# REVISTA MULTIDISCIPLINAR EPISTEMOLOGÍA DE LAS CIENCIAS

Volumen 2, Número 1
Enero- Marzo 2025

Edición Trimestral

CROSSREF PREFIX DOI: 10.71112

Revista Multidisciplinar Epistemología de las Ciencias

Volumen 2, Número 1
enero- marzo 2025

Publicación trimestral
Hecho en México

La Revista Multidisciplinar Epistemología de las Ciencias acepta publicaciones de cualquier área del conocimiento, promoviendo una plataforma inclusiva para la discusión y análisis de los fundamentos epistemológicos en diversas disciplinas. La revista invita a investigadores y profesionales de campos como las ciencias naturales, sociales, humanísticas, tecnológicas y de la salud, entre otros, a contribuir con artículos originales, revisiones, estudios de caso y ensayos teóricos. Con su enfoque multidisciplinario, busca fomentar el diálogo y la reflexión sobre las metodologías, teorías y prácticas que sustentan el avance del conocimiento científico en todas las áreas.

Contacto principal: admin@omniscens.com





## Cintillo legal

Revista Multidisciplinar Epistemología de las Ciencias Vol. 2, Núm. 1, enero-marzo 2025, es una publicación trimestral editada por el Dr. Moises Ake Uc, C. 51 #221 x 16B , Las Brisas, Mérida, Yucatán, México, C.P. 97144 , Tel. 9993556027, Web: https://www.omniscens.com, admin@omniscens.com, Editor responsable: Dr. Moises Ake Uc. Reserva de Derechos al Uso Exclusivo No. 04-2024-121717181700-102, ISSN: 3061-7812, ambos otorgados por el Instituto Nacional del Derecho de Autor (INDAUTOR). Responsable de la última actualización de este número, Dr. Moises Ake Uc, fecha de última modificación, 1 enero 2025.

Revista Multidisciplinar Epistemología de las Ciencias

Volumen 2, Número 1, 2025, enero-marzo

DOI: https://doi.org/10.71112/0pq8fb18

# SOBRE LA SOLUCIÓN A UN PROBLEMA PENDIENTE:

# NO EXISTE UN COMPUESTO C QUE SATISFAGA LA ECUACIÓN $2^{c-1} \equiv 1 \ (mod\ c^2)$

# ABOUT THE SOLUTION TO A PENDING PROBLEM:

# THERE IS NO COMPOUND C THAT SATISFIES THE EQUATION $2^{c-1} \equiv 1 \ (mod\ c^2)$

**Alexander José Villarroel Salazar**

**Francisco Javier Villarroel Rosillo**

**Venezuela**

DOI: https://doi.org/10.71112/0pq8fb18

# Sobre la solución a un problema pendiente: no existe un compuesto c que satisfaga la ecuación $2^{c-1} \equiv 1\ (mod\ c^2)$

# About the solution to a pending problem: there is no compound c that satisfies the equation $2^{c-1} \equiv 1\ (mod\ c^2)$

Alexander José Villarroel Salazar[1]
alexvills76@gmail.com
https://orcid.org/0000-0002-4628-1894
Investigador independiente
Venezuela.

Francisco Javier Villarroel Rosillo[2]
fjvillr02@gmail.com
https://orcid.org/0000-0002-9159-5892
Investigador independiente
Venezuela.

## RESUMEN

En el presente artículo se hace un estudio de las posibles soluciones de la ecuación $2^{c-1} \equiv 1\ (mod\ c^2)$ para determinar que solo los números compuestos impares pueden ser posibles soluciones. Luego se asume $c = 2k + 1$ para llegar a expresiones del tipo $4^k - 1$ y por medio del estudio desde $k = 1\ a\ k = 70$ y la inserción a la teoría de números del concepto de "primos codependientes del exponente k", del cual se muestran ejemplos, así como características de su uso, se llega a argumentos matemáticos que evidencian la inexistencia de algún número compuesto que satisfaga la ecuación indicada. A lo largo del artículo se hace la relación entre los factores primos y los exponentes, se presentan tablas explicativas y argumentos de los exponentes y los posibles divisores (factores primos) para llegar a concluir que es imposible la existencia de soluciones.

**Palabras clave:** aritmética modular, divisibilidad, factorización, números primos, números compuestos, m.c.m., pequeño teorema de Fermat

**ABSTRACT**

In this article, a study is made of the possible solutions of the equation 2^(c-1)≡1 (mod c^2 ) to determine that only odd composite numbers can be possible solutions. Then, c=2k+1 is assumed to arrive at expressions of the type 〖4〗^k-1 and through the study from k=1 to k=70 and the insertion into the number theory of the concept of “codependent primes of the exponent k”, of which examples are shown, as well as characteristics of its use, mathematical arguments are reached that show the nonexistence of any composite number that satisfies the indicated equation. Throughout the article, the relationship between the prime factors and the exponents is made, explanatory tables and arguments of the exponents and the possible divisors (prime factors) are presented to conclude that the existence of solutions is impossible.

**Keywords**: modular arithmetic, divisibility, factorization, prime numbers, composite numbers, l.c.m., Fermat's little theorem

Recibido: 21 de diciembre 2024 | Aceptado: 27 de marzo 2025

## INTRODUCCIÓN

Desde la aparición de la teoría de aritmética modular y de las congruencias en el libro de disquisiciones aritméticas de Gauss en 1801 son muchos los problemas que han surgido en base a congruencias estudiando diversos aspectos de los números primos y compuestos.

En la list of unsolved problems in math, que se encuentra en Google en la sección de teoría de números presenta varios problemas pendientes, entre los cuales están los siguientes:

- Problema 1: Are there any composite c satisfying $2^{c-1} \equiv 1\ (mod\ c^2)$?
- Problema 2: ¿Can a prime p satisfy $2^{p-1} \equiv 1\ (mod\ p^2)$ and $3^{p-1} \equiv 1\ (mod\ p^2)$ simultaneously ?
- Problema 3: For any given integer a > 0, are there infinitely many primes p such that $a^p - 1 \equiv 1\ (mod\ p^2)$?

El objetivo del presente artículo es resolver el problema 1 de los 3 enunciados en la lista de problemas irresueltos en matemáticas. Por tal motivo, a lo largo de este artículo se usan una serie de argumentos matemáticos para determinar la posible existencia de soluciones para el problema 1.

## METODOLOGÍA

Luego de presentar la base referencial en los resultados se sigue un proceso de trabajo que se basará en lo siguiente:

- Se estudiarán en la ecuación de congruencia original los casos de posibles soluciones para compuestos pares o impares del exponente.
- Se expresará la ecuación original en congruencias en función de las posibles soluciones para crear una expresión de trabajo.
- Posteriormente, se hará un estudio de los números compuestos que puedan ser posibles soluciones y se hace uso de la estrategia de Villarroel y Villarroel (2022) y Villarroel y Villarroel (2023) respecto a triángulos generadores de números compuestos para determinar los valores de los exponentes $(k)$ y de los posibles divisores $(2k+1)$ compuestos
- Se definirán los “primos codependientes del exponente k”, mostrando programas en lenguaje C, ejemplos de su aplicación en factorización y los detalles de su aparición en diversos exponentes

- Se tabulan las potencias de la expresión de trabajo $4^k - 1$ para determinar sus factores primos para valores desde $k = 1\ a\ k = 70$
- Se hará uso de la teoría de "primos codependientes del exponente $k$" para comprobar que no hay soluciones para valores desde $k = 1\ a\ k = 70$, analizando el comportamiento de los primos codependientes.
- Se harán apreciaciones sobre las posibilidades de obtener el divisor total $(2k + 1)^2$ en las diferentes expresiones $4^k - 1$
- Por último, se estudiarán los exponentes y posibles divisores tomando en cuenta la figura 2, la tabla 1 y la ecuación 4 y usando ciertos criterios de divisibilidad de los posibles divisores considerando los factores existentes y los factores pendientes por ser hallados para explicar la improbabilidad de que se den coincidencias y soluciones desde k=70 hasta infinito.

1. Preliminares

   A continuación, se presentan aspectos relacionados con el problema tratado como lo son la aritmética modular, la divisibilidad y la factorización, los números primos y compuestos y el pequeño teorema de Fermat.

   1.1 Aritmética modular

Villarroel y Villarroel (2022, p.321) citan a Gracián (2010, p.97) quien menciona que "En la aritmética modular de Gauss se habla de congruencias en vez de igualdades, de manera que la forma correcta de referirse a la expresión 17 ≡ 2 modulo 5 es «17 es congruente con 2 módulo 5». Para saber si dos números cualesquiera son congruentes módulo 5 basta con hacer la diferencia y ver si el resultado es múltiplo de 5.

82 ≡ 58 (mod 4) porque 82 - 58 = 24, que es múltiplo de 4.

