Title: Argentest, primality test for Sophie Germain's prime numbers and safe prime numbers.

Author: Zeolla, Gabriel Martin

Comments: 10 pages

gabrielzvirgo@hotmail.com

Keywords: Primality Test, Sophie Germain Prime Numbers, Safe Prime Numbers.

Abstract:

As there is no special primality test for Sophie Germain primes and safe primes as is the case with Fermat primes and Mersenne primes.
Argentest is born, a personal research project that develops a new exclusive deterministic primality test for Sophie Germain's prime numbers and safe prime numbers.

Introduction: Primes building Primes

A prime (P_S) is said to be safe if, in addition to being a prime, it is the result of multiplying a smaller prime (P) by two and adding one to it. For example, the number 23 is a safe prime because 23 = 2 x 11 + 1, where 11 and 23 are prime numbers.
Safe prime numbers are constructed by a Sophie Germain prime number.

Sophie Germain's prime numbers

Characteristics:

$$\mathrm{P} > 2 \equiv 1 \vee 3\ (mod\ 4)$$

$P\ = \{2,3,5,11,23,29,41,53,83,89,113,131,173,179,191,233,239,251,281,293,359,$
$419,431,443,491,509, \ldots\ldots\}$
Referencia OEIS (A005384)

Safe Prime Numbers

With the exception of 7, all safe primes have the form 6n - 1, that is, they are congruent with 5 modulo 6. Similarly, with the exception of 5, all safe primes have the form 4n - 1, that is that is, they are congruent with 3 modulo 4, as can be easily verified, considering that p must be an odd number. Since the least common multiple of 6 and 4 is 12, all safe primes greater than 7 must be able to be expressed in the form 12n - 1, that is, they must be congruent with 11 modulo 12.

Safe Prime Numbers $P_S = (2P + 1)$

$P_S = \{5, 7, 11, 23, 47, 59, 83,107,167, 179,227,263,347,359,383,467,479,503,563,$
$587,719,839,863,887,983, \ldots\ldots\}$
Referencia OEIS (A00538)

Algorithm to determine primality of the prime numbers Sophie Germain

Given an input odd natural number (r), the algorithm checks if (r) is a Sophie Grermain prime number and consequently constructs a safe prime.

The algorithm has a congruence that must be met to have an affirmative result. It combines Euler's criterion with Fermat's little theorem.

The algorithm checks the primality of an odd number (r)
If the algorithm is **affirmative**, (r) will be equal to Sophie Germain's prime number and consequently we will identify a safe prime number in the form (2p + 1).

If the algorithm is **negative**, (r) is not a prime of Sophie Germain and in turn does not construct a safe prime number.

Theorems

Theorem [1]: Fermat's Little Theorem, If p is a prime number, then, for each natural number a, with a> 0

$$a^p \equiv a\,(mod\,p)$$

Theorem [2]: Euler's Criterion
[2.1] Let p> 2 be a prime number and a coprime integer with p. Then a is a quadratic remainder modulo p if and only if

$$2^{\frac{p-1}{2}} \equiv 1\,(mod\,p)$$

[2.2] As a corollary of this theorem, it follows that if a is not a quadratic remainder modulo p then

$$2^{\frac{p-1}{2}} \equiv -1\,(mod\,p)$$

[2.3] It is well known that $2m+1 \mid 2^m - 1$, when 2m + 1 is prime and $2^m - 1$ is composite. Ultimately, a prime number divides a Mersenne number.

[2.4] It is well known that $2m+1 \mid 2^m + 1$, when 2m + 1 is prime and $2^m + 1$ is composite.

Then
But theorem 3 is not sufficient for the development of a proof of primality, since the pseudo-primes are present. The same happens with Theorem [1 and 2].

Example:
$2 * 280 + 1 | \, 2^{280} - 1 \; = \; 561 | \, 2^{280} - 1$
but $561 = 187 * 3$

Then starting from Theorem [2.3] and applying an improvement in the development and combining the Euler criterion with the small Fermat theorem is how the Argentest algorithm works to determine the primality of an odd natural number and validate if it belongs to the primes of Sophie Germain.
In this algorithm the pseudoprimes fail to pass the test, since the base 2 exponent is always a composite number for the pseudoprimes, I have verified this up to the number 500,000,000 with a satisfactory result.

