Properties Of Strong Pseudoprimes On Base *b*

Kamala Parhi* and Pushpam Kumari**
* Associate Professor, Dept. of Mathematics, Marwari College, Bhagalpur
T.M. Bhagalpur University, Bhagalpur, Bihar, India

** Research Scholar, Univ. Dept. of Mathematics,
T.M. Bhagalpur University, Bhagalpur, Bihar, India

ABSERACT

In this paper, we make a study of special kind of pseudoprimes (strong pseudoprimes) on base *b* that are very useful in primality testing.

Keywords : strong pseudoprimes, nonnegative integer, Euler pseudoprime.

Introduction

In number theory, a strong pseudoprime is a composite number that passes a primality test. All primes pass this test, but a small fraction of composites pass as well, making them false prime. Unlike Carmichael numbers, which are pseudoprimes to all bases, there do not exists composite numbers that are strong pseudoprimes to all bases. This fact forms the basis of the Miller-Rabin probabilistic primality test [4]. Define n to be the smallest integer that is a strong pseudoprime to the first n prime bases. The problem of finding strong pseudoprimes has a long history. Pomerance, Selfridge, and Wagstaff [3] computed F_n for m = 2, 3, and 4. Jaeschke [1] computed F_n for n = 5, 6, 7 and 8. By looking at a narrow class of numbers, Zhang [5] gave upper bounds on F_n for $9 \le n \le 19$. Recently, Jian and Deng [2] verified some of Zhang's conjectures and computed F_n for n = 9, 10 and 11.

Fermat's Little Theorem states that if p is prime and gcd(b, p) = 1, then

$b^{p-1} \equiv \pmod p$.

A composite number for which this congruence holds is called a pseudoprime to the base b. We can restate Fermat's Little Theorem by algebraically factoring (repeatedly) the difference of squares that arises in $b^{p-1} - 1$. In which case, let p be a prime and b a positive integer relatively prime to p. Assume that $p - 1 = 2^s t$, where t is odd and s is a nonnegative integer. We have $a^{p-1} \equiv 1 \pmod p$, and since $x^2 \equiv 1 \pmod p$ hold if and only if $x = \pm 1 \pmod p$, then $a^{2^j t} \equiv \pm 1 \pmod p$ for every j = 0, 1, 2, ..., s. Thus, we can define a type of pseudoprime (strong pseudoprime) based on the observation above.

Definition 1. Let n be an odd composite integer. Let $n-1 = 2^s t$, where s is a nonnegative integer and t is odd positive integer. Let b be an integer such that $1 < b < n$, and gcd(b, n) = 1, we say that n is a strong pseudopprime to the base b if either $b^t \equiv -1 \pmod n$, or there exists j, $0 \le j < s$ such that $b^{2^j t} \equiv -1 \pmod n$.

Lemma 1. If d and n are positive integers such that d divides n, then for any integer a, $a^d - 1$ divides $a^n - 1$.

Proof. Since $d|n$, there is a positive integer t with $dt = n$. Consider the identity $(x^n - 1) = (x - 1)(x^{n-1} + x^{n-2} + ... + 1)$. Putting $n = dt$, and $x = a$, we obtain

$((a^d)^t - 1) = (a^d - 1)(a^{d(t-1)} + a^{d(t-2)} + ... + a^d + 1)$

or $(a^n - 1) = (a^d - 1)(a^{d(t-1)} + a^{d(t-2)} + ... + a^d + 1)$,

consequently $a^d - 1 \mid a^n - 1$. QED.

Theorem 1. If n is a strong pseudoprime to the b then n is pseudoprime to the base b.

Proof. If n is a strong pseudoprime, then either $b^t \equiv -1 \pmod{n}$ or $b^{2^j t} \equiv -1 \pmod{n}$ for some j with j, $0 \le j \le s-1$ where $n-1 = 2^s t$ as in the definition. Thus if $b^t \equiv -1 \pmod{n}$, then $b^{n-1} = (b^t)^{2^n} \equiv 1 \pmod{n}$. On the other hand if $b^{2^j t} \equiv -1 \pmod{n}$ for some j, with $0 \le j \le s-1$, then since $b^{n-1} = (b^{2^j t})^{s-j}$, for $j = 0, 1, 2, \ldots, s$, we have $b^{n-1} \equiv 1 \pmod{n}$. Thus in either case $b^{n-1} \equiv 1 \pmod{n}$ and hence n is a pseudoprime to the base b. This completes the proof.

