkel, *PGP: Pretty Good Privacy*, O'Reilly & Associates, 1995. Good on the practical and legal issues associated with PGP [137].

[58] Carl (or Karl) F. Gauss, *Theoria interpolationis methodo nova tractata*, Carl Friedrich Gauss Werke, Band **3**, Königlichen Gessellschaft der Wissenschaften, Göttingen, 1866. The first known use of the FFT idea, written in 1805 and published posthumously in 1866. The FFT has been rediscovered several times, most notably by Cooley and Tukey [47]. See [66] for the history.

[59] Israel Gohberg (editor), *I. Schur Methods in Operator Theory and Signal Processing* (Operator Theory: Advances and Applications, Volume 18), Birkhäuser Verlag, Basel, 1986. There are several interesting items in this collection, including a translation of Schur's 1917 paper [113].

[60] Israel Gohberg, Thomas Kailath and Vadim Olshevsky, *Gaussian Elimination with Partial Pivoting for Matrices with Displacement Structure*, Math. Comp. **64** (1995), 1557–1576. Using an idea of Heinig [67], shows how to transform Toeplitz-type matrices to Cauchy-type matrices, and shows how Gaussian elimination with partial pivoting can be used without destroying the structure (the GKO algorithm). For comments on stability, see [29, 64, 125].

[61] → Shafi Goldwasser and Mihir Bellare, *Lecture Notes on Cryptography*, July 10, 1996, 192 pp. `ftp://theory.lcs.mit.edu/pub/classes/6.875/crypto-notes.ps`. Lecture notes for a course given at MIT in 1996; excellent on the mathematical aspects of cryptography, including one-way and trapdoor functions, pseudo-random bit generators, public-key encryption, message authentication, digital signatures, key distribution, and protocols, with a good bibliography.

[62] Solomon W. Golomb, *Shift Register Sequences*, Holden-Day, San Francisco, 1967. Reprinted by Aegean Park Press, 1982. Contains many results on sequences generated by linear feedback shift registers (LFSRs). These are often used in stream ciphers (see Schneier [111, Ch. 16]).

[63] Gene H. Golub and Charles F. Van Loan, *Matrix Computations*, third edition, Johns Hopkins Press, Baltimore, Maryland, 1996. A classic on numerical linear algebra.

[64] Ming Gu, *Stable and efficient algorithms for structured systems of linear equations*, Tech. Report LBL-37690, Lawrence Berkeley Laboratory, Aug. 1995. Improves the stability of the GKO algorithm by doing almost complete pivoting efficiently, and shows that orthogonalizing the generators puts an upper bound on the generator growth, as Olshevsky had conjectured.

[65] Martin H. Gutknecht and Marlis Hochbruck, *The Stability of Inversion Formulas for Toeplitz Matrices*, IPS Research Report 93–13, ETH, Zürich, October 1993. Shows that the Gohberg-Semencul and Heinig inversion formulas are weakly stable.

[66] M. Heideman, D. Johnson and C. Burrus, *Gauss and the history of the fast Fourier transform*, Arch. Hist. Exact Sciences **34** (1985), 265–277. For the history of the FFT from Gauss [58].

[67] Georg Heinig, *Inversion of generalized Cauchy matrices and other classes of structured matrices*, Linear Algebra for Signal Processing, IMA Volumes in Mathematics and its Applications, **69** Springer, 1994, 95–114. The first paper to give the Toeplitz ↔ Cauchy transformation used in the GKO algorithm [60].

[68] Nick J. Higham and Des J. Higham, *Large growth factors in Gaussian elimination with pivoting*, SIAM J. Matrix Anal. Appl. **10** (1989), 155–164. Shows that large growth factors do occur in some practical problems when partial pivoting is used. The (attainable) upper bound is 2^{n-1}, but the folklore is that this bound should not be taken too seriously: see [63, 135, 136].

