ESTUDIO DE ALGUNAS PROPOSICIONES, RESULTADOS Y MÉTODOS QUE DESARROLLÓ GAUSS EN LA SECCIÓN TERCERA DE DISQUISITIONES ARITHMETICAE

EDWIN CASTRO SUÁREZ

IBETH NATHALIA MORENO BERMÚDEZ

Trabajo de grado como requisito
para optar al título de Licenciado en Matemáticas

DIRECTOR

Prof. Juan Carlos Ávila Mahecha

UNIVERSIDAD PEDAGÓGICA NACIONAL

LICENCIATURA EN MATEMÁTICAS

BOGOTÁ D.C

2015

1. Información General	
Tipo de documento	Trabajo de grado
Acceso al documento	Universidad Pedagógica Nacional. Biblioteca Central
Titulo del documento	Estudio de algunas proposiciones, resultados y métodos que desarrolló gauss en la sección tercera de Disquisitiones Arithmeticae.
Autor(es)	Castro Suarez, Edwin; Moreno Bermúdez, Ibeth Nathalia
Director	Juan Carlos Ávila Mahecha
Publicación	Bogotá, Universidad Pedagógica Nacional, 2015. 47p.
Unidad Patrocinante	Universidad Pedagógica Nacional UPN.
Palabras Claves	Congruencia, residuo, exponente, exponente mínimo, potencia, Números primos, estructura algebraica, función, conjuntos y subconjuntos.

2. Descripción
Este trabajo de grado muestra el estudio y análisis de cinco proposiciones y métodos que aparecen en la sección tercera del libro *Disquisitiones Arithmeticae* (Gauss,1995) en la que se analizan los residuos de potencias. En los tres capítulos elaborados, se trata la información dada de forma detallada y concisa con el fin de enfatizar algunos aspectos no directamente observables y así generar una mejor comprensión al lector. Se emplearon procedimientos de reconstrucción y sistematización de resultados y mecanismos dados; todo esto bajo la racionalidad matemática que exige el presente documento, pues se puede evidenciar un lenguaje formalizado bajo una estructura lógica, derivado de la actividad matemática de conjeturar, ensayar, errar y generalizar. Como aporte adicional, gracias a la amplia utilización de diferentes sistemas de notación simbólica (números, letras, tablas, gráficos, etc.), se construyen estructuras algebraicas (exactamente cinco) a partir de lo estudiado como producto final del razonamiento que se realiza durante toda la temática dada.

3. Fuentes

Ángel, J. Software Álgebra finita 1.0. [CD-ROM]: Windows 95 o posterior. Bogotá, Colombia: Universidad Pedagógica Nacional, 2011.

Ávila, J. C. (2011). *Actividades matemáticas para formular teoremas en teoría de números y grupos*. Bogotá: Universidad Pedagógica Nacional.

García, J. (2005). Capítulo 3. Recuperado el junio de 2015, de Conjuntos ordenados. Retículos y álgebra de Boole.: http://www.ugr.es/~jesusgm/Curso%202005-2006/Matematica%20Discreta/Ordenes.pdf

Gauss, C. F. (1995). Disquisitiones Arithmeticae. (M. J. Hugo Barrantes, Trad.) Costa Rica: Universidad de Costa Rica.

Leveque, W. (1968). Teoría elemental de los números. (C. E. Gortari, Trad.) México: Herreros Hermanos, sucesores S.A.

Luque, C., Mora, L., Torres, J. (2014). Actividades matemáticas para el desarrollo de procesos lógicos: Clasificar, medir e invertir. Bogotá: Universidad Pedagógica Nacional.

Moreno, N., Fernández, J., Beltrán, Y., & García, J. (2014). Residuos de potencias: estudio de casos. Bogotá: Universidad Pedagógica Nacional.

4. Contenidos

El estudio se realizó en tres etapas: la primera estuvo enfocada en la lectura de la sección tercera del libro *Disquisitiones Arithmeticae,* específicamente en las proposiciones escogidas y en otras posibles fuentes que aportaran claridad en la temática; la segunda se basó en los diferentes análisis a través de tablas, uso de software, organización de información, etc., de casos particulares con el fin de explorar la información dada y así formular hipótesis, hacer conjeturas, predicciones y extraer de ella información no percibida a primera vista. Por último, la tercera etapa se constituyó en la formalización de los resultados encontrados, mediante demostraciones que justificaran las estrategias y procedimientos puestos en acción en la segunda etapa.

