References

1. Adleman, L.M., and Huang, M.-D.A. *Primality testing and abelian varieties over finite fields*, Lecture Notes in Mathematics, Vol. 1512. Springer-Verlag, Berlin, Heidelberg, New York 1992.
2. Adleman, L.M., Pomerance, C., and Rumely, R.S., On distinguishing prime numbers from composite numbers. Ann. Math. 117 (1983) 173–206.
3. Agrawal, M., Kayal, N., and Saxena, N., PRIMES is in P. Preprint, `http://www.cse.iitk.ac.in/news/primality.ps`, August 8, 2002.
4. Agrawal, M., Kayal, N., and Saxena, N., PRIMES is in P. Preprint (revised), `http://www.cse.iitk.ac.in/news/primality_v3.ps`, March 1, 2003.
5. Alford, W., Granville, A., and Pomerance, C., There are infinitely many Carmichael numbers. Ann. Math. 139 (1994) 703–722.
6. Apostol, T., *Introduction to Analytic Number Theory*. 3rd printing. Springer-Verlag, Berlin, Heidelberg, New York 1986.
7. Artjuhov, M., Certain criteria for the primality of numbers connected with the Little Fermat Theorem (in Russian). Acta Arith. 12 (1966/67) 355–364.
8. Bach, E., Explicit bounds for primality testing and related problems. Inform. and Comput. 90 (1990) 355–380.
9. Baker, R.C., and Harman, G., The Brun-Titchmarsh Theorem on average. In: Berndt, B.C., *et al.*, *Eds.*, *Analytic Number Theory, Proceedings of a Conference in Honor of Heini Halberstam*, pages 39–103. Birkhäuser, Boston 1996.
10. Bernstein, D.G., Proving primality after Agrawal, Kayal, and Saxena. Preprint, `http://cr.yp.to/papers#aks`, January 25, 2003.
11. Bernstein, D.G., Distinguishing prime numbers from composite numbers: The state of the art in 2004. Preprint, `http://cr.yp.to/primetests.html#prime2004`, February 12, 2004.
12. Bosma, W., and van der Hulst, M.-P., *Primality Proving with Cyclotomy*. PhD thesis, University of Amsterdam, 1990.
13. Bornemann, F., PRIMES is in P: A breakthrough for "everyman". Notices of the AMS 50 (2003) 545–552.
14. Burthe, R., Further investigations with the strong probable prime test. Math. Comp. 65 (1996) 373–381.
15. Cormen, T.H., Leiserson, C.E., Rivest, R.L., and Stein, C., *Introduction to Algorithms*. 2nd Ed. MIT Press, Cambridge 2001.
16. Crandall, R., and Pomerance, C., *Prime Numbers: A Computational Perspective*. Springer-Verlag, Berlin, Heidelberg, New York 2001.
17. Damgård, I., Landrock, P., and Pomerance, C., Average case error estimates for the strong probable prime test. Math. Comp. 61 (1995) 513–543.
18. Feller, W., *An Introduction to Probability Theory and Its Applications*, Vol. 1. 3rd Ed. Wiley, New York 1968.
19. Fouvry, E., Théorème de Brun-Titchmarsh; application au théorème de Fermat. Invent. Math. 79 (1985) 383–407.

20. Gauss, C.F., Disquisitiones Arithmeticae, 1801.
21. Graham, R.L., Knuth, D.E., and Patashnik, O., *Concrete Mathematics*. 2nd Ed. Addison-Wesley, Boston 1994.
22. Hardy, G., and Wright, E., *An Introduction to the Theory of Numbers*, 5th Ed. Clarendon Press, Oxford 1979.
23. Hopcroft, J.E., Motwani, R., and Ullman, J.D., *Introduction to Automata Theory, Languages, and Computation*. 2nd Ed. Addison-Wesley, Boston 2001.
24. Koblitz, N., *A Course in Number Theory and Cryptography*. 2nd Ed. Springer-Verlag, Berlin, Heidelberg, New York 1994.
25. Knuth, D.E., *Seminumerical Algorithms*. Volume 2 of *The Art of Computer Programming*. 3rd Ed. Addison-Wesley, Boston 1998.
26. Lehmann, D.J., On primality tests. SIAM J. Comput. 11 (1982) 374–375.
27. Lenstra, H.W., Primality testing with cyclotomic rings. Unpublished. August 2002.
28. Lidl, R., and Niederreiter, H., *Introduction to Finite Fields and Cryptography*. Cambridge University Press, Cambridge 1986.
29. Miller, G.M., Riemann's hypothesis and tests for primality. J. Comput. Syst. Sci. 13 (1976) 300–317.
30. Nair, M., On Chebyshev-type inequalities for primes. Amer. Math. Monthly 89 (1982) 126–129.
31. Niven, I., Zuckerman, H.S., and Montgomery, H.L., *An Introduction to the Theory of Numbers*. 5th Ed. Wiley, New York 1991.
32. Pinch, R.G.E., The Carmichael numbers up to 10^{15}. Math. Comp. 61 (1993) 381–391. Website: `http://www.chalcedon.demon.co.uk/rgep/car3-18.gz`.
33. Pinch, R.G.E., The pseudoprimes up to 10^{13}. In: Bosma, W., University of Nijmegen, The Netherlands (Ed.), Algorithmic Number Theory, 4th International Symposium, Proceedings, pages 459–474. Lecture Notes in Computer Science, Vol. 1838. Springer-Verlag, Berlin, Heidelberg, New York 2000.
34. Pratt, V., Every prime has a succinct certificate. SIAM J. Comput. 4 (1975) 214–220.
35. Rabin, M.O., Probabilistic algorithm for testing primality. J. Number Theory 12 (1980) 128–138.
36. Rivest, R., Shamir, A., and Adleman, L., A method for obtaining digital signatures and public-key cryptosystems. Comm. Assoc. Comput. Mach. 21 (1978) 120–126.
37. Salomaa, A., *Public-Key Cryptography*. 2nd Ed. Springer-Verlag, Berlin, Heidelberg, New York 1996.
38. Schönhage, A., and Strassen, V., Schnelle Multiplikation großer Zahlen. Computing 7 (1971) 281–292.
39. Solovay, R., and Strassen, V., A fast Monte-Carlo test for primality. SIAM J. Comput. 6 (1977) 74–86.
40. Stinson, D.R., *Cryptography: Theory and Practice*. CRC Press, Boca Raton 2002.
41. Von zur Gathen, J., and Gerhard, J., *Modern Computer Algebra*. 2nd Ed. Cambridge University Press, Cambridge 2003.

Index