ILLINOIS JOURNAL OF MATHEMATICS
Volume 26, Number 1, Spring 1982

A NEW LOWER BOUND FOR THE PSEUDOPRIME COUNTING FUNCTION

BY

CARL POMERANCE

1. Introduction

A composite natural number n is called a *pseudoprime* (to base 2) if

$$2^{n-1} \equiv 1 \pmod{n}.$$

The least pseudoprime is $341 = 11 \cdot 31$. Let $\mathscr{P}(x)$ denote the number of pseudoprimes not exceeding x. It is known that there are positive constants c_1, c_2 such that for all large x,

$$c_1 \log x \leq \mathscr{P}(x) \leq x \cdot \exp\{-c_2(\log x \cdot \log\log x)^{1/2}\}.$$

The lower bound is implicit in Lehmer [6] and the upper bound is due to Erdös [4]. Very recently in [9] we have obtained an improvement in the upper bound. There have been improvements on the lower bound, but they have only concerned the size of the constant c_1. For example, see Rotkiewicz [13].

In this paper we show that there is a positive constant α such that for all large x,

$$\mathscr{P}(x) \geq \exp\{(\log x^{\alpha})\}.$$

In particular, we may take $\alpha = 5/14$.

Erdös conjectures that $\mathscr{P}(x) = x^{1-\varepsilon(x)}$ where $\varepsilon(x) \to 0$ as $x \to \infty$. See Pomerance, Selfridge, Wagstaff [10] for more on this.

Our main result holds for pseudoprimes to any base and in fact for strong pseudoprimes to any base (see Section 2 for definitions). Moreover our result holds if we just count those pseudoprimes n with at least $(\log n)^{5/14}$ distinct prime factors.

On the negative side, if $\mathscr{P}'(x)$, $\mathscr{P}''(x)$, and $\mathscr{P}^k(x)$ denote respectively the counting functions for pseudoprimes that are square-free, not square-free, and have at most k distinct prime factors, then we cannot show any one of $\mathscr{P}'(x)/\log x$, $\mathscr{P}''(x)$, $\mathscr{P}^k(x)/\log x$ is unbounded.

We wish to thank H. W. Lenstra, Jr. and S. S. Wagstaff, Jr. for some helpful comments during early stages of this paper.

Received January 11, 1980.