En resumen, se muestran los capítulos del presente documento, destacando los elementos fundamentales de cada uno de ellos:

CAPITULO 1: Estudio de las proposiciones 52, 53 y 54 (Gauss, 1995) en las cuales se definen la pertenencia de un número a a un exponente d, dadas unas condiciones iniciales, entre esas la más

importante la congruencia con la unidad entre números enteros positivos, mediante el estudio de un caso particular y de construcciones auxiliares y demostraciones formales. A partir de los resultados encontrados se definen algunas estructuras algebraicas.

CAPÍTULO 2: Estudio y análisis sobre raíces primitivas, bases e índices, proposición 57 (Gauss, 1995). Se justifican los razonamientos propuestos en el anterior capítulo enmarcados en una nueva concepción (raíces primitivas) bajo análisis de diferentes sistemas de notación simbólica (números, letras, tablas, gráficos, etc.).

CAPITULO 3: Algoritmos de los índices, proposición 58 (Gauss, 1995): comprensión, interpretación y justificación mediante teoremas de las propiedades que cumplen los índices.

5. Conclusiones

A lo largo del presente estudio logró demostrarse un campo amplio de exploración y comprobación de ideas expuestas por el matemático Gauss. Esto implicó un uso extensivo y reflexivo de conocimientos previos, argumentos, reglas y algoritmos lo que conllevó a la elaboración de hipótesis y conjeturas; procesos que posibilitaron una mejor comprensión e interpretación de los resultados.

Las afirmaciones y resultados encontrados fueron sometidos a pruebas de las cuales algunos se refutaron, juzgando su validez y otros se aceptaron bajo argumentos lógicos, como es el caso específico de la construcción de la función $\aleph: D(p-1) \rightarrow R_p$, función que en principio tiene un comportamiento similar a la función φ de Euler y cuyo proceso de construcción permite probar la igualdad de estas dos funciones a partir de los residuos de la congruencia $a^d \equiv 1\ (m\acute{o}d\ p)$; así, a través de la solución de un problema se obtiene un camino alternativo para estudiar la función φ de Euler.

De otro lado, los procesos de estudio posibilitaron la construcción de estructuras algebraicas como el grupo $\mathbb{Z}_{18}$ a partir de una partición en el conjunto de todas las potencias de 2 obtenida al evaluar los residuos que estas dejan al ser divididas entre 19. Ahora bien, la otra estructura algebraica construida, fue la de un retículo, el cual surgió al restringir el dominio de la función $\aleph$, donde se

estudiaron los elementos de la forma $\Re = \{N^*(\{d\})|\ d \in D(p-1)\}$. Con ayuda de tablas y de software matemático se definió operaciones y estudio su estructura. En general, las dos estructuras algebraicas son aportes que dinamizan la estructura del trabajo, pues como se evidenció, la teoría de números es el eje principal del estudio, luego la creación de estructuras algebraicas es uno de los productos finales de este trabajo aprovechando los resultados obtenidos.

Elaborado por:	Edwin Castro y Nathalia Moreno
Revisado por:	Juan Carlos Ávila Mahecha

Fecha de elaboración del Resumen:	05	11	2015

Contenido

Introducción

Las ideas que propuso Gauss en el libro *Disquisitiones Arithmeticae* han sido de gran importancia en la Teoría de Números de los siglos XIX y XX. Estas grandes contribuciones se han constituido en punto de partida para el desarrollo intelectual de todo aquel que se interese por estos estudios. Como el interés del presente documento radica en el análisis de los residuos que se generan a partir de ciertas potencias de números al ser divididas entre números primos, el trabajo se centra en una pequeña parte de este problema (estudio de cinco proposiciones), incluyendo ejemplificaciones y procedimientos alternativos a los que aparecen en el libro de Disquisitiones, todo esto con el fin de poder estudiar las demostraciones que Gauss establece en su obra, así como aprovecharlos para construir algunas estructuras algebraicas.

