Fundamental Journal of Mathematics and Mathematical Sciences
p-ISSN: 2395-7573; e-ISSN: 2395-7581
Volume 19, Issue 1, 2025, Pages 137-154
This paper is available online at http://www.frdint.com/
Published online June 3, 2025

# A POSSIBLE BETTER IMPLEMENTATION OF THE BAILLIE-PSW PRIMALITY TEST

**DONATO DI IORIO**

Department of Economics, Management, Society and Institutions
University of Molise
via Francesco De Sanctis 1, (86100) Campobasso
Italy
e-mail: donato.diiorio@unimol.it

## Abstract

In this manuscript, we show first a more synthetic definition of strong pseudoprimality to base 2 and then a possible better implementation of the Baillie-PSW primality test. In particular, about the implementation of the Baillie-PSW primality test, we show that some operations can be avoided [1, 2].

## 1. Introduction

The main objective of this manuscript is to show the possibility of implementing the Baillie-PSW primality test more appropriately with reference to strong pseudoprimality to base 2. In particular we first show, by means of the characterization of Fermat's little theorem in the

Keywords and phrases: prime number, composite integer, Carmichael number, strong pseudoprime, primality test.

2020 Mathematics Subject Classification: Primary: 11Y11; secondary: 11A51.

Received May 8, 2025; Accepted May 22, 2025

congruence classes mod 8, a more concise definition of strong pseudoprimality to base 2 and then a possible better implementation of the Baillie-PSW primality test.

## 2. A Necessary Condition of Primality Deriving from Euler's Criterion and Legendre Symbol

Fermat's little theorem states that:

if $p$ is a prime number and $a$ is any integer coprime with $p$, then it is:

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

We can express Fermat's little theorem in another way:

if $p$, $p > 2$, is a prime number and $a$ is any integer coprime with $p$, then it is:

$$a^{\frac{p-1}{2}} \equiv 1 \pmod{p} \quad \text{or} \quad a^{\frac{p-1}{2}} \equiv -1 \pmod{p}.$$

By means of Euler's criterion and Legendre symbol we can characterize the above condition with respect to the base $a = 2$ in the congruence classes $p \equiv 1 \pmod{8}$, $p \equiv 3 \pmod{8}$, $p \equiv 5 \pmod{8}$ and $p \equiv 7 \pmod{8}$. In fact, we have the following proposition.

**Proposition 2.1.** *If* $p$, $p > 2$, *is a prime number*, $p \equiv 1 \ (mod\ 8)$ *or* $p \equiv 7 \ (mod\ 8)$, *then it is*: $2^{\frac{p-1}{2}} \equiv 1 \ (mod\ p)$; *if* $p$, $p > 2$, *is a prime number*, $p \equiv 3 \ (mod\ 8)$ *or* $p \equiv 5 \ (mod\ 8)$, *then it is*: $2^{\frac{p-1}{2}} \equiv -1 \ (mod\ p)$.

**Proof.** If $p$, $p > 2$, is prime and if, moreover, $p \equiv 1 \pmod{8}$, i.e., if $p = 8k + 1$, $k \in N$, $k > 1$, since:

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = (-1)^{\frac{(8k+1)^2-1}{8}} = (-1)^{\frac{64k^2+1+16k-1}{8}} = (-1)^{2k(4k+1)} = 1,$$

from Euler's criterion $a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \pmod{p}$ for $a = 2$ it is: $2^{\frac{p-1}{2}} \equiv 1 \pmod{p}$. Similarly in other cases $p \equiv 3 \pmod{8}$, $p \equiv 5 \pmod{8}$ and $p \equiv 7 \pmod{8}$.

Proposition 2.1 can also be expressed in the following way.

**Proposition 2.2.** *If* $p$, $p > 2$, *is a prime number such that* $p - 1 = 2^s \cdot t$, $s \in N$, $s \geq 1$, $t \in N$, $t$ *odd, we have the following*:

a) *if* $p \equiv 1\ (mod\ 8)$ $(s \geq 3)$, *then we have*:

$2^t \equiv 1\ (mod\ p)$ *or* $2^{2^r \cdot t} \equiv -1\ (mod\ p)$ *for some integer* $r$, $0 \leq r \leq s-2$;

b) *if* $p \equiv 3\ (mod\ 8)$, *then we have*: $2^t \equiv -1\ (mod\ p)$;

c) *if* $p \equiv 5\ (mod\ 8)$, *then we have*: $2^{2t} \equiv -1\ (mod\ p)$;

d) *if* $p \equiv 7\ (mod\ 8)$, *then we have*: $2^t \equiv 1\ (mod\ p)$.

