Some remarks on primality tests

Koichiro OHTAKE
Department of Mathematics, Faculty of Education, Gunma University

(Accepted on September 17th, 2014)

Abstract

Let n be an odd composite integer. In Solovay-Strassen primality test there are at most $\varphi(n)/2$ integers which say that n may be prime, where φ is Euler's function. On the other hand, there are at most $\varphi(n)/4$ such integers in Miller-Rabin test. In this paper we show examples of n such that there are just $\varphi(n)/2$ such integers in Solovay-Strassen test and just $\varphi(n)/4$ such integers in Miller-Rabin test. Since the author is not an expert of this area, we try to give a proof that Miller-Rabin test is better than Solovay-Strassen test even if it is well known. Moreover we will try to prove Rabin's theorem.

1 Preface

Let $n > 1$ be an odd integer. Let $E_n = \{1, 2, \ldots, n-1\}$ and $G_n = \{a \in E_n \,|\, (a, n) = 1\}$, where (a, n) denotes the greatest common divisor of a and n. Then G_n is a multiplicative group of order $\varphi(n)$, where φ is Euler's function. Let $\left(\frac{m}{p}\right)$ be Legendre's symbol, where p is an odd prime number and $m \in \boldsymbol{Z}$ with $(p, m) = 1$. Suppose $n = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$ is a prime factor decomposition of n, and put $\left(\frac{m}{n}\right) = \left(\frac{m}{p_1}\right)^{e_1}\left(\frac{m}{p_2}\right)^{e_2} \cdots \left(\frac{m}{p_r}\right)^{e_r}$ if $(m, n) = 1$ and $\left(\frac{m}{n}\right) = 0$ if $(m, n) \neq 1$ ($\left(\frac{m}{n}\right)$ is known as Jacobi's symbol). Now put $H_n = \{a \in G_n \,|\, a^{\frac{n-1}{2}} \equiv \left(\frac{a}{n}\right) \pmod{n}\}$. Then H_n is a subgroup of G_n. Solovay-Strassen's theorem states that if n is a composite number then $|H_n| \leqslant \varphi(n)/2$ (see [1] or [4] for the proof of this and see [1] or any textbook of an introduction to the theory of integers for properties of Legendre's and Jacobi's symbols). In particular $|H_n| < (n-1)/2$. If we take $a \in E_n$ arbitrarily the possibility that a is in H_n is at most $\frac{|H_n|}{n-1} < \frac{1}{2}$. This is so-called Solovay-Strassen primality test. It should be noted that if n is prime then $E_n = G_n = H_n$ holds. In the case of n being composite if we take a_1, a_2 in E_n arbitrarily then the probability that both a_1, a_2 are in H_n is less than $\frac{|H_n|}{n-1}\frac{|H_n|-1}{n-2} < \frac{1}{2}\frac{\frac{n-3}{2}}{n-2} < \frac{1}{2^2}$. Like this if we take k elements of E_n arbitrarily then the probability (say P) that all of them are in H_n is less than $\frac{1}{2^k}$. It should be noted that $1-P$ is the probability that there appears an witness that n is a composite integer. If $n > 1$ is an odd composite integer, the author expects that there does not occur as a real case that $P < \frac{1}{2^k} \leqslant \frac{1}{10^{30}}$ because $1 - P > 0.999999999999999999999999999999$. Then we can say that n is a prime number. In this case how is k? Since $2^k \geqslant 10^{30}$, $k \geqslant 30/\log_{10} 2 > 99$. Therefore if we take $a_i \in E_n$ $(i = 1, 2, \ldots, 100)$ arbitrarily and assume $a_i \in H_n$ for all i then we can say that n is a prime number. One sometimes says that P is the probability of n being a composite number. Thus one also says that $1 - P$ is the probability of n being a prime number. These are not correct usage.

Now suppose $n-1=2^e m$, where m is odd. Let $S_n=\{a\in E_n \mid a^m\equiv 1 \pmod n$ or $\exists i\,(0\leqslant i<e)$ such that $a^{2^i m}\equiv -1 \pmod n\}$ and $T_n=\{a\in E_n \mid a^{n-1}\not\equiv 1 \pmod n$ or $\exists i\,(1\leqslant i<e)$ such that $1<(a^{2^{i-1}m}-1,\,n)<n\}$. Then Rabin [3] proved that $|T_n|\leqslant 3(n-1)/4$ if n is composite. This means $|S_n|\leqslant (n-1)/4$, too. It is known that $S_n\subset H_n$. This fact implies that Miller-Rabin primality test is better than Solovay-Strassn's test.

In this paper we give a proof of Rabin's theorem and a proof of the fact that S_n is a subset of H_n. Moreover we give examples of n such that $|H_n|=\varphi(n)/2$ and $|S_n|=\varphi(n)/4$ hold.

2 Rabin's theorem

Let $n>1$ be an odd integer, $E_n=\{1,2,\ldots,n-1\}$ and $n-1=2^e m$, where $(2,m)=1$. Put

$S_n=\{a\in E_n \mid a^m\equiv 1 \pmod n$ or $\exists i\ (0\leqslant i<e)$ such that $a^{2^i m}\equiv -1 \pmod n\}$ and

$T_n=\{a\in E_n \mid a^{n-1}\not\equiv 1 \pmod n$ or $\exists i\ (1\leqslant i<e)$ such that $1<(a^{2^{i-1}m}-1,\,n)<n\}$.

