

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

- $D(n)$, 24
- $I(u, f)$, 125
- $O(f(n))$, 16
- $O(f)$, 16
- $R[X]$, 97
- $R[X]/(h)$, 106
- X , 98
- $\Omega(f(n))$, 16
- $\Omega(f)$, 16
- $\Theta(f(n))$, 16
- $\Theta(f)$, 16
- $\deg(f)$, 98
- $\gcd(n, m)$, 24
- $\langle a \rangle$, 60
- \leftarrow , 14
- $\lfloor x \rfloor$, $\lceil x \rceil$, 136
- $\ln n$, 4
- $\log n$, 4
- div , 25
- mod , 25
- $|$, 23
- $\text{ord}_G(a)$, 62
- $\text{ord}_p(n)$, 71
- $\pi(x)$, 45
- $\varphi(n)$, 34, 38, 70
- $f \bmod h$, 105
- $f(X)$, 101
- $f(s)$, 100

- A-liar, 80
- A-witness, 80
- abelian group, 57
- addition, 68
- additive notation, 57
- Adleman, 2
- Agrawal, 115
- algorithm, deterministic, 8
- algorithm, randomized, 15
- arithmetic, fundamental theorem of, 43
- array, 13
- assignment, 14

- associated polynomials, 108
- associativity, 55

- binary operation, 55
- binomial coefficient, 46, 50, 115, 133
- binomial theorem, 47, 136
- bit operation, 18
- boolean values, 14
- break statement, 14

- cancellation rule, 34, 57
- Carmichael number, 76
- ceiling function, 136
- certificate, 8
- Chebychev, 45
- Chinese Remainder Theorem, 36, 37
- coefficient, 96
- commutative group, 57
- commutative monoid, 66
- commutative ring, 67
- comparison of coefficients, 98
- composite, 39
- composite number, 1
- congruence, 32
- congruence class, 33
- congruence of polynomials, 104
- congruent, 32
- constant, 13
- constant polynomial, 98

- deterministic algorithm, 8
- deterministic primality test, 115
- distributive law, 67
- divisibility, 23
- divisibility of polynomials, 104
- division, 25, 68
- division of polynomials, 102, 103
- division with remainder, 25
- divisor, 23, 25

- E-liar, 93
- E-witness, 93

- efficient algorithm, 2
- equivalence relation, 32, 58, 104
- Eratosthenes, 39, 118
- Euclid, 39
- Euclidean Algorithm, 27
- Euclidean Algorithm, extended, 30
- Euler liar, 93
- Euler witness, 93
- Euler's criterion, 86
- Euler's totient function, 34
- Euler, a theorem of, 64
- exponentiation, fast, 69

- F-liar, 74
- F-witness, 73
- factorial, 133
- factoring problem, 10
- fast exponentiation, 69
- Fermat liar, 74
- Fermat test, 74
- Fermat test, iterated, 76
- Fermat witness, 73
- Fermat's Little Theorem, 64, 73, 101
- field, 68, 95
- finite fields, 68
- floor function, 136
- for loop, 15
- Fouvry's theorem, 120
- fundamental theorem, 43

- Gauss, 2
- generate, 61
- generated subgroup, 60
- generating element, 61
- generator, 70
- Germain, 122
- greatest common divisor, 24, 26
- group, 55

- half system, 137
- harmonic number, 137

- if statements, 14
- indentation, 14
- integers, 23
- introspective, 125
- inverse element, 55, 57
- irreducible, 108

- Jacobi symbol, 87, 91

- Kayal, 115

- leading coefficient, 98
- Legendre, 47
- Legendre symbol, 87
- linear combination, 26

- Miller-Rabin test, 81
- modular arithmetic, 32
- modulus, 25, 32
- monic polynomial, 99
- monoid, 66
- monoid, commutative, 66
- multiple, 23
- multiplication, 68
- multiplication of polynomials, 99
- multiplicative group, 34

- natural numbers, 23
- neutral element, 55, 57
- nonconstant polynomial, 98
- nonresidue, 85

- operation, binary, 55
- order, 62
- order (of a group element), 62
- order modulo p , 71

- parentheses, 55
- perfect power, 20, 118
- permutation, 133
- polynomial, 95
- polynomial division, 102, 103
- polynomials over R , 97
- power, of group element, 59
- primality proving, 9
- prime, 39
- prime decomposition, 2, 42
- prime generation, 10
- prime number, 1, 39
- Prime Number Theorem, 45
- primitive r th root of unity, 113
- primitive element, 70, 71
- proper divisor (for polynomials), 104
- proper divisor (of a polynomial), 108
- pseudoprimes, 74

- quadratic nonresidue, 85
- quadratic reciprocity law, 90, 137, 140, 141
- quadratic residue, 85
- quotient, 25
- quotient of rings, 106

- randomization, 3
- randomized algorithm, 15

- reflexivity, 32
- relatively prime, 24, 27
- remainder, 25
- repeat loop, 15
- return statement, 14
- ring, 67, 95
- ring, commutative, 67
- Rivest, 2
- root (of polynomial), 111
- root of a polynomial, 100
- RSA system, 2, 10

- Saxena, 115
- Shamir, 2
- Solovay-Strassen test, 94
- Sophie Germain prime, 122
- square, 85
- square root modulo p , 86
- square root of 1 mod n , 78
- subgroup, 57

- subgroup criterion, 58
- subgroup, cardinality of, 59
- subring, 97, 99
- substitution, 100
- subtraction, 68
- symmetry, 32

- totient function, 34, 70
- transitivity, 32
- trial division, 1

- unique factorization (for polynomials),
109
- unit, 67, 99, 104

- variable, 13, 96

- while loop, 15

- zero divisor, 67, 99