MATHEMATICS OF COMPUTATION
Volume 65, Number 213
January 1996, Pages 373–381

FURTHER INVESTIGATIONS WITH THE STRONG PROBABLE PRIME TEST

RONALD JOSEPH BURTHE, JR.

ABSTRACT. Recently, Damgård, Landrock and Pomerance described a procedure in which a k-bit odd number is chosen at random and subjected to t random strong probable prime tests. If the chosen number passes all t tests, then the procedure will return that number; otherwise, another k-bit odd integer is selected and then tested. The procedure ends when a number that passes all t tests is found. Let $p_{k,t}$ denote the probability that such a number is composite. The authors above have shown that $p_{k,t} \leq 4^{-t}$ when $k \geq 51$ and $t \geq 1$. In this paper we will show that this is in fact valid for all $k \geq 2$ and $t \geq 1$.

1. INTRODUCTION

Let n be an odd number with $n-1 = 2^s u$, where u is odd. The following notation will be used in this article:

$\mathcal{S}(n) = \{a \in [1, n-1] : a^u \equiv 1 \bmod n \text{ or } a^{2^i u} \equiv -1 \bmod n \text{ for some } i = 0, 1, ..., s-1\}$,

$S(n) = \mid \mathcal{S}(n) \mid$.

If $a \in \mathcal{S}(n)$ for some pair a and n, we say that n is a *strong probable prime to base a*. If n is prime, then $S(n) = n-1$, and if n is an odd composite number, then $S(n)/(n-1) \leq 1/4$ (see Monier [4], Rabin [5]).

Now if for a given n we can find an integer $a \in [1, n-1]$ such that $a \notin \mathcal{S}(n)$, then we know that n is composite. If one picks t a's at random from $[1, n-1]$ and discovers that each is in $\mathcal{S}(n)$, one cannot however conclude that n is prime. We can conclude that if n is an odd composite number, the probability that all the t randomly chosen a's are in $\mathcal{S}(n)$ is less than or equal to 4^{-t}.

These results suggest a procedure for finding random integers that are likely to be prime in the set M_k of odd k-bit integers. Choose a random n in M_k and then choose an $a_1 \in [1, n-1]$ and see if $a_1 \in \mathcal{S}(n)$. If $a_1 \in \mathcal{S}(n)$, then choose an $a_2 \in [1, n-1]$ and test to see if it is in $\mathcal{S}(n)$. This procedure is then repeated until either an a_i is discovered such that $a_i \notin \mathcal{S}(n)$ or until t a_i's are found that are all in $\mathcal{S}(n)$. In the former case, another n is picked from M_k, and in the latter case, the number n will be given as output. This procedure, as described in [1] will be referred to here as the random bases procedure.

Let $p_{k,t}$ denote the probability that the number which is given as output by the random bases procedure is composite. In [2], it is left as an open question to find a value k_0 such that $p_{k,t} \leq 4^{-t}$ for all $t \geq 1$ and $k \geq k_0$. From Monier's and Rabin's

Received by the editor May 3, 1994.
1991 *Mathematics Subject Classification.* Primary 11Y11; Secondary 11A51.

result one sees that if n is an odd composite integer, then the probability that it passes t random strong pseudoprime tests is less than or equal to 4^{-t}. However, this is not sufficient to show that $p_{k,t} \leq 4^{-t}$ as the following discussion shows. For a fixed $t \geq 1$ choose k sufficiently large such that the density of the primes in M_k is much less than 4^{-t}. Assume also that for most composite m in M_k that the probability that m passes a random bases test is about $1/4$. Then, of course, the probability of it passing t tests is about 4^{-t}. Suppose that we have an n from M_k that passes t tests. Since we are assuming that the primes in M_k are scarce, it will be much more likely that n is composite rather than prime. So $p_{k,t}$ would be close to 1. However, it will be shown in this dissertation, that $p_{k,t} \leq 4^{-t}$ for $k \geq 2$ and $t \geq 1$. The flawed assumption that led us to the conclusion that $p_{k,t}$ was close to 1 is the assumption that the probability of a composite n in M_k passing a test was about $1/4$. In actuality the probability is usually much smaller and this is essentially the conclusion of Proposition 1.