Example 1. Let $n = 2047$. Then $2^{2046} = (2^{11})^{186} = (2048)^{186} \equiv 1 \pmod{2047}$, so that 2047 is a pseudoprime to the base 2. Since $2^{2046/2} = 2^{1023} = (2^{11})^{93} = (2048)^{93} \equiv 1 \pmod{2047}$. Hence, 2047 is a strong pseudoprime to the base 2.

The converse of Theorem 1 is not true. For example, $n = 1387 = 19*73$ is a pseudoprime to the base 2 but is not strong pseudoprime to the base 2.

Although strong pseudoprimes are exceedingly rare, there are still infinitely many of them. We demonstrate this for the base 2 with the following theorem.

Theorem 2. There are infinitely many strong pseudoprime to the base 2.

Proof. We shall show that if n is a pseudoprime to the base 2, then $2^n - 1$ is a strong pseudoprime to the base 2.

Let n be an odd integer which is a pseudoprime to the base 2. Hence, n and $N = 2^n - 1$ are composite, and $2^n - 1 \equiv 1 \pmod{n}$. From this congruence, We see that $2^{n-1} - 1 = nk$ for some integer k, furthermore, k must be odd. We have

$$N - 1 = 2^n - 2 = 2\,(2^{n-1} - 1) = 2^1 nk,$$

this is a factorization of $N-1$ into an odd integer and a power of 2. We now note that

$$2^{(N-1)/2} = 2^{nk} = (2^n)^k \equiv 1 \pmod{N},$$

because $2^n = (2^n - 1) + 1 = N + 1 \equiv 1 \pmod{N}$. This implies that N is a strong pseudoprime to the base 2. Since every pseudoprime $2^n - 1$ yields a strong pseudoprime to the base 2 and since there are infinitely many pseudoprimes to the base 2. Thus we conclude that there are infinitely many strong pseudoprime to the base 2.

Corollary 1. There exists infinitely many strong pseudoprime to the base 2 with arbitrarily many prime factors.

Proof. It follows that for every integer $k \ge$ there are infinitely many square free pseudoprimes to the base 2 with exactly k prime factors. By the theorem above, if n is a pseudoprime to the base 2, with k prime factors, then $2^n - 1$ is a strong pseudoprime to the base 2. Moreover, if p is one of the prime factors of ^{n}, then by Lemma 1, we have $2^p - 1 | 2^n - 1$. Since the number $2^p - 1$ with distinct primes p are relatively prime, the number $2^n - 1$ has at least as many prime factor as n. Thus $2^n - 1$ is a strong pseudoprime to the base 2 with at least k prime factors.

Theorem 3. Every composite Fermat number $F_n = 2^{2^n} + 1$ is a strong pseudoprime to the base 2.

Proof. Since $F_n - 1 = 2^{2^n}$, then

$$2^{F_n - 1} = 2^{2^n} = (2^{2^n})^{2^{2^n - n}} = (F_n - 1)^{2^{2^n - n}}.$$

$$(F_n - 1)^{2^{2^n - n}} \equiv (-1)^{2^{2^n - n}} = 1 \pmod{F_n}.$$

Now, taking square roots will always give 1's until eventually, after $2^n - n$ times, a (-1) will appear. Thus F_n is a strong pseudoprime whenever F_n is composite. This completes the proof.

We know that every Euler pseudoprime is a pseudoprime. Next we show that every strong pseudoprime is an Euler pseudoprime.

Theorem 4. If n is a strong pseudoprime to the base b, then n is an Euler pseudoprime to this base.

Proof. If n be a strong pseudoprime to the base b. Then if $n-1 = 2^s t$, where t is odd, either $b^t = 1 \pmod n$ or $b^{2^r t} \equiv -1 (\mathrm{mod}\, n)$, where $0 \le j \le s-1$. Let $n = \prod_{i=1}^{m} p_i^{a_i}$ be the prime-power factorization of n.