El presente documento articula actividades y procesos matemáticos que dan cuenta del cómo y del porqué de los procedimientos inmersos en el análisis (), mediante procesos como la formulación de hipótesis, la construcción de conjeturas, búsqueda de contraejemplos, manejo de propiedades y conocimientos previos; para favorecer el desarrollo de los objetivos del estudio, ya que en el documento original las pruebas se sintetizan y algunos análisis se evitan por brevedad.

En el primer capítulo (estudio de tres proposiciones) se analizan las potencias de un número natural a al ser divididas entre un número primo p, donde se caracterizan las bases a de manera que si t es un divisor de $p-1$, entonces $a^t \equiv 1\ (mód\ p)$, de manera que t sea la menor potencia positiva que satisfaga la congruencia anterior. Para llevar a cabo este análisis se definen conceptos como **periodo**, que hace referencia a los conjuntos formados por los residuos que arroja la congruencia, y **pertenencia** a un exponente, que trata la correspondencia entre los exponentes y las bases de dicha congruencia, para mayor claridad a esta correspondencia se le asignó una función. En particular, producto del análisis anteriormente mencionado, surgen demostraciones formales que justifican los hechos

encontrados y construcciones auxiliares que dan punto de partida para diseño de algunas estructuras algebraicas, como son $\mathbb{Z}_{18}$ y el retículo $(\mathfrak{R}, \preccurlyeq)$.

En el segundo capítulo se pone de manifiesto lo demostrado en el capítulo anterior (pertenencia, periodo, etc.), en razón que los hechos y procedimientos que se demostraron en este apartado, se justifican por medio de tablas y se relacionan con los nuevos conceptos a estudiar: raíces primitivas, bases e índices. Se redirecciona el estudio hacia las bases a, que según condiciones dadas se renombran como raíces primitivas respecto a la congruencia $a^e \equiv b\ (mód\ p)$, donde se analizan particularidades de los residuos b (base) con respecto a los exponentes e (índices); entre dichas particularidades se destaca que cada b está relacionado con infinitos valores para e, de la misma manera cada e está relacionado con infinitos valores de b, todos estos en módulo $p-1$.

Para finalizar, en el último y tercer capítulo se continúa con la metodología de analizar casos particulares y procesos algorítmicos, luego la temática se centra en los índices, denotados como $IND(b)$ lo cual se lee como el índice de un número b; y sus algoritmos. Según el capítulo anterior, al mantener la relación encontrada entre b y e, surge la idea de encontrar el índice para cualquier número teniendo en cuenta si dicho índice se encuentra entre los números mayores, menores o múltiplos de p, todo esto a partir de propiedades cuyos comportamientos son similares a las propiedades de los logaritmos y que se justifican por medio de teoremas.

Justificación

La idea del presente estudio nació del trabajo Residuos de potencias: estudio de casos (Moreno, 2014), realizado en el espacio académico Tópicos de la historia de las matemáticas (temática: historia del álgebra) a cargo del profesor Juan Carlos Ávila. En dicho espacio se desarrollaron estudios similares al presente (nivel de complejidad mínimo) en los cuales se abordaron ideas presentes en el trabajo de grado de maestría del profesor (Ávila, 2011).

El problema que motiva el presente estudio, consiste en hallar todos los residuos que dejan las potencias de un número natural a al ser divididas entre diferentes números primos p. Tal problema fue estudiado por Gauss en *Disquisitiones Arithmeticae*; en este sentido, uno de los objetivos del presente trabajo, consiste en ejemplificar algunos de los procedimientos dados por Gauss para desarrollar el estudio, así por ejemplo, en la *Tabla 1* se listan los residuos que se obtienen al dividir potencias de 2 entre 19:

n	$res\left(\frac{2^n}{19}\right)$
1	2
2	4
3	8
4	16
5	13
6	7
7	14
8	9
9	18
10	17
11	15
12	11
13	3
14	6
15	12
16	5
17	10
18	1

n	$res\left(\frac{2^n}{19}\right)$
19	2
20	4
21	8
22	16
23	13
24	7
25	14
26	9
27	18
28	17
29	15
30	11
31	3
32	6
33	12
34	5
35	10
36	1

Tabla 1. Residuos al dividir las primeras treinta y seis potencias de dos entre diecinueve.