Sophie Germain's Primality Test

$$\exists\ k \in \mathbb{N}/2k+1=r$$

$$r \equiv 1 \vee 3\ (Mod\ 4) \wedge\ 2 \vee 5 \vee 8\ (\text{Mod } 9)$$

$$\frac{2^r \pm 1}{2r+1} \equiv 1 \vee 3(Mod\ r) \rightarrow\ r = P\ \ \wedge\ 2r+1 = P_s$$

$P\ = Sophie\ Germain\ prime > 2$
$P_s = Safe\ Prime$

So in order to execute the algorithm correctly, I separate the algorithm into two variables called Algorithm A and Algorithm B.

Algorithm A

$$\exists\ k \in \mathbb{N}/2k+1=n$$

$$n \equiv 1\ (Mod\ 4) \wedge\ 2 \vee 5 \vee 8\ (\text{Mod } 9)$$

$$\boldsymbol{\frac{2^n+1}{2n+1} \equiv 3(Mod\ n) \rightarrow\ n = P\ \wedge 2n+1 = P_s}$$

Affirmative example of the test: $n = 29$

$$29 \equiv 1\ (Mod\ 4) \wedge\ \ \mathbf{2}\ (\text{Mod } 9)$$

$$\frac{2^{29}+1}{59} \equiv 3(Mod\ 29) \rightarrow\ 29 = P\ \ \wedge (2*29+1) = 59 = P_s$$

Negative test example: $n = 65$

$$65 \equiv 1\ (Mod\ 4) \wedge\ \ \mathbf{2}\ (\text{Mod } 9)$$

$$\frac{2^{65}+1}{131} \not\equiv 3(Mod\ 65) \rightarrow\ 65 \neq P\ \ \wedge (2*65+1) = 131 \neq P_s$$

Proof A: Primality test of (n, q)
$q =\ \text{Safe}\ prime$
$n =\ Sophie\ Germain\ prime$

By definition of a safe prime number we know that:

$$q = 2n+1 \rightarrow\ n = \frac{q-1}{2}$$

<u>Part One</u>: I demonstrate the primality of (q)

$$\frac{2^n+1}{2n+1}$$

Theorem [2.4]

$$2n+1 | 2^n+1$$

Then

$$= 2^n+1 \equiv 0(mod\ 2n+1)$$

Replacement (n)

$$= 2^{\frac{q-1}{2}}+1 \equiv 0(mod\ q)$$

$$\boldsymbol{= 2^{\frac{q-1}{2}} \equiv -1(mod\ q)}$$

Euler's criterion[2.2]

Part Two: I demonstrate the primality of(n)

$$\frac{2^n+1}{2n+1} \equiv 3(Mod\; n)$$

$$= 2^n + 1 \equiv 3(2n+1)(Mod\; n)$$
$$= 2^n + 1 \equiv 6n + 3\;(Mod\; n)$$

$$Then\; 6n \equiv 0\;(Mod\; n)$$
$$= 2^n + 1 \equiv 3\;(Mod\; n)$$
$$\therefore \mathbf{2^n \equiv 2\;(Mod\; n)}$$

Fermat's little theorem [1]

This implies that if both congruences work (n) it will be a prime number of Sophie Germain.

Algorithm B:

$$\exists\; k \in \mathbb{N}/2k + 1 = m$$

$$m \equiv 3\;(Mod\; 4) \wedge\;\; 2 \vee 5 \vee 8\;(\mathrm{Mod}\; 9)$$
$$\frac{2^m-1}{2m+1} \equiv 1(Mod\; m) \rightarrow\; m = P\;\; \wedge 2m+1 = P_s$$

Affirmative example of the test: $n = 83$

$$83 \equiv 3\;(Mod\; 4) \wedge\; 2\;\;(\mathrm{Mod}\; 9)$$
$$\frac{2^{83}-1}{167} \equiv 1(Mod\; 83) \rightarrow\; 83 = P\;\; \wedge (2*83+1) = 167 = P_s$$

