References

[1] L. Adleman, A subexponential algorithm for the discrete logarithm problem with applications to cryptography (abstract). In *20th Annual Symposium on Foundations of Computer Science (FOCS)*, pp. 55–60, IEEE, New York, 1979

[2] M. Agrawal, CS681: Computational number theory and algebra. Lecture 1 & 2: Integer and modular arithmetic. 2009, lecture notes, https://www.cse.iitk.ac.in/users/manindra/CS681/lecture1and2.pdf, visited on 2 September 2025

[3] M. Agrawal, N. Kayal, and N. Saxena, PRIMES is in P. *Ann. of Math. (2)* **160** (2004), no. 2, 781–793

[4] D. Aharonov and M. Ben-Or, Fault-tolerant quantum computation with constant error rate. *SIAM J. Comput.* **38** (2008), no. 4, 1207–1282

[5] S. Ahmad, Cycle structure of automorphisms of finite cyclic groups. *J. Combinatorial Theory* **6** (1969), 370–374

[6] A. V. Aho, J. E. Hopcroft, and J. D. Ullman, *The design and analysis of computer algorithms*. 2nd edn., Addison-Wesley Ser. Comput. Sci. Inf. Process., Addison-Wesley, MA, 1975

[7] F. Annexstein, M. Baumslag, and A. L. Rosenberg, Group action graphs and parallel architectures. *SIAM J. Comput.* **19** (1990), no. 3, 544–569

[8] T. M. Apostol, *Introduction to analytic number theory*. Undergrad. Texts Math., Springer, New York, 1976

[9] L. Babai, Graph isomorphism in quasipolynomial time. Version 2.5. 2018, preprint, https://people.cs.uchicago.edu/∼laci/quasi25.pdf, visited on 2 September 2025

[10] E. Bach, Comments on search procedures for primitive roots. *Math. Comp.* **66** (1997), no. 220, 1719–1727

[11] E. Bach and J. Shallit, *Algorithmic number theory. Vol. 1*. Found. Comput. Ser., MIT Press, Cambridge, MA, 1996

[12] R. Beals, H. Buhrman, R. Cleve, M. Mosca, and R. de Wolf, Quantum lower bounds by polynomials. *J. ACM* **48** (2001), no. 4, 778–797

[13] A. Bors, On the dynamics of endomorphisms of finite groups. *Appl. Algebra Engrg. Comm. Comput.* **28** (2017), no. 3, 205–214

[14] A. Bors and Q. Wang, Coset-wise affine functions and cycle types of complete mappings. *Finite Fields Appl.* **83** (2022), article no. 102088

[15] A. Bors and Q. Wang, Generalized cyclotomic mappings: Switching between polynomial, cyclotomic, and wreath product form. *Commun. Math. Res.* **38** (2022), no. 2, 246–318

[16] A. Caranti, Quasi-inverse endomorphisms. *J. Group Theory* **16** (2013), no. 5, 779–792

[17] P.-Y. Chen, Solutions to introduction to algorithms third edition. 31-2 Analysis of bit operations in Euclid's algorithm. 2023, online resource, https://walkccc.me/CLRS/Chap31/Problems/31-2/, visited on 2 September 2025

[18] W.-S. Chou and I. E. Shparlinski, On the cycle structure of repeated exponentiation modulo a prime. *J. Number Theory* **107** (2004), no. 2, 345–356

[19] A. H. Clifford and G. B. Preston, *The algebraic theory of semigroups. Vol. II*. Math. Surveys 7, American Mathematical Society, Providence, RI, 1967

[20] T. H. Cormen, C. E. Leiserson, R. L. Rivest, and C. Stein, *Introduction to algorithms*. 3rd edn., MIT Press, Cambridge, MA, 2009

[21] G. Deng, Isomorphic digraphs from affine maps of finite cyclic groups. *ISRN Combinatorics* **2013** (2013), article no. 398641

[22] J. Dubrois and J.-G. Dumas, Efficient polynomial time algorithms computing industrial-strength primitive roots. *Inform. Process. Lett.* **97** (2006), no. 2, 41–45

[23] P. Flajolet and A. M. Odlyzko, Random mapping statistics. In *Advances in cryptology—EUROCRYPT '89 (Houthalen, 1989)*, edited by J. J. Quisquater and J. Vandewalle, pp. 329–354, Lecture Notes in Comput. Sci. 434, Springer, Berlin, 1990