De esta tabla, se puede ver que los residuos comienzan a repetirse en el mismo orden después de cierta potencia (n), esto es:

n	$res\left(\frac{2^n}{19}\right)$
18, 36, 54, 72, …	1
1, 19, 37, 55, 73, …	2
2, 20, 38, 56, 74, …	4
3, 21, 39, 57, 75, …	8
4, 22, 40, 58, 76, …	16
5, 23, 41, 59, 77, …	13
6, 24, 42, 60, 78, …	7
7, 25, 43, 61, 79, …	14
8, 26, 44, 62, 80, …	9
9, 27, 45, 63, 81, …	18
10, 28, 46, 64, 82, …	17
11, 29, 47, 65, 83, …	15
12, 30, 48, 66, 84, …	11
13, 31, 49, 67, 85, …	3
14, 32, 50, 68, 86, …	6
15, 33, 51, 69, 87, …	12
16, 34, 52, 70, 88, …	5
17, 35, 53, 71, 89, …	10

Tabla 2. Números que dejan un mismo residuo al ser divididos entre 19

Luego del exponente 17, se repiten los mismos residuos, en el mismo orden. Si se observa la tabla anterior, se ha clasificado al conjunto de los números naturales en 18 subconjuntos, cuyos representantes de dichos subconjuntos son los números que aparecen en la columna izquierda de la *Tabla 2*; luego al conjunto formado por los números representantes se le asocian todas las propiedades de $\mathbb{z}_p$, para este caso $p = 18$. En resumen si tenemos a $\mathbb{z}_{18}$, cumple todas las propiedades de la adición; en cuanto a la multiplicación cumple la propiedad

de la distribución con respecto a la suma, además la multiplicación cumple las propiedades asociativa y elemento neutro (Luque, 2014), esto es:

$$\mathbb{z}_{18} = \{[1],[2],[4],[8],[16],[13],[7],[14],[9],[18],[17],[15],[11],[3],[6],[12],[5],[10]\}$$

Retomando la *Tabla 1* y variando los valores de a por 3,4 y 5 se puede apreciar, que los residuos de las potencias al ser divididas entre 19 se repiten en el mismo orden a partir de cierto n que al parecer depende tanto de a como del número por el cual se divide (en este caso 19), a tal conjunto de residuos se le denomina ***periodo***, así, para los ejemplos:

$P_{a=2} = \{1,2,4,8,16,13,7,14,9,18,17,15,11,3,6,12,5,10\}$ con 18 elementos

$P_{a=3} = \{1,3,9,8,5,15,7,2,6,18,16,10,11,14,4,12,17,13\}$ con 18 elementos

$P_{a=4} = \{1,4,16,7,9,17,11,6,5\}$ con 9 elementos

$P_{a=5} = \{1,5,6,11,17,9,7,16,4\}$ con 9 elementos

Son los periodos para $p = 19$ y $a = 2,3,4\ y\ 5$ respectivamente.

Como es sabido, (Luque,2014) si a y b son enteros positivos y tienen el mismo residuo al ser divididos entre un número p, se tiene que $a \equiv b\ (mód\ p)$. Así, para los ejemplos previos, las potencias de a que son congruentes con la unidad son:

$\boldsymbol{a = 2}$	$\boldsymbol{a = 3}$	$\boldsymbol{a = 4}$	$\boldsymbol{a = 5}$
$2^0 \equiv 1\ (mod\ 19)$	$3^0 \equiv 1\ (mod\ 19)$	$4^0 \equiv 1\ (mod\ 19)$	$5^0 \equiv 1\ (mod\ 19)$
$2^{18} \equiv 1(mod\ 19)$	$3^{\mathbf{18}} \equiv 1\ (mod\ 19)$	$4^{\mathbf{9}} \equiv 1\ (mod\ 19)$	$5^{\mathbf{9}} \equiv 1\ (mod\ 19)$
$2^{36} \equiv 1(mod\ 19)$	$3^{36} \equiv 1\ (mod\ 19)$	$4^{18} \equiv 1\ (mod\ 19)$	$5^{18} \equiv 1\ (mod\ 19)$
⋮	⋮	⋮	⋮

Tabla 3. Cada columna representa las potencias para las bases $a = 2,3,4\ y\ 5$ congruentes con la unidad.