In the next section we will prove that $p_{k,t} \leq \left(1/4\right)^{t-l} p_{k,l}/(1-p_{k,l})$ for integer l with $1 \leq l \leq t-1$. Taking $l = 1$ we get that $p_{k,t} \leq 4^{1-t} p_{k,1}/(1-p_{k,1})$, so to show that $p_{k,t} \leq 4^{-t}$ for all $t \geq 1$, it suffices to show that $p_{k,1} \leq 1/5$. In [3], it is shown that this is true for $k \geq 55$. Taking $l = 2$ in the above inequality, we can see that to show that $p_{k,t} \leq 4^{-t}$ for all $t \geq 1$ it will also suffice to show that $p_{k,1} \leq 1/4$ and $p_{k,2} \leq 1/17$. In [3], this is shown to be true for all k with $51 \leq k \leq 54$. In this paper we will improve the results in [3] and show that $p_{k,t} \leq 4^{-t}$ for all k with $k \geq 2$ and $t \geq 1$. This will be done by extending some of the ideas in [3] and sharpening the upper bounds found there as well. Some improvements are due to simple observations of the properties of certain numbers and easily lead to a lower upper bound. Other improvements are not quite as obvious and require more work while only minimally improving some of the results. The overall net effect is to reduce in general the upper bound for $p_{k,t}$ by a factor of a fourth. We are able to prove a theorem that enabled us to verify that $p_{k,t} \leq 4^{-t}$ for all $k \geq 25$ and $t \geq 1$. For $2 \leq k \leq 24$, the result is verified by actually computing $p_{k,t}$ using an equation due to Monier. Thus we can take k_0 to be 2.

2. Preliminaries

We will start by recalling Lemma 1 from [3]. Here, $\omega(n)$ is the number of distinct prime factors of n, $\Omega(n)$ is the number of prime factors of n counted with multiplicity, $\phi(n)$ is the Euler phi function, and $\alpha(n) = S(n)/\phi(n)$. For the remainder of the paper, p will always be used to denote a prime.

Lemma 1. *If $n > 1$ is odd, then*

$$\frac{1}{\alpha(n)} \geq 2^{\omega(n)-1} \prod_{p^\beta \| n} p^{\beta-1} \frac{p-1}{(p-1, n-1)} \geq 2^{\Omega(n)-1} \prod_{p|n} \frac{p-1}{(p-1, n-1)}.$$

The following lemma is a generalization of Lemma 2 in [3] and gives a slightly improved result.

Lemma 2. *If $t \in \mathbb{R}, t \geq s, s \in \mathbb{Z}^+$, then*

$$\sum_{n=\lfloor t \rfloor + 1}^{\infty} \frac{1}{n^2} < \frac{c_s}{t},$$

where

$$c_s = (s+1)\Big(\frac{\pi^2}{6} - \sum_{n=1}^{s} \frac{1}{n^2}\Big).$$

Proof. Let $m = \lfloor t \rfloor$. So $m \in \mathbb{Z}, m \geq s$. Then

$$\sum_{n=m+1}^{\infty} \frac{1}{n^2} = \sum_{n=1}^{\infty} \frac{1}{n^2} - \sum_{n=1}^{m} \frac{1}{n^2} = \frac{\pi^2}{6} - \sum_{n=1}^{m} \frac{1}{n^2}$$
$$< \frac{(m+1)}{t}\Big(\frac{\pi^2}{6} - \sum_{n=1}^{m} \frac{1}{n^2}\Big) = \frac{1}{t} c_m.$$

Letting $k \in \mathbb{Z}^+$ with $k \geq s+1$, we have that

$$c_{k-1} - c_k = -\frac{\pi^2}{6} + \frac{1}{k} + \sum_{n=1}^{k} \frac{1}{n^2}$$
$$= -\frac{\pi^2}{6} + \int_k^{\infty} \frac{1}{x^2} dx + \sum_{n=1}^{k} \frac{1}{n^2} > -\frac{\pi^2}{6} + \sum_{n=1}^{\infty} \frac{1}{n^2} = 0.$$