Lemma 2.1 *The following equalities hold.*

(1) $S_n\cap T_n=\varnothing$,

(2) $E_n=S_n\cup T_n$.

Proof (1) *Suppose $S_n\cap T_n\neq\varnothing$. Then there exists $a\in S_n\cap T_n$. Since $a\in S_n$, $a^{n-1}\equiv 1 \pmod n$ holds. On the other hand $a\in T_n$ implies that $\exists i\ (1\leqslant i<e)$ such that $1<(a^{2^{i-1}m}-1,\,n)<n$. By putting $d=(a^{2^{i-1}m}-1,\,n)$, $a^{2^{i-1}m}\equiv 1 \pmod d$ holds. But $n\nmid (a^{2^{i-1}m}-1)$ implies $a^{2^{i-1}m}\not\equiv 1 \pmod n$. In particular $a^m\not\equiv 1 \pmod n$. Since $a\in S_n, \exists j\ (0\leqslant j<e)$ such that $a^{2^j m}\equiv -1 \pmod n$. If $j<i-1$ then $a^{2^{i-1}m}\equiv 1 \pmod n$ holds. This is a contradiction. If $i-1\leqslant j$ then $a^{2^j m}\equiv 1 \pmod d$ since $a^{2^{i-1}m}\equiv 1 \pmod d$. But $a^{2^j m}\equiv -1 \pmod n$ implies $a^{2^j m}\equiv -1 \pmod d$. This is impossible since $d>1$ is an odd integer. Therefore $S_n\cap T_n=\varnothing$ holds.*

(2) *Take any $a\in E_n$. If $a^{n-1}\not\equiv 1 \pmod n$ then $a\in T_n$. Hence suppose $a^{n-1}\equiv 1 \pmod n$. Let i be the smallest integer of j such that $a^{2^j m}\equiv 1 \pmod n$ with $(0\leqslant j\leqslant e)$. Such an integer j exists since $n-1=2^e m$. If $i=0$ then $a\in S_n$ since $a^m\equiv 1 \pmod n$. Suppose $i>0$. Then $a^{2^i m}-1=(a^{2^{i-1}m}-1)(a^{2^{i-1}m}+1)\equiv 0 \pmod n$ holds. Besides $a^{2^{i-1}m}-1\not\equiv 0 \pmod n$ by the property of i. Thus $(a^{2^{i-1}m}-1,\,n)<n$ holds. If $a^{2^{i-1}m}+1\equiv 0 \pmod n$ then $a\in S_n$. If $a^{2^{i-1}m}+1\not\equiv 0 \pmod n$ then $1<(a^{2^{i-1}m}-1,\,n)<n$, for if $(a^{2^{i-1}m}-1,\,n)=1$ then $n\mid a^{2^{i-1}m}+1$, which contradicts to $a^{2^{i-1}m}+1\not\equiv 0 \pmod n$. Therefore $1<(a^{2^{i-1}m}-1,\,n)<n$ holds. Hence $a\in T_n$. Thus in any case $a\in S_n$ or $a\in T_n$ holds. This completes the proof.*

Let $G_m=\{a\in E_m \mid (a,\,m)=1\}$, where m is a positive integer. When $a\in \boldsymbol{Z}$ let $\overline{a}$ denote the element of $\{0,1,\ldots,m-1\}$ such that $\overline{a}\equiv a \pmod m$. For the rest of this paper unless otherwise specified let $n>1$ be an odd composite integer.

Lemma 2.2 *Assume $m_i\mid n\ (1\leqslant i\leqslant k)$ and $(m_i,\,m_j)=1\ (1\leqslant i<j\leqslant k)$. Let*

$f: G_n\to G_{m_1}\times G_{m_2}\times\cdots\times G_{m_k}$ *be as* $f(a)=(\overline{a},\ldots,\overline{a})$.

Then f is an epimorphism.

Proof *Clearly $m_1\cdots m_k\mid n$. When we consider the prime factor decomposition of n we can find the decomposition $n=m_1'm_2'\cdots m_k'm_{k+1}'$ with $m_i\mid m_i'\ (1\leqslant i\leqslant k)$, $(m_i',\,m_j')=1\ (1\leqslant i<j\leqslant k+1)$. By Chinese Remainder Theorem the natural homomorphism $\phi: G_n\to G_{m_1'}\times\cdots\times G_{m_{k+1}'}$ is an isomorphism. Since $\pi_i: G_{m_i'}\to G_{m_i}\ (\pi_i(a)=\overline{a})\ (1\leqslant i\leqslant k)$ are epimorphisms,*

$g : G_{m'_1} \times \cdots \times G'_{m_{k+1}} \to G_{m_1} \times \cdots \times G_{m_k}$ defined by $g(a_1, \ldots, a_{k+1}) = (\overline{a_1}, \ldots, \overline{a_k})$ is an epimorphism, too. Therefore f is an epimorphism since $f = g \circ \phi$.

For a finite set S, let $|S|$ denote the cardinality of S.

Corollary 2.3 *Let f be the same as in Lemma 2.2. Then $|f^{-1}(a_1, \ldots, a_k)| = |Ker\, f|$ for any $(a_1, \ldots, a_k) \in G_{m_1} \times \cdots \times G_{m_k}$.*

Let $U_n = \{a \in E_n \mid a^{n-1} \equiv 1 \pmod n\}$. Then clearly $S_n \subset U_n \subset G_n$, $H_n \subset U_n$ and U_n is a subgroup of G_n.

