LABORATORY FOR COMPUTER SCIENCE

MASSACHUSETTS INSTITUTE OF TECHNOLOGY

MIT/LCS/TM-108

AN ANALYSIS OF THE SOLOVAY AND STRASSEN TEST FOR PRIMALITY

Alan E. Baratz

July 1978

545 TECHNOLOGY SQUARE, CAMBRIDGE, MASSACHUSETTS 02139

MIT/LCS/TM-108

AN ANALYSIS OF THE SOLOVAY AND STRASSEN TEST FOR PRIMALITY

Alan E. Baratz

July 1978

MASSACHUSETTS INSTITUTE OF TECHNOLOGY
Laboratory for Computer Science

CAMBRIDGE MASSACHUSETTS 02139

AN ANALYSIS OF THE SOLOVAY AND STRASSEN+ TEST FOR PRIMALITY

Alan E. Baratz
Department of Electrical Engineering
and Computer Science
MIT
Cambridge, Massachusetts

Abstract: In this paper we will analyze the performance of the Solovay and Strassen probabilistic primality testing algorithm. We will show that iterating Solovay and Strassen's algorithm r times, using independent random numbers at each iteration, results in a test for the primality of any positive odd integer, n>2, with error probability 0 (if n is prime), error probability at most 4^{-r} (if n is composite and non-Carmichael), and error probability at most 2^{-r} (if n is composite and Carmichael).

Key words: Carmichael number, Jacobi symbol, primality, probabilistic algorithm, quadratic residue

+This research was supported by NSF grant MCS77-19754-A02

Introduction

Several years ago, R. Solovay and V. Strassen [5] developed a probabilistic algorithm for determining whether or not a positive odd integer, $n>2$, is prime. The algorithm consists of choosing a random number, a, from a uniform distribution on the set of integers $\{1,2,\ldots,n-1\}$ and then determining if

$$(1)\qquad \begin{cases} \text{either } (a,n)\neq 1^{*} \\ \text{or } a^{(n-1)/2}\not\equiv\left(\frac{a}{n}\right)\pmod{n}.^{**} \end{cases}$$

Letting $W_n(a)$ denote the condition (1), it is clear that $W_n(a)$ will <u>not</u> hold if n is prime. Therefore, if $W_n(a)$ holds, n must be composite and thus the algorithm can simply halt and say "n is composite." However, if $W_n(a)$ does not hold, it is not certain that n is prime. In the case where $W_n(a)$ does not hold, the algorithm can either repeat itself choosing a new independent random number or else simply halt. If the algorithm halts in this case, however, it is required to say "n is prime" even though this may not be the correct answer.

Letting $\overline{W}_n=\{a\in\mathbb{Z} \mid 1\le a<n \text{ and } W_n(a) \text{ does } \underline{\text{not}} \text{ hold}\}$, Solovay and Strassen [5] were able to show that if n is positive, odd and composite,

$$|\overline{W}_n| \le \tfrac{1}{2}(n-1).$$

----

* (a,n) denotes $\gcd(a,n)$ ** $\left(\frac{a}{n}\right)$ is the Jacobi symbol

Therefore, for all such n, the probability of their algorithm giving an incorrect answer after a single iteration is at most 1/2. Further, their algorithm will always give the correct answer if n is prime. Thus, iterating Solovay and Strassen's algorithm r times, using independent random numbers at each iteration, results in a test for primality with error probability 0 (if n is prime) and error probability at most 2^{-r} (if n is positive, odd and composite).

In this paper we will show that if n is positive, odd, composite and <u>non-Carmichael</u>,

$$|\bar{W}_n| \le \tfrac{1}{4}(n-1).$$

This result will follow as the corollaries of two new number theoretic theorems which will be stated here and proven in the next section.

<u>Theorem 1</u>:

Let $n=p_1^{e_1}\cdot p_2^{e_2}\cdot\ldots\cdot p_z^{e_z}$ where z is any positive integer ($z\ge 1$), the e_i are all positive integers ($1\le i\le z$), and the p_i are all distinct odd primes ($p_i>2$). If $A=\{a\in\mathbb{Z} \mid 1\le a<n \text{ and } (a,n)=1 \text{ and } a^{(n-1)/2}\equiv\left(\frac{a}{n}\right)(\text{mod } n)\}$, then

$$|A| \le \prod_{i=1}^{z}(p_i-1).$$

<u>Theorem 2</u>:

Let $n=p_1^{e_1}\cdot p_2^{e_2}\cdot\ldots\cdot p_z^{e_z}$ where z is any positive integer such that $z\ge 2$, the e_i are all positive integers ($1\le i\le z$) such that at least one e_j ($1\le j\le z$) is odd, and the p_i are all distinct odd primes ($p_i>2$). If

$$A=\{a\in\mathbb{Z} \mid 1\le a<n \text{ and } (a,n)=1 \text{ and } a^{(n-1)/2}\equiv\left(\frac{a}{n}\right)(\text{mod } n)\}$$

and

$$B=\{a\in\mathbb{Z} \mid 1\le a<n \text{ and } (a,n)=1 \text{ and } a^{n-1}\equiv 1(\text{mod } n)\}$$

then $A \subsetneq B$.