Thus the sequence $c_s, c_{s+1}, \ldots$ is decreasing, and in particular $c_m \leq c_s$. Substituting into the previous inequality gives the desired result. □

Lemma 3. *If $l, t \in \mathbb{Z}^+$ with $1 \leq l \leq t-1$, then*

$$p_{k,t} \leq 4^{-l} \frac{p_{k,l}}{1 - p_{k,l}}.$$

Proof. The event that a number chosen at random from M_k passes the ith test will be denoted by D_i, and we define the event E_i by

$$E_i = D_1 \cap D_2 \cap \cdots \cap D_i.$$

We will also let C denote the event that a number chosen at random from M_k is composite, and C' will denote the set of composites. Also let $\overline{\alpha}(n) = S(n)/(n-1)$, and recall that for odd composite n we will have $\overline{\alpha}(n) \leq 1/4$. $P(A)$ will be used here to denote the probability that event A occurs. Note that $P(C \cap E_i) = 2^{-(k-2)} \sum_{n \in C' \cap M_k} \overline{\alpha}(n)^i$.

Now for $1 \leq l \leq t-1$ we have

$$p_{k,t} = P(C \mid E_t) = \frac{P(C \cap E_t)}{P(E_t)}$$
$$= \frac{P(C \cap E_t)}{P(C \cap E_{t-1})} \frac{P(C \cap E_{t-1})}{P(C \cap E_{t-2})} \cdots \frac{P(C \cap E_{l+1})}{P(C \cap E_l)} \frac{P(C \cap E_l)}{P(E_t)}.$$

Now

$$\frac{P(C \cap E_i)}{P(C \cap E_{i-1})} = \frac{\sum_{n \in C' \cap M_k} \overline{\alpha}(n)^i}{\sum_{n \in C' \cap M_k} \overline{\alpha}(n)^{i-1}} \leq \frac{\sum_{n \in C' \cap M_k} \frac{1}{4} \overline{\alpha}(n)^{i-1}}{\sum_{n \in C' \cap M_k} \overline{\alpha}(n)^{i-1}} = \frac{1}{4}.$$

Letting A^c denote the complement of event A, we see that C^c is the event that a number is prime. Since a prime in M_k will always pass each test we see that $P(C^c \cap E_t) = P(C^c) = P(C^c \cap E_l)$. Thus we see that

$$p_{k,t} \leq \left(\frac{1}{4}\right)^{t-l} \frac{P(C \cap E_l)}{P(E_l)} \frac{P(E_l)}{P(E_t)} = \left(\frac{1}{4}\right)^{t-l} p_{k,l} \frac{P(E_l)}{P(E_t)}.$$

Also

$$\frac{P(E_l)}{P(E_t)} \leq \frac{P(E_l)}{P(C^c \cap E_t)} = \frac{P(E_l)}{P(C^c)} = \frac{P(E_l)}{P(C^c \cap E_l)} = \frac{1}{P(C^c \mid E_l)} = \frac{1}{1 - p_{k,l}}$$

which completes the proof of the lemma. □

3. Estimates

Now as in [3], C_m will denote the set of odd composite integers n with $\alpha(n) > 2^{-m}$. However, we will allow m to assume nonintegral values. Since $\alpha(n) \leq 1/4$ for odd composite $n \neq 9$ (see [4] or [5]) and since $\alpha(9) = 1/3$, we will have $C_m = \emptyset$ for $0 < m \leq \ln 3/\ln 2$ and $C_m = \{9\}$ for $\ln 3/\ln 2 < m \leq 2$.

We will now generalize Theorem 1 from [3] for the case where m is not necessarily an integer.