Lemma 2.4 ([3, Lemma 3]) *Let p_1, p_2 be distinct odd primes and $q_i = p_i^{k_i}$ $(k_i \geqslant 1,\ i = 1, 2)$. Suppose $q_1 q_2 \mid n$. Put $t_i = (\varphi(q_i), n-1)$, $m_i = \varphi(q_i)/t_i$ $(i = 1, 2)$. Then the following inequalities hold.*

(1) $|U_n| \leqslant \dfrac{\varphi(n)}{m_1 m_2}$

(2) *If t_1 or t_2 is even then* $|S_n| \leqslant \dfrac{\varphi(n)}{2m_1 m_2}$.

Proof *The proof is the same as* [3]*. But we write it here for the sake of self-containedness. Let $f : G_n \to G_{q_1} \times G_{q_2}$ be the canonical epimorphism.*

(1) *Let a_i be a primitive root* $\bmod q_i$ $(i = 1, 2)$*. Take any $b \in U_n$ and let $b \equiv {a_i}^{r_i} \pmod{q_i}$ $(i = 1, 2)$. Since ${a_i}^{r_i(n-1)} \equiv 1 \pmod{q_i}$, $\varphi(q_i) \mid r_i(n-1)$. The facts that $t_i m_i \mid r_i(n-1)$ and $(m_i, (n-1)/t_i) = 1$ imply $m_i \mid r_i$. Thus there exist h_i $(i = 1, 2)$ such that $b \equiv {a_i}^{h_i m_i} \pmod{q_i}$ $(1 \leqslant h_i \leqslant \varphi(q_i)/m_i)$. If we fix (h_1, h_2) the number of b such that $f(b) = ({a_1}^{h_1 m_1}, {a_2}^{h_2 m_2})$ is $|Ker\, f|$ by Corollary 2.3. Since $U_n \subset f^{-1}(\{({a_1}^{h_1 m_1}, {a_2}^{h_2 m_2}) \in G_{q_1} \times G_{q_2} \mid 1 \leqslant h_i \leqslant \varphi(q_i)/m_i\ (i = 1, 2)\})$, $|U_n| \leqslant \frac{\varphi(q_1)}{m_1}\frac{\varphi(q_2)}{m_2}|Ker\, f|$ holds. On the other hand, since $G_n/Ker\, f \simeq G_{q_1} \times G_{q_2}$, $\varphi(n) = \varphi(q_1)\varphi(q_2)|Ker\, f|$ holds. Therefore $|U_n| \leqslant \varphi(n)/m_1 m_2$ holds.*

(2) *Let $t_1 = 2^{e_1} t'_1$ $(e_1 \geqslant 1)$, $t_2 = 2^{e_2} t'_2$ $(e_1 \geqslant e_2)$, where t'_1, t'_2 are odd integers. Since $n - 1 = 2^e m$, $e \geqslant e_1$ and $t'_i \mid m$ $(i = 1, 2)$ hold. Take any $b \in U_n$. Using the same symbols as in (1), let $b \equiv {a_i}^{h_i m_i} \pmod{q_i}$ $(i = 1, 2)$.*

(i) *When $e_1 = e_2$. Clearly $b^{\frac{n-1}{2^{e-e_1+1}}} \equiv {a_i}^{h_i m_i \frac{n-1}{2^{e-e_1+1}}} \pmod{q_i}$ $(i = 1, 2)$. Since $t_1 \mid \frac{n-1}{2^{e-e_1}}$ and $t_1 \nmid \frac{n-1}{2^{e-e_1+1}}$ (similarly $t_2 \mid \frac{n-1}{2^{e-e_1}}$ and $t_2 \nmid \frac{n-1}{2^{e-e_1+1}}$), if h_1 is even and h_2 is odd then $b^{\frac{n-1}{2^{e-e_1+1}}} \equiv 1 \pmod{q_1}$ and $b^{\frac{n-1}{2^{e-e_1+1}}} \not\equiv 1 \pmod{q_2}$. This implies $1 < (b^{\frac{n-1}{2^{e-e_1+1}}} - 1, n) < n$. Hence $b \in T_n$ in this case. Similarly if h_1 is odd and h_2 is even then $b \in T_n$. If both of h_1 and h_2 are even or odd we cannot say $b \in S_n$ or $b \in T_n$. The number of h_i which are even (or odd) is $\varphi(q_i)/2m_i$ $(i = 1, 2)$. Thus the number of (h_1, h_2) such that $(h_1, h_2) =$ (even, odd) or (odd, even) is $\frac{\varphi(q_1)}{2m_1} \times \frac{\varphi(q_2)}{2m_2} \times 2 = \frac{\varphi(q_1)\varphi(q_2)}{2m_1 m_2}$. Hence $|U_n \cap T_n| \geqslant \frac{\varphi(q_1)\varphi(q_2)}{2m_1 m_2}|Ker\, f| = \frac{\varphi(n)}{2m_1 m_2}$. Therefore $|S_n| = |U_n| - |U_n \cap T_n| \leqslant \frac{\varphi(n)}{m_1 m_2} - \frac{\varphi(n)}{2m_1 m_2} = \frac{\varphi(n)}{2m_1 m_2}$.*