De este listado se puede inducir que el mínimo exponente $t \neq 0$ que hace a^t congruente con la unidad, representa la cantidad de términos del periodo que conforma el listado de residuos. Gauss en la proposición 49 de Disquisiciones Aritméticas demuestra este hecho y adicional muestra que el mínimo exponente t, diferente de cero, para el cual $a^t \equiv 1\ (mód\ p)$ divide a $(p-1)$, o sea, $t \mid (p-1)$.

CAPÍTULO 1

1. ¿Cuántos y cuáles números corresponden a un mismo periodo?[I]

El resultado anterior motiva el estudio del problema de cómo encontrar bases a de manera que si t es un divisor de $p - 1$, entonces $a^t \equiv 1\ (mód\ p)$, donde t es el menor exponente diferente de cero, que cumple la anterior congruencia (vale recordar que t representa el número de término del periodo relacionados con la base a y módulo p). Si se realizan más tablas como la anterior (variando la base a y teniendo en cuenta que solo interesa la segunda fila de cada familia de congruencias) se puede generar un indicio para buscar las bases menores, esto es, números entre 1 y p, y exponentes mínimos t, que cumplan $t \mid (p - 1)$. Por ejemplo, tomando de nuevo a $p = 19$, se definen los conjuntos: R_{19} conformado por los enteros positivos entre 0 y 19, y $D(18)$ formado por todos los divisores positivos de 18. Si para cada $a \in R_{19}$ y cada $d \in D(18)$ se busca que $a^d \equiv 1\ (mód\ 19)$, donde d es el menor entero positivo que cumpla con esta congruencia, se clasifican los diferentes elementos de R_{19} como aparecen en la siguiente tabla (Gauss, 1995):

Base (a)	Exponente (d)
1	1
18	2
7, 11	3
8, 12	6
4, 5, 6, 9, 16, 17	9
2, 3, 10, 13, 14, 15	18

Tabla 4. Correspondencia entre los $a \in R_p$ y los divisores $d \in D(p-1)$, tal que $a^d \equiv 1\ (mód\ 19)$

Así por ejemplo, para la última fila de la T*abla 4*, aparece en la primera columna los números $2, 3, 10, 13, 14, 15$ y en la segunda columna el número 18, esto quiere decir que para cada uno

[I] Este capítulo contiene el estudio y análisis de las proposiciones 52,53 y 54 de la sección tercera del libro Disquisitiones Arithmeticae.

de los números a anteriores, $a^{18} \equiv 1\ (mód\ 19)$, donde 18 es el menor entero positivo que hace ciertas estas congruencias. Para nuestro estudio diremos que $2, 3, 10, 13, 14$ y 15 **pertenecen** al exponente 18, precisando:

Definición. Sean a, d y p números naturales, si $a^d \equiv 1\ (mód\ p)$, donde d es el menor exponente positivos que satisface esta congruencia, diremos que a **pertenece al exponente** d.

Así, el problema a abordar consiste en encontrar cómo están distribuidos los números de 1 a $p-1$, conjunto al cual se simbolizará como R_p, entre los diferentes divisores de $p-1$, conjunto que simbolizamos como $D(p-1)$, de modo que $a^d \equiv 1(mód\ p)$, donde $a \in R_p$ y $d \in D(P-1)$, con d, exponente mínimo. Esta relación se expresa mediante la función $N\colon R_p \rightarrow D(p-1)$, la cual asigna a cada elemento a de R_p el divisor d al cual **pertenece** a. Esta relación en efecto es una función ya que como se ha dicho previamente, en la proposición 49 (Gauss, 1995), para cada a y p existe un entero positivo t mínimo de modo que $a^t \equiv 1\ (mód\ p)$ donde además t es un divisor de $p-1$.