Theorem 1. *Assume* $k \in \mathbb{Z}^+,\ k \geq 2,\ m \in \Re^+,\ s \in \mathbb{Z}^+$ *such that*

$$s \leq (2^{(k-1)/j} - 1)2^{j-m-2} \quad \textit{for } j = 2, 3, ..., \lceil m \rceil.$$

Then

$$\frac{\mid C_m \cap M_k \mid}{\mid M_k \mid} < 2c_s \sum_{j=2}^{\lceil m \rceil} \frac{\lceil 2^{m+1-j} \rceil - 1}{2^{\frac{k-1}{j}} - 1}$$

where c_s *is defined as in Lemma* 2.

Proof. From Lemma 1, we have $1/\alpha(n) \geq 2^{\Omega(n)-1}$ for all odd n. So if $n \in C_m$, we have $2^m > 1/\alpha(n) \geq 2^{\Omega(n)-1}$ and thus $m+1 > \Omega(n)$. Since $\Omega(n) \in \mathbb{Z}^+$, this implies that $\Omega(n) \leq \lceil m \rceil$. Now letting $N(m,k,j) = \{n \in C_m \cap M_k \mid \Omega(n) = j\}$, we see that

$$\mid C_m \cap M_k \mid \ = \sum_{j=2}^{\lceil m \rceil} \mid N(m,k,j) \mid .$$

Let $n \in N(m,k,j)$, $2 \leq j \leq \lceil m \rceil$, and let p be the largest prime factor of n. Now $2^{k-1} < n \leq p^j$ implies that $p > 2^{(k-1)/j}$. Let $d(p,n) = (p-1)/(p-1, n-1)$. Lemma 1 implies that $2^m > \alpha(n)^{-1} \geq 2^{\Omega(n)-1} d(p,n) = 2^{j-1} d(p,n)$, so we must have $d(p,n) < 2^{m+1-j}$.

Given p, d such that $p > 2^{(k-1)/j}$, $d \mid p-1$, and $d < 2^{m+1-j}$, we want to get an upper bound for the number of $n \in N(m,k,j)$ with largest prime factor p and $d(p,n) = d$; it will suffice to consider the set $S_{k,d,p} := \{n \in M_k : p \mid n,\ d = d(p,n),\ n \text{ composite}\}$. The set $S_{k,d,p}$ is contained in the set $R_{k,d,p} := \{n \in \mathbb{Z} : n \equiv 0 \bmod p,\ n \equiv 1 \bmod (p-1)/d,\ p < n < 2^k\}$ which has, via the Chinese Remainder Theorem,

less than $2^k d/(p(p-1))$ elements. If $S_{k,d,p} \neq \emptyset$, then there exists an $n \in S_{k,d,p}$ with $(n-1, p-1) = (p-1)/d$, and thus $(p-1)/d$ must be even since n and p are odd. Thus we need only consider those d and p such that $(p-1)/d$ is even. Letting $\sum^o$ denote a sum over p with $2^{\frac{k-1}{j}} < p < 2^k$, $d \mid p-1$ and $(p-1)/d$ even, we get that

$$\begin{aligned} \mid N(m,k,j) \mid \; &\leq \sum_{d<2^{m+1-j}} \sum^{o} \mid S_{k,d,p} \mid \leq \sum_{d<2^{m+1-j}} \sum^{o} \mid R_{k,d,p} \mid \\ &\leq 2^k \sum_{d<2^{m+1-j}} \sum^{o} \frac{d}{p(p-1)}. \end{aligned}$$

Now

$$\begin{aligned} \sum^{o} \frac{d}{p(p-1)} &\leq \sum_{2ud>2^{(k-1)/j}-1} \frac{d}{(2ud+1)2ud} \leq \frac{1}{4d} \sum_{u>\frac{2^{(k-1)/j}-1}{2d}} \frac{1}{u^2} \\ &< \frac{1}{4d} \frac{2c_s d}{(2^{(k-1)/j}-1)} = \frac{c_s}{2} \frac{1}{(2^{(k-1)/j}-1)} \end{aligned}$$

with the last inequality coming from Lemma 2. Note: to use Lemma 2, we must have that $(2^{(k-1)/j}-1)/(2d) \geq s$, but this follows from the hypothesis that $s \leq (2^{(k-1)/j}-1)2^{j-m-2}$, since $d < 2^{m+1-j}$. Thus,

$$\mid N(m,k,j) \mid \leq 2^k \frac{c_s}{2} \sum_{d<2^{m+1-j}} \frac{1}{2^{(k-1)/j}-1} = 2^k \frac{c_s}{2} \frac{\lceil 2^{m+1-j} \rceil - 1}{2^{(k-1)/j}-1}.$$