Finally, we would like to mention that we have recently become aware of a new result by Louis Monier [6] which gives a closed form for $|\overline{W}_n|$. We feel, however, that the proof of our results are still of interest.

Proofs of Theorems

Theorem 1:

Let $n=p_1^{e_1}\cdot p_2^{e_2}\cdot\ldots\cdot p_z^{e_z}$ where z is any positive integer ($z\geq 1$), the e_i are all positive integers ($1\leq i\leq z$), and the p_i are all distinct odd primes ($p_i>2$). If $A=\left\{a\in\mathbb{Z} \mid 1\leq a<n \text{ and } (a,n)=1 \text{ and } a^{(n-1)/2}\equiv\left(\frac{a}{n}\right)(\text{mod } n)\right\}$, then

$$|A| \leq \prod_{i=1}^{z}(p_i-1).$$

Proof of Theorem 1:

$$\begin{aligned}
A&=\left\{a\in\mathbb{Z} \mid 1\leq a<n \text{ and } (a,n)=1 \text{ and } a^{(n-1)/2}\equiv\left(\tfrac{a}{n}\right)(\text{mod } n)\right\}\\
&\subseteq\left\{a\in\mathbb{Z} \mid 0\leq a<n \text{ and } (a,n)=1 \text{ and } a^{(n-1)/2}\equiv\pm 1(\text{mod } n)\right\}\\
&\subseteq\left\{a\in\mathbb{Z} \mid 0\leq a<n \text{ and } (a,n)=1 \text{ and } a^{n-1}\equiv 1(\text{mod } n)\right\}\\
&\subseteq\left\{a\in\mathbb{Z} \mid 0\leq a<n \text{ and } a^{n-1}\equiv 1(\text{mod } n)\right\}.
\end{aligned}$$

If we let $f(h)=h^{n-1}-1$ and $B=\left\{a\in\mathbb{Z} \mid 0\leq a<n \text{ and } f(a)\equiv 0(\text{mod } n)\right\}$, then we have that

$$A \subseteq B$$

and thus

$$|A| \leq |B|. \tag{1.0}$$

Now let $B_i=\left\{a\in\mathbb{Z} \mid 0\leq a<p_i^{e_i} \text{ and } f(a)\equiv 0(\text{mod } p_i^{e_i})\right\}$.

Since $f(h)$ is an integral polynomial (i.e. $f(h)$ has only integer coefficients), the cardinality of B is simply the number of incongruent roots of $f(h)\equiv 0 \pmod{n}$, and the cardinality of B_i is simply the number of incongruent roots of $f(h)\equiv 0 \pmod{p_i^{e_i}}$, we have the relation

(1.1) $\qquad |B| = \Pi_{i=1}^{z}|B_i|$ (Theorem 122 in [3]).

We must now to derive an upper bound on $|B_i|$. We first present the following lemma and then show how it can be used to obtain the bound $|B_i|\le p_i-1$.

Lemma 1:

If $x,y \in B_i$ and $x\equiv y \pmod{p_i}$ then $x=y$.

Proof of Lemma 1:

(Lemma 1 follows from Theorem 5.30, case (a) in [1]. We present here, however, a slightly more direct proof.)

Case ($e_i=1$):

$x,y \in B_i \Rightarrow 0\le x<p_i$ and $0\le y<p_i$

$\Rightarrow x \pmod{p_i}=x$ and $y \pmod{p_i}=y$.

Thus, $x\equiv y \pmod{p_i} \Rightarrow x=y$.

Case ($e_i\ge 2$):

Assume (wlog) that $x\ge y$.

Since $x,y \in B_i$, we have that

$$(1.2)\qquad \begin{cases} f(x)\equiv 0 \pmod{p_i^{e_i}} & 0\le x<p_i^{e_i} \\ f(y)\equiv 0 \pmod{p_i^{e_i}} & 0\le y<p_i^{e_i}. \end{cases}$$

Further,

$x\equiv y \pmod{p_i}$

(1.3) $\Rightarrow x=k_1p_i+y$ [for some integer $0\le k_1<p_i^{e_i-1}$].

Substituting for x in (1.2),

$$\begin{cases} f(k_1p_i+y)\equiv 0 \pmod{p_i^{e_i}} \\ f(y)\equiv 0 \pmod{p_i^{e_i}} \end{cases}$$

and more explicitly

$$(1.4)\qquad \begin{cases} (k_1p_i+y)^{n-1}\equiv 1 \pmod{p_i^{e_i}} \\ y^{n-1}\equiv 1 \pmod{p_i^{e_i}}. \end{cases}$$

From (1.4), however, $(k_1p_i+y)^{n-1}\equiv y^{n-1} \pmod{p_i^{e_i}}$

$$\Rightarrow (k_1p_i+y)^{n-1}-y^{n-1}\equiv 0 \pmod{p_i^{e_i}}$$

$$\Rightarrow [\textstyle\sum_{j=0}^{n-1}\binom{n-1}{j}y^{n-1-j}(k_1p_i)^j]-y^{n-1}\equiv 0 \pmod{p_i^{e_i}}$$

$$(1.5)\qquad \Rightarrow [\textstyle\sum_{j=1}^{n-1}\binom{n-1}{j}y^{n-1-j}(k_1p_i)^j]\equiv 0 \pmod{p_i^{e_i}}.$$