Por otro lado, también interesará estudiar cuántos elementos a se relacionan con d, para ello, usaremos la función imagen reciproca de N, $N^!\colon \mathcal{P}\big(D(p-1)\big) \rightarrow \mathcal{P}\big(R_p\big)$, esto es:

$$\text{Para todo } Q \subseteq D(P-1),\ N^!(Q) = \big\{a \in R_p \mid (\exists d \in Q)(N(a) = d)\big\}.$$

Con un uso especial de $N^!$ se puede generar una partición de R_p, esto es, una colección de subconjuntos no vacíos de R_p, tal que la intersección de dos elementos cualesquiera de la colección es vacío y la unión de todos ellos es R_p. Veamos cómo construir tal partición:

Para cada $a \in R_p$, según la proposición 49[II] (Gauss, 1995), existe $d \mid (p-1)$ de modo que a pertenece el exponente d, por tanto, $N^!(\{d\}) \neq \emptyset$, pues al menos $a \in N^!(\{d\})$. Ahora, sean d y d', divisores cualesquiera de $p-1$ diferentes entre sí, se mostrará que $T = N^!(\{d\}) \cap N^!(\{d'\}) = \emptyset$. Por contradicción se procede a demostrar, suponiendo que $T \neq \emptyset$, entonces existe un $a \in T$ de manera que $a^d \equiv 1(mód\ p)$ y $a^{d'} \equiv 1(mód\ p)$, pero esto implica que $d = d'$ debido a la minimalidad de d, luego esto contradice la hipótesis, por tanto $T = \emptyset$.

[II] Si p es un número primo que no divide a a, y si a^t es la menor potencia de a congruente a la unidad, según el módulo p, el exponente t será $= p-1$, o será un factor de este número.

Ahora se prueba $\bigcup_{d|p-1} N^{!}(\{d\}) = R_p$. Es claro que $\bigcup_{d|p-1} N^{!}(\{d\}) \subseteq R_p$. Como N es una función que relaciona cada elemento de R_p con los elementos de $D(p-1)$, entonces para cada $a \in R_p$, existe $d \in D(p-1)$ de modo que $N(a) = d$ y por tanto $a \in N^{!}(\{d\})$, así, $R_p \subseteq \bigcup_{d|p-1} N^{!}(\{d\})$ y por tanto, $\bigcup_{d|p-1} N^{!}(\{d\}) = R_p$.

Luego, de las afirmaciones anteriores se afirma que $\mathfrak{C} = \{N^{!}(\{d\}) \mid d \mid (p-1)\}$ es una partición de R_p.

Como el interés del presente estudio radica en saber cuántos a pertenecen al exponente d, entonces la siguiente función cuenta el número de elementos de cada elemento de $\mathfrak{C}$, así:

$$\aleph: D(p-1) \to R_p$$

$$d \to |N^{!}(\{d\})|$$

Donde $|N^{!}(\{d\})|$ indica el número de elementos de $N^{!}(\{d\})$.

Dado que $\mathfrak{C} = \{N^{!}(\{d\}) \mid d \mid (p-1)\}$ es una partición de R_p, entonces:

$$\left|\bigcup_{d|p-1} N^{!}(\{d\})\right| = \sum_{d|p-1} |N^{!}(\{d\})| = \sum_{d|p-1} \aleph(d) = p-1.$$

En la siguiente sección, se caracterizarán los números $\aleph(d)$.

1.1 Análisis de los números $\aleph(d)$ mediante ejemplificación.

A continuación, se ejemplifica cómo Gauss encuentra el número de elementos de los conjuntos que se han llamado $\aleph(d)$, asunto que se soluciona en la proposición 52 de la sección tercera de Disquisitiones (Gauss, 1995). En la siguiente tabla se muestra el caso particular que se empleará para iniciar el análisis.

Base (a)	Exponente (d)
2,3,10,13,14,15	18

Tabla 5. Caso particular escogido a partir de la Tabla 6 con $d = 18$ y $a = 2$.

Sabiendo que $2^{18} \equiv 1\ (mod\ 19)$, entonces toda potencia de 2^{18} también cumple la propiedad de ser congruente con la unidad, esto es, $(2^{18})^n \equiv 1 (mód\ 19)$ o también $(2^n)^{18} \equiv 1$

$(mód\ 19)$. En particular se estudiarán los *n* menores o iguales a *d* (i = 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17 y 18). En este punto es importante aclarar que 2^i para *i* = 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17 y 18 es solución de la congruencia $x^{18} \equiv 1\ (mod\ 19)$, donde $x = 2^i$.