Therefore,

$$\mid C_m \cap M_k \mid = \sum_{j=2}^{\lceil m \rceil} \mid N(m,k,j) \mid < 2^k \frac{c_s}{2} \sum_{j=2}^{\lceil m \rceil} \frac{\lceil 2^{m+1-j} \rceil - 1}{2^{(k-1)/j}-1}.$$

Now since $k \geq 2$, we have $\mid M_k \mid = 2^{k-2}$. So by dividing each side of the inequality by 2^{k-2} we get the desired result and our proof of Theorem 1 is complete. □

Now let $\sum'$ denote a sum over composite integers. As in [3], recalling that p denotes a prime, we have

$$\begin{aligned} p_{k,t} &= \big(\sum_{n \in M_k} \overline{\alpha}(n)^t \big)^{-1} \sum_{n \in M_k}{}' \overline{\alpha}(n)^t = \big(\sum_{n \in M_k}{}' \overline{\alpha}(n)^t + \sum_{p \in M_k} 1 \big)^{-1} \sum_{n \in M_k}{}' \overline{\alpha}(n)^t \\ &= \big(\sum_{n \in M_k}{}' \overline{\alpha}(n)^t + \pi(2^k) - \pi(2^{k-1}) \big)^{-1} \sum_{n \in M_k}{}' \overline{\alpha}(n)^t. \end{aligned}$$

Now if we have an upper bound N_1 for $\sum'_{n \in M_k} \overline{\alpha}(n)^t$ and a lower bound P_1 for $\pi(2^k) - \pi(2^{k-1})$, then

$$p_{k,t} \leq \frac{N_1}{N_1 + P_1}. \tag{1}$$

Let $\sum^{(q)}$ denote a sum with increments of length $1/q$ where $q \in \mathbb{Z}^+$.

Proposition 1. *Let $k, M, t, s, q \in \mathbb{Z}^+$ with $k \geq 5$, $M \geq 3$ and $s \leq (2^{(k-1)/j} - 1)2^{j-M-2}$ for $j = 2, 3, ..., M$. Then*

$$\sum_{n \in M_k}{}' \overline{\alpha}(n)^t \leq 2^{-Mt+k-2} + 2^{k-1} c_s (2^{t/q} - 1) \sum_{m=2+\frac{1}{q}}^{M(q)} 2^{-mt} \sum_{j=2}^{\lceil m \rceil} \frac{\lceil 2^{m+1-j} \rceil - 1}{2^{\frac{k-1}{j}} - 1}.$$

Proof. Since $k \geq 5$, we have $9 \notin M_k$. So for all m with $0 < m \leq 2$, we have $C_m \cap M_k = \emptyset$. Thus

$$\begin{aligned}
\sum_{n \in M_k}{}' \overline{\alpha}(n)^t &= \sum_{m=2+\frac{1}{q}}^{\infty(q)} \sum_{n \in M_k \cap (C_m \setminus C_{m-\frac{1}{q}})} \overline{\alpha}(n)^t \leq \sum_{m=2+\frac{1}{q}}^{\infty(q)} \sum_{n \in M_k \cap (C_m \setminus C_{m-\frac{1}{q}})} \alpha(n)^t \\
&\leq \sum_{m=2+\frac{1}{q}}^{\infty(q)} 2^{-(m-\frac{1}{q})t} \mid M_k \cap (C_m \setminus C_{m-\frac{1}{q}}) \mid \\
&\leq 2^{-Mt} \sum_{m=M+\frac{1}{q}}^{\infty(q)} \mid M_k \cap (C_m \setminus C_{m-\frac{1}{q}}) \mid + \sum_{m=2+\frac{1}{q}}^{M(q)} 2^{-(m-\frac{1}{q})t} \mid M_k \cap (C_m \setminus C_{m-\frac{1}{q}}) \mid \\
&= 2^{-Mt} \mid M_k \setminus C_M \mid + \sum_{m=2+\frac{1}{q}}^{M(q)} 2^{-(m-\frac{1}{q})t} \mid M_k \cap (C_m \setminus C_{m-\frac{1}{q}}) \mid .
\end{aligned}$$