[69] Frank R. de Hoog, *A new algorithm for solving Toeplitz systems of equations*, Linear Algebra Appl. **88/89** (1987), 123–138. Gives another $O(n(\log n)^2)$ algorithm. The same algorithm was found independently by Musicus [92].

[70] Thomas Kailath, *A theorem of I. Schur and its impact on modern signal processing*, in [59], 9–30. Explains how Schur's 1917 paper [113] has applications, e.g. it gives an algorithm for the fast solution of positive-definite symmetric Toeplitz systems. The algorithm is essentially a case of Bareiss's algorithm [8].

[71] Thomas Kailath and J. Chun, *Generalized displacement structure for block-Toeplitz, Toeplitz-block, and Toeplitz-derived matrices*, SIAM J. Matrix Anal. Appl. **15** (1994), 114–128. Introduces a generalisation of displacement rank. Gives algorithms for triangular and orthogonal factorisation, using Schur complement to avoid back-substitution. Stability shown by Stewart and Van Dooren [123] in the positive definite case.

[72] Thomas Kailath and Ali H. Sayed, *Displacement structure: theory and applications*, SIAM Review **37** (1995), 297–386. A useful survey of low displacement-rank theory.

[73] Thomas Kailath, A. Vieira and M. Morf, *Inverses of Toeplitz operators, innovations and orthogonal polynomials*, SIAM Review **20** (1978), 106–119. Explains the connection between algorithms for Toeplitz matrices (or operators) and Szegő's recursions for certain orthogonal polynomials [126].

[74] Donald E. Knuth, *Big Omicron and Big Omega and Big Theta*, SIGACT News **8**, 2 (April–June 1976), 18–24. Defines "O", "Ω" notation and discusses reasons for it.

[75] → Donald E. Knuth, *The Art of Computer Programming, Volume 2: Seminumerical Algorithms*, third edition, Addison-Wesley, 1997. A classic text for the basic "seminumerical" algorithms, e.g. multiple-precision arithmetic, greatest common divisors, random number generators, etc. The third edition has just gone to the printer (as at September 1997); the second edition will soon be obsolete.

[76] A. N. Kolmogorov, *Interpolation and extrapolation of stationary random sequences*, Izvestia Akad. Nauk SSSR **5** (1941), 3–11 (in Russian); German summary, *ibid* 11–14. Kolmogorov discovered an $O(n^2)$ Toeplitz algorithm independently of Wiener and Levinson.

[77] J. van Leeuwen (editor), *Handbook of Theoretical Computer Science*, Elsevier, Amsterdam, 1990.

[78] Arjen K. Lenstra and Hendrik W. Lenstra, Jr., *Algorithms in number theory*, in [77], 675–715. A good survey of number-theoretic algorithms.

[79] → Arjen K. Lenstra and Hendrik W. Lenstra, Jr. (editors), *The development of the number field sieve*, Lecture Notes in Mathematics **1554**, Springer-Verlag, Berlin, 1993. A source book on the number field sieve (NFS), including both SNFS and GNFS. For recent developments see [55, 91, 98, 99].

[80] Arjen K. Lenstra, Hendrik W. Lenstra, Jr., Mark S. Manasse, and John M. Pollard, *The factorization of the ninth Fermat number,* Math. Comp. **61** (1993), 319–349. Describes the most notable early success of the special number field sieve (SNFS), the complete factorization of $F_9 = 2^{2^9} + 1$. Also gives some history of attempts to factor Fermat numbers. and a nice test for a prime power. For F_{10} and F_{11} (which were factored by ECM) see Brent [30, 31].

[81] Hendrik W. Lenstra, Jr., *Factoring integers with elliptic curves,* Annals of Mathematics (2) **126** (1987), 649–673. The original ECM paper. Other early papers, which introduced a second phase and various practical refinements, are [23, 86].

[82] Norman Levinson, *The Wiener RMS (Root-Mean-Square) error criterion in filter design and prediction*, J. Math. Phys. **25** (1947), 261–278. The original paper on Levinson's algorithm, but see also Kolmogorov [76] and Wiener [133]. A slight improvement by Durbin [54] is often called the Levinson-Durbin algorithm.