Negative test example: $n = 35$

$$35 \equiv 3\;(Mod\; 4) \wedge\; 8\;(\mathrm{Mod}\; 9)$$
$$\frac{2^{35}-1}{71} \not\equiv 1(Mod\; 35) \rightarrow\; 35 \neq P\;\; \wedge (2*35+1) = 71 \neq P_s$$

Proof B: Primality test of (m, q)
$q =$ Safe $prime$
$m =\;\; Sophie\; Germain\; prime$

By definition of a safe prime number we know:

$$q = 2m + 1 \rightarrow\; m = \frac{q-1}{2}$$

Part One: I demonstrate the primality of (q)

$$\frac{2^m-1}{2m+1}$$

Theorem [2.3]

$$2m + 1 | 2^m - 1$$

Then

$$= 2^m - 1 \equiv 0(mod\; 2m+1)$$

Replacement (m)

$$= 2^{\frac{q-1}{2}} - 1 \equiv 0 (mod\ q)$$

$$= \mathbf{2^{\frac{q-1}{2}} \equiv 1 (mod\ q)}$$

$$\text{Euler's criterion [2.1]}$$

Second part: I demonstrate the primality of (m)

$$\frac{2^m - 1}{2m+1} \equiv 1 (Mod\ m)$$

$$= 2^m - 1 \equiv 1(2m+1)(Mod\ m)$$

$$=2^m - 1 \equiv 2m + 1\ (Mod\ m)$$

$$= 2^m \equiv 2m + 2\ (Mod\ m)$$

Entonces $2m \equiv 0\ (Mod\ m)$

$$\therefore \mathbf{2^m \equiv 2 (Mod\ m)}$$

Fermat's little theorem [1]

This implies that if both congruences work (m) will be a prime number of Sophie Germain.

Inverse algorithm for determining primality of the safe prime numbers

Given an input odd natural number (z), the algorithm checks if (z) is a Safe prime number and consequently it is constructed by another Sophie Germain prime number.

The algorithm has a congruence that must be met to have an affirmative result. It combines Euler's criterion with Fermat's little theorem.

The algorithm checks the primality of (z)
If the algorithm is **affirmative** (z) it will be a safe prime number and consequently
(p-1) / 2 will be Sophie Germain's prime number.

If the algorithm is **negative** (z) it is not a safe prime number and consequently it is not built by a cousin of Sophie Germain.

$P = Sophie\ Germain\ prime$ >2
$P_s = Safe\ prime$

Safe prime numbers have the following characteristic:

$$P_s > 5 \equiv 3\ (mod\ 4)$$

Primality Test Algorithm for Safe Prime Numbers

$$\exists\ k \in \mathbb{N}/2k + 1 = z$$

$$k \equiv 1 \vee 3\ (Mod\ 4) \wedge\ 2 \vee 5 \vee 8\ (\text{Mod } 9)$$

$$\frac{2^{\frac{z-1}{2}} + 1}{z} \equiv\ 1 \vee 3 \left(Mod\ \frac{z-1}{2}\right) \rightarrow\ z = P_s \wedge \frac{z-1}{2} = P = k$$

So in order to execute the algorithm correctly I separate the algorithm into two variables called Algorithm C and Algorithm D.

Algorithm C

$$\exists\ k \in \mathbb{N}/2k + 1 = n$$

$$k \equiv 1\ (Mod\ 4) \wedge\ 2 \vee 5 \vee 8\ (\text{Mod } 9)$$

$$\frac{2^{\frac{n-1}{2}} + 1}{n} \equiv 3 \left(Mod\ \frac{n-1}{2}\right) \rightarrow\ n = P_s \wedge \frac{n-1}{2} = P = k$$

Affirmative example of the test: $n = 59$

$$\frac{59-1}{2} \equiv 1\ (Mod\ 4) \wedge\ \ 2\ (\text{Mod } 9)$$

$$\frac{2^{\frac{59-1}{2}}+1}{59} \equiv 3\left(Mod\ \frac{59-1}{2}\right)$$

$$\frac{2^{29}+1}{59} \equiv 3(Mod\ 29) \rightarrow\ 59 = P_s \wedge \left(\frac{59-1}{2}\right) = 29 = P$$