Defining S_1 and S_2 as

$$S_1=[\textstyle\sum_{j=1}^{n-1}\binom{n-1}{j}y^{n-1-j}(k_1p_i)^j]$$

$$S_2=[\textstyle\sum_{j=2}^{n-1}\binom{n-1}{j}y^{n-1-j}(k_1p_i)^j],$$

we have that

$$S_1=S_2+[\binom{n-1}{1}y^{n-1-1}(k_1p_i)^1]$$

$$\Rightarrow S_1=S_2+(n-1)y^{n-2}(k_1p_i).$$

Further, from (1.5), the definition of S_1, and the fact that p_i^2 will divide every term in S_2, we can show that

$$S_1\equiv 0 \pmod{p_i^{e_i}} \Rightarrow p_i^{e_i}|S_1 \Rightarrow p_i^2|S_1$$

$$\Rightarrow p_i^2|S_2+(n-1)y^{n-2}(k_1p_i)$$

$$\Rightarrow p_i^2|(n-1)y^{n-2}(k_1p_i).$$

Notice, however, that

$$p_i|n \Rightarrow p_i\nmid n-1$$

and

$$p_i \nmid y^{n-1} \Rightarrow p_i \nmid y^{n-2}.$$

Thus,

(1.6) $\quad p_i^2 | k_1 p_i \Rightarrow p_i | k_1.$

Further, if $e_i \geq 3$ then we can apply (1.6) to show that p_i^3 will divide every term in S_2 and thus

$$p_i^{e_i} | S_1 \Rightarrow p_i^3 | S_1$$

$$\Rightarrow p_i^3 | S_2 + (n-1) y^{n-2} (k_1 p_i)$$

$$\Rightarrow p_i^3 | (n-1) y^{n-2} (k_1 p_i)$$

$$\Rightarrow p_i^3 | k_1 p_i \Rightarrow p_i^2 | k_1.$$

We can continue this argument, however, until we have shown that

(1.7) $\quad p_i^{e_i} | S_1 \Rightarrow p_i^{e_i - 1} | k_1.$

Therefore, from (1.3) and (1.7), we have that

$$0 \leq k_1 < p_i^{e_i - 1} \Rightarrow k_1 = 0$$

and thus

$$x = y.$$

This concludes the proof of Lemma 1.

Using Lemma 1, we derive the upper bound on $|B_i|$ as follows:

If $x \in B_i \Rightarrow f(x) \equiv 0 \pmod{p_i^{e_i}}$ and $0 \leq x < p_i^{e_i}$

$$\Rightarrow f(x) \equiv 0 \pmod{p_i} \text{ and } 0 \leq x < p_i^{e_i}$$

(1.8) $\quad \Rightarrow x^{n-1} \equiv 1 \pmod{p_i}$ and $0 \leq x < p_i^{e_i}.$

Letting $x \pmod{p_i} \equiv x'$

$$\Rightarrow x = k_2 p_i + x',\ 0 \leq x' < p_i, \text{ and } x' \in \mathbb{Z} \text{ [for some integer } k_2 \geq 0].$$

Substituting now for x in (1.8) yields $(k_2 p_i + x')^{n-1} \equiv 1 \pmod{p_i}$

$$\Rightarrow [k_2 p_i \pmod{p_i} + x' \pmod{p_i}]^{n-1} \equiv 1 \pmod{p_i}$$

$\Rightarrow [x'(\text{mod } p_i)]^{n-1} \equiv 1 (\text{mod } p_i)$

$\Rightarrow (x')^{n-1} \equiv 1 (\text{mod } p_i)$

$\Rightarrow f(x') \equiv 0 (\text{mod } p_i)$ and $0 \le x' < p_i$ and $x' \in \mathbb{Z}$.

If we define $D_i = \{a \in \mathbb{Z} \mid 0 \le a < p_i \text{ and } f(a) \equiv 0 (\text{mod } p_i)\}$, then we have shown that

$$x \in B_i \Rightarrow x' \in D_i.$$

Therefore, for any $x \in B_i$ we can show that $x' \in D_i$ where $x' \equiv x (\text{mod } p_i)$ as defined above. Further, by Lemma 1, for each distinct $x \in B_i$, there will be a distinct $x' \in D_i$ [i.e. If $x \in B_i$ and $y \in B_i$ and $x \equiv y (\text{mod } p_i)$, then $x = y$].