[83] James F. McKee, *Subtleties in the distribution of the numbers of points on elliptic curves over a finite prime field,* J. London Math. Soc., to appear. Gives plausible reasons why ECM performs better than the asymptotic results predict.

[84] G. L. Miller, *Riemann's hypothesis and tests for primality,* J. Comp. System Sci. **13** (1976), 300–317. Gives a polynomial-time primality test which valid on the assumption of the Extended Riemann Hypothesis (ERH). For more precise results, see Bach [7].

[85] L. Monier, *Evaluation and comparison of two efficient probabilistic primality testing algorithms,* Theoret. Comput. Sci. **12** (1980), 97–108. Compares the Rabin [103] and Solovay-Strassen [121] algorithms.

[86] Peter L. Montgomery, *Speeding the Pollard and elliptic curve methods of factorization,* Math. Comp. **48** (1987), 243–264. An excellent description of both the Pollard $p-1$ method and ECM, with a discussion of variants of phase 2 and choice of initial curves.

[87] Peter L. Montgomery, *An FFT extension of the elliptic curve method of factorization,* Ph. D. dissertation, Mathematics, University of California at Los Angeles, 1992. `ftp://ftp.cwi.nl/pub/pmontgom/ucladissertation.psl.Z`. Describes one of the best (and most complicated) versions of ECM, using the FFT to speed up the second phase.

[88] Peter L. Montgomery, *A survey of modern integer factorization algorithms,* CWI Quarterly **7** (1994), 337–366. `ftp://ftp.cwi.nl/pub/pmontgom/cwisurvey.psl.Z`. Excellent survey of integer factorization algorithms, including ECM and NFS, with numerical examples.

[89] François Morain, *Courbes elliptiques et tests de primalité,* Ph. D. thesis, Univ. Claude Bernard – Lyon I, France, 1990. `ftp://ftp.inria.fr/INRIA/publication/Theses/TU-0144.tar.Z`. For fast, rigorous primality testing. See also [6].

[90] Rajeev Motwani and Prabhakar Raghavan, *Randomized Algorithms*, Cambridge University Press, 1995. A good introduction to randomized algorithms with one chapter on number-theoretic algorithms. Has a large bibliography.

[91] Brian A. Murphy and Richard P. Brent, *On quadratic polynomials for the number field sieve,* Tech. Report TR-CS-97-17, CS Lab, ANU, August 1997. `ftp://nimbus.anu.edu.au/pub/Brent/rpb178tr.dvi.gz`. Discusses polynomial selection, an important practical aspect of NFS implementations.

[92] B. R. Musicus, *Levinson and fast Choleski algorithms for Toeplitz and almost Toeplitz matrices,* Tech. Report, Electronics Research Lab., MIT, Cambridge, Mass., 1984. Gives another $O(n(\log n)^2)$ algorithm. The same algorithm was found independently by de Hoog [69].

[93] D. J. Newman, *A simplified version of the fast algorithms of Brent and Salamin,* Math Comp. **44** (1985), 207–210. Gives a relatively simple, stand-alone proof of the Brent-Salamin (Gauss-Legendre) algorithm for computation of π.

[94] H. J. Nussbaumer, *The Fast Fourier Transform and Convolution Algorithms*, Springer-Verlag, New York, 1981. For the connection between the FFT and fast convolution. See also Burrus [42], Crandall [49] and Van Loan [131], Chapter 4.

[95] Andrew M. Odlyzko, *The rise and fall of knapsack cryptosystems*, in Cryptology and Computational Number Theory (C. Pomerance, ed.), American Math. Soc., Proc. Symp. Appl. Math. #42, 1990. Describes how most (but not all) proposed cryptosystems based on the knapsack (subset sum) problem have been broken. This and many other papers by Odlyzko are available from `http://www.research.att.com/~amo/doc/complete.html`.