Let $T_m = \mid C_m \cap M_k \mid$, and let U_m be an upper bound for T_m. Rewriting the above inequality, we get

$$\begin{aligned}
\sum_{n \in M_k}{}' \overline{\alpha}(n)^t &\leq 2^{-Mt}(\mid M_k \mid - \ T_M) + \sum_{m=2+\frac{1}{q}}^{M(q)} 2^{-(m-\frac{1}{q})t}(T_m - T_{m-\frac{1}{q}}) \\
&= 2^{-Mt}(2^{k-2} - T_M) + \sum_{m=2+\frac{1}{q}}^{M-\frac{1}{q}(q)} \big(2^{-(m-\frac{1}{q})t} - 2^{-mt}\big) T_m + 2^{-(M-\frac{1}{q})t} T_M - 2^{-2t} T_2 \\
&\leq 2^{-Mt+k-2} + \sum_{m=2+\frac{1}{q}}^{M(q)} \big(2^{-(m-\frac{1}{q})t} - 2^{-mt}\big) T_m \\
&\leq 2^{-Mt+k-2} + \sum_{m=2+\frac{1}{q}}^{M(q)} \big(2^{-(m-\frac{1}{q})t} - 2^{-mt}\big) U_m.
\end{aligned}$$

Now $2^{-(m-\frac{1}{q})t} - 2^{-mt} = (2^{\frac{t}{q}} - 1)2^{-mt}$, and since we can take

$$U_m = 2^{k-1} c_s \sum_{j=2}^{\lceil m \rceil} \frac{\lceil 2^{m+1-j} \rceil - 1}{2^{\frac{k-1}{j}} - 1}$$

from Theorem 1, this gives

$$\sum_{n\in M_k}{}' \overline{\alpha}(n)^t \leq 2^{-Mt+k-2} + 2^{k-1}c_s(2^{\frac{t}{q}}-1)\sum_{m=2+\frac{1}{q}}^{M(q)} 2^{-mt}\sum_{j=2}^{\lceil m\rceil}\frac{\lceil 2^{m+1-j}\rceil - 1}{2^{\frac{k-1}{j}}-1}.$$

This concludes our proof of Proposition 1. □

From Proposition 2 in [3], we know that for $k \geq 21$ we have

$$\pi(2^k) - \pi(2^{k-1}) > (.71867)\frac{2^k}{k}.$$

Thus, we may take N_1 and P_1 in (1) as

$$N_1 = 2^{-Mt+k-2} + 2^{k-1}c_s(2^{\frac{t}{q}}-1)\sum_{m=2+\frac{1}{q}}^{M(q)} 2^{-mt}\sum_{j=2}^{\lceil m\rceil}(\lceil 2^{m+1-j}\rceil - 1)/(2^{\frac{k-1}{j}}-1)$$

and

$$P_1 = (.71867)\frac{2^k}{k}$$

for $k \geq 21$, where $M \geq 3$ and $s \leq (2^{(k-1)/j}-1)2^{j-M-2}$ for $2 \leq j \leq M$.