First, we consider the case where $b^t \equiv -1 \pmod n$. Let p be a prime divisor of n. Since $b^t \equiv -1 \pmod n$, we know that $\mathrm{ord}_p(b) \mid t$. Because t is odd, we see that $\mathrm{ord}_p(b)$ is also odd. Hence, $\mathrm{ord}_p(b) \mid (p-1)/2$, since $\mathrm{ord}_p(b)$ is an odd divisor of the even integer $\phi(p-1) = p-1$. Therefore, $b^{(p-1)/2} \equiv 1 \pmod p$.

Consequently, by Euler's criterion, we have $\left[\frac{b}{p}\right] = 1$. To compute the Jaccobi symbol $\left[\frac{b}{n}\right]$, we note that $\left[\frac{b}{p}\right] = 1$ for all primes p dividing n. Hence,

$$\left[\frac{b}{p}\right] = \left[\frac{b}{\prod_{i=1}^{m} p_i^{a_i}}\right] = \prod_{i=1}^{m}\left[\frac{b}{p_i}\right]^{a_i} = 1.$$

Since $b^t \equiv -1 \pmod n$, we know that $b^{(n-1)/2} = (b^t)^{s-1} \equiv 1 (\mathrm{mod}\, n)$. Therefore, we have

$$b^{(n-1)/2} \equiv \left[\frac{b}{n}\right] \equiv 1 (\mathrm{mod}\, n).$$

We conclude that n is an Euler's pseudoprime to the base b.

Next, we consider the case where

$$b^{2^r t} \equiv -1 (\mathrm{mod}\, n)$$

for some r with $0 \le r \le s-1$. If p is a prime divisor of n, then

$$b^{2^r t} \equiv -1 (\mathrm{mod}\, p)$$

Squaring both sides of this congruence, we obtain

$$b^{2^{r+1} t} \equiv 1 (\mathrm{mod}\, p).$$

This implies that $\mathrm{ord}_p(b) \mid 2^{r+1} t$, but that $\mathrm{ord}_p(b) \nmid 2^r t$ Hence,

$$\mathrm{ord}_p(b) \mid 2^{r+1} c,$$

where c is an odd integer. Since $\mathrm{ord}_p(b) \mid (p-1)$ and $2^{r+1} \mid \mathrm{ord}_p(b)$, it follows that $2^{r+1} \mid (p-1)$.

Therefore, we have $p = 2^{r+1} d + 1$, where d is an integer. Since

$$b^{(\mathrm{ord}_p(b))/2} \equiv -1 (\mathrm{mod}\, p).$$

We have

$$\left[\frac{b}{p}\right] \equiv b^{(p-1)/2} = b^{(\mathrm{ord}_p(b)/2)(p-1)/(\mathrm{ord}_p(b))}$$
$$\equiv (-1)^{(p-1)/(\mathrm{ord}_p(b))} = (-1)^{(p-1)/2^{r+1} c} (\mathrm{mod}\, p).$$

Because c is odd, we know that $(-1)^c = -1$. Hence,

$$\left[\frac{b}{p}\right] = (-1)^{(p-1)/2^{r+1}c} = \langle -1\rangle^d. \qquad (1)$$

recalling that $d = (p-1)/2^{r+1}$. Since each prime p_i dividing n is of the form $p_i = 2^{r+1}d_i + 1$, it follows that

$$n = \prod_{i=1}^{m} p_i^{a_i} = \prod_{i=1}^{m}(2^{r+1}d_i + 1)^{a_i} \equiv \prod_{i=1}^{m}(1 + 2^{r+1}a_i d_i) \equiv 1 + 2^{r+1}\sum_{i=1}^{m} a_i d_i \pmod{2^{2r+2}}.$$

Therefore,

$$t2^{s-1} = (n-1)/2 \equiv 2^r \sum_{i=1}^{m} a_i d_i \pmod{2^{r+1}}.$$

This congruence implies that

$$t2^{s-1-r} \equiv \sum_{i=1}^{m} a_i d_i \pmod 2, \text{ and}$$

$$b^{(n-1)/2} = (b^{2^r t})^{2^{s-1-r}} \equiv (-1)^{2^{s-1-r}} = (-1)^{\sum_{i=1}^{m} a_i d_i} \pmod n. \qquad (2)$$