Por su parte, Koscielny et al. (2013) al definir congruencia establecen lo siguiente

Sean $a, b\ y\ n$ números naturales ($a, b, n \in \mathbb{N};\ n \neq 0$). Si dos enteros, a y b, tienen el mismo resto cuando se dividen entre n entonces se dice que son congruentes módulo n. Denotamos esto por $a \equiv b\ mod\ n$. En símbolos:

$$a \equiv b\ mod\ n \leftrightarrow (a\ mod\ n) = (b\ mod\ n)$$

Sobre las congruencias Tillborg y Jajodia (2011) indican una serie de propiedades importantes respecto a las congruencias:

1. $N \equiv 0\ (mod\ N)$
2. $A + 0 \equiv A\ (mod\ N)$
3. $1 \times A \equiv A\ (mod\ N)$
4. $si\ A \equiv B\ (mod\ N), entonces\ B \equiv A\ (mod\ N)$
5. $si\ A \equiv B\ (mod\ N) \wedge B \equiv C\ (mod\ N), entonces\ A \equiv C\ (mod\ N)$
6. $si\ A \equiv B\ (mod\ N) \wedge C \equiv d\ (mod\ N), entonces\ A\ +\ C \equiv B\ +\ d\ (mod\ N)$
7. $si\ A \equiv B\ (mod\ N) \wedge C \equiv d\ (mod\ N), entonces\ A \times C \equiv B \times d\ (mod\ N)$
8. $A + B \equiv B + A\ (mod\ N)$
9. $A \times B \equiv B \times A\ (mod\ N)$
10. $A + (B + C) \equiv (A\ +\ B) + C\ (mod\ N)$
11. $A \times (B \times C) \equiv (A \times B) \times C\ (mod\ N)$
12. $A \times (B + C) \equiv (A \times B)\ +\ (A \times C)\ (mod\ N)$

Respecto al mismo tema, Villarroel y Villarroel (2023) citan a Gauss (1965), Zaragoza and Cipriano (2009, p. 25) e Include Poetry (2020)

1.2. Divisibilidad y factorización

Villarroel y Villarroel (2023) citan aspectos variados acerca de la factorización y la divisibilidad donde planteados por Bodi (2008, p. 20). Al estudiar sobre los criterios de divisibilidad en los libros de teoría de números y buscar en las páginas web hay estudios importantes entre los cuales pueden citarse: Mora (2010, pp. 51-52) presenta una sección titulada trucos de divisibilidad donde presenta la división entre 2, 3, 9 y 11; Niven y Zuckerman (1976, pp. 9-19) trata sobre conceptos de divisibilidad sin detenerse al estudio de divisores particulares; Varona (2019, pp.32-39) expone el tema de divisibilidad y habla sobre criterios de divisibilidad; Otros autores que estudian sobre divisibilidad son Dickson(2005), Bogomolny (2018), McDowell (2018) y Blancas (2020).

Sin embargo, las estrategias de divisibilidad planteadas por los autores mencionados son muy incompletas pues no brindan gran información sobre todos los divisores. Al respecto, el artículo de Villarroel y Villarroel (2023) es muy interesante en relación a este tema, ya que constituye un importante referente en cuanto al tema de la divisibilidad entre diversos divisores se refiere

Según Romo (2023, p.33) Dados dos números enteros $a, b$ , se dirá que $a$ divide a $b$, o que $b$ es divisible entre $a$, y se escribe $a \mid b$ , cuando exista un tercer número entero $c$ tal que $a\ c\ =\ b$. Además, respecto a la división exacta, Tiborashi (2020, p.42-43) indica que “Dados

dos enteros $x\ e\ y$ decimos que $y$ es un divisor de $x$ y escribimos $y|x\ \ si\ x = yq$ para algún $q\ \epsilon\ Z$. También se dice que $y$ es un factor de $x$ o divide a $x$, que x es divisible entre $y$ o que es múltiplo de y".

**Tabla 1**

*Factorización de $a^n - 1$ con a=2 hasta a 10 y n=1 hasta n=12*

| | | |
|---|---|---|
| 2^(1)-1=1 | 3^(1)-1=2 | 4^(1)-1=3 |
| 2^(2)-1=3 | 3^(2)-1=2*2*2 | 4^(2)-1=3*5 |
| 2^(3)-1=7 | 3^(3)-1=2*13 | 4^(3)-1=3*3*7 |
| 2^(4)-1=3*5 | 3^(4)-1=2*2*2*2*5 | 4^(4)-1=3*5*17 |
| 2^(5)-1=31 | 3^(5)-1=2*11*11 | 4^(5)-1=3*11*31 |
| 2^(6)-1=3*3*7 | 3^(6)-1=2*2*2*7*13 | 4^(6)-1=3*3*5*7*13 |
| 2^(7)-1=127 | 3^(7)-1=2*1093 | 4^(7)-1=3*43*127 |
| 2^(8)-1=3*5*17 | 3^(8)-1=2*2*2*2*2*5*41 | 4^(8)-1=3*5*17*257 |
| 2^(9)-1=7*73 | 3^(9)-1=2*13*757 | 4^(9)-1=3*3*3*7*19*73 |
| 2(10)-1=3*11*31 | 3^(10)-1=2*2*2*11*11*61 | 4^(10)-1=3*5*5*11*31*41 |
| 2(11)-1=23*89 | 3^(11)-1=2*23*3851 | 4^(11)-1=3*23*89*683 |
| 2(12)-1=3*3*5*7*13 | 3^(12)-1=2*2*2*2*5*7*13*73 | 4^(12)-1=3*3*5*7*13*17*241 |
| 5^(1)-1=2*2 | 6^(1)-1=5 | 7^(1)-1=2*3 |
| 5^(2)-1=2*2*2*3 | 6^(2)-1=5*7 | 7^(2)-1=2*2*2*2*3 |
| 5^(3)-1=2*2*31 | 6^(3)-1=5*43 | 7^(3)-1=2*3*3*19 |
| 5^(4)-1=2*2*2*2*3*13 | 6^(4)-1=5*7*37 | 7^(4)-1=2*2*2*2*2*3*5*5 |
| 5^(5)-1=2*2*11*71 | 6^(5)-1=5*5*311 | 7^(5)-1=2*3*2801 |
| 5^(6)-1=2*2*2*3*3*7*31 | 6^(6)-1=5*7*31*43 | 7^(6)-1=2*2*2*2*3*3*19*43 |
| 5^(7)-1=2*2*19531 | 6^(7)-1=5*55987 | 7^(7)-1=2*3*29*4733 |
| 5^(8)-1=2*2*2*2*2*3*13*313 | 6^(8)-1=5*7*37*1297 | 7^(8)-1=2*2*2*2*2*2*3*5*5*1201 |
| 5^(9)-1=2*2*19*31*829 | 6^(9)-1=5*19*43*2467 | 7^(9)-1=2*3*3*3*19*37*1063 |
| 5^(10)-1=2*2*2*3*11*71*521 | 6^(10)-1=5*5*7*11*101*311 | 7^(10)-1=2*2*2*2*3*11*191*2801 |
| 5^(11)-1=2*2*12207031 | 6^(11)-1=5*23*3154757 | 7^11)-1=2*3*1123*293459 |
| | 6^(12)-1=5*7*13*31*37*43*97 | |

| | | |
|---|---|---|
| 5^(12)-1=2*2*2*2*3*3*7*13*31*601 | | 7^(12)-1=2*2*2*2*2*3*3*5*5*13*19*43*181 |
| 8^(1)-1=7<br>8^(2)-1=3*3*7<br>8^(3)-1=7*73<br>8^(4)-1=3*3*5*7*13<br>8^(5)-1=7*31*151<br>8^(6)-1=3*3*3*7*19*73<br>8^(7)-1=7*7*127*337<br>8^(8)-1=3*3*5*7*13*17*241<br>8^(9)-1=7*73*262657<br>8^(10)-1=3*3*7*11*31*151*331<br>8^(11)-1=7*23*89*599479<br>8^(12)-1=3*3*3*5*7*13*19*37*73*109 | 9^(1)-1=2*2*2<br>9^(2)-1=2*2*2*2*5<br>9^(3)-1=2*2*2*7*13<br>9^(4)-1=2*2*2*2*2*5*41<br>9^(5)-1=2*2*2*11*11*61<br>9^(6)-1=2*2*2*2*5*7*13*73<br>9^(7)-1=2*2*2*547*1093<br>9^(8)-1=2*2*2*2*2*2*5*17*41*193<br>9^(9)-1=2*2*2*7*13*19*37*757<br>9^(10)-1=2*2*2*2*5*5*11*11*61*1181<br>9^(11)-1=2*2*2*23*67*661*3851<br>9^(12)-1=2*2*2*2*2*5*7*13*41*73*6481 | 10^(1)-1=3*3<br>10^(2)-1=3*3*11<br>10^(3)-1=3*3*3*37<br>10^(4)-1=3*3*11*101<br>10^(5)-1=3*3*41*271<br>10^(6)-1=3*3*3*7*11*13*37<br>10^(7)-1=3*3*239*4649<br>10^(8)-1=3*3*11*73*101*137<br>10^(9)-1=3*3*3*3*37*333667<br>10^(10)-1=3*3*11*41*271*9091<br>10^(11)-1=3*3*21649*513239<br>10^(12)-1=3*3*3*7*11*13*37*101*9901 |

Fuente: Elaboración propia de los autores

En la tabla 1 se presenta los procesos de factorización de los resultados de las potencias hasta exponente 12 de las bases que van desde 2 hasta 10. Las bases se indican fuera de paréntesis y los exponentes se indican dentro de paréntesis en la parte izquierda de cada igualdad. Se pueden apreciar los siguientes aspectos importantes

- Las potencias de cada exponente 4 depende de los factores de la potencia del exponente 2,
- Las potencias de cada exponente 6 dependen de los factores de las potencias de exponentes 2 y 3,

- Las potencias de cada exponente 8 dependen de los factores de exponente 4,
- Las potencias de exponente 10 dependen de los factores de las potencias de exponentes 2 y 5
- Las potencias de exponente 12 dependen de los factores de las potencias de exponentes 4 y 6

Además, puede verse que las potencias de exponente primo 2, 3, 5, 7 y 11 son generadores de primos cada vez más grandes que no han aparecido en potencias previas de ninguna otra base. Vea por ejemplo que:

- Para las potencias de exponente 7: se generan un conjunto de primos 127, 1093, 19531, 55987, 4733, 377, 4069. Se repite 127 que aparece en las potencias de base 2, de base 4 y de base 8 y se repite 1093 en el caso de las bases 3 y 9
- Para las potencias de exponente 11: se generan un conjunto de primos 23, 89, 3851, 683, 12207031, 3154757, 1123, 293459, 599479, 67, 661, 21649, 513239. Para las potencias de base 3 y base 9 e igual pasa con el 89 en el caso de las bases 2, 4 y 8 y se repite 3851 en el caso de base 3 y 9 con exponente 11.
- Siempre hay aspectos similares para cada uno de los exponentes

### 1.3. Números primos y compuestos

Pace (2012) al referirse a los números primos, señala que “son números mayores que 1, que son exactamente divisibles solo por 1 y ellos mismos”, tienen una larga historia en matemáticas, ya que se relacionan con la noción de números atómicos, es decir, que no pueden ser construidos como un producto de números más pequeños. Para probar si un número tiene varios divisores se debe probar con números primos en forma ascendente los cuales son:

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97, \ldots$$

Los números compuestos son aquellos que aparte de ser divisibles entre 1 y n también deben tener un divisor entre uno o más de los divisores de 2 y n-1, es decir, como mínimo tienen 3 divisores, pudiendo existir hasta números ampliamente compuestos debido a la gran cantidad de factores primos que poseen.