Now in our computations we need s to be a positive integer at most $(2^{(k-1)/j}-1)2^{j-M-2}$ for each j with $2 \leq j \leq M$. So we choose M such that the greatest integer less than or equal to $(2^{(k-1)/j}-1)2^{j-M-2}$ is positive. So essentially we want to have $g(j) := (k-1)/j + j - M - 2 \geq 1$. Taking M and k as fixed, we see that g has a minimum of $-M-2+2\sqrt{k-1}$ at $j = \sqrt{k-1}$. So for our purposes, it is sufficient to choose M such that $3 \leq M \leq 2\sqrt{k-1}-3$. This guarantees that we can find a largest positive integer—say s_1— with $s_1 \leq (2^{(k-1)/j}-1)2^{j-M-2}$ for each j with $2 \leq j \leq M$. Choosing $s = s_1$ gives us the best possible constant for c_s (but computing c_{s_1} for large s_1 uses more running time while yielding only negligible improvements). So for each M with $3 \leq M \leq 2\sqrt{k-1}-3$, we choose s to be the minimum of s_1 and 30 and compute our upper bound using that s and taking $q = 4$. Taking the minimum of all the upper bounds we were able to show that $p_{k,1} \leq 1/4$ and $p_{k,2} \leq 1/17$ for $25 \leq k \leq 50$. Thus we were able to show that $p_{k,t} \leq 4^{-t}$ for all k with $25 \leq k \leq 50$. In our approximations for the upper bound of $p_{k,t}$, the s-value we chose was only dependent upon M but if we brought the c_s inside the summation over m in the above expression for N_1, we could have in fact chosen our s so that it would be dependent upon m instead, and it would only have to satisfy the inequality $s \leq (2^{(k-1)/j}-1)2^{j-m-2}$. This was attempted for some values of k but it did not produce any significant improvements. Subsequently, we continued to use the value for s determined by M. The main results of our computations are shown in Table I and Table II.

TABLE I. u_k: upper bound for $p_{k,1}$ for $25 \leq k \leq 50$

k	u_k	k	u_k	k	u_k	k	u_k
25	0.248692	32	0.173705	39	0.119921	46	0.080952
26	0.237095	33	0.165640	40	0.113131	47	0.076863
27	0.225027	34	0.157518	41	0.107492	48	0.072736
28	0.215733	35	0.150928	42	0.102743	49	0.069210
29	0.209292	36	0.144473	43	0.099016	50	0.066400
30	0.196233	37	0.135932	44	0.091629		
31	0.185387	38	0.126492	45	0.086431		

TABLE II. $u_{k,2}$: upper bound for $p_{k,2}$ for $25 \le k \le 50$

k	$u_{k,2}$	k	$u_{k,2}$	k	$u_{k,2}$	k	$u_{k,2}$
25	.021590	32	.008395	39	.003472	46	.001476
26	.018884	33	.007394	40	.003027	47	.001315
27	.016233	34	.006436	41	.002659	48	.001160
28	.014140	35	.005650	42	.002349	49	.001029
29	.012564	36	.004996	43	.002099	50	.000922
30	.011127	37	.004471	44	.001869		
31	.009791	38	.003928	45	.001672		

4. Exact values

The above upper bound method fails to give us the desired result for $k \le 24$ and in this section the method used to handle these cases will be discussed. Let $\nu(n)$ denote the largest integer such that $2^{\nu(n)} \mid p-1$ for each prime $p \mid n$, and let u denote the largest odd factor of $n-1$. If one recalls that $\overline{\alpha}(n) = S(n)/(n-1)$, it is computationally possible to compute $p_{k,1}$ exactly for $k \le 24$, using (as described in [4]) Monier's result

$$S(n) = \Big(1 + \frac{2^{\omega(n)\nu(n)} - 1}{2^{\omega(n)} - 1}\Big) \prod_{p|n} (p-1, u)$$

and our previous formula (recalling that $\sum'$ is a sum over composite integers)

$$p_{k,1} = \big(\sum_{n \in M_k} \overline{\alpha}(n)\big)^{-1} \sum_{n \in M_k}{}' \overline{\alpha}(n).$$

To compute $S(n)$, all of the prime factors of n must be determined so computationally we can only use this formula for fairly small values of k. The C program we used for our computations first found all the primes less than 4096 (the square root of 2^{24}) and put these primes into a file. Then for each odd n with $2^{k-1} < n < 2^k$, we were able to determine $\omega(n)$ and $\nu(n)$, using this file and trial division. These computations were done on a SPARC I computer and took only several hours to run.