[96] John M. Pollard, *Theorems in factorization and primality testing,* Proc. Cambridge Philos. Soc. **76** (1974), 521–528. For Pollard's "$p-1$" method, which is still useful and a key ingredient of ECM.

[97] John M. Pollard, *A Monte Carlo method for factorization,* BIT **15** (1975), 331–334. The original paper on Pollard's "rho (ρ)" algorithm. A practical improvement is given in [22]. For an early success of the (slightly modified) algorithm, see [35].

[98] Carl Pomerance, *The number field sieve,* Proceedings of Symposia in Applied Mathematics **48**, Amer. Math. Soc., Providence, Rhode Island, 1994, 465–480. A recent refererence on the general number field sieve (GNFS).

[99] Carl Pomerance, *A tale of two sieves*, Notices Amer. Math. Soc. **43** (1996), 1473–1485. A good introduction to the quadratic sieve and number field sieve methods for integer factorization.

[100] Vaughan Pratt, *Every prime has a succinct certificate*, SIAM J. Computing **4** (1975), 214–220. Shows that primality testing is in NP. The result is clear by considering the factorization of $p-1$ into prime powers (and recursion).

[101] Michael O. Rabin, *Probabilistic algorithms*, in [130], 21–39. An early introduction to probabilistic algorithms, with examples involving nearest neighbours and primality testing. See also [85, 103].

[102] Michael O. Rabin, *Complexity of computations*, Comm. ACM **20** (1977), 625–633. Corrigendum *ibid* **21** (1978), 231. The 1976 Turing Award Lecture. §4.7 is on probabilistic algorithms. More details are given in [101].

[103] Michael O. Rabin, *Probabilistic algorithms for testing primality,* J. Number Theory **12** (1980), 128–138. A good, probabilistic primality test which is sufficient for all practical purposes. Algorithm P of Knuth [75], §4.5.4, incorporates improvements by Miller, so is often called the Rabin-Miller algorithm (invented independently by Selfridge ?). Slower but surer alternatives are given in [1, 2, 6].

[104] Michael O. Rabin, *Probabilistic algorithms in finite fields*, SIAM J. Computing **9** (1980). Shows how to find a zero of a polynomial of degree n over $GF(p)$ in $O(n \log n \mathrm{loglog} n \log p)$ operations. See also Ben-Or [11].

[105] C. M. Rader, *Discrete Fourier transforms when the number of data samples is prime*, Proc. IEEE **5**, 1107–1108. Shows how the FFT can be performed when the size n is a prime. See also Van Loan [131], Chapter 4.

[106] ⇒ Hans Riesel, *Prime Numbers and Computer Methods for Factorization*, second edition, Birkhäuser, Boston, 1994. A good introduction to computational number theory.

[107] Ronald L. Rivest, Adi Shamir, and Leonard M. Adleman, *A method for obtaining digital signatures and public-key cryptosystems,* Comm. ACM **21** (1978), 120–126. The original reference on the RSA public-key cryptosystem. The idea of public-key cryptography is due to Diffie and Hellman [53].

[108] Eugene Salamin, *Computation of π using arithmetic-geometric mean*, Math. Comp. **30**, 1976, 565–570. Gives an elegant, quadratically convergent algorithm for the computation of π. Written independently and about the same time as [20, 21]. For related algorithms see [17].

[109] Ali H. Sayed and Thomas Kailath, *Fast algorithms for generalized displacement structures and lossless systems*, Linear Algebra Appl. **219** (1995), 49–78. A recent paper on algorithms which exploit low displacement rank and its generalizations.

[110] Bruce Schneier, *E-Mail Security: How to Keep your Electronic Messages Private*, Wiley, 1995. An easy introduction to *Pretty Good Privacy* (PGP), *Privacy Enhanced Mail* (PEM) and related topics.