**Proof.** a) From proposition 2.1: $\left(2^{\frac{p-1}{4}}\right)^2 - 1 \equiv 0 \pmod{p}$, (in this case it is $p \equiv 1 \pmod{8}$, i.e., $p = 8k + 1$, $k \in N$, $k > 1$; $p - 1 = 2^3 k$, $k \in N$, $k > 1$; so $\frac{p-1}{4}$ is an integer number and it is also $s \geq 3$) we have:

$$\left(2^{\frac{p-1}{4}} + 1\right)\left(2^{\frac{p-1}{8}} + 1\right) \cdot \ldots \cdot \left(2^{\frac{p-1}{2^{s-1}}} + 1\right)\left(2^{\frac{p-1}{2^s}} + 1\right)\left(2^{\frac{p-1}{2^s}} - 1\right)$$

$\equiv 0 \pmod{p}$;

so, since $\frac{p-1}{2^s} = t$, we have:

$$(2^t - 1)(2^t + 1)(2^{2t} + 1) \cdot \ldots \cdot (2^{2^{s-3} \cdot t} + 1)(2^{2^{s-2} \cdot t} + 1) \equiv 0 \pmod{p},$$

i.e.: $2^t \equiv 1 \pmod{p}$ or $2^{2^r \cdot t} \equiv -1 \pmod{p}$ for some integer $r$, $0 \le r \le s-2$;

b) since it is $p - 1 = 2(4k+1) = 2t$, $k \in N$, i.e., $t = \frac{p-1}{2}$, from Proposition 2.1 we have: $2^t \equiv -1 \pmod{p}$;

c) since it is $p - 1 = 2^2(2k+1) = 2^2 t$, $k \in N$, i.e., $2t = \frac{p-1}{2}$, from Proposition 2.1 we have: $2^{2t} \equiv -1 \pmod{p}$;

d) since it is $p - 1 = 2(4k+3) = 2t$, $k \in N$, i.e., $t = \frac{p-1}{2}$, from Proposition 2.1 we have: $2^t \equiv 1 \pmod{p}$.

## 3. The Classical Necessary Condition of Primality Deriving from Fermat's Little Theorem

On prime numbers we have the following proposition.

**Proposition 3.1.** *If* $p$, $p > 2$, *is a prime number such that* $p - 1 = 2^s \cdot t$, $s \in N$, $s \ge 1$, $t \in N$, $t$ *odd, for each integer* $a$ *coprime with* $p$, $1 \le a < p$, *we have*:

$$a^t \equiv 1 \ (mod\ p) \ or\ a^{2^r \cdot t} \equiv -1 \ (mod\ p) \ for\ some\ integer\ r,$$
$$0 \le r \le s-1.$$

**Proof.** From Fermat's little theorem: $\left(a^{\frac{p-1}{2}}\right)^2 - 1 \equiv 0 \pmod{p}$, it is:

$$\left(a^{\frac{p-1}{2}} + 1\right)\left(a^{\frac{p-1}{4}} + 1\right) \cdot \ldots \cdot \left(a^{\frac{p-1}{2^{s-1}}} + 1\right)\left(a^{\frac{p-1}{2^s}} + 1\right)\left(a^{\frac{p-1}{2^s}} - 1\right)$$

$$\equiv 0 \pmod{p};$$

so, since $\frac{p-1}{2^s} = t$, we have:

$$(a^t - 1)(a^t + 1)(a^{2t} + 1) \cdot \ldots \cdot (a^{2^{s-2} \cdot t} + 1)(a^{2^{s-1} \cdot t} + 1) = 0 \pmod{p},$$

i.e.: $a^t \equiv 1 \pmod{p}$ or $a^{2^r \cdot t} \equiv -1 \pmod{p}$ for some integer $r$, $0 \le r \le s - 1$.

With reference to the congruence classes $p \equiv 1 \pmod{8}$, $p \equiv 3 \pmod{8}$, $p \equiv 5 \pmod{8}$ and $p \equiv 7 \pmod{8}$, Proposition 3.1 becomes the following.