On the other hand, from (1), we have

$$\left[\frac{b}{n}\right] = \prod_{i=1}^{m}\left[\frac{b}{n}\right]^{a_i} = \prod_{i=1}^{m}((-1)^{d_i})^{a_i} = \prod_{i=1}^{m}(-1)^{a_j d_j} \equiv (-1)^{\sum_{i=1}^{m} a_i d_i}.$$

Therefore, combining the previous equation with (2), we see that

$$b^{(n-1)/2} \equiv \left[\frac{b}{n}\right] \pmod n.$$

Consequently, n is an Euler pseudoprime to the base b. This completes the proof.

Corollary 2. There exist infinitely many Euler pseudoprime to the base 2 with arbitrarily many prime factors.

Proof. The proof follows directly from the theorem above and the corollary to Theorem 2.

Although every strong pseudopsrime to the base b is an Euler pseudoprime to this base b, the converse is not true, as the following example shows.

Example. We have previously shown that the integer 1105 is an Euler pseudoprime to the base 2. However, 1105 is not a strong pseudoprime to the base 2 since

$$2^{(1105-1)/2} = 2^{552} \equiv 1 \pmod{1105},$$

while

$$2^{(1105-1)/2^2} = 2^{276} \equiv 781 \pm 1 \pmod{1105}.$$

Although an Euler pseudoprime to the base b is not always a strong pseudoprime to this base, when certain extra conditions are met, an Euler pseudoprime to the base b is, in fact, a strong pseudoprime to this base. The following two theorems give results of this kind.

Theorem 5. If $n \equiv 3 \pmod 4$ and n is an Euler Pseudoprime to the base b, then n is a strong pseudoprime to the base b.

Proof. From the congruence $n \equiv 3 \pmod 4$, we know that $n-1 = 2 \cdot t$ where $t = (n-1) \mid 2$ is odd. Since n is Euler pseudoprime to the base b, it follows that

$$b^t = b^{(n-1)/2} \equiv \left[\frac{b}{n}\right] (\mathrm{mod}\, n).$$

since $\left[\frac{b}{n}\right] = \pm 1,$ we know that either $b^t \equiv 1 \pmod{n}$ or $b^t \equiv -1 \pmod{n}$. Hence, one of the congruences in the definition of a strong pseudoprime to the base b must hold. Consequently, n is a strong pseudoprime to the base b.

Theorem 6 [5]. If n is a an Euler Pseudoprime to the base b, and $\left[\frac{b}{n}\right] = -1,$ then n is a strong pseudoprime to the base b.

Proof. We write $n-1 = 2^s t$, where t is odd and s is a positive integer. Since n is an Euler pseudoprime to the base b, we have

$$b^{2^{s-1}t} = b^{(n-1)/2} \equiv \left[\frac{b}{n}\right] (\mathrm{mod}\, n).$$

But since

$$\left[\frac{b}{n}\right] = -1,$$

we see that

$$b^{t2^{s-1}} \equiv -1 (\mathrm{mod}\, n).$$

This is one of the congruences in the definition of strong pseudoprime to the base b. Since n is composite, it is a strong pseudoprime to the base b. This completes the proof.

References

[1] Jaeschke, G. (1993) : On strong pseudoprimes to several bases, Math. Comp. 61(204):915-926.

[2] Jiang, Y. and Deng, Y. (2014) : Strong pseudoprimes to the first eight prime bases, Math. Comp., 1-10 (electronic).

[3] Pomerance, C.; Selfridge, J.L. and Wagstaff Jr., S.S. (1980) : The pseudoprimes to 25.10^9, Math. Comp., 35:1003-1026.

[4] Rabin, Michael O. (1980) : Probabilistic algorithm for testing primality, J. Number Theory, 12(1):128-138.

[5] Zhang, Z. (2007) : Two kinds of strong pseudoprimes up to 10^{36}, Math. Comp. 76(260):2095-2107 (electronic).