(ii) *When $e_1 > e_2$. Then $t_2 \mid \frac{n-1}{2^{e-e_2}}$, $t_1 \nmid \frac{n-1}{2^{e-e_2}}$. Since $\varphi(q_2) \mid h_2 m_2 \frac{n-1}{2^{e-e_2}}$, $b^{\frac{n-1}{2^{e-e_2}}} \equiv 1 \pmod{q_2}$ holds. On the other hand $\varphi(q_1) \mid h_1 m_1 \frac{n-1}{2^{e-e_2}}$, iff $t_1 \mid h_1 \frac{n-1}{2^{e-e_2}}$, iff $2^{e_1} \mid 2^{e_2} h_1$ and iff $2^{e_1 - e_2} \mid h_1$. Thus if $h_1 = 2^{e_1 - e_2} h'_1$, there are $\frac{\varphi(q_1)}{2^{e_1 - e_2} m_1}$ of $a_1^{2^{e_1 - e_2} h'_1 m_1} \in G_{q_1}$ (since $1 \leqslant h'_1 \leqslant \frac{\varphi(q_1)}{2^{e_1 - e_2} m_1}$), and in this case $b^{\frac{n-1}{2^{e_1 - e_2}}} \equiv 1 \pmod{q_1}$, thus $b \in S_n$ may happen. If $2^{e_1 - e_2} \nmid h_1$ then $b^{\frac{n-1}{2^{e_1 - e_2}}} \not\equiv 1 \pmod{q_1}$. This means $b \in T_n$. Therefore $|S_n| \leqslant \frac{\varphi(q_1)}{2^{e_1 - e_2} m_1} \cdot \frac{\varphi(q_2)}{m_2} \cdot |Ker\, f| = \frac{\varphi(n)}{2^{e_1 - e_2} m_1 m_2} \leqslant \frac{\varphi(n)}{2m_1 m_2}$. This completes the proof.*

Theorem 2.5 (c.f. [3, Theorem 1]) *Let $n > 1$ be an odd composite integer. Then* $|S_n| \leqslant \dfrac{n-1}{4}$

holds. Moreover if $n \neq 9$ *then* $|S_n| \leqslant \dfrac{\varphi(n)}{4}$ *holds.*

Proof *The process of the proof is the same as* [3]. *The proof is divided to three cases* (1) $\sim$ (3). (3) *is also divided to three cases.*

(1) *When* n *is a power of a prime. Let* p *be an odd prime and* $n = p^k$ $(k \geqslant 2)$. *Then* $n-1 = p^k-1 = (p-1)(1+p+\cdots+p^{k-1})$ *and* $\varphi(p^k) = p^{k-1}(p-1)$. *Hence* $(\varphi(p^k), n-1) = p-1$. *Let* a *be a primitive root* $\bmod p^k$. *Take any* $b \in U_n$ *and let* $b \equiv a^r \pmod{p^k}$. *Then* $p^{k-1}(p-1) \mid r(p-1)(1+p+\cdots+p^{k-1})$ *since* $b^{n-1} \equiv a^{r(n-1)} \equiv 1 \pmod{p^k}$. *Thus* $p^{k-1} \mid r$, *which implies* $r = hp^{k-1}$ *for some* h $(0 \leqslant h \leqslant p-2)$. *Conversely it is obvious that* $(a^{hp^{k-1}})^{n-1} \equiv 1 \pmod n$ *for any* h. *Hence* $U_n = \{a^{hp^{k-1}} \mid 0 \leqslant h \leqslant p-2\}$, *and as a result* $|U_n| = p-1$ *holds. On the other hand,* $\frac{n-1}{4} - (p-1) = (p-1)(\frac{1+p+\cdots+p^{k-1}}{4} - 1) = (p-1)\frac{p+\cdots+p^{k-1}-3}{4} \geqslant 0$ $(\because p \geqslant 3)$. *Therefore* $|S_n| \leqslant |U_n| \leqslant \frac{n-1}{4}$. *Next suppose* $n \neq 9$. *Then* $p > 3$ *or* $p = 3$ *with* $k \geqslant 3$. *In this case* $p^{k-1} > 4$. *So* $\frac{\varphi(n)}{4} - (p-1) = (p-1)(\frac{p^{k-1}}{4} - 1) > 0$. *Therefore if* $n \neq 9$ *then* $|S_n| < \frac{\varphi(n)}{4}$ *holds. When* $n = 9$, $S_n = \{1, 8\}$ [1]. *Thus* $|S_n| = 2 > \frac{\varphi(n)}{4} = \frac{6}{4}$, *but* $|S_n| \leqslant \frac{n-1}{4} = 2$ *holds.*

(2) *Let* $n = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$ $(r \geqslant 2)$, *where* p_i $(1 \leqslant i \leqslant r)$ *are different primes, and suppose* $\varphi(p_1^{e_1}) \nmid (n-1)$. *Then* $m_1 = \frac{\varphi(p_1^{e_1})}{t_1} \geqslant 2$ *since* $t_1 = (\varphi(p_1^{e_1}), n-1) < \varphi(p_1^{e_1})$. *And* t_1 *is clearly even. Hence by Lemma 2.4,* $|S_n| \leqslant \frac{\varphi(n)}{2m_1m_2} \leqslant \frac{\varphi(n)}{4m_2} \leqslant \frac{\varphi(n)}{4} < \frac{n-1}{4}$.