**Proposition 3.2.** *If* $p$, $p > 2$, *is a prime number such that* $p - 1 = 2^s \cdot t$, $s \in N$, $s \ge 1$, $t \in N$, $t$ *odd, for each integer* $a$ *coprime with* $p$, $1 \le a < p$, *we have*:

a) *if* $p \equiv 1 \pmod{8}$ $(s \ge 3)$, *then we have*: $a^t \equiv 1 \pmod{p}$ *or* $a^{2^r \cdot t} \equiv -1 \pmod{p}$ *for some integer* $r$, $0 \le r \le s - 1$;

b) *if* $p \equiv 3 \pmod{8}$, *then we have*: $a^t \equiv 1 \pmod{p}$ *or* $a^t \equiv -1 \pmod{p}$;

c) *if* $p \equiv 5 \pmod{8}$, *then we have*: $a^t \equiv 1 \pmod{p}$ *or*

$a^t \equiv -1 \ (mod \ p)$ *or* $a^{2t} \equiv -1 \ (mod \ p)$;

d) *if* $p \equiv 7 \ (mod \ 8)$, *then we have*: $a^t \equiv 1 \ (mod \ p)$ *or* $a^t \equiv -1 \ (mod \ p)$.

**Proof.** a) As in Proposition 3.1, (since $p \equiv 1 \ (\text{mod } 8)$, we have $p - 1 = 2^3 \cdot k$, $k \in N$, $k > 1$, that is, $s \geq 3$);

b) in fact, since $p = 8k + 3$, $k \in N$, i.e., $p - 1 = 2(4k + 1)$, $k \in N$, in reference to Proposition 3.1 we have $s = 1$, that is, $r = 0$;

c) in fact, since $p = 8k + 5$, $k \in N$, i.e., $p - 1 = 2^2(2k + 1)$, $k \in N$, in reference to Proposition 3.1 we have $s = 2$, that is, $r = 0$ or $r = 1$;

d) in fact, since $p = 8k + 7$, $k \in N$, i.e., $p - 1 = 2(4k + 3)$, $k \in N$, in reference to Proposition 3.1 we have $s = 1$, that is, $r = 0$.

## 4. On Strong Pseudoprimality to Base 2

Since there are some odd composite integers $n$ that verify the conditions of Proposition 3.1, we can define the strong pseudoprimality as follows.

**Definition 4.1.** If $n$ is an odd composite integer, such that $n - 1 = 2^s \cdot t$, $s \in N$, $s \geq 1$, $t \in N$, $t$ odd, then $n$ is a strong pseudoprime to the integer base $a$ $(spsp(a))$, $1 \leq a < n$, coprime with $n$, if we have:

$a^t \equiv 1 \ (\text{mod } n)$ or $a^{2^r \cdot t} \equiv -1 \ (\text{mod } n)$ for some integer $r$, $0 \leq r \leq s - 1$ (see [2] and [4]).

Regarding to Proposition 3.2, we have the following definition of strong pseudoprimality to integer base $a$, $1 \leq a < n$, coprime with $n$, in reference to congruence classes $n \equiv 1 \pmod{8}$, $n \equiv 3 \pmod{8}$, $n \equiv 5 \pmod{8}$ and $n \equiv 7 \pmod{8}$.

**Definition 4.2.** If $n$ is an odd composite integer, such that $n - 1 = 2^s \cdot t$, $s \in N$, $s \geq 1$, $t \in N$, $t$ odd, then $n$ is a strong pseudoprime to integer base $a$ $(spsp(a))$, $1 \leq a < n$, coprime with $n$, if we have:

$$n \equiv 1 \pmod{8} \ (s \geq 3) \text{ and}$$

$$a^t \equiv 1 \pmod{n} \text{ or } a^{2^r \cdot t} \equiv -1 \pmod{n} \text{ for some integer } r,\ 0 \leq r \leq s - 1$$

or

$$n \equiv 3 \pmod{8} \quad \text{and} \quad (a^t \equiv 1 \pmod{n} \quad \text{or} \quad a^t \equiv -1 \pmod{n})$$

or

$$n \equiv 5 \pmod{8} \text{ and}$$

$$a^t \equiv 1 \pmod{n} \text{ or } a^t \equiv -1 \pmod{n} \text{ or } a^{2t} \equiv -1 \pmod{n}$$

or

$$n \equiv 7 \pmod{8} \text{ and } (a^t \equiv 1 \pmod{n} \text{ or } a^t \equiv -1 \pmod{n}).$$

Since some odd composite integers $n$ satisfy the conditions of Proposition 2.2, it is possible to define the strong pseudoprimality to base 2 in a more synthetic way than Definition 4.2 with $a = 2$ as follows.

