a is stored as an r-tuple $(a_1, \ldots, a_r)$, where a_i is the least nonnegative residue of a mod $2^{m_i} - 1$. Prove that a, b and ab are each uniquely determined by the corresponding r-tuple, and estimate the number of bit operations required to find the r-tuple corresponding to ab from the r-tuples corresponding to a and b.

References for Chapter I

1. J. Brillhart, D. H. Lehmer, J. L. Selfridge, B. Tuckerman, and S. S. Wagstaff, Jr., *Factorizations of $b^n \pm 1$, $b = 2, 3, 5, 6, 7, 10, 11, 12$, up to High Powers*, Amer. Math. Society, 1983.
2. L. E. Dickson, *History of the Theory of Numbers*, three volumes, Chelsea, 1952.
3. R. K. Guy, *Unsolved Problems in Number Theory*, Springer–Verlag, 1982.
4. G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, 5th ed., Oxford University Press, 1979.
5. W. J. LeVeque, *Fundamentals of Number Theory*, Addison–Wesley, 1977.
6. H. Rademacher, *Lectures on Elementary Number Theory*, Krieger, 1977.
7. K. H. Rosen, *Elementary Number Theory and Its Applications*, 3rd ed., Addison–Wesley, 1993.
8. M. R. Schroeder, *Number Theory in Science and Communication*, 2nd ed., Springer–Verlag, 1986.
9. D. Shanks, *Solved and Unsolved Problems in Number Theory*, 3rd ed., Chelsea Publ. Co., 1985.
10. W. Sierpínski, *A Selection of Problems in the Theory of Numbers*, Pergamon Press, 1964.
11. D. D. Spencer, *Computers in Number Theory*, Computer Science Press, 1982.