[24] Z. Gao and Q. Wang, A probabilistic approach to value sets of polynomials over finite fields. *Finite Fields Appl.* **33** (2015), 160–174

[25] D. Gottesman, An introduction to quantum error correction and fault-tolerant quantum computation. In *Quantum information science and its contributions to mathematics. Proceedings of the American Mathematical Society Short Course held in Washington, DC, January 3–4, 2009*, edited by S. J. Lomonaco, Jr., pp. 13–58, Proc. Sympos. Appl. Math. 68, American Mathematical Society, Providence, RI, 2010

[26] L. K. Grover, A fast quantum mechanical algorithm for database search. In *Proceedings of the Twenty-eighth Annual ACM Symposium on the Theory of Computing (Philadelphia, PA, 1996)*, edited by G. L. Miller, pp. 212–219, ACM Press, New York, 1996

[27] H. Halberstam, On the distribution of additive number-theoretic functions. III. *J. London Math. Soc.* **31** (1956), 14–27

[28] H. Halberstam, Footnote to the Titchmarsh–Linnik divisor problem. *Proc. Amer. Math. Soc.* **18** (1967), 187–188

[29] D. Harvey and M. Hittmeir, A log-log speedup for exponent one-fifth deterministic integer factorisation. *Math. Comp.* **91** (2022), no. 335, 1367–1379

[30] D. Harvey and J. van der Hoeven, Integer multiplication in time $O(n \log n)$. *Ann. of Math. (2)* **193** (2021), no. 2, 563–617

[31] H. Helfgott, J. Bajpai, and D. Dona, Graph isomorphisms in quasi-polynomial time. 2017, arXiv:1710.04574v1

[32] H. A. Helfgott, Isomorphismes de graphes en temps quasi-polynomial [d'après Babai et Luks, Weisfeiler–Leman,...]. *Astérisque* **2019** (2019), no. 407, 135–182; Séminaire Bourbaki. Vol. 2016/2017. Exposés 1120–1135

[33] R. A. Hernández Toledo, Linear finite dynamical systems. *Comm. Algebra* **33** (2005), no. 9, 2977–2989

[34] W. M. L. Holcombe, *Algebraic automata theory*. Cambridge Stud. Adv. Math. 1, Cambridge University Press, Cambridge, 1982

[35] J. E. Hopcroft, R. Motwani, and J. D. Ullman, *Introduction to automata theory, languages, and computation*. 3rd edn., Addison-Wesley, Boston, 2007

[36] A. S. Jarrah, R. Laubenbacher, B. Stigler, and M. Stillman, Reverse-engineering of polynomial dynamical systems. *Adv. in Appl. Math.* **39** (2007), no. 4, 477–489

[37] P. Kaye, R. Laflamme, and M. Mosca, *An introduction to quantum computing*. Oxford University Press, Oxford, 2007

[38] A. Y. Kitaev, Fault-tolerant quantum computation by anyons. *Ann. Physics* **303** (2003), no. 1, 2–30

[39] E. Knill, R. Laflamme, and W. H. Zurek, Resilient quantum computation. *Science* **279** (1998), no. 5349, 342–345

[40] D. E. Knuth, *The art of computer programming. Vol. 3. Sorting and searching*. 2nd edn., Addison-Wesley, Reading, MA, 1998

[41] R. Kumanduri and C. Romero, *Number theory with computer applications*. Prentice Hall, Upper Saddle River, NJ, 1998

[42] S. Lang, *Introduction to Diophantine approximations*. 2nd edn., Springer, New York, 1995

[43] R. Laubenbacher and B. Pareigis, Equivalence relations on finite dynamical systems. *Adv. in Appl. Math.* **26** (2001), no. 3, 237–251

[44] M. Le Borgne, A. Benveniste, and P. Le Guernic, Polynomial dynamical systems over finite fields. In *Algebraic computing in control. Proceedings of the First European Conference held in Paris, March 13–15, 1991*, edited by G. Jacob and F. Lamnabhi-Lagarrigue, pp. 212–222, Lect. Notes Control Inf. Sci. 165, Springer, Berlin, 1991

[45] H. W. Lenstra, Jr. and C. Pomerance, Primality testing with gaussian periods. 2011, preprint, https://math.dartmouth.edu/∼carlp/aks041411.pdf, visited on 2 September 2025