Respecto a los números primos, los autores Villarroel y Villarroel (2022, p.325) citan a los autores García (2005, p.87), Mora (2010, p.17), y Bernaschini(2017, p.30) y en su otro

artículo, Villarroel y Villarroel (2023, p.4) citan a Niven y Zuckerman (2004), Burton (1965) y Pérez (2022) quienes hacen importantes apreciaciones sobre los números primos.

1.4. Mínimo común múltiplo (m.c.m.)

Romo (2023, p. 39) al hablar acerca del mínimo común múltiplo menciona que "Dados dos números positivos a, b, el conjunto de múltiplos comunes a ambos no está vacío, pues a*b es un múltiplo común, y está acotado inferiormente por max(a, b). Luego, tiene sentido definir el mínimo común múltiplo de a y b como el menor de los múltiplos comunes a ambos, y se denotará por [a, b]"

Aquí se usará el concepto de mínimo común múltiplo de los factores comunes de las potencias de la forma $\boldsymbol{a^{ki} - 1\ con\ k1, k2, k3, hasta\ kn}$ según la forma del exponente n en la expresión $\boldsymbol{a^n - 1}$, lo cual será explicado al presentar en los resultados los factores primos que dependen del exponente $\boldsymbol{n}$. Sin embargo, la consideración de estos detalles será ampliado en la sección resultados **en una forma más amplia.**

1.5. Pequeño teorema de Fermat

Según Zhao (2004) Alrededor de 1636, Pierre de Fermat enunció el teorema. Aparece en una de sus cartas a su confidente Frénicle de Bessy, fechada el 18 de octubre de 1640, con el siguiente texto:

*p* divide a $a^{p-1}$ - 1 cuando *p* sea primo y *a* sea coprimo con *p*.

Es decir, que el pequeño teorema de Fermat afirma que si, $p$ es cualquier número primo y $a$ es cualquier entero tal que $p \nmid a$, entonces $a^{p-1} \equiv 1\ (mod\ p)$.

Según Euler (1741) la primera demostración publicada se debe a Leonhard Euler en 1736 y daría otras dos demostraciones más a lo largo de su vida, la primera demostración era un manuscrito de Gottfried Leibniz de 1683 y que nunca publicó. Por otra parte, Caldwell (1994) señala que "Gauss publicó una prueba más en su libro Disquisitiones Arithmeticae en 1801", lo cual es también referido por Barrantes et al. (2006)

## RESULTADOS

A partir de la ecuación originalmente dada en el título del artículo, se deduce

$$2^{c-1} - 1 \equiv 0\ (mod\ c^2)\ \ (ecuación\ 1)$$

2.1. Soluciones para exponentes compuestos pares o impares

En la (ecuación 1) si c es un compuesto par entonces $2^{c-1}$ es par, por lo cual $2^{c-1}-1$ es impar y así $c^2$ es par, pero como no hay ningún impar que sea divisible entre un divisor par entonces la división es imposible, lo que indica que no pueden existir soluciones para valores de c par. Además, si en la (ecuación 1) c es un compuesto impar entonces $2^{c-1}$ es par, por lo cual $2^{c-1}-1$ es impar y así $c^2$ es impar, como un impar puede ser divisible entre otro impar, entonces la división es posible, lo cual indica que si es posible (pero no seguro) que haya soluciones para valores de c impar.

2.2. Posibles valores solución

Dado que todo exponente compuesto c impar puede escribirse en la forma general:

$$c = 2k+1 \; para \; algún \; k \; \in \aleph \; \; (ecuación\; 2)$$

Es posible sustituir la (ecuación 2) en la (ecuación 1), de lo cual se obtiene que:

$$2^{c-1}-1 \equiv 0 \; mod \; (c^2)$$

$$2^{(2k+1)-1}-1 \equiv 0 \; mod \; ((2k+1)^2)$$

$$2^{2k}-1 \equiv 0 \; mod \; ((2k+1)^2)$$

$$4^{k}-1 \equiv 0 \; mod \; ((2k+1)^2) \; \; (ecuación\; 3)$$

La ecuación anterior plantea la división exacta indicada por la ecuación:

$$4^k-1 = q((2k+1)^2) \; con \; q \; \epsilon \; \aleph \; \; (ecuación\; 4)$$

2.3. Uso del triángulo generador de números compuestos

Villarroel y Villarroel en sus artículos de (2022) y (2023) establecieron los llamados triángulos generadores de números compuestos, los cuales son una herramienta útil en base a las congruencias. Aunque en aquellos artículos implementaron el uso de dichos triángulos con un sentido de exclusión de los compuestos para hallar posteriormente los primos, en este artículo lo usan para determinar los valores del exponente k, que generan posibles divisores compuestos $2k+1$. Por lo tanto, se deben buscar entonces los valores de k que hacen que $2k+1$ sea siempre un número compuesto.

Al proceder como en los artículos citados con:

$$c1 = 2k+1 \; (ecuación\; 5)$$

En $ecuación\; 5$ se determina que el exponente "$c1$" es compuesto para los valores de k = 4, 7, 10, 12, 13, 16, 17, 19, 22, 24, 25, 27, 28, 31, 32, 34, 37, 38, 40, 42, 43, 45, 47, 49, 52, 55, 57, 58, 59, 60, 61, 62, 64, … y así sucesivamente. Lo anterior puede representarse en el

siguiente triángulo generador que permite ir determinando los siguientes valores que dan números compuestos**.**

**Figura 1**

*Triángulo generador de los exponentes k*

4

7 7

10 12 10

13 17 17 13

16 22 24 22 16

19 27 31 31 27 19

22 32 38 40 38 32 22

25 37 45 49 49 45 37 25

28 42 52 58 60 58 52 42 28

31 47 59 67 71 71 67 59 47 31

34 52 66 76 82 84 82 76 66 52 34

37 57 73 85 93 97 97 93 85 73 57 37

40 62 80 94 104 110 112 110 104 94 80 62 40

43 67 87 103 115 123 127 127 123 115 103 87 67 43

Fuente: Elaboración propia de los autores

Los valores de k se evalúan en ecuación 5 y resultan los posibles divisores c resultando los valores

9, 15, 21, 25, 27, 33, 35, 39, 45, 49, 51, 55, 57, 63, 65, 69, 75, 77, 81, 85, 87, 91, 93, 95, 99, 105, 111, 115, 117, 119, 121, 123, 125, 129, 133, 135, 141, 143, 145, y los siguientes compuestos. Lo anterior puede generalizarse en el siguiente triángulo que permite seguir hallando los compuestos sin la necesidad de tanteo y comprobación en 2k+1.

**Figura 2**

*Triángulo generador de divisores compuestos del tipo 2k+1*

9

15 15

21 25 21

27 35 35 27

33 45 49 45 33

39 55 63 63 55 39

45 65 77 81 77 65 45

51 75 91 99 99 91 75 51

57 85 105 117 121 117 105 85 57

63 95 119 135 143 143 135 119 95 63

69 105 133 153 165 169 165 153 133 105 69

75 115 147 171 187 195 195 187 171 147 115 75

81 125 161 189 209 221 225 221 209 189 161 125 81

87 135 175 207 231 247 255 255 247 231 207 175 135 87

Fuente: Elaboración propia de los autores

Es preciso estudiar las expresiones $\boldsymbol{4^k - 1}$ en cuanto a su factorización en los exponentes k generados en la figura 1, tomando los divisores presentados en la figura 2 estudiando su expresión en factores primos y los factores faltantes de manera de apreciar si en los primeros valores se da una coincidencia que permita visualizar la divisibilidad entre $(2k+1)^2$ según lo expresado en la ecuación 4.

Esto es importante para posteriormente establecer una serie de argumentos matemáticos importantes para la comprensión y solución del problema. Entre esos argumentos están la consideración de los factores primos de las expresiones generales de la forma $a^n - 1$ en relación a la base a y al exponente n

2.4. Factores primos de $a^n - 1$

2.4.1. Factores dependientes de la base.

Si tenemos $\boldsymbol{a^n - 1}$ hay dos factores dependientes de la base que son siempre $\boldsymbol{a - 1}$ y $\boldsymbol{a + 1}$. Ambos factores pueden aparecer con exponente 1 o superior. Se cumple que:

- $\boldsymbol{(a - 1)}$ aparece siempre que el exponente $n$ de $\boldsymbol{a^n - 1}$ es impar

- Tanto $(\boldsymbol{a-1})$ como $(\boldsymbol{a+1})$ aparecen siempre que $\boldsymbol{n}$ es par, es decir, aparecen en toda expresión $\boldsymbol{a^{2k}-1}$

En muchos casos ambos factores pueden aparecer con exponente superior a 1.

2.4. 2. Factores dependientes de los exponentes.

El exponente $n$ puede ser primo o compuesto, por ello es pertinente hacer el análisis de los casos.

