LEAST DIRICHLET CHARACTER NONRESIDUES AND INTEGER FACTORING PROBLEM

JACEK POMYKAŁA (Warsaw University)

ABSTRACT: Let $F(x, \mathcal{A}, \mathcal{O}, t_{\mathcal{A}}, t_{\mathcal{O}})$ denote the the number of composite positive integers $n \leq x$, that can be factored completely by algorithm $\mathcal{A}$ in time $t_{\mathcal{A}}$ with at most $t_{\mathcal{O}}$ queries to oracle O. We investigate the deterministic, polynomial time algorithms $\mathcal{A}$ for which

$$F(x, \mathcal{A}, \mathcal{O}, t_{\mathcal{A}}, t_{\mathcal{O}}) \geq x\left(1 - \frac{1}{A(x)}\right).$$

where $t_{\mathcal{A}}(n) = O(\log^c n)$, $t_{\mathcal{O}}(n) = O(\log n)$, $(c > 0)$ and $A(x)$ is some function tending to infinity as x tends to infinity. Here we consider two types of oracles Φ and $Dec\Phi$ answering with the value of the totient Euler function and its prime powers decomposition, respectively. The proofs of the estimates for both type of oracles $\mathcal{O}$ depend of the average bounds for the least quadratic characters nonresidues, Iwaniec's shifted sieve and the zero density estimates for Dirichlet L-functions.

NTW2017