[46] J. V. Linnik, *The dispersion method in binary additive problems*. Transl. Math. monographs 4, American Mathematical Society, Providence, RI, 1963

[47] L. Lovász, *Combinatorial problems and exercises*. 2nd edn., North-Holland, Amsterdam, 1993

[48] M. Martelli, *Introduction to discrete dynamical systems and chaos*. Wiley-Intersci. Ser. Discrete Math. Optim., Wiley-Interscience, New York, 1999

[49] R. Martins, D. Panario, and C. Qureshi, A survey on iterations of mappings over finite fields. In *Combinatorics and finite fields—difference sets, polynomials, pseudorandomness and applications*, pp. 135–172, Radon Ser. Comput. Appl. Math. 23, De Gruyter, Berlin, 2019

[50] R. S. V. Martins and D. Panario, On the heuristic of approximating polynomials over finite fields by random mappings. *Int. J. Number Theory* **12** (2016), no. 7, 1987–2016

[51] A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone, *Handbook of applied cryptography*. CRC Press Ser. Discrete Math. Appl., CRC Press, Boca Raton, FL, 1997

[52] G. A. Miller and H. C. Moreno, Non-abelian groups in which every subgroup is abelian. *Trans. Amer. Math. Soc.* **4** (1903), no. 4, 398–404

[53] J. C. P. Miller, On factorisation, with a suggested new approach. *Math. Comp.* **29** (1975), 155–172

[54] D. Milligan and M. Wilson, The behaviour of affine Boolean sequential networks. *Connection Science* **5** (1993), no. 2, 153–167

[55] H. L. Montgomery and R. C. Vaughan, The large sieve. *Mathematika* **20** (1973), 119–134

[56] H. Niederreiter and A. Winterhof, Cyclotomic $\mathcal{R}$-orthomorphisms of finite fields. *Discrete Math.* **295** (2005), no. 1-3, 161–171

[57] D. Panario and L. Reis, The functional graph of linear maps over finite fields and applications. *Des. Codes Cryptogr.* **87** (2019), no. 2-3, 437–453

[58] A. Peinado, F. Montoya, J. Muñoz, and A. J. Yuste, Maximal periods of $x^2 + c$ in $\mathbb{F}_q$. In *Applied algebra, algebraic algorithms and error-correcting codes. Proceedings of the 14th International Symposium (AAECC-14) held in Melbourne, November 26–30, 2001*, edited by S. Boztaş and I. E. Shparlinski, pp. 219–228, Lecture Notes in Comput. Sci. 2227, Springer, Berlin, 2001

[59] J. M. Pollard, A Monte Carlo method for factorization. *Nordisk Tidskr. Informationsbehandling (BIT)* **15** (1975), no. 3, 331–334

[60] C. Pomerance, Fast, rigorous factorization and discrete logarithm algorithms. In *Discrete algorithms and complexity. Proceedings of the Japan-U.S. joint seminar held in Kyoto, June 4–6, 1986*, edited by D. S. Johnson et al., pp. 119–143, Perspect. Comput. 15, Academic Press, Boston, MA, 1987

[61] C. Qureshi and D. Panario, Rédei actions on finite fields and multiplication map in cyclic group. *SIAM J. Discrete Math.* **29** (2015), no. 3, 1486–1503

[62] C. Qureshi and D. Panario, The graph structure of Chebyshev polynomials over finite fields and applications. *Des. Codes Cryptogr.* **87** (2019), no. 2-3, 393–416

[63] G. Robin, Grandes valeurs de la fonction somme des diviseurs et hypothèse de Riemann. *J. Math. Pures Appl. (9)* **63** (1984), no. 2, 187–213

[64] A. Schönhage, Schnelle Berechnung von Kettenbruchentwicklungen. *Acta Inform.* **1** (1971), 139–144

[65] A. Schönhage and V. Strassen, Schnelle Multiplikation grosser Zahlen. *Computing (Arch. Elektron. Rechnen)* **7** (1971), 281–292

[66] M. Sha, Digraphs from endomorphisms of finite cyclic groups. *J. Combin. Math. Combin. Comput.* **83** (2012), 105–120

[67] C. E. Shannon, The synthesis of two-terminal switching circuits. *Bell System Tech. J.* **28** (1949), 59–98