2.4. 2.1. Para exponentes compuestos

En este artículo, se tomará cada exponente n como un m.c.m y se usarán los primos que lo generan como sus divisores (sin tomar en cuenta exponentes de los primos)

Y para efectos de factorización se tomará el m.c.m de los factores de las expresiones del tipo $\boldsymbol{a^{ki}-1}$

Proposición:

Siempre que se tenga una expresión de la forma $a^n$-1 con n compuesto entonces según la expresión en factores primos del exponente n que se tenga

$n = p1^{a1} * p2^{b1} * p3^{c1} *$ … (Ecuación 6)

Se hallarán cocientes para cada uno de los primos que sean bases en el número n por medio de:

$k1 = \frac{n}{p1}, k2 = \frac{n}{p2}, k3 = \frac{n}{p3}$ …. (ecuación 7)

De manera que siempre la expresión $a^n - 1$ es divisible entre el mínimo de los factores de las potencias cuyos exponentes sean los cocientes previos:

$$a^n - 1 = q * \left[m.c.m\left(factores\left(a^{k1}-1, a^{k2}-1, \quad a^{k3}-1, \ldots.\right)\right)\right], con\ q \epsilon \aleph$$

(ecuación 8)

Y esto ocurre indiferentemente de la base $a$ y el exponente $n$ que se tenga y de los valores de $a1, b1, c1$ de los exponentes de los primos en la descomposición factorial que representen al exponente n, según lo indicado en la (ecuación 6)

En la proposición puede verse que se parte de los conceptos elementales de la diferencia de cuadrados y la diferencia de cubos, los cuales están dados por las ecuaciones:

$a^{2n} - 1 = (a^n - 1)\ (a^n - 1)$ (ecuación 9)

$a^{3n} - 1 = (a^n - 1)\ (a^{2n} + a^n + 1)$ (ecuación 10)

Los cuales se aplican reiterativamente para los diferentes exponentes que se tengan.

Primer ejemplo:

Supongamos que tengamos que factorizar $\boldsymbol{a^{24}-1}$ entonces $\boldsymbol{n=24=2^3*3}$ es un m.c.m que depende de las bases $\boldsymbol{2\ y\ 3}$ entonces se buscan dos cocientes:

k1 $=\frac{24}{2}=12\ y\ k2=\frac{24}{3}=8$

En este caso $\boldsymbol{a^{24}-1}$ dependerá del $m.c.m.\left(factores\ (a^{12}-1, a^8-1)\right)$, es decir, es divisible entre dicho m.c.m. En efecto, puede expresarse por diferencia de cuadrados y diferencia de cubos lo siguiente:

$a^{24}-1=(a^{12}-1)(\ a^{12}+1)$

$a^{24}-1=(a^8-1)(\ a^{16}+a^8+1)$

Aquí se observa que ciertamente $a^{24}-1$ depende de $a^{12}-1$ y $a^8-1$

Puede verse que para $24$ sus divisores propios son $1, 2, 3, 4, 6, 8, 12\ y\ 12$ contiene a los números $1, 2, 3, 4, 6$, pero no contiene al $8$ entonces en la factorización de $24$ entrarán factores de $12\ y\ 8$

Segundo ejemplo:

Para $a^{60}-1$ se tiene que $60=2^2\times3\times5$, entonces $60$ es un m.c.m que depende de las bases $2, 3\ y\ 5$**,** por lo cual se buscan 3 cocientes:

$$k1=\frac{60}{2}=30,\qquad k2=\frac{60}{3}=20\ \ y\ \ k3=\frac{60}{5}=12$$

Es decir, que $a^{60}-1$ es divisible (tiene por factor o contiene) entre el

$$m.c.m.\left(factores(\ a^{30}-1, a^{20}-1, a^{12}-1)\right).$$

Puede verse que los divisores de **60** son:

$1, 2, 3, 4, 5, 6, 10, 12, 15, 20, 30$ y ocurre que $30$ contiene a $1, 2, 3, 5, 6, 10, 15$ (que se eliminan) quedan sin incluir $4, 12, 20$ y $\boldsymbol{20}$ contiene a $\boldsymbol{4}$ por lo que quedan $12, 20\ y\ 30$ que corresponden a los cocientes $k1. k2\ y\ k3$ antes hallados

Tercer ejemplo**:**

Para $a^8-1$ Tenemos que $8=2^3$ que depende de una sola base que es $2\ y\ \frac{8}{2}=4$ por lo cual $a^8-1$ contiene en su factorización a los factores de $a^4-1$

Entonces para expresiones que dependen de un solo primo como $a^{27}-1$ se trabaja con $a^9-1$ y para $a^{125}-1$ se usa $a^{25}-1$. Es decir que en el caso de tener un exponente n

que dependa de una potencia de un único primo siempre se usa la potencia del primo al exponente anterior al de n.

Nota: En general si un número tiene una descomposición en factores primos con 100 primos diferentes se deben calcular los cocientes desde k1 a k100 y buscar el mínimo de las potencias que tienen como exponentes a los mencionados cocientes.

2.4.2.2. Para exponentes primos

En el caso de expresiones de la forma $\boldsymbol{a^n - 1}$ donde el exponente n sea alguno de los números primos es imposible encontrar factores en potencias previas excepto en $\mathbf{a^1 - 1}$, ya que todo primo es solo divisible entre 1 y el mismo primo.

Esto sucede porque a similitud de la prueba de Euclides de infinitos primos (ver Romo (2023, p.54), Apóstol (2020, p. 19), Sardonil y Varona (2021, p.5)**)** la existencia de exponentes primos es generador de primos cada vez más grandes de acuerdo al valor del exponente $n$ que se tenga y dichos primos tienden a ser cada vez más grandes a medida que aumenta el exponente.

Nota importante: para evitar los procesos anteriores es que se toma a $n$ como un m.c.m y se divide entre cada una de las bases primas que lo generan, ya que ese procedimiento es muchísimo más directo que buscar todos los divisores y ver cuáles son coprimos (determinando cuales contienen a otros). De esta manera, con la búsqueda del mínimo común múltiplo de los factores se avanza sustancialmente en la factorización para expresiones donde los exponentes son números compuestos.

2.5. Otros factores primos de expresiones $a^k - 1$

En los incisos 2.4.1. y 2.4.2. se plantean factores relacionados con la base y con los exponentes sean estos primos o compuestos. Sin embargo, en la factorización de expresiones de la forma $a^n - 1$, en muchos casos aparecen factores primos que son más grandes que el exponente. Esto puede apreciarse en la siguiente tabla:

**Tabla 2**

*Factorización de potencias de base 2 a base 4 exponentes de 1 a 12*

| Potencias de base 2 | Potencias de base 3 | Potencias de base 4 |
|---|---|---|
| $2^1 - 1 = 1$ | $3^1 - 1 = 2$<br>Contiene a 2 que deben aparecer en todas las potencias de exponente impar | $4^1 - 1 = 3$<br>Contiene a 3 que deben aparecer en todas las potencias de exponente impar |
| $2^2 - 1 = 3$<br>Contiene a 3 y 5 que deben aparecer en todas las potencias de exponente par | $3^2 - 1 = 2^3$<br>Contiene a 3 y 5 que deben aparecer en todas las potencias de exponente par | $4^2 - 1 = 3 \times 5$<br>Contiene a 3 y 5 que deben aparecer en todas las potencias de exponente par |
| $2^3 - 1 = 7$<br>Es primo | $3^3 - 1 = 2 \times 13$<br>$contiene\ a\ 2$<br>$falta\ 13$ | $4^3 - 1 = 3^2 \times 7$<br>$contiene\ a\ 3$<br>$falta\ 7$ |
| $2^4 - 1 = 3 * 5$<br>$contiene\ 3\ falta\ 5$ | $3^4 - 1 = 2^4 \times 5$<br>$contiene\ a\ 2\ \ y\ a\ 4$<br>$falta\ \ 5$ | $4^4 - 1 = 3 \times 5 \times 17$<br>$contiene\ a\ 3\ y\ 5$<br>$falta\ 17$ |
| $2^5 - 1 = 31$<br>Es primo | $3^5 - 1 = 2 \times 11^2$<br>$contiene\ a\ 2$<br>$falta\ 11$ | $4^5 - 1 = 3 \times 11 \times 31$<br>$contiene\ al\ 3$<br>$falta\ 11\ y\ 31$ |
| $2^6 - 1 = 3^2 \times 7$<br>$contiene\ 3\ y\ 7$ | $3^6 - 1 = 2^3 \times 7 \times 13$<br>$contiene\ 2^3 y\ 13$<br>$falta\ 7$ | $4^6 - 1 = 3^2 \times 5 \times 7 \times 13$<br>$contiene\ 3^2 \times 5 \times 7$<br>$falta\ 13$ |
| $2^7 - 1 = 127$ | $3^7 - 1 = 2 \times 1093$ | $4^7 - 1 = 3 \times 43 \times 127$ |