Table III shows the values of $p_{k,1}$ (approximated to six place accuracy) obtained by using the above equations in our program for $2 \le k \le 24$. Since all these values are less than $1/5$ we can conclude that $p_{k,t} \le 4^{-t}$ for all k with $2 \le k \le 24$ and $t \ge 1$. Combining these results with the results obtained using the upper bounds, we have shown that $p_{k,t} \le 4^{-t}$ for all $k \ge 2$ and $t \ge 1$.

TABLE III. Computed values of $p_{k,1}$ for $2 \le k \le 24$

k	$p_{k,1}$	k	$p_{k,1}$	k	$p_{k,1}$	k	$p_{k,1}$
2	0.000000	8	0.038004	14	0.005934	20	0.000609
3	0.000000	9	0.030837	15	0.003944	21	0.000402
4	0.164179	10	0.020525	16	0.002626	22	0.000276
5	0.064299	11	0.017394	17	0.001929	23	0.000188
6	0.065348	12	0.010710	18	0.001258	24	0.000126
7	0.056655	13	0.007949	19	0.000905		

5. Further numerical results

Using the upper bound $p_{k,t} \le N_1/(N_1 + P_1)$ where N_1 and P_1 are defined as in §3, we can improve most of the values found in Table 2 of [3]. For each possible k and t in the table, we computed a lower bound for $-\lg p_{k,t}$ in the following way. For each M within a well chosen range, we chose our s as before to be the minimum of the largest allowable value for s and 30 to obtain a lower bound for $-\lg p_{k,t}$ and we then took the maximum of all these lower bounds. The entries in Table IV reflect the maximum of the computed values and the entries from Table 2 of [3] where the italicized entries are those entries from [3] which were *not* improved upon by our computations. We believe that it is possible to improve this table even more by using the combined method discussed in [3] and the results obtained in this paper, but we did not attempt to do so.

Table IV. Lower bounds for $-\lg p_{k,t}$

$k\backslash t$	1	2	3	4	5	6	7	8	9	10
100	7	17	23	28	32	35	38	41	44	46
150	11	22	30	36	41	46	50	53	56	60
200	14	27	36	43	49	54	59	63	67	71
250	16	32	42	49	56	62	68	72	77	81
300	*19*	36	46	55	63	69	75	81	86	90
350	*28*	39	51	60	69	76	82	88	94	99
400	*37*	*46*	*55*	65	74	82	89	95	101	107
450	*46*	*54*	*62*	*70*	79	88	95	102	108	114
500	*56*	*63*	*70*	*78*	*85*	93	101	108	115	121
550	*65*	*72*	*79*	*86*	*93*	*100*	*107*	114	121	128
600	*75*	*82*	*88*	*95*	*102*	*108*	*115*	*121*	128	135

Acknowledgment

Special thanks go to Carl Pomerance who was instrumental in all aspects of writing this paper and without whom this paper could not have been written. The comments of Andrew Granville were also very much appreciated.

References

1. P. Beauchemin, G. Brassard, C. Crépeau, and C. Goutier, *Two observations on probabilistic primality testing*, Advances in Cryptology—Crypto 86 Proceedings (A.M. Odlyzko, ed.), Lecture Notes in Comput. Sci., vol. 263, Springer-Verlag, Berlin, 1987, pp. 443-450. MR **89c:**11180
2. P. Beauchemin, G. Brassard, C. Crépeau, C. Goutier, and C. Pomerance, *The generation of random numbers that are probably prime, J. Cryptology* **1** (1988), 53–64. MR **89g:**11126
3. I. Damgård, P. Landrock, and C. Pomerance, *Average case error estimates for the strong probable prime test*, Math. Comp. **61** (1993), 177–194. MR **94b:**11124
4. L. Monier, *Evaluation and comparison of two efficient probabilistic primality testing algorithms*, Theoret. Comput. Sci. **12** (1980), 97–108. MR **82a:**68078
5. M. O.Rabin, *Probabilistic algorithm for testing primality*, J. Number Theory **12** (1980), 128–138. MR **81f:**10003

Department of Mathematics, University of Georgia, Athens, Georgia 30602-7403
E-mail address: ronnie@alpha.math.uga.edu