Negative test example: $n = 131$

$$\frac{131-1}{2} \equiv 1\ (Mod\ 4) \wedge\ 2\ (\text{Mod } 9)$$

$$\frac{2^{\frac{131-1}{2}}+1}{131} \equiv 3\left(Mod\ \frac{131-1}{2}\right)$$

$$\frac{2^{65}+1}{131} \not\equiv 3(Mod\ 65) \rightarrow\ 65 \neq P_s \wedge \left(\frac{65-1}{2}\right) = 131 \neq P$$

Proof C: Primality test of (n, q)
$n =\ Safe\ prime$
$q =\ Sophie\ Germain\ prime$

By definition of a safe prime number we know that a safe prime number (n) is equal:

$$n = 2q + 1 \rightarrow\ q = \tfrac{n-1}{2}$$

<u>Part One:</u> We demonstrate the primality of (n)

$$\frac{2^{\frac{n-1}{2}}+1}{n}$$
$$= 2^{\frac{n-1}{2}} + 1 \equiv 0(mod\ n)$$
$$= \boldsymbol{2^{\frac{n-1}{2}} \equiv -1(mod\ n)}$$
$$\text{Euler's criterion[2.2]}$$

<u>Part Two:</u> We Prove the Primality of (q)

$$\frac{2^{\frac{n-1}{2}}+1}{n} \equiv 3\left(Mod\ \frac{n-1}{2}\right)$$

Replacement

$$\frac{2^q+1}{2q+1} \equiv 3(Mod\ q)$$

$$2^q + 1 \equiv 3(2q+1)(Mod\ q)$$
$$= 2^q + 1 \equiv 6q + 3\ (Mod\ q)$$

$$Then\ 6q \equiv 0\ (Mod\ q)$$
$$= 2^q + 1 \equiv 3\ (Mod\ n)$$
$$\therefore \boldsymbol{2^n \equiv 2\ (Mod\ n)}$$

Fermat's little theorem [1]

This implies that if both congruences work (n) will be a Safe prime number and (n-1) / 2 will be a Sophie Germain prime number.

Algorithm D

$$\exists\, k \in \mathbb{N}/2k + 1 = m$$
$$k \equiv 3\ (Mod\ 4) \wedge\ \ 2 \vee 5 \vee 8\ (\text{Mod } 9)$$

$$\frac{2^{\frac{m-1}{2}} - 1}{m} \equiv 1 \left(Mod\ \frac{m-1}{2}\right) \rightarrow\ m = P_s\ \wedge \frac{m-1}{2} = P = k$$

Affirmative example of the test: $m = 167$

$$\frac{167-1}{2} \equiv 3\ (Mod\ 4) \wedge\ \ \mathbf{2}\ \vee\ 5\ \vee\ 8\ (\text{Mod } 9)$$

$$\frac{2^{\frac{167-1}{2}} - 1}{167} \equiv 1 \left(Mod\ \frac{167-1}{2}\right)$$

$$\frac{2^{83} - 1}{167} \equiv 1(Mod\ 83) \rightarrow\ 167 = P_s\ \wedge \left(\frac{167-1}{2}\right) = 83 = P$$

Negative test example: $m = 71$

$$\frac{71-1}{2} \equiv 3\ (Mod\ 4) \wedge\ \ \mathbf{2}\ \vee\ 5\ \vee\ 8\ (\text{Mod } 9)$$

$$\frac{2^{\frac{71-1}{2}} - 1}{71} \equiv 1 \left(Mod\ \frac{71-1}{2}\right)$$

$$\frac{2^{35} - 1}{71} \not\equiv 1(Mod\ 35) \rightarrow\ 71 \neq P_s\ \wedge \left(\frac{167-1}{2}\right) = 35 \neq P$$

Proof D: Primality test of (m, q)
$m =\ Safe\ prime$
$q =\ Sophie\ Germain\ prime$