| Es primo | $Contiene\ a\ 2$<br>$Falta\ 1093$ | $contiene\ a\ 3$<br>$faltan\ 43\ y\ 127$ |
|---|---|---|
| $2^8 - 1 = 3 * 5 * 17$<br>$contiene\ 3y5$<br>$falta\ 17$ | $3^8 - 1 = 2^5 \times 5 \times 41$<br>$Contiene\ a\ 2^4 \times 5$<br>$falta\ 41$ | $4^8 - 1 = 3 \times 5 \times 17 \times 257$<br>$contiene\ a\ 3 \times 5 \times 17$<br>$falta\ 257$ |
| $2^9 - 1 = 7 * 73$<br>$contiene\ 7$<br>$falta\ 73$ | $3^9 - 1 = 2 \times 13 \times 757$<br>$Contiene\ a\ 2 \times 13$<br>$Falta\ 757$ | $4^9 - 1 = 3^2 \times 7 \times 19 \times 73$<br>$contiene\ 3^2 * 7$<br>$faltan\ 19\ y\ 73$ |
| $2^{10} - 1 = 3 * 11 * 31$<br>$contiene\ 3\ y\ 31$<br>$falta\ 11$ | $3^{10} - 1 = 2^3 \times 11^2 \times 617$<br>$contiene\ 2^3 \times 11^2$<br>$Falta\ 61$ | $4^{10} - 1 = 3 \times 5^2 \times 11 \times 31 \times 41$<br>$contiene\ a\ 3 \times 5 \times 11 \times 31$<br>$falta\ 41$ |
| $2^{11} - 1 = 23 \times 89$<br>$contiene\ a\ 1$<br>$faltan\ 23\ y\ 89$ | $3^{11} - 1 = 2 \times 23 \times 3851$<br>$contiene\ a\ 2$<br>$faltan\ 23\ y\ 3851$ | $4^{11} - 1 = 3 * 23 * 89 * 683$<br>$contiene\ a\ 3$<br>$faltan\ 23, 89\ y\ 683$ |
| $2^{12} - 1 = 3^2 \times 5 \times 7 \times 13$<br>Contiene a $3^2 \times 5 \times 7$<br>Falta 13 | $3^{12} - 1 = 2^4 \times 5 \times 7 \times 13 \times 73$<br>$contien\ e\ 2^4 \times 5 \times 7 \times 13$<br>$Falta\ 73$ | $4^{12} - 1 = 3^2 \times 5 \times 7 \times 13 \times 17 \times 241$<br>$contiene\ a\ 3^2 \times 5 \times 7 \times 13 \times 17$<br>$falta\ 241$ |

Fuente: Elaboración propia de los autores

2.6.- Primos codependientes del exponente n.

Es pertinente en este punto hacer la introducción a la teoría de números de los que hemos llamados primos codependientes del exponente $n$ que se denotan $p(\rightarrow n)$ que se definen como aquellos primos de la forma:

$p(\rightarrow n) = kn + 1\ con\ k \epsilon \aleph\ y\ siempre\ p(\rightarrow n) es\ primo$ (ecuación 11)

A continuación, se presenta la lista de los 100 primeros primos codependientes para cada uno de los exponentes de 3, 5 y 7.

Exponente= 3

7 , 13 , 19 , 31 , 37 , 43 , 61 , 67 , 73 , 79 , 97 , 103 , 109 , 127 , 139 , 151 , 157 , 163 , 181 , 193 , 199 , 211 , 223 , 229 , 241 , 271 , 277 , 283 , 307 , 313 , 331 , 337, 349 , 367 , 373 , 379 , 397 , 409 , 421 , 433 , 439 , 457 , 463 , 487 , 499 , 523 , 541, 547 , 571 , 577 , 601 , 607 , 613 , 619 , 631 , 643 , 661 , 673 , 691 , 709 , 727 , 733, 739 , 751 , 757 , 769 , 787 , 811 , 823 , 829 , 853 , 859 , 877 , 883 , 907 , 919 , 937, 967 , 991 , 997 , 1009 , 1021 , 1033 , 1039 , 1051 , 1063 , 1069 , 1087 , 1093 , 1117, 1123 , 1129 , 1153 , 1171 , 1201 , 1213 , 1231 , 1237 , 1249 , 1279 , 1291 , 1297 , 1303 , 1321 , 1327 , 1381 , 1399 , 1423 , 1429 , 1447 , 1453 , 1459 , 1471 , 1483 , 1489 , 1531 , 1543 , 1549 , 1567 , 1579 , 1597 , 1609 , 1621 , 1627 , 1657 , 1663 , 1669 , 1693 , 1699 , 1723 , 1741 , 1747 , 1753 , 1759 , 1777 , 1783 , 1789 , 1801 , 1831 , 1861 , 1867 , 1873 , 1879 , 1933 , 1951 , 1987 , 1993 , 1999 , 2011 , 2017 , 2029 , 2053 , 2083 , 2089 , 2113 , 2131 , 2137 , 2143 , 2161 , 2179 , 2203 , 2221 , 2239 , 2251 , 2269 , 2281 , 2287 , 2293 , 2311 , 2341 , 2347 , 2371 , 2377 , 2383 , 2389 , 2437 , 2467 , 2473 , 2503 , 2521 , 2539 , 2551 , 2557 , 2593 , 2617 , 2647 , 2659 , 2671 , 2677 , 2683 , 2689 , 2707 , 2713 , 2719 , 2731 , 2749 , 2767 , 2791 , 2797 , 2803 , 2833 , 2851 , 2857 , 2887 , 2917 , 2953 , 2971 , 3001.

Exponente=5

11 , 31 , 41 , 61 , 71 , 101 , 131 , 151 , 181 , 191 , 211 , 241 , 251 , 271 , 281 , 311 , 331 , 401 , 421 , 431 , 461 , 491 , 521 , 541 , 571 , 601 , 631 , 641 , 661 , 691 , 701, 751 , 761 , 811 , 821 , 881 , 911 , 941 , 971 , 991 , 1021 , 1031 , 1051 , 1061 , 1091, 1151 , 1171 , 1181 , 1201 , 1231 , 1291 , 1301 , 1321 , 1361 , 1381 , 1451 , 1471 , 1481 , 1511 , 1531 , 1571 , 1601 , 1621 , 1721 , 1741 , 1801 , 1811 , 1831 , 1861 , 1871 , 1901 , 1931 , 1951 , 2011 , 2081 , 2111 , 2131 , 2141 , 2161 , 2221 , 2251 , 2281 , 2311 , 2341 , 2351 , 2371 , 2381 , 2411 , 2441 , 2521 , 2531 , 2551 , 2591 , 2621 , 2671 , 2711 , 2731 , 2741 , 2791 , 2801 , 2851 , 2861 , 2971 , 3001 , 3011 , 3041 , 3061 , 3121 , 3181 , 3191 , 3221 , 3251 , 3271 , 3301 , 3331 , 3361 , 3371 , 3391 , 3461 , 3491 , 3511 , 3541 , 3571 , 3581 , 3631 , 3671 , 3691 , 3701 , 3761 , 3821 , 3851 , 3881 , 3911 , 3931 , 4001 , 4021 , 4051 , 4091 , 4111 , 4201 , 4211 , 4231 , 4241 , 4261 , 4271 , 4391 , 4421 , 4441 , 4451 , 4481 , 4561 , 4591 , 4621 , 4651 , 4691 , 4721 , 4751 , 4801 , 4831 , 4861 , 4871 , 4931 , 4951 .

Exponente=7

29 , 43 , 71 , 113 , 127 , 197 , 211 , 239 , 281 , 337 , 379 , 421 , 449 , 463 , 491 , 547 , 617 , 631 , 659 , 673 , 701 , 743 , 757 , 827 , 883 , 911 , 953 , 967 , 1009 , 1051 , 1093 , 1163 , 1289 , 1303 , 1373 , 1429 , 1471 , 1499 , 1583 , 1597 , 1667 , 1709 , 1723 , 1877 , 1933 , 2003 , 2017 , 2087 , 2129 , 2143 , 2213 , 2269 , 2297 , 2311 , 2339 , 2381 , 2423 , 2437 , 2521 , 2549 , 2591 , 2633 , 2647 , 2689 , 2731 , 2801 , 2843 , 2857 , 2927 , 2969 , 3011 , 3067 , 3109 , 3137 , 3221 , 3319 , 3347 , 3361 , 3389 , 3529 , 3557 , 3571 , 3613 , 3697 , 3739 , 3767 , 3823 , 3851 , 3907 , 4019 , 4159 , 4201 , 4229 , 4243 , 4271 , 4327 , 4397 , 4481 , 4523 , 4621 , 4649 , 4663 , 4691 , 4733 , 4789 , 4817 , 4831 , 4943 , 4957 , 4999 , 5153 , 5167 , 5209 , 5237 , 5279 , 5419 , 5503 , 5531 , 5573 , 5657 , 5741 , 5783 , 5839 , 5867 , 5881 , 5923 , 6007 , 6091 , 6133 , 6203 , 6217 , 6287 , 6301 , 6329 , 6343 , 6427 , 6469 , 6553 , 6581 , 6637 , 6679 , 6763 , 6791 , 6833 , 6917 , 6959 , 7001.

El lector al detallar los primos de tabla 1 puede apreciar que los primos codependientes aparecen completos en el caso de la potencia 3 y 5 y que en el caso de la potencia 7 faltan los primos 19531 y 55987, pero la (ecuación 11) puede usarse para probar si un número primo es codependiente de un exponente n en una forma muy sencilla.

**Nota importante**: Sería ilógico y muy poco intuitivo (matemáticamente hablando), esperar que una expresión de la forma $\boldsymbol{a^n - 1}$ dependa de primos que no guarden ninguna relación con los valores de $\boldsymbol{a}$ y $\boldsymbol{n}$.

A continuación, se presentan unos ejemplos de verificaciones que han sido realizadas usando la calculadora online Alpertron

Ejemplo 1:

$$2^{178} - 1 = 383123885216472214589586756787577295904684780545900 54$$
$$= 3 \times 179 \times 62020897 \times 18584774046020617$$
$$\times 61897001964269013744956 2111$$

Al trabajar con los primos de la línea anterior ocurre que:

Los divisores relacionados con la base son 1 y 3. Además, 179 que es primo cumple con el teorema de Fermat, ya que es divisor de la potencia presentada.