(3) *Let* $n = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$ $(r \geqslant 2)$ *be the same as* (2) *and suppose* $\varphi(p_i^{e_i}) \mid (n-1)$ *for all* i. *Since* $p_i \nmid (n-1)$, $e_i = 1$ *for all* i. *Thus* $n = p_1p_2\cdots p_r$ *and* $(p_i-1) \mid (n-1)$ $(i = 1, 2, \ldots, r)$. *Suppose* $p_1 < p_2$. *If* $n = p_1p_2$ *then* $n-1 = p_1p_2-1 = p_1(p_2-1)+(p_1-1)$ *and* $(p_2-1) \mid (n-1)$ *imply* $(p_2-1) \mid (p_1-1)$, *which contradicts* $p_2-1 > p_1-1$. *Thus* $r \geqslant 3$ *must hold. Let us put* $p_i - 1 = 2^{f_i}\ell_i$ $(2 \nmid \ell_i,\ i = 1, 2, \ldots, r)$. *Then* $f_i \leqslant e$ *and* $\ell_i \mid m$ *hold for all* i.

(3-1) *When* $f_1 = f_2 = f_3$. *Clearly* $e \geqslant f_1 \geqslant 1$ *holds. Let* a_i *be a primitive root* $\bmod p_i$ $(1 \leqslant i \leqslant r)$. *Take any* $b \in U_n$ *and let* $b \equiv a_i^{r_i} \pmod{p_i}$. *Let* $\psi : G_n \to G_{p_1} \times G_{p_2} \times G_{p_3}$ *be the canonical epimorphism. Since* $\frac{p_i-1}{2} = \frac{2^{f_i}\ell_i}{2} \mid 2^{f_1-1}m$ *and* $p_i - 1 \nmid 2^{f_1-1}m$ $(i = 1, 2, 3)$, $b^{2^{f_1-1}m} \equiv a_i^{2^{f_1-1}mr_i} \equiv 1 \pmod{p_i}$ *iff* $2 \mid r_i$. *For example, suppose* r_1 *is even and* r_2 *is odd. Then since* $b^{2^{f_1-1}m} \equiv a_1^{2^{f_1-1}r_1m} \equiv 1 \pmod{p_1}$, $p_1 \mid (b^{2^{f_1-1}m} - 1, n)$. *Similarly since* $b^{2^{f_1-1}m} \equiv a_2^{2^{f_2-1}r_2m} \not\equiv 1 \pmod{p_2}$, $p_2 \nmid (b^{2^{f_1-1}m} - 1, n)$. *Thus* $1 < (b^{2^{f_1-1}m} - 1, n) < n$ *holds, and* $b \in T_n$. *This implies that* $b \in S_n$ *may occur only when all of* r_1, r_2, r_3 *are simultaneously even or odd. The number of* b *such that all of* r_1, r_2, r_3 *are simultaneously even (or odd) is* $\frac{p_1-1}{2} \cdot \frac{p_2-1}{2} \cdot \frac{p_3-1}{2} \cdot |Ker\, \psi| = \frac{\varphi(n)}{8}$. *Therefore* $|S_n| \leqslant \frac{\varphi(n)}{8} + \frac{\varphi(n)}{8} = \frac{\varphi(n)}{4}$.

(3-2) *When* $f_1 = f_2 < f_3$. *Note that* $\frac{p_1-1}{2} \mid 2^{f_1-1}m$ *and* $p_1 - 1 \nmid 2^{f_1-1}m$ *hold. Let* $b \in G_n$ *and suppose* $b \equiv a_3^{r_3} \pmod{p_3}$. *Then* $b^{2^{f_1-1}m} \equiv a_3^{2^{f_1-1}mr_3} \pmod{p_3}$. *Thus* $b^{2^{f_1-1}m} \equiv 1 \pmod{p_3}$, *iff* $p_3 - 1 = 2^{f_3}\ell_3 \mid 2^{f_1-1}mr_3$, *iff* $2^{f_3} \mid 2^{f_1-1}r_3$ *and iff* $2^{f_3-f_2+1} \mid r_3$. *Thus the number of* r_3 *such that* $b \equiv a_3^{r_3} \pmod{p_3}$ $(0 \leqslant r_3 \leqslant \varphi(p_3) - 1)$ *and* $b^{2^{f_1-1}m} \equiv 1 \pmod{p_3}$ *is* $\frac{\varphi(p_3)}{2^{f_3-f_2+1}}$. *On the other hand, for* $i = 1, 2$, $b^{2^{f_1-1}m} \equiv a_i^{2^{f_1-1}mr_i} \equiv 1 \pmod{p_i}$ *iff* r_i *is even. Thus* $b \in S_n$ *may occur only when* r_1, r_2 *are even and* $2^{f_3-f_2+1} \mid r_3$ *or* r_1, r_2 *are odd and* $2^{f_3-f_2+1} \nmid r_3$. *Therefore* $|S_n| \leqslant \frac{\varphi(p_1)}{2} \cdot \frac{\varphi(p_2)}{2} \cdot \frac{\varphi(p_3)}{2^{f_3-f_2+1}} \cdot |Ker\, \psi| + \frac{\varphi(p_1)}{2} \cdot \frac{\varphi(p_2)}{2}(\varphi(p_3) - \frac{\varphi(p_3)}{2^{f_3-f_2+1}}) \cdot |Ker\, \psi| = \frac{\varphi(n)}{4}$.