Thus,

$$(1.9) \qquad |B_i| \le |D_i|.$$

Notice, however, that $|D_i| \le p_i - 1$ since $f(0) \not\equiv 0 (\text{mod } p_i)$ and there are only $p_i - 1$ other possible values of a in the range $0 \le a < p_i$. Combining this fact with (1.9), we have

$$|B_i| \le p_i - 1$$

and thus from (1.0) and (1.1)

$$|A| \le |B| = \prod_{i=1}^{z} |B_i| \le \prod_{i=1}^{z} (p_i - 1).$$

□

Corollary 1:

Let $n = p_1^{e_1} \cdot p_2^{e_2} \cdot \ldots \cdot p_z^{e_z}$; $z \ge 1$; $e_i \ge 1$ $[1 \le i \le z]$; $\max(e_i) \ge 2$; all p_i are distinct odd primes. The cardinality of the set $\overline{W}_n$ satisfies the following relation:

$$|\overline{W}_n| \le \tfrac{1}{4}(n-1).$$

Proof of Corollary 1:

Since n satisfies the conditions of Theorem 1 and the set $\overline{W}_n$ is exactly the same as the set A defined in Theorem 1:

$$|\bar{W}_n| \le \prod_{i=1}^{z}(p_i-1).$$

Therefore,

$$\begin{aligned} |\bar{W}_n|/(n-1) &= |\bar{W}_n|/\{[\prod_{i=1}^{z}(p_i^{e_i})]-1\} \\ &\le \{\prod_{i=1}^{z}(p_i-1)\}/\{[\prod_{i=1}^{z}(p_i^{e_i})]-1\} \\ &\le \{\prod_{i=1}^{z}(p_i-1)\}/\{\prod_{i=1}^{z}(p_i^{e_i}-1)\} \\ &= \prod_{i=1}^{z}[(p_i-1)/(p_i^{e_i}-1)] \\ &\le (p_j-1)/(p_j^2-1) \text{ [for some } j \text{ such that } e_j \ge 2] \\ &\le 1/4. \end{aligned}$$

Thus,

$$\begin{aligned} |\bar{W}_n|/(n-1) &\le 1/4 \\ &\Rightarrow |\bar{W}_n| \le \tfrac{1}{4}(n-1). \end{aligned}$$

□

Theorem 2:

Let $n=p_1^{e_1}\cdot p_2^{e_2}\cdot\ldots\cdot p_z^{e_z}$ where z is any positive integer such that $z\ge 2$, the e_i are all positive integers $(1\le i\le z)$ such that at least one e_j $(1\le j\le z)$ is odd, and the p_i are all distinct odd primes $(p_i>2)$. If

$$A=\{a\in\mathbb{Z} \mid 1\le a<n \text{ and } (a,n)=1 \text{ and } a^{(n-1)/2}\equiv\left(\frac{a}{n}\right)(\text{mod } n)\}$$

and

$$B=\{a\in\mathbb{Z} \mid 1\le a<n \text{ and } (a,n)=1 \text{ and } a^{n-1}\equiv 1(\text{mod } n)\}$$

then $A \subsetneq B$.

Proof of Theorem 2:

It is clear that any element of A is an element of B and thus $A\subseteq B$.

It therefore only remains to be shown that there exists some element of B which is not an element of A. The proof of this fact will be broken into two parts:

1) There exists some p_j $(1 \le j \le z)$ such that e_j is odd and the highest power of 2 dividing $(p_j-1)/2$ is strictly less than the highest power of 2 dividing $n-1$.

2) There exists some p_j $(1 \le j \le z)$ such that e_j is odd and the highest power of 2 dividing $(p_j-1)/2$ is greater than or equal to the highest power of 2 dividing $n-1$.

Case (1):

We first prove the existence of a $c \in B$ such that $\left(\frac{c}{n}\right)=-1$.

Let t be the highest power of 2 dividing $(p_j-1)/2$. $[t \in \{2^0, 2^1, \ldots\}]$

We then have that

(2.0) $t \mid (p_j-1)/2$ and $2t \nmid (p_j-1)/2$

(2.1) $\Rightarrow t \mid n-1$ and $2t \mid n-1$.

Now let b be such that $b^t \equiv -1 \pmod{p_j^{e_j}}$.

We prove the existence of such a b by induction on t as follows:

For $t=2^0$:

If we let $b=-1$, then $b^t \equiv (-1)^t \equiv -1 \pmod{p_j^{e_j}}$.

For $t=2^s$ $(s>0)$:

Assume there exists a b' such that $(b')^{t/2} \equiv -1 \pmod{p_j^{e_j}}$ and we will show that there exists a b such that $b^t \equiv -1 \pmod{p_j^{e_j}}$ [Note - $t/2$ will be a positive integer since $t=2^s$ $(s>0)$].

If we let b be such that $b^2 \equiv b' \pmod{p_j^{e_j}}$, then from the definition of b',

$$b^t \equiv b^{2(t/2)} \equiv (b^2)^{t/2} \equiv (b')^{t/2} \equiv -1 \pmod{p_j^{e_j}}.$$

Thus we must simply show that b' is a quadratic residue modulo $p_j^{e_j}$. But, b' is a quadratic residue modulo $p_j^{e_j}$ if and only if b' is a quadratic residue modulo p_j. Further, b' is a quadratic residue modulo p_j if and only if:

$$\left(\frac{b'}{p_j}\right) \equiv (b')^{(p_j-1)/2} \equiv 1 \pmod{p_j}.$$

From (2.0) and the definition of b', however,

$$(b')^{(p_j-1)/2} \equiv (b')^{t(k_3)} \equiv (b')^{2(t/2)(k_3)}$$

$$\equiv ((b')^{t/2})^{2(k_3)} \equiv (-1)^{2(k_3)} \equiv 1^{k_3} \equiv 1 \pmod{p_j}.$$

[for some positive integer k_3]

Thus we conclude that such a b does in fact exist.