En cuanto a los otros primos que son factores debe probarse si son primos codependientes del exponente 178. Para ello se divide el compuesto previo a cada primo entre 178 y si cada división es exacta entonces ciertamente los primos son codependientes de 178

$$\frac{62020896}{178} = 348432$$

$$\frac{18584774046020616}{178} = 104408842955172$$

$$\frac{6189700196426901374495621 10}{178} = 347735966091398953623 3495$$

Es obvio que los primos son entonces codependientes con el exponente 178

**2.8. Descomposición factorial de potencias de la forma $4^k - 1$**

Si se retoman los valores de la figura 1 y de figura 2 para ubicar respectivamente los exponentes $k$ y los divisores $2k + 1$ al cuadrado y para cada valor se buscan sus factores primos, tomando los exponentes que generan divisores compuestos hasta 70 se pueden observar los comportamientos de los diversos factores y hacer una verificación importante acerca de los factores primos que se obtienen en el proceso. De hacer lo antes indicado resulta la siguiente tabla de valores que se presenta a continuación:

**Tabla 3**

*Factores de $4^k - 1$ para exponentes según figura 1*

| Potencia | Factorización realizada con la calculadora en línea alpertron | Divisor Cuadr | Expresión en primos | Factores faltantes |
|---|---|---|---|---|
| $4^4 - 1$ | $3 * 5 * 17$ | 1 | 3*3*3*3 | 3*3*3 |
| $4^7 - 1$ | $3 * 43 * 127$ | 25 | 3*3*5*5 | 3*5*5 |
| $4^{10} - 1$ | $3 * 5^2 * 11 * 31 * 41$ | 41 | 3*3*7*7 | 3*7*7 |
| $4^{12} - 1$ | $3^2 * 5 * 7 * 13 * 17 * 241$ | 25 | 5*5*5*5 | 5*5*5 |
| $4^{13} - 1$ | $3 * 2731 * 8191$ | 29 | 3*3*3*3*3 | 3*3*3*3*3 |
| $4^{16} - 1$ | $3 * 5 * 17 * 257 * 65537$ | 089 | 3*3*11*11 | 3*11*11 |

| | | | | |
|---|---|---|---|---|
| $4^{19}-1$ | $3*174763*524287$ | 521 | 3*3*13*13 | 3*13*13 |
| $4^{22}-1$ | $3*5*23*89*397*683*2113$ | 025 | 3*3*3*5*5 | 3*3*3*5 |
| $4^{24}-1$ | $3^2*5*7*13*17*97*241*257*673$ | 401 | 7*7*7*7 | 7*7*7 |
| $4^{25}-1$ | $3*11*31*251*601*1801*4051$ | 601 | 3*3*17*17 | 3*17*17 |
| $4^{27}-1$ | $3^4*7*19*73*87211*262657$ | 025 | 5*5*11*11 | 5*5*11*11 |
| $4^{28}-1$ | $3*5*17*29*43*113*127*15790321$ | 249 | 3*3*19*19 | 3*19*19 |
| $4^{31}-1$ | $3*715827883*2147483647$ | 969 | 3*3*3*7*7 | 3*3*3*7*7 |
| $4^{32}-1$ | $3*5*17*257*641*65537*6700417$ | 225 | 5*5*13*13 | 5*13*13 |
| $4^{34}-1$ | $3*5*137*953*26317*43691*131071$ | 761 | 3*3*23*23 | 3*23*23 |
| $4^{37}-1$ | $3*223*1777*25781083*616318177$ | 625 | 3*3*5*5*5*5 | 3*5*5*5*5 |
| $4^{38}-1$ | $3*5*229*457*174763*524287*525313$ | 929 | 7*7*11*11 | 7*7*11*11 |
| $4^{40}-1$ | $3*5^2*11*17*31*41*257*61681*4278255361$ | 561 | 3*3*3*3*3*3*3 | 3*3*3*3*3*3*3 |
| $4^{42}-1$ | $3^2*5*7^2*13*29*43*113*127*337*1429*5419*14449$ | 225 | 5*5*17*17 | 5*17*17 |

| | | | | |
|---|---|---|---|---|
| $4^{43}-1$ | $3*431*9719*2099863*2932031007403$ | 569 | 3*3*29*29 | 3*29*29 |
| $4^{45}-1$ | $3^3*7*11*19*31*73*151*331*631*23311*18837001$ | 281 | 7*7*13*13 | 7*13*13 |
| $4^{46}-1$ | $3*5*47*277*1013*1657*30269*178481*2796203$ | 649 | 3*3*31*31 | 3*31*31 |
| $4^{47}-1$ | $3*283*2351*4513*13264529*165768537521$ | 025 | 5*5*19*19 | 5*5*19*19 |
| $4^{49}-1$ | $3*43*127*4363953127297*4432676798593$ | 801 | 3*3*3*11*11 | 3*3*3*11*11 |
| $4^{52}-1$ | $3*5*17*53*157*1613*2731*8191*858001*308761441$ | 1025 | 3*3*5*5*7*7 | 3*5*7*7 |
| $4^{55}-1$ | $3*11^2*23*31*89*683*881*2971*3191*201961*48912491$ | 2321 | 3*3*37*37 | 3*37*37 |
| $4^{57}-1$ | $3^2*7*571*32377*174763*524287*1212847*160475489$ | 3225 | 5*5*23*23 | 5*5*23 |
| $4^{58}-1$ | $3*5*59*233*1103*2089*3033169*107367629*536903681$ | 3689 | 3*3*3*13*13 | 3*3*3*13*13 |
| $4^{59}-1$ | $3*2833*37171*179951*1824726041*3203431780337$ | 4161 | 7*7*17*17 | 7*7*17*17 |
| $4^{60}-1$ | $3^2*5^2*7*11*13*17*31*41*61*151*241*331*1321*61681*4562284561$ | 4641 | 11*11*11*11 | 11*11*11 |
| $4^{61}-1$ | $3*768614336404564651*2305843009213693951$ | 5129 | 3*3*41*41 | 3*41*41 |

| | | | | |
|---|---|---|---|---|
| $4^{62}-1$ | $3*5*5581*8681*49477*384773*715827883*2147483647$ | 5625 | 5*5*5*5*5*5 | 5*5*5*5*5 |
| $4^{66}-1$ | $3^2*5*7*13*23*67*89*397*683*2113*20857*312709*599479*4327489$ | 7689 | 7*7*19*19 | 7*19*19 |
| $4^{67}-1$ | $3*7327657*193707721*761838257287*6713103182899$ | 8225 | 3*3*3*3*3*3*5*5 | 3*3*3*3*5*5 |
| $4^{70}-1$ | $3*5^2*11*29*31*41*43*71*113*127*281*86171*122921*7416361*47392381$ | 9881 | 3*3*47*47 | 3*47*47 |

Elaboración propia de los autores

De la tabla 3 puede observarse que siempre hay más de un factor faltante en la última columna, lo cual indica que para los exponentes hasta 70 es imposible que se dé la división exacta planteada en la ecuación 4.

2.9. Factores primos de $4^k-1$ y primos codependientes del exponente k

Es importante hacer un conjunto de apreciaciones importantes

1) Toda expresión $4^k-1$ independientemente de su exponente k par o impar, primo o compuesto es divisible entre 3 y toda expresión $\mathbf{4^k-1}$ con exponente k par es divisible entre 5 pues 3 y 5 son los vecinos de la base.
2) Toda expresión $\mathbf{4^k-1}$ con exponente $\boldsymbol{k}$ par previo a algún primo es divisible entre el primo (que es un primo codependiente del exponente n). Esto se debe al primer teorema de Fermat.
3) Toda expresión $\mathbf{4^k-1}$ con $k$ primo es generador de primos que no aparecen en ninguna factorización previa de ese tipo con el exponente $k$ menor. En este caso la expresión es divisible entre 3 y entre primos codependientes del exponente k
4) Toda expresión $\mathbf{4^k-1}$ con k compuesto es divisible entre el m.c.m de los factores de las expresiones $\mathbf{4^{ki}-1}$ con $k1,\ k2,\ k3,\ \ldots, kn.$ Aparte de los primos que se heredan como factores provenientes del mínimo común múltiplo de los factores resultan también primos codependientes del exponente k que se tenga.

Se debe tener en cuenta que para los exponentes antes de 70 como puede apreciarse en tabla 3 siempre son superiores a los términos de los factores faltantes y por la teoría de primos codependientes es inconcebible pensar que si de las factorizaciones previas no resultan esos factores faltantes pequeños al compararse con el exponente mucho menos podrán salir de los primos codependientes que son como mínimo una unidad superior (kn+1= k+1 si n=1) o iguales al doble del exponente más 1 (2k+1) cuando son valores pequeños, pero pueden ser cualquier múltiplo de k aumentado en 1 como fue indicado antes en (ecuación 11). Los primos codependientes generados en el caso de exponentes primos tienden a ser muy grandes.

Además, el hecho de que los exponentes k y los posibles divisores 2k+1 crecen muestra que:

(i) La diferencia entre los factores faltantes y los exponentes va en aumento y por lo tanto dado que generalmente no hay repeticiones de las bases no se ve la aparición de $(2k+1)$ compuesto y mucho menos que se pueda dar la aparición de $(2k+1)^2$ compuesto.

(ii) La repetición de las bases 3 y 5 se da para los siguientes casos de potencia

$(ii.1)$ El factor $3^n$ aparece exclusivamente en las potencias $4^{3n}-1$ cumpliéndose que mientras mayor es la factorización del exponente en potencias de 3, mayor será el exponente con que aparezca el 3 en la factorización de la potencia respectiva. Por ello si el exponente tiene $3^1$ como en el caso de los exponentes 3, 6, 12, 15, 21 en la factorización aparece $3^2$ , si el exponente tiene $3^2$ como 9, 18, 36, 45, y sus otros múltiplos en la factorización aparece $3^3$ y el exponente es mayor si en el exponente aparece $3^n$ con n>2

$(ii.2)$ El factor $5^2$ solo aparece en potencias del tipo $4^{10n}-1$ , es decir, en potencias donde el exponente es 10, 20, 30, 40 y las siguientes decenas. En potencias de exponente 100 que tiene $5^2$ aparece $5^3$ en la factorización. Esto se cumple para el 5 solo con potencias pares ya que se dijo que toda potencia de exponente impar contiene el número anterior a la base que sería 3, pero nunca el número posterior a la base que sería el 5.