(3-3) *When* $f_1 < f_2 \leqslant f_3$ *(i.e.* $f_1 < f_2 = f_3$ *or* $f_1 < f_2 < f_3$*). In this case* $\frac{p_2-1}{2} = 2^{f_2-1}\ell_2 \mid 2^{f_2-1}m$, $p_2 - 1 \nmid 2^{f_2-1}m$ *hold. On the other hand* $p_1 - 1 = 2^{f_1}\ell_1 \mid 2^{f_2-1}m$ *holds. Let* b *and* a_i $(i = 1, 2, 3)$ *be the same as* (3-2). *Then since* $b^{2^{f_1-1}}m \equiv 1 \pmod{p_1}$, $b \in S_n$ *may occur*

[1] This is calculated by the following Mathematica program.

```
For[i = 2, i ⩽ 8, i++, For[j = 0, j ⩽ 2, j++, If[mod[i^j, 9] == 8, Print[i, "    ", j, "    ", mod[i^j, 9]]]]]
```

only when $b^{2^{f_1-1}m} \equiv 1 \pmod{p_i}$ $(i = 2, 3)$ *hold.* $b^{2^{f_2-1}m} \equiv a_i^{2^{f_2-1}mr_i} \equiv 1 \pmod{p_i}$ $(i = 2, 3)$ *hold only when* r_2 *is even and* $2^{f_3-f_2+1} \mid r_3$. *Thus the numbers of such* r_2 *and* r_3 *are* $\frac{\varphi(p_2)}{2}$ *and* $\frac{\varphi(p_3)}{2^{f_3-f_2+1}}$, *respectively. Therefore* $|S_n| \leqslant \varphi(p_1) \cdot \frac{\varphi(p_2)}{2} \cdot \frac{\varphi(p_3)}{2^{f_3-f_2+1}} \cdot |Ker\,\psi| = \frac{\varphi(n)}{2^{f_3-f_2+2}} \leqslant \frac{\varphi(n)}{4}$. *This completes the proof.*

3 The relation between Solovey-Strassen's primality test and Miller-Rabin's test

First we prove the following.

Theorem 3.1 *Let* $n > 1$ *be an odd integer. Then* $S_n \subset H_n$ *holds.*

Proof *If* n *is prime then* $S_n = H_n = U_n = G_n$ *holds. So let* n *be a composite integer and* $n = p_1 p_2 \cdots p_k$ *a prime factor decomposition, where* $p_i = p_j$ *is allowed even if* $i \neq j$. *Let* $n - 1 = 2^e m$, $p_i - 1 = 2^{e_1} m_i$ $(i = 1, 2, \ldots, k)$, *where* m *and* m_i $(i = 1, 2, \ldots, k)$ *are odd. First note that:*

$$\begin{aligned} n-1 &= p_1(p_2 \cdots p_k - 1) + p_1 - 1 \\ &= p_1(p_2(p_3 \cdots p_k - 1) + p_2 - 1) + p_1 - 1 \\ &= p_1 p_2 (p_3 \cdots p_k - 1) + p_1(p_2 - 1) + p_1 - 1 \\ &\;\vdots \\ &= p_1 - 1 + p_1(p_2 - 1) + \cdots + p_1 \cdots p_{k-1}(p_k - 1). \end{aligned}$$

We may assume that e_1 *is the smallest among* $\{e_1, e_2, \ldots, e_k\}$ *by re-arranging the ordering of* $p_1, p_2, \ldots, p_k$. *So* $2^e m = 2^{e_1}(m_1 + 2^{e_2-e_1} m_2 + \cdots + 2^{e_r-e_1} p_1 \cdots p_{k-1} m_k)$ *implies* $e_1 \leqslant e$. *Let us put* $f = m_1 + 2^{e_2-e_1} m_2 + \cdots + 2^{e_r-e_1} p_1 \cdots p_{k-1} m_k$. *Let* $\forall b \in S_n$. *Let* a_i *be a primitive root mod* p_i *and* $b \equiv a_i^{r_i} \pmod{p_i}$.

(1) *When* $b^m \equiv 1 \pmod{n}$. $a_i^{mr_i} \equiv 1 \pmod{p_i}$ *implies* $p_i - 1 = 2^{e_i} m_i \mid mr_i$. *Since* m *is odd,* $2^{e_i} \mid r_i$. *In particular* r_i *is even. Thus* $(\frac{b}{p_i}) = 1$ $(i = 1, 2, \ldots, k)$, *which implies* $(\frac{b}{n}) = 1$. *On the other hand,* $b^{\frac{n-1}{2}} \equiv b^{2^{e-1}m} = (b^m)^{2^{e-1}} \equiv 1 \pmod{n}$. *Therefore* $b \in H_n$.