**Definition 4.3.** If $n$ is an odd composite integer, such that $n - 1 = 2^s \cdot t$, $s \in N$, $s \geq 1$, $t \in N$, $t$ odd, then $n$ is a strong pseudoprime to base 2 $(spsp(2))$ if we have:

$$n \equiv 1 \pmod{8} \ (s \geq 3) \text{ and}$$

$$2^t \equiv 1 \pmod{n} \text{ or } 2^{2^r \cdot t} \equiv -1 \pmod{n} \text{ for some integer } r,\ 0 \leq r \leq s - 2$$

or

$$n \equiv 3 \pmod{8} \quad \text{and} \quad 2^t \equiv -1 \pmod{n}$$

or

$$n \equiv 5 \pmod{8} \quad \text{and} \quad 2^{2t} \equiv -1 \pmod{n}$$

or

$$n \equiv 7 \pmod{8} \quad \text{and} \quad 2^t \equiv 1 \pmod{n}.$$

**Remark 4.1.** If $n$, $n > 2$, is an odd integer such that $n - 1 = 2^s \cdot t$, $s \in N$, $s \geq 1$, $t \in N$, $t$ odd, considered the proof of Proposition 2.2, to calculate $n \equiv 1 \pmod{8}$, $n \equiv 3 \pmod{8}$, $n \equiv 5 \pmod{8}$ and $n \equiv 7 \pmod{8}$, it is sufficient to compute only $s$ and $t$. In fact we have:

$$n \equiv 1 \pmod{8} \Leftrightarrow s \geq 3;\ n \equiv 3 \pmod{8} \Leftrightarrow s = 1 \text{ and } t = 4k + 1,\ k \in N;$$

$$n \equiv 5 \pmod{8} \Leftrightarrow s = 2;\ n \equiv 7 \pmod{8} \Leftrightarrow s = 1 \text{ and } t = 4k + 3,\ k \in N.$$

We can give Definition 4.3, using only the values $s$ and $t$.

**Definition 4.4.** If $n$ is an odd composite integer, such that $n - 1 = 2^s \cdot t$, $s \in N$, $s \geq 1$, $t \in N$, $t$ odd, then $n$ is a strong pseudoprime to base 2 $(spsp(2))$ if we have:

$$s \geq 3 \ (n \equiv 1 \pmod{8}) \text{ and}$$

$$2^t \equiv 1 \pmod{n} \text{ or } 2^{2^r \cdot t} \equiv -1 \pmod{n} \text{ for some integer } r,\ 0 \leq r \leq s - 2$$

or

$$s = 1 \text{ and } t \equiv 1 \pmod{4} \ (n \equiv 3 \pmod{8}) \text{ and } 2^t \equiv -1 \pmod{n}$$

or

$$s = 2 \ (n \equiv 5 \pmod{8}) \text{ and } 2^{2t} \equiv -1 \pmod{n}$$

or

$$s = 1 \text{ and } t \equiv 3 \pmod{4} \ (n \equiv 7 \pmod{8}) \text{ and } 2^t \equiv 1 \pmod{n}.$$

**4.1. Some examples on the application of Proposition 2.2 and Definition 4.4**

In this section, we study some odd integers, using Proposition 2.2 and Definition 4.4.

**Example 4.1.** Considering $n = 220729$, it is: $n > 2$, $n - 1 = 220728 = 2^3 \cdot 27591$, $s = 3$, $t = 27591$, $220729 \equiv 1 \pmod{8}$; moreover, since we have:

$$2^t = 2^{27591} \equiv 1 \pmod{220729},$$

$n = 220729 = 103 \cdot 2143$ is a $spsp(2)$ (Def. 4.4).