[68] P. W. Shor, Algorithms for quantum computation: Discrete logarithms and factoring. In *35th Annual Symposium on Foundations of Computer Science. Proceedings of the IEEE Symposium held in Santa Fe, NM, November 20–22, 1994*, edited by S. Goldwasser, pp. 124–134, IEEE Computer Society Press, Los Alamitos, CA, 1994

[69] P. W. Shor, Fault-tolerant quantum computation. In *37th Annual Symposium on Foundations of Computer Science. Held in Burlington, VT, October 14–16, 1996*, pp. 56–65, IEEE Computer Society Press, Los Alamitos, CA, 1996

[70] The GAP Group, GAP–groups, algorithms, and programming. 2022, version 4.12.0, http://www.gap-system.org, visited on 2 September 2025

[71] S. Ugolini, Graphs associated with the map $x \mapsto x + x^{-1}$ in finite fields of characteristic two. In *Theory and applications of finite fields. Proceedings of the 10th International Conference on Finite Fields and Their Applications (Fq 10) held in Ghent, July 11–15, 2011*, edited by M. Lavrauw et al., pp. 187–204, Contemp. Math. 579, American Mathematical Society, Providence, RI, 2012

[72] S. Ugolini, Graphs associated with the map $X \mapsto X + X^{-1}$ in finite fields of characteristic three and five. *J. Number Theory* **133** (2013), no. 4, 1207–1228

[73] T. Vasiga and J. Shallit, On the iteration of certain quadratic maps over GF(p). *Discrete Math.* **277** (2004), no. 1-3, 219–240

[74] A. Veliz-Cuba and R. Laubenbacher, On the computation of fixed points in Boolean networks. *J. Appl. Math. Comput.* **39** (2012), no. 1-2, 145–153

[75] J. von zur Gathen and J. Gerhard, *Modern computer algebra*. 3rd edn., Cambridge University Press, Cambridge, 2013

[76] J. von zur Gathen and D. Panario, Factoring polynomials over finite fields: A survey. *J. Symbolic Comput.* **31** (2001), no. 1-2, 3–17

[77] S. Wagstaff, The Cunningham project. 2022, online database, https://homes.cerias.purdue.edu/∼ssw/cun/, visited on 2 September 2025

[78] D. Q. Wan and R. Lidl, Permutation polynomials of the form $x^r f(x^{(q-1)/d})$ and their group structure. *Monatsh. Math.* **112** (1991), no. 2, 149–163

[79] Q. Wang, Cyclotomic mapping permutation polynomials over finite fields. In *Sequences, subsequences, and consequences. Revised invited papers from the International Workshop (SSC 2007) held at the University of Southern California, Los Angeles, CA, May 31–June 2, 2007*, edited by S. W. Golomb et al., pp. 119–128, Lecture Notes in Comput. Sci. 4893, Springer, Berlin, 2007

[80] Q. Wang, Cyclotomy and permutation polynomials of large indices. *Finite Fields Appl.* **22** (2013), 57–69

[81] Q. Wang, A note on inverses of cyclotomic mapping permutation polynomials over finite fields. *Finite Fields Appl.* **45** (2017), 422–427

[82] Q. Wang, Polynomials over finite fields: An index approach. In *Combinatorics and finite fields—difference sets, polynomials, pseudorandomness and applications*, edited by K.-U. Schmidt and A. Winterhof, pp. 319–346, Radon Ser. Comput. Appl. Math. 23, De Gruyter, Berlin, 2019

[83] X. Wang and V. Y. Pan, Acceleration of Euclidean algorithm and rational number reconstruction. *SIAM J. Comput.* **32** (2003), no. 2, 548–556

[84] J. Watrous, Quantum computational complexity. In *Computational complexity. Vols. 1–6*, pp. 2361–2387, Springer, New York, 2012

[85] W.-D. Wei, X.-H. Gao, and B.-F. Yang, Equivalence relation on the set of subsets of z_v and enumeration of the equivalence classes (Research Announcement). *Adv. Math.* **17** (1988), 326–327

[86] W. D. Wei and J. Y. Xu, Cycle index of direct product of permutation groups and number of equivalence classes of subsets of Z_v. *Discrete Math.* **123** (1993), no. 1-3, 179–188

[87] Y. Zheng, Y. Yu, Y. Zhang, and D. Pei, Piecewise constructions of inverses of cyclotomic mapping permutation polynomials. *Finite Fields Appl.* **40** (2016), 1–9