$(ii.3)$ Los incisos $(ii.1)$ $y$ $(ii.2)$ explican porque, por ejemplo, en $4^{55}-1$ como en $4^5-1$ aparece $11$ como factor y se tiene $55=5*11$ hay una repetición como $11^2$, es decir, si en una expresión previa aparece un factor y se consigue otra expresión con exponente múltiplo del factor siempre habrá repeticiones del factor (al cuadrado o con otro exponente), pero eso no ocurre sin que se den apariciones previas de un factor en una potencia anterior. Obsérvese por ejemplo, que 3 aparece en $4^1-1$, pero en $4^3-1$ aparece $3^2$ y en $4^9-1$ aparece $3^3$ porque se

va multiplicando el exponente por 3 en cada caso. Entonces si en $4^3 - 1$ aparece por primera vez el factor 7, la aparición de $7^2$ se da en $4^{21} - 1$, ya que $21 = 3 * 7$. Otro ejemplo para animar la imaginación del lector es este $4^4 - 1$ contiene al 17, por lo tanto, se requiere $exponente = 4 * 17 = 68$ para encontrar $17^2$. En efecto:

$$4^{68} - 1 = 87112\ 285931760246646623899502532662132735\ (41\ dígitos)$$
$$= 3 \times 5 \times 17^2 \times 137 \times 953 \times 26317 \times 43691 \times 131071 \times 354689 \times 2\ 879347902817$$

De esta manera, para encontrar una potencia $4^k - 1$ que sea divisible entre $(15)^2 = (3^2 * 5^2) = 225$ se debe buscar la primera aparición de 3 y la primera de 5 en alguna potencia de 4 y considerar multiplicar ese exponente por 15, entonces como $4^2 - 1 = 15 = 3.5$ que se cumple para exponente 2, se debe multiplicar ese exponente por 15 así $k = 2 * 15 = 30$ , por lo cual $4^{30} - 1$ es divisible entre 225. En efecto, al calcular dicha expresión:

$$4^{30} - 1 = 3^2 \times 5^2 \times 7 \times 11 \times 13 \times 31 \times 41 \times 61 \times 151 \times 331 \times 1321$$

Aquí puede verse que en este caso para 2k+1=15 se necesita no k=7 como exponente sino k=30 para hallar que es divisible entre $15^2$

$(iii)$ Mientras aumenta el divisor su factorización tiende a ser más complicada e incluso con más primos lo que dificulta aún más poder llegar a que se disminuya el número de factores faltantes

2.10. Alcanzando a los cuadrados de los divisores

A continuación, se presenta un cuadro que muestra cuando las expresiones $4^n - 1$ son divisibles entre los cuadrados de los divisores compuestos de la figura 2, es decir, se pretende evidenciar con el uso de los incisos $(i), (ii) y\ (iii)$ cuando verdaderamente los valores de tabla 1 ampliada (es decir, tomando en cuenta todos los exponentes, desde 1 a 70 sin excepciones) contienen los factores primos de los exponentes. Para ello en la tabla siguiente en la columna 1 se presenta el divisor y el exponente, la primera aparición de la base o incluso parte del cuadrado en un determinado exponente y cuál es el exponente en el que se completa el cuadrado.

El lector puede ver, por ejemplo, que en $4^2 - 1 = 3 * 5$ aparece la base 15 y en $4^3 - 1 = 3^2 * 7$ más que el 21 aparece casi su cuadrado faltando solo un 7, ya que $21^2 = (3^2 * 7) * 7$. Al seguir trabajando de esta forma es posible listar los factores que aparecen y asimismo indicar los factores faltantes. Así, al seguir esa forma de trabajo tomando en cuenta todas las

potencias hasta el exponente 70 se puede entonces realizar la tabla que muestra lo que sucede en cada uno de los casos y se obtiene que al trabajar con los diferentes exponentes resulta la siguiente tabla:

**Tabla 4**

*Exponente que contiene a los divisores al cuadrado*

| Divisor(2k+1) según figura 2) | Exponente (k) Según figura 1 | Primer exponente donde aparece el divisor (2k+1) (tabla3) | Expresión que aparece | Expresión que falta en el cuadrado | Exponente donde estará el cuadrado |
|---|---|---|---|---|---|
| 9 | 4 | 3 | 9 | 9 | 3*9=27 |
| 15 | 7 | 2 | 15 | 15 | 2*15=30 |
| 21 | 10 | 3 | 63 | 7 | 3*7=21 |
| 25 | 12 | 10 | 25 | 25 | 10*25=250 |
| 27 | 13 | 9 | 27 | 27 | 9*27=243 |
| 33 | 16 | 5 | 33 | 33 | 5*33=165 |
| 35 | 17 | 6 | 35 | 35 | 6*35=210 |
| 39 | 19 | 6 | 117 | 13 | 6*13=78 |
| 45 | 22 | 6 | 45 | 45 | 6*45=270 |

| | | | | | |
|---|---|---|---|---|---|
| 49 | 24 | 21 | 49 | 49 | 21*49 =1029 |
| 51 | 25 | 4 | 51 | 51 | 4*51= 204 |
| 55 | 27 | 10 | 275 | 11 | 10*11 = 110 |
| 57 | 28 | 9 | 171 | 19 | 9*19= 171 |
| 63 | 31 | 3 | 63 | 63 | 3*63= 189 |
| 65 | 32 | 6 | 65 | 65 | 6*65= 390 |
| 69 | 34 | 11 | 69 | 69 | 11*69 =759 |
| 75 | 37 | 10 | 75 | 75 | 10*75 =750 |
| 77 | 38 | 15 | 77 | 77 | 15*77 = 1155 |
| 81 | 40 | 27 | 81 | 81 | 27*81 = 2187 |
| 85 | 42 | 4 | 85 | 85 | 4*85= 340 |
| 87 | 43 | 28 | 87 | 87 | 28*87 =2436 |
| 91 | 45 | 6 | 91 | 91 | 6*91= 546 |
| 93 | 46 | 5 | 93 | 93 | 5*93= 465 |
| 95 | 47 | 18 | 95 | 95 | 18*95 =1710 |

| | | | | | |
|---|---|---|---|---|---|
| **99** | **49** | **15** | **99** | **99** | **15*99 =1435** |
| **105** | **52** | **6** | **210** | **35** | **6*35= 210** |
| **111** | **55** | **18** | **333** | **37** | **18*37 =666** |
| **115** | **57** | **22** | **115** | **115** | **22*11 5= 2530** |
| **117** | **58** | **6** | **117** | **117** | **6*117 = 702** |
| **119** | **59** | **12** | **119** | **119** | **12*11 9=1428** |
| **121** | **60** | **55** | **121** | **121** | **55*12 1=6655** |
| **123** | **61** | **10** | **41** | **41** | **10*41 =410** |
| **125** | **62** | **50** | **125** | **125** | **50*12 5= 6250** |
| **129** | **64** | **7** | **129** | **129** | **7*129 =903** |
| **133** | **66** | **9** | **133** | **133** | **9*133 =1197** |
| **135** | **67** | **18** | **135** | **135** | **18*13 5= 2430** |
| **141** | **70** | **23** | **141** | **141** | **23*14 1=3243** |

Fuente: Elaboración propia de los autores

Entre los aspectos resaltantes de la tabla 4 antes mostrada se pueden mencionar elementos de interés entre los cuales están los siguientes:

La tabla 4 establece que para encontrar los divisores presentes en la columna 1 al cuadrado es necesario ubicar la columna 6 donde el número corresponde al exponente de la

expresión $4^n - 1$ donde aparecerá la factorización del divisor compuesto de la columna 1 por primera vez. La última columna siempre será el producto de los valores de dos columnas, que son la columna 3 y la columna 5. La columna 3 indica el exponente de $4^k - 1$ donde se da la primera aparición de parte de los factores del cuadrado (como en la tabla 1) y la columna 5 es el factor faltante para alcanzar el cuadrado. La columna 4 es el valor totalizado que aparece del divisor al cuadrado que se encuentra en la potencia de exponente en la columna 2

Es decir, si se piensa en el divisor $9$ su cuadrado es $81\ y\ 9$ que es $3^2$ se ubica por primera vez en la expresión $4^3 - 1$ y como $\frac{81}{9} = 9$ entonces se debe buscar la expresión $4^{3*9} - 1 = 4^{27} - 1$ para encontrar $81 = 3^4$ en su factorización. También $15$ se encuentra expresado en $4^2 - 1$ y para hallar $15^2$ es necesario $4^{2*15} - 1 = 4^{30} - 1$ y en el caso de $21$ se encuentra por primera vez en $4^3 - 1 = 63$, pero $21^2$ contiene a $63$ y al dividir resulta $7$ por lo cual $21^2$ aparecerá en $4^{3*7} - 1 = 4^{21} - 1$. Los aspectos indicados respecto a los divisores, aparición de los divisores por primera vez y los divisores pueden verse en la tabla 3

2.11. La tabla 4, la ecuación 4 y los exponentes mayores que 70.

La tabla 3 muestra que siempre los exponentes necesarios para asegurar la aparición de los divisores al cuadrado $(2k+1)^2$ son siempre un múltiplo del divisor $(2k+1)$ como consta en la última columna y dicho valor es superior en cada caso a los exponentes k en la columna 2, es decir, que siempre el cuadrado aparecerá en una expresión del tipo $4^M - 1$ donde:

$$M = L * (2k+1)\ para\ algún\ L > 1\ con\ L\epsilon\ \aleph\ \ y\ M > k\ \ (ecuación\ 12)$$

Para los exponentes menores que 70, donde se dan las mayores cercanías entre factores primos, como por ejemplo $15 = 3 * 5,\ 33 = 3 * 11\ y\ 63 = 3^2 * 7$ los factores primos son cercanos, pero para exponentes mayores a 70, los factores primos están distanciados y en consecuencia los valores de M, serán muy grandes si se comparan tanto con $k$ como con $2k + 1$, y en consecuencia es imposible pensar que para factores más grandes se encuentre algún factor M que se iguale con el exponente de turno $k$. En consecuencia, no hay soluciones de la ecuación 4. Es decir, nunca se va a cumplir la división completa entre un divisor al cuadrado del tipo $(2k+1)$ que sea compuesto.