[111] ⇒ Bruce Schneier, *Applied Cryptography: Protocols, Algorithms, and Source Code in C*, second edition, John Wiley and Sons, 1996. A great source-book for cryptographic topics. Does not include all the mathematics, but has a bibliography of 1653 items. The programs are available on floppy discs (in USA only). For a more theoretical treatment, see Stinson [124].

[112] ⇒ Manfred R. Schroeder, *Number Theory in Science and Communication: With Applications in Cryptography, Physics, Digital Information, Computing, and Self-Similarity*, third edition, Springer-Verlag, 1997. Gives many applications of number theory as indicated in the title.

[113] Issai Schur, *Über Potenzreihen, die im Innern des Einheitskreises beschränkt sind*, J. fur die Reine und Angewandte Mathematik **147** (1917), 205–232. The original paper on Schur's algorithm for finding the continued fraction representation of a holomorphic function in the unit disk. There is an English translation *On power series which are bounded in the interior of the unit circle*, in [59], 31–59. For a commentary, see [70].

[114] Jennifer Seberry and Josef Pieprzyk, *Cryptography: An Introduction to Computer Security*, Prentice-Hall, 1989. A less comprehensive introduction than Schneier [111].

[115] Alan L. Selman, *Complexity issues in cryptography*, Proc. Symposia in Applied Mathematics, **38**, 1989, 92–107. Considers public-key cryptosystems and the "P = NP?" problem. See also Brassard [18] and Taylor [127].

[116] Adi Shamir, *Factoring numbers in $O(\log n)$ arithmetic steps*, Information Processing Letters **8** (1979), 28–31. Shows that when analyzing the complexity of factorization algorithms it is more reasonable to consider the bit-complexity than the total number of arithmetic operations.

[117] Peter W. Shor, *Algorithms for quantum computation: discrete logarithms and factoring,* Proc. 35th Annual IEEE Symposium on Foundations of Computer Science, IEEE Computer Society Press, Los Alamitos, California, 1994, 124–134. Shows that an idealized quantum computer can factor integers and compute discrete logarithms in random polynomial time. This paper caused a surge of interest in quantum computation. For a revision see [118].

[118] Peter W. Shor, *Polynomial time algorithms for factorization and discrete logarithms on a quantum computer*, SIAM J. Computing **26**, 5, October 1997. A revision of [117]. The issue has a special section on quantum computation.

[119] Joseph H. Silverman, *The arithmetic of elliptic curves,* Graduate Texts in Mathematics **106**, Springer-Verlag, New York, 1986. A good introduction to the mathematics of elliptic curves. Contains a proof of Hasse's Theorem (pp. 134–136).

[120] Robert D. Silverman, *The multiple polynomial quadratic sieve,* Math. Comp. **48** (1987), 329–339. Discusses implementation of the MPQS factoring algorithm.

[121] R. Solovay and Volker Strassen, *Fast Monte Carlo test for primality*, SIAM J. on Computing **6** (1977), 84–85; *erratum* **7** (1978), 118. An alternative to the Rabin-Miller algorithm (but not so efficient – see [85]), using the Jacobi symbol.

[122] Michael Stewart, *Stable pivoting for the fast factorization of Cauchy-like matrices*, preprint, Jan. 13, 1997. Makes the result of [125] more intelligible and simplifies some of Ming Gu's results [64] on the stability of fast algorithms.

[123] Michael Stewart and Paul Van Dooren, *Stability issues in the factorization of structured matrices*, SIAM J. Matrix Anal. Appl. **18** (1997), 104–118. A generalization of the results of [15]. For an independent and slightly different generalization, see [43].

[124] → Douglas R. Stinson, *Cryptography: Theory and Practice*, CRC Press, Boca Raton, Florida, 1995 (reprinted 1996). Covers more theory than Schneier [111], including several chapters on public-key cryptography. For more information, see `http://bibd.unl.edu/~stinson/CTAP.html`.