Para continuar se aclara que solamente se estudiarán las potencias 2^i con $0 < i < 19$, puesto que las otras $(2^{19}, 2^{20}, 2^{21}, \dots, 2^n)$ son congruentes a las primeras; por ejemplo:

$$2 \equiv 2^1 \equiv 2^{19} \equiv 2^{37} \equiv 2^{18k+1}\ (mod\ 19)$$

$$4 \equiv 2^2 \equiv 2^{20} \equiv 2^{38} \equiv 2^{18k+2}\ (mod\ 19)$$

Dado esto se puede observar la existencia de infinitos números que cumplen con la condición de tener el mismo residuo al dividirlos entre 19, de manera general los exponentes de todos los enteros positivos de la forma 2^k, con $k = 18r + 1, 18r + 2, 18r + 3, \dots, 18r + (p - 1)$ se pueden agrupar en conjuntos de la forma:

$$[2^q] = \{k \in \mathbb{N} \mid q \equiv k\ \ (mód\ 18)\} \text{ con } 0 < q \leq 18\}$$

Por otro lado sea a, tal que $0 < a < 19$ y $2^q \equiv a\ (mód\ 19)$, entonces para todo $k \in [2^q]$, $2^k \equiv a\ (mód\ 19)$, pues como $k = 18r + q$ (pues $q \equiv k\ \ (mód\ 18)$) para algún r, por tanto, $2^k = 2^{18r+q} = 2^{18} \cdot 2^q$, pero como $2^{18} \equiv 1 (mód\ 19)$, entonces, es claro que $2^{18} \cdot 2^q \equiv 2^q (mód\ 19)$ y por la propiedad transitiva de la congruencia, $2^k \equiv a\ (mód\ 19)$. Por otro lado, hemos dicho que toda potencia 2^i es solución de la congruencia $x^{18} \equiv 1\ (mód\ 19)$, por tanto, 2^k es solución y dada la congruencia de este número con a módulo 19, entonces, todos los a son soluciones también de la congruencia $x^{18} \equiv 1 (mód\ 19)$.

De lo anterior se tienen que los conjuntos $[2^q]$ pueden escribirse también como:

$$[2^q] = \{k \in \mathbb{N} \mid k = 18r + q, r \in \mathbb{N}\} \text{ con } 0 < q\ \leq 18.$$

Retomando la idea inicial de encontrar la distribución y correspondencia entre los números de la Tabla 7 y siguiendo con la secuencia de los resultados ya obtenidos se tiene que existe una correspondencia entre los conjuntos que se han mostrado previamente, con los residuos al dividir los elementos de dichos conjuntos entre 19, para hacer esto más visible, se muestra a

continuación las congruencias para 2^i con $0 < i < 19$, módulo 19; las llamaremos **congruencias 2^i**, donde la notación $[2^i] \equiv a\ (mód\ p)$ significa que para cada $b \in [2^i]$, $2^b \equiv a\ (mód\ p)$:

$[2^{18}] \equiv 1\ (mod\ 19)$	$[2^{12}] \equiv 11\ (mod\ 19)$	$[2^6] \equiv 7\ (mod\ 19)$
$[2^{17}] \equiv 10\ (mod\ 19)$	$[2^{11}] \equiv 15\ (mod\ 19)$	$[2^5] \equiv 13\ (mod\ 19)$
$[2^{16}] \equiv 5 (mod\ 19)$	$[2^{10}] \equiv 17\ (mod\ 19)$	$[2^4] \equiv 16\ (mod\ 19)$
$[2^{15}] \equiv 12\ (mod\ 19)$	$[2^9] \equiv 18\ (mod\ 19)$	$[2^3] \equiv 8\ (mod\ 19)$
$[2^{14}] \equiv 6\ (mod\ 19)$	$[2^8] \equiv 9\ (mod\ 19)$	$[2^2] \equiv 4\ (mod\ 19)$
$[2^{13}] \equiv 3\ (mod\ 19)$	$[2^7] \equiv 14\ (mod\ 19)$	$[2^1] \equiv 2\ (mod\ 19)$