**DISCUSIÓN**

Los métodos planteados para la factorización de las expresiones de la forma general $a^n - 1$ independientemente del valor de $a\ y\ n$ evidencian un conjunto de herramientas útiles entre las cuales se precisan las siguientes:

- El mínimo común múltiplo de las potencias ofrece información útil para factorizar
- Las expresiones exponenciales antes indicadas en una forma práctica en base a los factores primos del exponente n, lo cual es por supuesto útil en el estudio de la ecuación 3 o ecuación 4.
- La teoría de los números primos codependientes del exponente (expuesto en las secciones 2.6 y 2.7) de las expresiones estudiadas ofrece un ahorro de cálculos que es interesante en los procesos de factorización, ya que ofrece una economía computacional interesante, al descartar muchísimos primos, en base al exponente.
- El análisis de la multiplicidad de los divisores en nuevas potencias que es presentado en las secciones 2.8, 2.9 y 2.10 constituye un elemento predictivo importante en cuanto a posibilidades de divisibilidad de cualquier expresión entre un determinado divisor al cuadrado.

  En tal sentido, este artículo muestra el uso de nuevas herramientas matemáticas cuya implementación sería importante en el estudio de varios problemas de la teoría de números.

**CONCLUSIONES**

Lo expuesto en este artículo es importante porque el mismo resalta un conjunto de aspectos interesantes sobre el problema planteado, entre los que pueden citarse los siguientes:

1) La (ecuación 1) luego del estudio de casos de posibles soluciones pares o impares resulta en las ecuaciones 3 y 4 al determinar que solo hay posibles soluciones impares, es decir, para $c = 2k + 1$, junto con el uso de los triángulos presentados en la figura 1 y en la figura 2, ayudan a encontrar los posibles valores de los exponentes $k$ (compuestos o primos) y de los posibles divisores $2k + 1$ (compuestos)
2) El estudio de las expresiones de la forma $a^n - 1$ y el estudio de sus posibles factores primos o divisores constituye un abordaje interesante que junto con los detalles mostrados de los primos codependientes del exponente y su reiterativa aparición en las potencias de base 2 hasta 10 permite contar con una estrategia para la factorización total de dichas expresiones, lo cual sumado al uso del m.c.m del exponente permite obtener ventajas en cuanto a los procesos de factorización actualmente usados.
3) El estudio de $4^n - 1$ y su factorización permite apreciar que en esas expresiones numéricas aparecen un conjunto de factores de los divisores compuestos según lo

sugerido en la ecuación 4, pero nunca en ningún caso aparece el divisor en forma total, ya que es compuesto y por supuesto factorizable, en la cual se reflejan los factores faltantes para cada divisor al cuadrado como se explicó en la tabla 4.

4) La tabla 4 constituye una forma de estudiar los exponentes M, en los cuales se encuentran los factores en los divisores al cuadrado, los cuales son mucho mayores que k y en consecuencia ello evidencia que no hay un compuesto $c = 2k + 1$ impar desde 9 hasta infinito que cumpla con la ecuación que le dé cumplimiento a las ecuaciones 1), 3) y 4), por lo tanto, se concluye que no hay solución del problema de congruencia planteado.

## Declaración de conflicto de interés

Los autores declaran no tener ningún conflicto de interés relacionado con esta investigación.

## REFERENCIAS


Barrantes, J., & Ruiz, A. (2006). *Disquisitiones Arithmeticae - Versión española*. Archivado desde el original el 10 de abril de 2008. Consultado el 3 de mayo de 2008.

Bernaschini, E. (2017). *Números primos: una historia sin fin*. *Revista de Educación Matemática, 32*(3), 29–36. Unión Matemática Argentina - Famaf (UNC).

Bodi, S. (2008). *Análisis de la comprensión de divisibilidad en el conjunto de los números naturales*. Facultad de Educación, Departamento de Innovación y Formación Didáctica, Universidad de Alicante.

Blancas, A., et al. (2020). *Sobre un criterio de divisibilidad entre 11*. *Publicación Semestral Padi, 8*(15), 72–76.

Bogomolny, A. (2018). *Divisibility by 7, 11, and 13*. Último acceso 10 de marzo de 2020. https://www.cut-the-knot.org/blue/div7-11-13.shtml

Burton, J. (1965). *Teoría de los números*. Biblioteca de Matemática Superior. Editorial Trillas.

Caldwell, C. (1994). *Proof of Fermat's Little Theorem - The primes page.* Consultado el 3 de mayo de 2008.

Dickson, E. (2005). *History of the Theory of Numbers. Divisibility and Primality* (Vol. 1). Dover.

Euler, L. (1741). *Theorematum Quorundam ad Numeros Primos Spectantium Demonstratio*. *Commentarii academiae scientiarum Petropolitanae, 8*, 141-146. Archivado desde el original el 22 de diciembre de 2006.

García, F. (2005). *Secretos de los números primos*. *Manual Formativo de ACTA, (37)*, 87-97. ISSN 1888-6051.

Gauss, C. (1965). *Cap.3 Powers' residues*. *Disquisitiones Arithmeticae*. Yale University Press. ISBN 0-300-09473-6. (Traducción al español). Archivado el 20 de septiembre de 2008 en Wayback Machine.

Gracián, E. (2010). *Los números primos: un largo camino al infinito*. RBA Libros. ISBN 9788498678185.

Include Poetry. (2020). *Aritmética modular*. https://www.include-poetry.com/Code/C++/Matematicas/Teoria-numeros/Aritmetica-modular/.

Koscielny, C., Kurkowski, M., & Srebrny, M. (2013). *Modern Cryptography Primer: Theoretical Foundations and Practical Applications*. Springer. ISBN 978-3-642-41385-8.

McDowell, E. (2018). *Divisibility tests: A history and user's guide*. *Convergence*. https://doi.org/10.4169/convergence20180513

Mora, W. (2010). *Introducción a la Teoría de Números: Ejemplos y algoritmos* (1ra ed.). Escuela de Matemática, Instituto Tecnológico de Costa Rica. ISBN 978-9968-641-11-1.

Niven, I., & Zuckerman, H. (2004). *Introducción a la teoría de números* (p. 19). ISBN 968-18-069-7.

Pace, G. (2011). *Mathematics of Discrete Structures for Computer Science*. Springer. ISBN 978-3-642-29839-4.

Pérez, M. (2022). *Definición de número primo*. https://conceptodefinicion.de/numero-primo/.

Pérez, J., & Merino, M. (2009). *Definición de números naturales*. https://definicion.de/numeros-naturales/.

Romo, G. (2023). *Teoría de números: Metodología Problem Solving con aplicaciones en criptografía y programación en Python*. https://www.youtube.com/c/GerardRomo. También disponible en la biblioteca Toomates: http://www.toomates.net/biblioteca.htm

Sadornil, D., & Varona, J. (2021). *Existen infinitos primos (desde Euclides hasta el siglo XXI)*. *La Gaceta de la RSME, 24*(2), 301–324. https://gaceta.rsme.es/abrir.php?id=1634#:~:text=Por%20otra%20parte%2C%20la%20d

emostraci%C3%B3n,compuesto%20por%20alg%C3%BAn%20n%C3%BAmero%20primo%C2%BB.

Tiborashi, A. (2020). *Matemáticas Discretas*.

Tilborg, H., & Jajodia, S. (2011). *Encyclopedia of Cryptography and Security* (2nd ed.). Springer. ISBN 978-1-4419-5906-5. https://doi.org/10.1007/978-1-4419-5906-5

Apostol, T. M. (2020). *Introducción a la teoría analítica de números*. Reverté. ISBN 9788429191059. Consultado el 8 de octubre de 2022.

Villarroel, A., & Villarroel, F. (2022). *Sobre la generación de los números primos: De la función pr = n+2, a la evasión de las congruencias de los números compuestos*. *Impacto Científico de Venezuela, 17*(2), 319-334.

Villarroel, A., & Villarroel, F. (2023). *Del test de Chika a un criterio general de divisibilidad entre cualquier número primo o compuesto (terminados en 1, 3, 7, 9): características y consecuencias*. *Revista digital Matemática, Educación e Internet, 23*(2). Recuperado de: https://tecdigital.tec.ac.cr/servicios/revistamatematica/material_didactico/revisado/Articulos/RevistaDigital_V24_n1_2023_Villarroel/.

Villarroel, A., & Villarroel, F. (2023). *De la función Pr =2Nx+5 y el descarte del triángulo de generadores de números compuestos a la generación de los números primos*. *Revista Matemática ESPOL, FCNM JOURNAL de Ecuador, 21*(2).

Zaragoza, S., & Cipriano, A. (2009). *Teoría de números*. Visión Libros. ISBN 9788498864601.

Zhao, D. (2004). *Carta de Pierre de Fermat a Frénicle de Bessy*. Archivado desde el original el 22 de diciembre de 2006. Consultado el 3 de mayo de 2008.