Dixon, John D.
Asymptotically fast factorization of integers. (English) Zbl 0452.10010

Summary: The paper describes a “probabilistic algorithm” for finding a factor of any large composite integer $n$ (the required input is the integer $n$ together with an auxiliary sequence of random numbers). It is proved that the expected number of operations which will be required is $O(\exp\{\beta(\ln n \ln \ln n)^{1/2}\})$ for some constant $\beta > 0$. Asymptotically, this algorithm is much faster than any previously analyzed algorithm for factoring integers; earlier algorithms have all required $O(n^\alpha)$ operations where $\alpha > 1/5$.

For a scan of this review see the web version.

MSC:
11Y05 Factorization
68W20 Randomized algorithms
11Y16 Number-theoretic algorithms; complexity

Keywords:
asymptotically fast factorization of integers; probabilistic algorithm; primality tests; algorithms

Full Text: DOI

References:

This reference list is based on information provided by the publisher or from digital mathematics libraries. Its items are heuristically matched to zbMATH identifiers and may contain data conversion errors. It attempts to reflect the references listed in the original paper as accurately as possible without claiming the completeness or perfect precision of the matching.