

This paper is concerned with the problem of obtaining theoretical estimates for the number of arithmetical operations required to factorize a large integer  $n$  or test it for primality. One way of making these problems precise uses a multi-tape Turing machine (e.g. (1), although we require a version with an input tape). At the start of the calculation  $n$  is written in radix notation on one of the tapes, and the machine is to stop after writing out the factors in radix notation or after writing one of two symbols denoting 'prime' or 'composite'. There are, of course, other definitions which could be used; but the differences between these are unimportant for our purpose.