Bibliography

Project LIMA

References

[1] Knuth, D The Art of Computer Programming, Vol 2

[2] Cormen,TH. Leiserson,CE. Rivest,RL. Stein, C. Introduction to Algorithms (Second Edition) MIT Press and McGraw-Hill

[3] Montgomery (A Survey of Modern Integer Factorization Algorithms, CWI Quarterly v 7 no 4 (1994) pp 337-366)

[4] R. P. Brent, “Algorithm 524: MP, a Fortran multipleÂprecision arithmetic package [A1], ACM Trans. on Mathematical Software 4 (1978), 71–81.

[5] R. P. Brent, “Parallel algorithms for integer factorisation”, in Number Theory and Cryptography (edited by J. H. Information about Gausian Elimantion http://www.damtp.cam.ac.uk/user/examples/D3Lb.pdf Information about Gausian Elimination: http://www.maths.cam.ac.uk/undergrad/tripos/catam/IB/2pt1.pdfLoxton), Cambridge University Press, 1990.

[6] R. P. Brent, “Vector and parallel algorithms for integer factorisation”, Proc. Third Australian Supercomputer Conference, Melbourne, 1990.

[7] T. R. Caron and R. D. Silverman, “Parallel implementation of the quadratic sieve”, J. Supercomputing 1 (1988), 273–290.

[8] C. Eldershaw and R. P. Brent, “Factorization of large integers on some vector and parallel computers

[9] P. L. Montgomery, “Speeding the Pollard and elliptic curve methods of factorisation”, Mathematics of Computation 48 (1987), 243–264.

[10] C. Pomerance, J. W. Smith and R. Tuler, “A pipeline architecture for factoring large integers with the quadratic sieve algorithm”, SIAM J. on Computing 17 (1988), 387– 403.

[11] R. L. Rivest, A. Shamir and L. Adelman, “A method for obtaining digital signatures and publicÂkey cryptosystems”, Comm. ACM 21 (1978), 120–126.

[12] H. J. J. te Riele, W. Lioen and D. Winter, “Factoring with the quadratic sieve on large vector computers”, Belgian J. Comp. Appl. Math. 27(1989), 267–278.

[13] O. Ãsbrink, J. Brynielsson, Factoring large integers using parallel Quadratic Sieve (2000).

[14] E. Landquist, The Quadratic Sieve Factoring Algorithm MATH 488: Cryptographic Algorithms (2001).

[15] Riesel, Hans. Prime Numbers and Computer Methods for Factorization 2nd Ed. Birkhauser, Boston, 1994.

[16] Silverman, Robert. \The Multiple Polynomial Quadratic Sieve Method of Computation," Math. Comput., 48 (1987), 329-340.

[17] Bressoud, David. Factorization and Primality Testing. Springer-Verlag,New York, 1989.

[18] Cavallar, S., Lioen, W., te Riele, H., Dodson, B., Lenstra, A., Montgomery, P., Murphy, B., et al. \Factorization of a 512-bit RSA modulus, Eurocrypt (2000).

[19] ”Information about Gausian Elimantion http://www.damtp.cam.ac.uk/user/examples/D3Lb.pdf

[20] Information about Gausian Elimination: http://www.maths.cam.ac.uk/undergrad/tripos/catam/IB/2pt1.pdf

[21] Proceedings of NeInformation about Gausian Elimantion http://www.damtp.cam.ac.uk/user/examples/D3Lb.pdf

[22] Parallel and Scientific Computations 1 (1995), 143Â148.

[23] Also Tech. Report TRÂCSÂ95Â01, CSL, ANU, January 1995, 6 pp.