**Example 4.2.** Considering $n = 280601$, it is: $n > 2$, $n - 1 = 280600 = 2^3 \cdot 35075$, $s = 3$, $t = 35075$, $280601 \equiv 1 \pmod{8}$; moreover, since we have:

$$2^t = 2^{35075} \equiv 251179 \not\equiv 1 \pmod{280601},$$

$$2^t = 2^{35075} \equiv 251179 \not\equiv -1 \pmod{280601},$$

$$2^{2^{s-2} \cdot t} = 2^{2t} = 2^{2 \cdot 35075} \equiv -1 \pmod{280601},$$

$n = 280601 = 277 \cdot 1013$ is a $spsp(2)$ (Def. 4.4).

**Example 4.3.** Considering $n = 396271$, it is: $n > 2$, $n - 1 = 396270 = 2 \cdot 198135$, $s = 1$, $t = 198135$, $198135 \equiv 3 \pmod{4}$, $396271 \equiv 7 \pmod{8}$; moreover, since we have:

$$2^t = 2^{198135} \equiv 282542 \not\equiv 1 \pmod{396271},$$

for the counternominal proposition of Proposition 2.2, $n = 396271$ is a composite integer. Furthermore, $n = 396271 = 223 \cdot 1777$ is not a $spsp(2)$ (Def. 4.4).

**Example 4.4.** Considering $n = 489997$, it is: $n > 2$, $n - 1 = 489996 = 2^2 \cdot 122499$, $s = 2$, $t = 122499$, $489997 \equiv 5 \pmod{8}$; moreover, since it is:

$$2^t = 2^{122499} \equiv 249759 \pmod{489997},$$

$$2^{2t} = 2^{2 \cdot 122499} \equiv -1 \pmod{489997},$$

$n = 489997 = 157 \cdot 3121$ is a $spsp(2)$ (Def. 4.4).

**Example 4.5.** Considering $n = 877099$, it is: $n > 2$, $n - 1 = 877098 = 2 \cdot 438549$, $s = 1$, $t = 438549$, $438549 \equiv 1 \pmod{4}$, $877099 \equiv 3 \pmod{8}$; moreover, since we have:

$$2^t = 2^{438549} \equiv -1 \pmod{877099},$$

$n = 877099 = 307 \cdot 2857$ is a $spsp(2)$ (Def. 4.4).

**Example 4.6.** Considering $n = 3828001$, it is: $n > 2$, $n - 1 = 3828000 = 2^5 \cdot 119625$, $s = 5$, $t = 119625$, $3828001 \equiv 1 \pmod{8}$; moreover, since it is:

$$2^t = 2^{119625} \equiv 2879722 \not\equiv 1 \pmod{3828001},$$

$$2^t = 2^{119625} \equiv 2879722 \not\equiv -1 \pmod{3828001},$$

$$2^{2t} = 2^{2 \cdot 119625} \equiv 1174932 \not\equiv -1 \pmod{3828001},$$

$$2^{2^2 \cdot t} = 2^{2^2 \cdot 119625} \equiv 1 \not\equiv -1 \pmod{3828001},$$

$$2^{2^{s-2}\cdot t} = 2^{2^3\cdot t} = 2^{2^3\cdot 119625} \equiv 1 \not\equiv -1 \pmod{3828001},$$

for the counternominal proposition of Proposition 2.2, $n = 3828001$ is a composite integer. Furthermore, $n = 3828001 = 101 \cdot 151 \cdot 251$ is not a $spsp(2)$ (Def. 4.4).

**Example 4.7.** Considering $n = 1251949$, it is: $n > 2$, $n - 1 = 1251948 = 2^2 \cdot 312987$, $s = 2$, $t = 312987$, $1251949 \equiv 5 \pmod{8}$; moreover, since it is:

$$2^t = 2^{312987} \equiv 755566 \pmod{1251949},$$

$$2^{2t} = 2^{2\cdot 312987} \equiv -1 \pmod{1251949},$$

$n = 1251949 = 409 \cdot 3061$ is a $spsp(2)$ (Def. 4.4).

**Example 4.8.** Considering $n = 3421589$, it is: $n > 2$, $n - 1 = 3421588 = 2^2 \cdot 855397$, $s = 2$, $t = 855397$, $3421589 \equiv 5 \pmod{8}$; moreover, since it is:

$$2^t = 2^{855397} \equiv 2301490 \pmod{3421589},$$

$$2^{2t} = 2^{2\cdot 855397} \equiv 358459 \not\equiv -1 \pmod{3421589},$$

for the counternominal proposition of Proposition 2.2, $n = 3421589$ is a composite integer. Furthermore, $n = 3421589 = 131 \cdot 26119$ is not a $spsp(2)$ (Def. 4.4).