(2) *When* $b^m \not\equiv 1 \pmod{n}$. *Since* $b \in S_n$, *there exists* $j\,(0 \leqslant j < e)$ *such that* $b^{2^j m} \equiv -1 \pmod{n}$. *This implies* $a_i^{2^j mr_i} \equiv -1 \pmod{p_i}$ $(i = 1, 2, \ldots, k)$. *Thus there exist odd integers* u_i *such that* $2^j mr_i = \frac{p_i - 1}{2} u_i = 2^{e_i - 1} m_i u_i$ $(i = 1, 2, \ldots, k)$. *Let* $r_i = 2^{\alpha_i} s_i$, *where* $\alpha_i \geqslant 0$ *and* s_i *are odd integers. Then* $j + \alpha_i = e_i - 1$, *i.e.* $e_i = j + \alpha_i + 1$ $(i = 1, 2, \ldots, k)$ *hold.*

(2-1) *When* $\alpha_1 = 0$. *Then* $e_1 = j + 1$. *If* $e_i = e_1$ *then* $\alpha_i = 0$ *since* $j + \alpha_i + 1 = e_i = e_1 = j + 1$. *Thus* r_i *is odd, and* $(\frac{b}{p_i}) = -1$. *If* $e_i > e_1$ *then* $\alpha_i > 0$ *since* $j + \alpha_i + 1 = e_i > \alpha_1 = j + 1$. *Thus* $(\frac{b}{p_i}) = 1$ *in this case.*

(2-1-1) *When* $j = e - 1$. *Then* $e_1 = e$ *and* $2^e m = 2^{e_1} m$, *which imply* $m = f$. *So* f *is odd. Thus the number of* i *such that* $e_i = e$ *is odd. Therefore* $(\frac{b}{n}) = \prod_{i=1}^{k} (\frac{b}{p_i}) = (-1)^{odd} \times 1 = -1$. *On the other hand* $b^{\frac{n-1}{2}} = b^{2^{e-1}m} = b^{2^j m} \equiv -1 \pmod{n}$. *Thus* $b \in H_n$.

(2-1-2) *When* $j < e - 1$. *Since* $e_1 = j + 1 < e$, $f = 2^{e-e_1} m$ *is even. Thus the number of* i *such that* $e_i = e$ *is even. Therefore* $(\frac{b}{n}) = (-1)^{even} \times 1 = 1$. *On the other hand* $b^{\frac{n-1}{2}} = b^{2^{e-1}m} = (b^{2^j m})^{2^{e-1-j}} \equiv (-1)^{2^{e-1-j}} \equiv 1 \pmod{n}$. *Thus* $b \in H_n$.

(2-2) *When* $\alpha_1 \geqslant 1$. *Since* $e_1 = j + \alpha_1 + 1$, $e_i = j + \alpha_i + 1 \geqslant e_1 = j + \alpha_1 + 1$, *which implies* $\alpha_i \geqslant \alpha_1$ $(i = 1, 2, \ldots, k)$. *Thus* $\alpha_i \geqslant \alpha_1 \geqslant 1$ $(i = 1, 2, \ldots, k)$. *Therefore* $r_1\ r_2, \ldots, r_k$ *are all even, and* $(\frac{b}{n}) = 1$. *On the other hand* $e \geqslant e_1 = j + \alpha_1 + 1 \geqslant j + 2$. *hence* $e - 1 - j \geqslant 1$. *Thus*

$b^{\frac{n-1}{2}} = b^{2^{e-1}m} = (b^{2^j m})^{2^{e-1-j}} \equiv (-1)^{2^{e-1-j}} \equiv 1 \pmod{n}$. *Therefore* $b \in H_n$. *This completes the proof.*

If $n > 1$ is an odd composite integer then H_n is a proper subgroup of G_n. Since $|H_n|$ divides $|G_n|$, we can say $|H_n| \leqslant \frac{\varphi(n)}{2}$. If we calculate several examples, $|H_n|$ is much smaller than $\frac{\varphi(n)}{2}$. The author expected $|H_n| \leqslant \frac{\varphi(n)}{4}$. Since the proof that H_n is a proper subgroup of G_n is very simple and beautiful, it is expected that Solovey-Strassen's primality test has the same value as Miller-Rabin's one.

Before to show examples it is useful to remind a Carmichael number. Let $n = p_1 \cdots p_k$ be a product of distinct primes, and suppose $p_i - 1 \mid n - 1$ for all i. Then n is called a Carmichael number. In order to find an example of an odd composite number n such that $|H_n| = \frac{\varphi(n)}{2}$, it is enough to check Carmichael numbers by the following lemma.

Lemma 3.2 *Let* $n > 1$ *be an odd composite integer such that* $|H_n| = \frac{\varphi(n)}{2}$. *Then* n *is a Carmichael number.*

Proof *Let* $n = p_1^{e_1} \cdots p_k^{e_k}$ *be a prime factor decomposition with* $e_i \geqslant 1$ $(i = 1, \ldots, k)$. *Note that* $G_n \simeq G_{p_1^{e_1}} \times \cdots \times G_{p_k^{e_k}}$. *If some* $e_i > 1$, *then there exists an* $a \in G_n$ *such that the order of* a *is* p_i. *Then* $a \notin H_n$ *since* $p_i \nmid n - 1$. *Moreover* $H_n, aH_n, \ldots, a^{p-1}H_n$ *are distinct residue classes in* G_n/H_n. *Thus* $|G_n : H_n| \geqslant p_i \geqslant 3$ *holds. Hence* $|H_n| \leqslant \frac{\varphi(n)}{3} < \frac{\varphi(n)}{2}$. *This contradicts to the hypothesis. Therefore* $e_1 = \cdots = e_k = 1$ *holds. If* $p_i - 1 \nmid n - 1$ *for some* i, *there exists an odd prime* q *such that* $q \mid p_i - 1$ *and* $q \nmid n - 1$. *Like the above argument there exists an* $a \in G_n$ *such that the order of* a *is* q. *Then* $a \notin H_n$ *since* $q \nmid n - 1$. *Moreover* $H_n, aH_n \ldots, a^{q-1}H_n$ *are distinct residue classes in* G_n/H_n *like the above. This is also a contradiction. Therefore* n *must be a Carmichael number.*

In order to find an example of an odd composite number such that $|S_n| = \frac{\varphi(n)}{4}$, we have to re-check the proof of Theorem 2.5. From (1) in the proof we get $|S_n| \neq \frac{\varphi(n)}{4}$. So the possibility that $|S_n| = \frac{\varphi(n)}{4}$ holds comes from (2) and (3). (3) is a case of Carmichael numbers. The author does not know if there is an example from (2). Anyway it is enough to check Carmichael numbers. We got the following examples.