Now let c be such that:

$$(2.2) \quad \begin{cases} c \equiv b \pmod{p_j^{e_j}} \\ c \equiv 1 \pmod{p_i^{e_i}} \quad [\text{for } 1 \le i \le z \text{ and } i \ne j]. \end{cases}$$

Since the moduli of the congruences (2.2) are all relatively prime in pairs, we can apply the Chinese Remainder Theorem to compute such a

$$c \le \prod_{i=1}^{z} p_i^{e_i}.$$

Further, it can easily be shown that

$$p_j \nmid c \text{ and}$$

$$p_i \nmid c \text{ [for } 1 \le i \le z \text{ and } i \ne j].$$

Thus none of the factors of n (other than 1) will divide c and therefore we have

(2.3) $$(c,n)=1 \text{ and } 1\le c<n.$$

From (2.2), however,

$$c^{n-1}\equiv 1 \pmod{p_i^{e_i}} \quad [\text{for } 1\le i\le z \text{ and } i\ne j]$$

and from (2.1) and the definition of b,

$$c^{n-1}\equiv b^{n-1}\equiv b^{2(t)(k_4)}\equiv (b^t)^{2(k_4)}\equiv(-1)^{2(k_4)}\equiv 1^{k_4}\equiv 1 \pmod{p_j^{e_j}}.$$

$$[\text{for some positive integer } k_4]$$

Therefore,

(2.4) $$\begin{cases} c^{n-1}\equiv 1 \pmod{p_j^{e_j}} \\ c^{n-1}\equiv 1 \pmod{p_i^{e_i}} \quad [\text{for } 1\le i\le z \text{ and } i\ne j]. \end{cases}$$

Since the moduli of the congruences (2.4) are all relatively prime in pairs, however, we have

(2.5) $$c^{n-1}\equiv 1 \pmod{\textstyle\prod_{i=1}^{z} p_i^{e_i}}.$$

Thus, combining (2.5) and (2.3),

$$1\le c<n \text{ and } (c,n)=1 \text{ and } c^{n-1}\equiv 1 \pmod n$$

$$\Rightarrow c\in B.$$

We must now show that $\left(\frac{c}{n}\right)=-1$. From (2.2) and the definition of $\left(\frac{c}{p}\right)$ (for any positive odd prime p), however,

$$\left(\frac{c}{p_i}\right)\equiv c^{(p_i-1)/2}\equiv 1^{(p_i-1)/2}\equiv 1 \pmod{p_i} \quad [\text{for } 1\le i\le z \text{ and } i\ne j].$$

Further, from (2.0), (2.2), and the definition of b,

$$\left(\frac{c}{p_j}\right)\equiv c^{(p_j-1)/2}\equiv b^{(p_j-1)/2}\equiv b^{t(k_5)}\equiv (b^t)^{k_5}\equiv (-1)^{k_5}\equiv -1 \pmod{p_j}.$$

[for some positive odd integer k_5]

Therefore,

$$\begin{cases} \left(\frac{c}{p_i}\right)=1 & \text{[for } 1\le i\le z \text{ and } i\ne j\text{]} \\ \left(\frac{c}{p_j}\right)=-1 & \end{cases}$$

and so we have

$$\left(\frac{c}{n}\right)=\left(\frac{c}{p_1}\right)^{e_1}\cdot\left(\frac{c}{p_2}\right)^{e_2}\cdot\ldots\cdot\left(\frac{c}{p_z}\right)^{e_z}=1\cdot\left(\frac{c}{p_j}\right)^{e_j}=-1.$$

Thus we have proven the existence of a $c\in B$ such that $\left(\frac{c}{n}\right)=-1$. It now remains to demonstrate an element of B which is not an element of A. Notice, however, that if $c^{(n-1)/2}\not\equiv -1 \pmod{n}$, then $c\notin A$ and thus $c\in B$ while $c\notin A$. Otherwise, if $c^{(n-1)/2}\equiv -1 \pmod{n}$, then we can apply Lemma 2 to obtain the desired $c'\in B$, $c'\notin A$.

<u>Lemma 2</u>:

Given a $c\in B$ such that $c^{(n-1)/2}\equiv -1 \pmod{n}$, a c' can be constructed such that $c'\in B$ and $c'\notin A$.