**Example 4.9.** Considering $n = 29111881$, it is: $n > 2$, $n - 1 = 29111880 = 2^3 \cdot 3638985$, $s = 3$, $t = 3638985$, $29111881 \equiv 1 \pmod{8}$; moreover, since it is:

$$2^t = 2^{3638985} \equiv -1 \pmod{29111881},$$

$n = 29111881 = 211 \cdot 281 \cdot 491$ is a $spsp(2)$ (Def. 4.4).

**Example 4.10.** Considering $n = 19384289$, it is: $n > 2$, $n - 1 = 19384288 = 2^5 \cdot 605759$, $s = 5$, $t = 605759$, $19384289 \equiv 1 \pmod{8}$; moreover, since it is:

$$2^t = 2^{605759} \equiv 16784867 \not\equiv 1 \pmod{19384289},$$

$$2^t = 2^{605759} \equiv 16784867 \not\equiv -1 \pmod{19384289},$$

$$2^{2t} = 2^{2 \cdot 605759} \equiv 19274464 \not\equiv -1 \pmod{19384289},$$

$$2^{2^2 \cdot t} = 2^{2^2 \cdot 605759} \equiv 4502867 \not\equiv -1 \pmod{19384289},$$

$$2^{2^{s-2} \cdot t} = 2^{2^3 \cdot t} = 2^{2^3 \cdot 605759} \equiv 1 \not\equiv -1 \pmod{19384289},$$

for the counternominal proposition of Proposition 2.2, $n = 19384289$ is a composite integer. Furthermore, $n = 19384289 = 89 \cdot 353 \cdot 617$ is not a $spsp(2)$ (Def. 4.4).

**Example 4.11.** Considering $n = 15247621$, it is: $n > 2$, $n - 1 = 15247620 = 2^2 \cdot 3811905$, $s = 2$, $t = 3811905$, $15247621 \equiv 5 \pmod{8}$; moreover, since we have:

$$2^t = 2^{3811905} \equiv 9141205 \pmod{15247621},$$

$$2^{2t} = 2^{2 \cdot 3811905} \equiv -1 \pmod{15247621},$$

$n = 15247621 = 61 \cdot 181 \cdot 1381$ is a $spsp(2)$ (Def. 4.4).

**Example 4.12.** Considering $n = 612816751$, it is: $n > 2$, $n - 1 = 612816750 = 2 \cdot 306408375$, $s = 1$, $t = 306408375$, $306408375 \equiv 3 \pmod{4}$, $612816751 \equiv 7 \pmod{8}$; moreover, since it is:

$$2^t = 2^{306408375} \equiv 550800674 \not\equiv 1 \pmod{612816751},$$

for the counternominal proposition of Proposition 2.2, $n = 612816751$ is a composite integer. Furthermore, $n = 612816751 = 251 \cdot 751 \cdot 3251$ is not a $spsp(2)$ (Def. 4.4).

**Example 4.13.** Considering $n = 7279379941$, it is: $n > 2$, $n - 1 = 7279379940 = 2^2 \cdot 1819844985$, $s = 2$, $t = 1819844985$, $7279379941 \equiv 5 \pmod{8}$; moreover, since we have:

$$2^t = 2^{1819844985} \equiv 852187010 \pmod{7279379941},$$

$$2^{2t} = 2^{2 \cdot 1819844985} \equiv 4443277458 \not\equiv -1 \pmod{7279379941},$$

for the counternominal proposition of Proposition 2.2, $n = 7279379941$ is a composite integer. Furthermore, $n = 7279379941 = 211 \cdot 3571 \cdot 9661$ is not a $spsp(2)$ (Def. 4.4).

