Kaltofen, Erich; Lavin, Mark
Efficiently certifying non-integer powers. (English) Zbl 1276.11202

Summary: We describe a randomized algorithm that, given an integer $a$, produces a certificate that the integer is not a pure power of an integer in expected $(\log a)^{1+o(1)}$ bit operations under the assumption of the Generalized Riemann Hypothesis. The certificate can then be verified in deterministic $(\log a)^{1+o(1)}$ time. The certificate constitutes for each possible prime exponent $p$ a prime number $q_p$ such that $a \mod q_p$ is a $p$th non-residue. We use an effective version of the Chebotarev density theorem to estimate the density of such prime numbers $q_p$.

MSC:
11Y16 Number-theoretic algorithms; complexity
68W30 Symbolic computation and algebraic computation
11R45 Density theorems
11Y05 Factorization

Full Text: DOI