<u>Proof of Lemma 2</u>:

Let c' be such that:

$$\text{(2.6)} \qquad \begin{cases} c'\equiv c \pmod{p_j^{e_j}} & \\ c'\equiv 1 \pmod{p_i^{e_i}} & \text{[for } 1\le i\le z \text{ and } i\ne j\text{]}. \end{cases}$$

Since the moduli of the congruences (2.6) are all relatively prime in pairs, we can apply the Chinese Remainder Theorem to compute such a

$$c' \le \prod_{i=1}^{z} p_i^{e_i}.$$

Further, it can easily be shown that

$$p_j \nmid c' \text{ and}$$

$$p_i \nmid c' \text{ [for } 1\le i\le z \text{ and } i\ne j].$$

Thus, none of the factors of n (other than 1) will divide c′ and therefore we have:

$$(2.7) \qquad (c',n)=1 \text{ and } 1\le c'<n.$$

From (2.6) and the definition of c, however, we have that

$$\begin{cases} (c')^{n-1}\equiv 1^{n-1}\equiv 1 \pmod{p_i^{e_i}} & \text{[for } 1\le i\le z \text{ and } i\ne j] \\ (c')^{n-1}\equiv c^{n-1}\equiv (c^{(n-1)/2})^2\equiv(-1)^2\equiv 1 \pmod{p_j^{e_j}}. & \end{cases}$$

Therefore,

$$(2.8) \qquad \begin{cases} (c')^{n-1}\equiv 1 \pmod{p_i^{e_i}} & \text{[for } 1\le i\le z \text{ and } i\ne j] \\ (c')^{n-1}\equiv 1 \pmod{p_j^{e_j}}. & \end{cases}$$

Since the moduli of the congruences (2.8) are all relatively prime in pairs, however, we have

$$(2.9) \qquad (c')^{n-1}\equiv 1 \left(\bmod \prod_{i=1}^{z} p_i^{e_i}\right).$$

Thus, combining (2.7) and (2.9), we have that

$$1\le c'<n \text{ and } (c',n)=1 \text{ and } (c')^{n-1}\equiv 1 \pmod n$$

$$\Rightarrow c'\in B.$$

Once again applying (2.6) and the definition of c, however, we obtain

$$\begin{cases} (c')^{(n-1)/2} \equiv 1^{(n-1)/2} \equiv 1 \pmod{p_i^{e_i}} & [\text{for } 1 \le i \le z \text{ and } i \ne j] \\ (c')^{(n-1)/2} \equiv c^{(n-1)/2} \equiv -1 \pmod{p_j^{e_j}}. \end{cases}$$

Therefore,

$$\begin{cases} (c')^{(n-1)/2} \equiv 1 \pmod{p_i^{e_i}} & [\text{for } 1 \le i \le z \text{ and } i \ne j] \\ (c')^{(n-1)/2} \equiv -1 \pmod{p_j^{e_j}}. \end{cases}$$

But, for any positive integer a,

$$a^{(n-1)/2} \equiv 1 \pmod{n} \Rightarrow a^{(n-1)/2} \equiv 1 \pmod{p_i^{e_i}} \quad [\text{for } \underline{\text{all}}\ i]$$

$$\therefore\ (c')^{(n-1)/2} \not\equiv 1 \pmod{n}.$$

Further, for any positive integer a,

$$a^{(n-1)/2} \equiv -1 \pmod{n} \Rightarrow a^{(n-1)/2} \equiv -1 \pmod{p_i^{e_i}} \quad [\text{for } \underline{\text{all}}\ i]$$

$$\therefore\ (c')^{(n-1)/2} \not\equiv -1 \pmod{n}.$$

Thus,

$$(c')^{(n-1)/2} \not\equiv \pm 1 \pmod{n} \Rightarrow (c')^{(n-1)/2} \not\equiv \left(\frac{c'}{n}\right) \pmod{n}$$

$$\Rightarrow c' \notin A.$$

This concludes the proof of Lemma 2 and Case (1).

Case (2):

In this case, we can prove directly the existence of an element of B which is not an element of A.

Let v be the highest power of 2 dividing (n-1)/2. $[v \in \{2^0, 2^1, \ldots\}]$

We then have that

(2.10) $v|(n-1)/2$ and $2v\nmid(n-1)/2$

(2.11) $\Rightarrow 2v|n-1 \Rightarrow 2v|(p_j-1)/2 \Rightarrow v|(p_j-1)/2.$

Let d be such that $d^v\equiv-1(\text{mod } p_j^{e_j})$.

We prove the existence of such a d by induction on v as follows:

For $v=2^0$:

$$\text{If we let } d=-1, \text{ then } d^v\equiv(-1)^v\equiv-1(\text{mod } p_j^{e_j}).$$

For $v=2^s$ $(s>0)$:

Assume there exists a d' such that $(d')^{v/2}\equiv-1(\text{mod } p_j^{e_j})$ and we will show that there exists a d such that $d^v\equiv-1(\text{mod } p_j^{e_j})$ [Note - $v/2$ will be a positive integer since $v=2^s$ $(s>0)$].