**Example 4.14.** Considering $n = 11239359601$, it is: $n > 2$, $n - 1 = 11239359600 = 2^4 \cdot 702459975$, $s = 4$, $t = 702459975$, $11239359601 \equiv 1 \pmod{8}$; moreover, since it is:

$$2^t = 2^{702459975} \equiv 6448799664 \not\equiv 1 \pmod{11239359601},$$

$$2^t = 2^{702459975} \equiv 6448799664 \not\equiv -1 \pmod{11239359601},$$

$$2^{2t} = 2^{2 \cdot 702459975} \equiv 5391256728 \not\equiv -1 \pmod{11239359601},$$

$$2^{2^{s-2} \cdot t} = 2^{2^2 \cdot t} = 2^{2^2 \cdot 702459975} \equiv 1 \not\equiv -1 \pmod{11239359601},$$

for the counternominal proposition of Proposition 2.2, $n = 11239359601$ is a composite integer. Furthermore $n = 11239359601 = 281 \cdot 4201 \cdot 9521$ is not a $spsp(2)$ (Def. 4.4).

**Example 4.15.** Considering $n = 83828294551$, it is: $n > 2$, $n - 1 = 83828294550 = 2 \cdot 41914147275$, $s = 1$, $t = 41914147275$, $41914147275 \equiv 3 \pmod{4}$, $83828294551 \equiv 7 \pmod{8}$; moreover, since we have:

$$2^t = 2^{41914147275} \equiv 1 \pmod{83828294551},$$

$n = 83828294551 = 1231 \cdot 6151 \cdot 11071$ is a $spsp(2)$ (Def. 4.4).

**Example 4.16.** Considering $n = 3215031751$, it is: $n > 2$, $n - 1 = 3215031750 = 2 \cdot 1607515875$, $s = 1$, $t = 1607515875$, $1607515875 \equiv 3 \pmod{4}$, $3215031751 \equiv 7 \pmod{8}$; moreover, since we have:

$$2^t = 2^{1607515875} \equiv 1 \pmod{3215031751},$$

$n = 3215031751 = 151 \cdot 751 \cdot 28351$ is a $spsp(2)$ (Def. 4.4).

## 5. A Possible Better Implementation of the Baillie-PSW Primality Test

The Baillie-PSW primality test (Pomerance 1984) is a probabilistic algorithm to study the primality of odd integers $n$, $n > 2$, which consists of the following steps (see [1] and [3]).

**Algorithm 1:**

a) A strong pseudoprimality test to base 2 is performed (Definition 4.1 with $a = 2$); if the test is not verified, for the counternominal proposition of Proposition 3.1 with $a = 2$, $n$ is a composite integer and the Algorithm 1 stops, otherwise, if it is verified, since $n$ can be a prime number or a strong pseudoprime to base 2, according to Definition 4.1, you go on to next step;

b) In the sequence $5, -7, 9, -11, \ldots$ the first number $D$ for which the symbol of Jacobi $\left(\frac{D}{n}\right) = -1$ is found; then a Lucas pseudoprimality test with discriminant $D$ on $n$ is performed. If the test is not verified $n$ is a composite integer, otherwise, $n$ is most likely prime.

To improve the above implementation of the Baillie-PSW primality test, with reference to the version of Pomerance (1984) (see [3]), it is possible to apply initially, instead of the strong pseudoprimality test to the base 2, according to the Definition 4.1 with $a = 2$, the strong pseudoprimality test to base 2, according to Definition 4.4. So in detail if $n$, $n > 2$, is an odd integer such that $n - 1 = 2^s \cdot t$, $s \in N$, $s \geq 1$, $t \in N$, $t$ odd, Algorithm 1 becomes the following, which is more synthetic.

**Algorithm 2:**

$\alpha)$ If $s \geq 3$ $(n \equiv 1 \pmod 8)$ you check if it is:

$2^t \equiv 1 \pmod n$ or $2^{2^r \cdot t} \equiv -1 \pmod n$ for some integer $r$, $0 \leq r \leq s - 2$ (5.1); if condition (5.1) is not verified, for the counternominal proposition of Proposition 2.2, $n$ is a composite integer and the Algorithm 2 stops, otherwise, if it is verified, since $n$ can be a prime number or a strong pseudoprime to base $p_1 = 2$, according to Definition 4.4, you go on to next step;

$\alpha_1)$ You apply Step b) of the Algorithm 1;

$\beta)$ If $s = 1$ and $t \equiv 1 \pmod 4$ $(n \equiv 3 \pmod 8)$, you check if it is:

$$2^t \equiv -1 \pmod n; \tag{5.2}$$

if condition (5.2) is not verified, for the counternominal proposition of Proposition 2.2, $n$ is a composite integer and the Algorithm 2 stops, otherwise, if it is verified, since $n$ can be a prime number or a strong pseudoprime to base $p_1 = 2$, according to Definition 4.4, you go on to next step;