[125] Douglas R. Sweet and Richard P. Brent, *Error analysis of a fast partial pivoting method for structured matrices*, Proceedings SPIE, Volume 2563, Advanced Signal Processing Algorithms SPIE, Bellingham, Washington, 1995, 266–280. `ftp://nimbus.anu.edu.au/pub/Brent/rpb157sp.dvi.gz`. Shows that the original GKO algorithm [60] is unstable even though it uses partial pivoting. The problem is generator growth, which can be avoided (or at least reduced) by more sophisticated algorithms – see [64, 122].

[126] Gabor Szegö, *Orthogonal Polynomials*, AMS Colloquium publ. XXIII, American Mathematical Society, Providence, Rhode Island, 1939. There is an interesting connection between orthogonal polynomials and fast algorithms for Toeplitz matrices: see [73].

[127] Richard Taylor, *Non-repudiation without public key*, Information Security and Privacy, Lecture Notes in Computer Science **1172**, Springer, 1996, 27–37. Discusses NP $\cap$ coNP and its connection with cryptography. See also Brassard [18] and Selman [115].

[128] Richard Taylor, *Uniqueness, Complexity and Symmetric Cryptography*, preprint, 1997. Considers the extension to symmetric cryptosystems of certain complexity properties enjoyed by public-key cryptosystems.

[129] Joseph F. Traub (editor), *Analytic Computational Complexity*, Academic Press, New York, 1975. Includes [20].

[130] Joseph F. Traub (editor), *Algorithms and Complexity*, Academic Press, New York, 1976. Includes several interesting papers, e.g. [101].

[131] $\Rightarrow$ Charles F. Van Loan, *Computational Frameworks for the Fast Fourier Transform*, SIAM, Philadelphia, 1992. A systematic description of the FFT and its many variants, with a good bibliography. Uses Matlab notation and Kronecker products extensively.

[132] A. M. Vershik, *The asymptotic distribution of factorizations of natural numbers into prime divisors,* Dokl. Akad. Nauk SSSR **289** (1986), 269–272; English transl. in Soviet Math. Dokl. **34** (1987), 57–61. Errata (for both the original and the translation): on the right side of equation (5) "$-\alpha_k$" should be "$-\alpha_{k-1}$" and "φ" should be "φ_1". There are also typos in Theorem 2 (defn of y_m) and in the last eqn of Theorem 6 (summation indices should involve k, probably second sum is from $m = k$ to ∞). Gives joint distribution of largest r prime factors of an integer or (equivalently) r largest cycles of a permutation. Theorem 3 deserves to be better known: informally, the ratios of logarithms of neighbouring prime divisors are asymptotically independent and uniformly distributed.

[133] Norbert Wiener, *Extrapolation, Interpolation and Smoothing of Stationary Time Series, with Engineering Applications*, Technology Press and Wiley, New York, 1949 (originally published in 1941 as a Technical Report). Levinson [82] published the first accessible account of an $O(n^2)$ algorithm for a class of Toeplitz systems. Kolmogorov [76] and Wiener discovered $O(n^2)$ algorithms independently during World War II. About forty years later $O(n(\log n)^2)$ algorithms were discovered [33].

[134] Stephen Wiesner, *Conjugate coding*, SIGACT News **15**, 1 (1983), 78–88. The paper which (in draft form, written about 1970!) started the field of quantum cryptography. For a bibliography, see Brassard [19].

[135] James H. Wilkinson, *Rounding Errors in Algebraic Processes*, Prentice-Hall, Englewood Cliffs, New Jersey, 1963. A useful book, easier to read than [136].

[136] James H. Wilkinson, *The Algebraic Eigenvalue Problem*, Oxford University Press, London, 1965. A classic by the inventor of backward error analysis.

[137] Philip R. Zimmermann, *The Official PGP User's Guide*, MIT Press, 1996. *Pretty Good Privacy* (PGP) is a public-domain package for encryption, using both public-key and symmetric algorithms. Most of the contents of this book are in the documentation which comes with PGP, but the book is easier to read and can legally be exported from USA (unlike the PGP program itself).