If we let d be such that $d^2\equiv d'(\text{mod } p_j^{e_j})$, then from the definition of d',

$$d^v\equiv d^{2(v/2)}\equiv(d^2)^{v/2}\equiv(d')^{v/2}\equiv-1(\text{mod } p_j^{e_j}).$$

Thus we must simply show that d' is a quadratic residue modulo $p_j^{e_j}$. But, d' is a quadratic residue modulo $p_j^{e_j}$ if and only if d' is a quadratic residue modulo p_j. Further, d' is a quadratic residue modulo p_j if and only if:

$$\left(\frac{d'}{p_j}\right)\equiv(d')^{(p_j-1)/2}\equiv1(\text{mod } p_j).$$

From (2.11) and the definition of d', however,

$$(d')^{(p_j-1)/2}\equiv(d')^{v(k_6)}\equiv(d')^{2(v/2)(k_6)}$$
$$\equiv((d')^{v/2})^{2(k_6)}\equiv(-1)^{2(k_6)}\equiv1^{k_6}\equiv1(\text{mod } p_j).$$

[for some positive integer k_6]

Thus we conclude that such a d does in fact exist.

Now let e be such that:

$$(2.12)\qquad \begin{cases} e \equiv d \pmod{p_j^{e_j}} \\ e \equiv 1 \pmod{p_i^{e_i}} \quad [\text{for } 1 \le i \le z \text{ and } i \ne j]. \end{cases}$$

Since the moduli of the congruences (2.12) are all relatively prime in pairs, we can apply the Chinese Remainder Theorem to compute such an

$$e \le \prod_{i=1}^{z} p_i^{e_i}.$$

Further, it can easily be shown that

$$p_j \nmid e \text{ and}$$

$$p_i \nmid e \quad [\text{for } 1 \le i \le z \text{ and } i \ne j].$$

Thus none of the factors of n (other than 1) will divide c and therefore we have

$$(2.13)\qquad (e,n)=1 \text{ and } 1 \le e < n.$$

From (2.12), however,

$$e^{n-1} \equiv 1 \pmod{p_i^{e_i}} \quad [\text{for } 1 \le i \le z \text{ and } i \ne j]$$

and from (2.10) and the definition of d,

$$e^{n-1} \equiv d^{n-1} \equiv d^{2(v)(k_7)} \equiv (d^v)^{2(k_7)} \equiv (-1)^{2(k_7)} \equiv 1^{k_7} \equiv 1 \pmod{p_j^{e_j}}.$$

$$[\text{for some positive integer } k_7]$$

Therefore,

$$(2.14)\qquad \begin{cases} e^{n-1} \equiv 1 \pmod{p_j^{e_j}} \\ e^{n-1} \equiv 1 \pmod{p_i^{e_i}} \quad [\text{for } 1 \le i \le z \text{ and } i \ne j]. \end{cases}$$

Since the moduli of the congruences (2.14) are all relatively prime in pairs, however, we have

(2.15) $$e^{n-1} \equiv 1 \pmod{\prod_{i=1}^{z} p_i^{e_i}}$$

Thus, combining (2.13) and (2.15), we have that

$$1 \le e < n \text{ and } (e,n)=1 \text{ and } e^{n-1} \equiv 1 \pmod n$$
$$\Rightarrow e \in B.$$

Once again applying (2.12), however, we obtain

$$e^{(n-1)/2} \equiv 1^{(n-1)/2} \equiv 1 \pmod{p_i^{e_i}} \quad [\text{for } 1 \le i \le z \text{ and } i \ne j]$$

and from (2.10) and the definition of d,

$$e^{(n-1)/2} \equiv b^{(n-1)/2} \equiv b^{v(k_8)} \equiv (b^v)^{k_8} \equiv (-1)^{k_8} \equiv -1 \pmod{p_j^{e_j}}.$$
$$[\text{for some positive odd integer } k_8]$$

Therefore,

$$\begin{cases} e^{(n-1)/2} \equiv 1 \pmod{p_i^{e_i}} & [\text{for } 1 \le i \le z \text{ and } i \ne j] \\ e^{(n-1)/2} \equiv -1 \pmod{p_j^{e_j}}. \end{cases}$$

But, for any positive integer a,

$$a^{(n-1)/2} \equiv 1 \pmod n \Rightarrow a^{(n-1)/2} \equiv 1 \pmod{p_i^{e_i}} \quad [\text{for } \underline{\text{all}}\ i]$$
$$\therefore e^{(n-1)/2} \not\equiv 1 \pmod n.$$

Further, for any positive integer a,

$$a^{(n-1)/2} \equiv -1 \pmod n \Rightarrow a^{(n-1)/2} \equiv -1 \pmod{p_i^{e_i}} \quad [\text{for } \underline{\text{all}}\ i]$$
$$\therefore e^{(n-1)/2} \not\equiv -1 \pmod n.$$

Thus,

$$e^{(n-1)/2} \not\equiv \pm 1 \pmod{n} \Rightarrow e^{(n-1)/2} \not\equiv \left(\frac{e}{n}\right) \pmod{n}$$

$$\Rightarrow e \notin A.$$

Therefore we have proven the existence of an $e \in B$ such that $e \notin A$.