$\beta_1)$ You apply Step b) of the Algorithm 1;

$\gamma)$ If $s = 2$ $(n \equiv 5 \pmod 8)$ you check if it is: $2^{2t} \equiv -1 \pmod n$; (5.3)

if condition (5.3) is not verified, for the counternominal proposition of Proposition 2.2, $n$ is a composite integer and the Algorithm 2 stops, otherwise, if it is verified, since $n$ can be a prime number or a strong pseudoprime to base $p_1 = 2$, according to Definition 4.4, you go on to next step;

$\gamma_1)$ You apply Step b) of the Algorithm 1;

$\delta)$ If $s = 1$ and $t \equiv 3 \pmod 4$ $(n \equiv 7 \pmod 8)$, you check if it is:

$$2^t \equiv 1 \pmod n; \qquad (5.4)$$

if condition (5.4) is not verified, for the counternominal proposition of Proposition 2.2, $n$ is a composite integer and the Algorithm 2 stops, otherwise, if it is verified, since $n$ can be a prime number or a strong pseudoprime to base $p_1 = 2$ according to Definition 4.4, you go on to next step;

$\delta_1)$ You apply Step b) of the Algorithm 1.

## 6. Conclusions

If $n$, $n > 2$, is an odd integer such that $n - 1 = 2^s \cdot t$, $s \in N$, $s \geq 1$, $t \in N$, $t$ odd, considering Algorithm 1 (Pomerance 1984) and Algorithm 2, related to the Baillie-PSW primality test, comparing Definition 4.2 with $a = 2$ (see Definition 4.1 with $a = 2$) and Definition 4.4, we can state that:

a) if $s \geq 3$ $(n \equiv 1 \pmod 8)$ it is not necessary to check if it is:

$$2^t \equiv 1 \pmod n \text{ or } 2^{2^r \cdot t} \equiv -1 \pmod n \text{ for some integer } r,\ 0 \leq r \leq s-1,$$

since it is sufficient to check only:

$$2^t \equiv 1 \pmod n \text{ or } 2^{2^r \cdot t} \equiv -1 \pmod n \text{ for some integer } r,\ 0 \leq r \leq s-2;$$

so it is not necessary to check if it is: $2^{2^{s-1} \cdot t} \equiv -1 \pmod n$;

b) if $s = 1$ and $t \equiv 1 \pmod 4$ $(n \equiv 3 \pmod 8)$, it is not necessary to check if it is:

$$2^t \equiv 1 \pmod n \quad \text{or} \quad 2^t \equiv -1 \pmod n,$$

since it is sufficient to check only: $2^t \equiv -1 \pmod n$;

c) if $s = 2$ $(n \equiv 5 \pmod 8)$, it is not necessary to check if it is:

$$2^t \equiv 1 \pmod n \quad \text{or} \quad 2^t \equiv -1 \pmod n \quad \text{or} \quad 2^{2t} \equiv -1 \pmod n,$$

since it is sufficient to check only: $2^{2t} \equiv -1 \pmod n$;

d) if $s = 1$ and $t \equiv 3 \pmod 4$ $(n \equiv 7 \pmod 8)$, it is not necessary to check if it is:

$$2^t \equiv 1 \pmod n \quad \text{or} \quad 2^t \equiv -1 \pmod n,$$

since it is sufficient to check only: $2^t \equiv 1 \pmod n$.

Therefore, some unnecessary checks can be avoided in the implementation of the Baillie-PSW primality test.

## References

[1] R. Baillie and S. S. Wagstaff Jr., Lucas pseudoprimes, Math. Comput. 35(152) (1980), 1391-1417.

[2] R. Crandall and C. Pomerance, Prime Numbers: A Computational Perspective, Springer, seconda edizione, New York, 2005.

[3] C. Pomerance, Are there counter-examples to the Baillie-PSW primality test?, 1984.

[4] C. Pomerance, J. L. Selfridge and S. S. Wagstaff Jr., The pseudoprimes to $25 \cdot 10^9$, Math. Comput. 35(151) (1980), 1003-1026.