

References

- [1] R. Alford, A. Granville and C. Pomerance, There are infinitely many Carmichael numbers, *Annals of Mathematics* **139** (1994), 703–722.
- [2] A. Archer, A modern treatment of the 15-puzzle, *American Mathematical Monthly* **106** (1999), 793–799.
- [3] E. Berlekamp, Factoring polynomials over finite fields, *Bell System Technical Journal* **46** (1967), 1853–1859.
- [4] R. Courant and H. Robbins, *What is Mathematics?*, Oxford University Press, 1941.
- [5] R. E. Crandall, *Mathematica for the Sciences*, Addison Wesley, 1991.
- [6] M. Demazure, *Cours d'algèbre*, Cassini, 1997.
- [7] L. E. Dickson, Finiteness of the odd perfect and primitive abundant numbers with n distinct prime factors, *American Journal of Mathematics* **35** (1913), 413–422.
- [8] W. Diffie and M. E. Hellman, New directions in cryptography, *IEEE Transactions on Information Theory* **22**, (1976), 644–654.
- [9] W. Feit and J. Thompson, Solvability of groups of odd order, *Pacific Journal of Mathematics* **13** (1963), 775–1029.
- [10] M. Gardner, *Mathematical Puzzles of SAM LOYD*, Dover Publications, 1959.
- [11] C. F. Gauss, *Disquisitiones Arithmeticae*, Springer Verlag, New York, 1993, English translation by Arthur A. Clarke.
- [12] G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, Oxford University Press, 1945.
- [13] D. Hilbert, Über die Theorie der algebraischen Formen, *Mathematische Annalen* **36** (1890), 473–534.

- [14] K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory*, Springer Verlag, New York, 1982.
- [15] J. L. W. Jensen, Om talteoretiske Egenskaber ved de Bernoulliske tal, *Nyt Tidsskrift for Mathematik* **26** (1915), 73–83.
- [16] D. E. Knuth, *The Art of Computer Programming*, second edition, vol. II: *Seminumerical Algorithms*, Addison Wesley, New York, 1981.
- [17] N. Koblitz, *A Course in Number Theory and Cryptography*, Springer Verlag, New York, 1987.
- [18] O. Ore, *Number Theory and its History*, Dover Publications, New York, 1948.
- [19] C. Pomerance, A tale of two sieves, *Notices of the American Mathematical Society* **43** (1996), 1473–1485.
- [20] M. Rabin, Probabilistic algorithm for testing primality, *Journal of Number Theory* **12** (1980), 128–138.
- [21] D. Redfern, *The Maple Handbook*, vol. Maple V Release 4, Springer Verlag, 1996.
- [22] R. Rivest and A. Shamir and L. Adleman, A method for obtaining digital signatures and public-key cryptosystems, *Communications of the ACM* **21** (1978), 120–126.
- [23] B. Sturmfels, *Gröbner Bases and Convex Polytopes*, American Mathematical Society, Providence, 1996.
- [24] L. Sylow, Théorèmes sur les groupes de substitutions, *Mathematische Annalen* **5** (1872), 584–594.
- [25] S. Wagon, The Euclidean algorithm strikes again, *American Mathematical Monthly* **97** (1990) 125–129.
- [26] A. Wiles, Modular elliptic curves and Fermat’s last theorem, *Annals of Mathematics* **142** (1995), 443–551.