$\square$

<u>Corollary 2</u>:

Let $n = p_1^{e_1} \cdot p_2^{e_2} \cdot \ldots \cdot p_z^{e_z}$; $z \geq 2$; $e_i = 1$ $[1 \leq i \leq z]$; all p_i are distinct odd primes. The cardinality of the set $\bar{W}_n$ satisfies the following relation:

$$|\bar{W}_n| \leq \tfrac{1}{4}(n-1) \quad \text{if } n \text{ is } \underline{\text{non-Carmichael}}$$

$$|\bar{W}_n| \leq \tfrac{1}{2}(n-1) \quad \text{if } n \text{ is } \underline{\text{Carmichael}}.$$

<u>Proof of Corollary 2</u>:

Let A and B be the sets as defined in Theorem 2. Since n satisfies the conditions of Theorem 2 and the set $\bar{W}_n$ is exactly the same as the set A:

$$\bar{W}_n \subsetneq B.$$

We notice, however, that $\bar{W}_n$ and B are both groups under multiplication (mod n) and thus

$$(2.16) \qquad |\bar{W}_n| \leq \tfrac{1}{2}|B|.$$

Further, it is clear that $|B| \leq n-1$ since there are only n-1 possible values of a in the range $1 \leq a < n$.

Therefore,

$$|\overline{W}_n| \le \tfrac{1}{2}(n-1).$$

Now, let $C=\{a\in\mathbb{Z} \mid 1\le a<n \text{ and } (a,n)=1\}$.

It is clear that any element of B is an element of C. Further, if n is a non-Carmichael number, then by definition there exists some w such that:

$$0<w<n \text{ and } (w,n)=1 \text{ and } w^{n-1}\not\equiv 1 \pmod n.$$

Thus,

$$w\in C \text{ and } w\notin B.$$

Therefore, if n is non-Carmichael,

$$B \subsetneq C.$$

We notice, however, that C is also a group under multiplication (mod n) and thus if n is non-Carmichael,

$$|B| \le \tfrac{1}{2}|C|.$$

Further, it is clear that $|C|\le n-1$ since there are only n-1 possible values of a in the range $1\le a<n$.

Therefore, if n is non-Carmichael,

$$|B| \le \tfrac{1}{2}(n-1). \tag{2.17}$$

Thus from (2.16) and (2.17), if n is non-Carmichael,

$$|\bar{W}_n| \le \tfrac{1}{2}|B| \le \tfrac{1}{2}(\tfrac{1}{2}(n-1)) = \tfrac{1}{4}(n-1).$$

We therefore have,

$$|\bar{W}_n| \le \tfrac{1}{4}(n-1) \text{ if } n \text{ is } \underline{\text{non-Carmichael}}$$

$$|\bar{W}_n| \le \tfrac{1}{2}(n-1) \text{ if } n \text{ is } \underline{\text{Carmichael}}.$$

□

<u>Conclusions</u>

From Corollaries 1 and 2, we have the result that if n is positive, odd, composite and <u>non-Carmichael</u>,

$$|\bar{W}_n| \le \tfrac{1}{4}(n-1)$$

and if n is positive, odd, composite and <u>Carmichael</u>,

$$|\bar{W}_n| \le \tfrac{1}{2}(n-1).$$

Therefore, for all such non-Carmichael n, the probability of Solovay and Strassen's algorithm giving an incorrect answer after a single iteration is at most 1/4. Further, for all such Carmichael n, the probability of Solovay and Strassen's algorithm giving an incorrect answer after a single iteration is at most 1/2 (as was also shown in [5]). Thus, iterating Solovay and Strassen's algorithm r times, using independent random numbers at each iteration, actually results in a test for the primality of any positive odd integer, n>2, with error probability 0 (if n is prime), error probability at most 4^{-r} (if n is composite and <u>non-Carmichael</u>), and error probability at most 2^{-r} (if n is composite and <u>Carmichael</u>).

Finally, we would like to point out that Theorems 1 and 2 can in fact be used to prove much better bounds on $|\bar{W}_n|$ for many different classes of integers. (eg. $|\bar{W}_n| \leq (n-1)/13$ if n is positive, odd and contains as a factor a prime to a power 3 or greater, $|\bar{W}_n| \leq (n-1)/26$ if n is positive, odd, not a prime power and contains as a factor a prime to an odd power 3 or greater)

Acknowledgments

I would like to thank Prof. Ron Rivest for introducing me to this problem and for his continued support and guidance. I am especially grateful for his suggestions concerning early versions of the proof of Theorem 2. I am also grateful to Jeff Jaffe for his many constructive criticisms and especially for his suggestions concerning the proof of Theorem 1. I would finally like to thank Prof. Len Adleman and Mike Loui for several enlightening discussions.

References

[1] Apostol, T.M., "Introduction to Analytic Number Theory," Springer-Verlag New York, Inc., 1976.

[2] Griffin, H., "Elementary Theory of Numbers," McGraw-Hill Book Company, Inc., 1954.

[3] Hardy, G.H., and E.M. Wright, "The Theory of Numbers," Oxford University Press, 1975.

[4] Niven, I., and H. Zuckerman, "An Introduction to the Theory of Numbers," John Wiley and Sons, Inc., 1972.

[5] Solovay, R., and V. Strassen, "A Fast Monte-Carlo Test for Primality," SIAM Journal of Computing, Vol. 6, No. 1, March 1977.

[6] Vuillemin, J., Communication with R. Rivest, May 1978.