By definition of a safe prime number we know that a safe prime number (m) is equal:

$$m = 2q + 1 \rightarrow\ q = \frac{m-1}{2}$$

Part One: I demonstrate the primality of (m)

$$\frac{2^{\frac{m-1}{2}}-1}{m}$$
$$=2^{\frac{m-1}{2}}-1\equiv 0(mod\,m)$$
$$=\boldsymbol{2^{\frac{m-1}{2}}\equiv 1\,(mod\,m)}$$
$$\text{Euler's criterion}[2.1]$$

Part Two: I demonstrate the primality of (q)

$$\frac{2^{\frac{m-1}{2}}-1}{m}\equiv 1\left(Mod\,\frac{m-1}{2}\right)$$

Replacement

$$\frac{2^{q}-1}{2q+1}\equiv 1(Mod\,q)$$

$$=2^{q}-1\equiv 1(2q+1)(Mod\,q)$$
$$=2^{q}-1\equiv 2q+1\,(Mod\,q)$$
$$=2^{q}\equiv 2q+2\,(Mod\,q)$$

Then $2q\equiv 0\,(Mod\,q)$

$$\boldsymbol{\therefore 2^{q}\equiv 2(Mod\,q)}$$
$$\text{Fermat's little theorem }[1]$$

This implies that if both congruences work (m) it will be a Safe prime number and
(m-1) / 2 will be a prime number of Sophie Germain.

Conclution

Argentets works with perfect determination and manages to pinpoint the primality of the primes of Sophie Germain and of the Safe primes efficiently.

The algorithm presents very simple and limited mechanisms in comparison with other existing primality tests. Since it calculates in 2 simple steps the primality of two closely related numbers.

Without a doubt, Argentest is fabulous for its simplicity and speed, computationally very fast and easy to program for the use of large numbers.

Professor Zeolla Gabriel Martín
San Vicente, Buenos Aires, Argentina.
2021

References

1. Löh, Günter (1989), "Cadenas largas de números primos casi duplicados”, Matemáticas de la computación , 53 (188): 751–759, doi : 10.1090 / S0025-5718-1989-0979939-8 , MR 0979939 .
2. Rivest, Ronald L.; Silverman, Robert D. (22 de noviembre de 1999), ¿Se necesitan primos 'fuertes' para RSA? (PDF)
3. Cheon, Jung Hee (2006), "Análisis de seguridad del problema fuerte de Diffie-Hellman", 24a Conferencia Internacional Anual sobre Teoría y Aplicaciones de Técnicas Criptográficas (EUROCRYPT'06), San Petersburgo, Rusia, 28 de mayo - 1 de junio, 2006, Actas (PDF), Lecture Notes in Computer Science , 4004 , Springer-Verlag, págs. 1-11, doi : 10.1007 / 11761679_1 .
4. Gordon, John A. (1985), "Los números primos fuertes son fáciles de encontrar", Actas de EUROCRYPT 84, Un taller sobre la teoría y aplicación de técnicas criptográficas, París, Francia, 9 al 11 de abril de 1984, Notas de la conferencia en computadora Science, 209, Springer-Verlag, págs. 216-223, doi : 10.1007 / 3-540-39757-4_19.
5. Yap, Wun-She; Yeo, Sze Ling; Heng, Swee-Huay; Henricksen, Matt (2013), "Análisis de seguridad de GCM para comunicaciones", Redes de seguridad y comunicación, doi : 10.1002 / sec.798.
6. Agrawal, Manindra; Kayal, Neeraj; Saxena, Nitin (2004), "PRIMES is in P" (PDF), Annals of Mathematics, 160 (2): 781–793, doi: 10.4007 / annals.2004.160.781, JSTOR 3597229
7. I.A. G. Nemron. Sophie Germain primes. J. Discrete Math. Sci. & Crypt. 11, 6, 715-726 (2008)
8. M. Mascagni, H. Chi. Parallel Linear Congruential generators with Sophie Germain moduli. Parallel Computing. 30, 11, 1217-1231 (2004).