Example 3.1 *When* $n = 2465 = 5 \cdot 17 \cdot 29$, $\varphi(n) = 1792$, $|H_n| = 896 = \varphi(n)/2$. *On the other hand,* $|S_n| = 70 < \varphi(n)/25$.

Example 3.2 *When* $n = 8911 = 7 \cdot 19 \cdot 67$, $\varphi(n) = 7128$, $|S_n| = 1782 = \varphi(n)/4 = |H_n|$.

In Example 3.1 $|S_n|$ does not divide $\varphi(n)$. Thus S_n is not a subgroup of G_n. But S_n has the following property.

Proposition 3.3 *If* $a \in S_n$ *then* $<a> \subset S_n$ *holds, where* $<a>$ *denotes the cyclic group generated by* a.

Proof *Remind that* $n - 1 = 2^e m$. *Let* $k \geqslant 0$ *be an integer. If* $a^m \equiv 1 \pmod{n}$ *then obviously* $(a^k)^m \equiv 1 \pmod{n}$. *Thus* $a^k \in S_n$. *Suppose there exists* i $(0 \leqslant i < e)$ *such that* $a^{2^i m} \equiv -1 \pmod{n}$. *Let* $k = 2^\ell t$, *where* $\ell \geqslant 0$ *and* t *is odd. If* $\ell = i$ *then* $(a^k)^m = (a^{2^i m})^t \equiv (-1)^t \equiv -1 \pmod{n}$. *If* $\ell > i$ *then* $(a^k)^m = (a^{2^i m})^{2^{\ell-i}t} \equiv ((-1)^{2^{\ell-i}})^t \equiv 1 \pmod{n}$. *If* $\ell < i$ *then* $(a^k)^{2^{i-\ell}m} = (a^{2^i m})^t \equiv (-1)^t \equiv -1 \pmod{n}$. *Therefore in any case* $a^k \in S_n$.

For the rest of this paper we show Mathematica programs to calculate above examples. In the following programs the module **beki**[ ] is very important to calculate $a^e \pmod{n}$. The idea is found in [1, Appendix 2]. Fist we show the program to compute Solovey-Strassen's case.

```
beki[a_, e_, n_]:=Module[{b, p, c},
b = a; p = 1; c = e;
While[c > 0,
If[Mod[c, 2] == 0, c = c/2,
p = Mod[bp, n];
c = (c − 1)/2];
b = Mod[b^2, n]];
Return[p]];
jacob[a_, n_]:=Module[{c, d, r},
c = a; d = n;
jcob = If[GCD[c, d] > 1, 0; Goto[end], 1];
While[c > 1,
c = Mod[c, d];
If[Mod[c, 2] == 0, r = Mod[(d^2 − 1)/8, 2]; jcob*=(−1)^r; c = c/2,
r = Mod[(c − 1)(d − 1)/4, 2];
jcob*=(−1)^r; tmp = c; c = d; d = tmp]];
Label[end]];
sls[a_, n_]:=Module[{}, (*Solovay-Strassen's primality test*)
j = beki[a, (n − 1)/2, n];
jacob[a, n]];
k = 0; n = 8911; For[i = 1, i ⩽ n, i++, sls[i, n];
If[Mod[j − jcob, n] == 0, k++]];
Print[k]
1782
```

Next we show the Miller-Rabin's case.

```
beki[a_, e_, n_](This is the same as the above module beki)
miller[a_, n_]:=Module[{k, q}, (*Miller-Rabin's primality test*)
k = 0; q = n − 1;
```

```
While[Mod[q, 2] == 0,
q/=2; k+=1];
i = 0; r = beki[a, q, n];
Label[repeat];
If[(i == 0&&r == 1)||(i ⩾ 0&&r==n − 1), Goto[end],
i+=1; r = Mod[r^2, n];
If[i < k, Goto[repeat]]];
Label[end]];
j = 0; n = 8911; For[a = 1, a ⩽ n, a++, miller[a, n];
If[(i == 0&&r == 1)||(i ⩾ 0&&r == n − 1), j++]];
Print[j]
1782
```

Remark. In the above programs **beki** can be replaced by **PowerMod**.

References

[1] S.C. Coutiho, "The Mathematics of Ciphers: Number Theory and RSA Cryptography", 1999, A K Peters, Ltd.

[2] K. Ohtake, "A first course of the theory of integers" (in Japanese), 2014(revised), unpublished textbook.

[3] M.O. Rabin, Probabilistic Algorithm for testing primality, J. Number Theory 12 (1980), 128-138.

[4] R. Solovey and V. Strassen, A fast Monte-Carlo test for primality, SIAM J. Comput. 6(1977), 84-85.