Tabla 6. Congruencias para las potencias de 2

Ahora bien, ya que el interés es verificar cuáles y cuántos son los números que pertenecen a un exponente dado (en este caso $d = 18$); se analiza la *Tabla 5* y se observa que los números que se encuentran en la primera columna de esta (2, 3, 10, 13, 14 y 15) **pertenecen** al exponente 18 y como se mostró anteriormente, cada uno de estos son residuos de los conjuntos $[2^1]$, $[2^5]$, $[2^7]$, $[2^{11}]$, $[2^{13}]$ y $[2^{17}]$ (marcados en la *Tabla 6*), además se observa que los números 1, 5, 7, 11, 13 y 17 **son primos relativos con** 18 . Para justificar que lo anterior siempre se da, se demuestra que todas las potencias de 2 cuyo exponente sea primo relativo con 18 **pertenecen** a este exponente**,** se comienza analizando un caso particular, por ejemplo 2^5.

Estas potencias son solución de la congruencia $x^{18} \equiv 1\ (mod\ 19)$, en otras palabras cualquiera de estas elevada a 18 es congruente con la unidad, además una conclusión que se infiere del análisis de las ***congruencias* 2^i** es que todas las potencias de 2 cuyos exponentes son menores que 18 son **incongruentes con la unidad,** esto se puede ver de forma general en la proposición 48 de Disquisiciones (Gauss, 1995) en resumen esto es:

- $2^i \not\equiv 1 (mód\ 19)$ siempre que $0 < i < 18$.
- $(2^5)^{18} \equiv 1\ (mód\ 19)$

Como se sabe, la congruencia es una relación de equivalencia por ende cumple la propiedad reflexiva, esto significa que cualquier número es congruente consigo mismo en cualquier módulo, en particular 2 es congruente con él mismo en módulo 19:

$$2 \equiv 2(mód\ 19)$$

Además es sabido que existe algún múltiplo de 5 quien es congruente con 1 módulo 18 (en realidad son infinitos), por ejemplo $55 = 5 \times 11$:

$$55 \equiv 1\ (mód\ 18)$$

Utilizando las dos anteriores congruencia y la proposición 46 (Gauss, 1995) se obtiene la siguiente congruencia:

$$2^{55} \equiv 2(mód\ 19)$$

Como $(2^5)^{18} \equiv 1(mód\ 19)$, se quiere probar que 18 es el menor exponente al cual elevar 2^5 para que resulte congruente con la unidad en módulo 19, es decir, para todo $0 < j < 18$, se desea demostrar que $(2^5)^j \not\equiv 1(mód\ 19)$, para esto, se procede por contradicción y se supone la existencia de un j con las condiciones dadas de manera que $(2^5)^j \equiv 1(mód\ 19)$. Elevando a 11 a ambos lados de la anterior congruencia se tienes:

$$\left((2^5)^j\right)^{11} \equiv (1)^{11}(mód\ 19)$$

que es equivalente a $(2^{55})^j \equiv 1(mód\ 19)$, y como $2^{55} \equiv 2(mód\ 19)$, entonces se afirma que $2^j \equiv 1(mód\ 19)$, pero esto es una contradicción, pues se ha visto que ninguna potencia de 2 cuyo exponente sea menor que 18 es congruente con la unidad, por tanto, 18 es el menor exponente al cual se eleva 2^5 para que resulte congruente con la unidad en módulo 19; esto significa que 2^5 **pertenece** al exponente 18.

Para los otros casos (2^1, $2^7, 2^{11}, 2^{13}$ y 2^{17}) es análogo el procedimiento. Por tanto, para todo $0 < j < 18$ que sea primo relativo con 18 tenemos que 2^j pertenece al exponente 18, lo que significa que por lo menos al 18 le **pertenecen** 6 números; para los demás d se realiza el mismo procedimiento, en resumen:

Divisor d	Cantidad
1	1
2	1
3	2
6	2
9	6
18	6

Tabla 7. Cantidad de números que por lo menos pertenecen al divisor d.

A simple vista cada uno de los exponentes de las otras soluciones ($2^2, 2^3, 2^4, 2^6, 2^8, 2^9, 2^{10}, 2^{12}, 2^{14}, 2^{15}, 2^{16}$ y 2^{18}) de la congruencia $x^{18} \equiv 1\ (mod\ 19)$ comparten por lo menos un divisor en común con 18 $\big((k, 18) \neq 1\big)$, lo que hace pensar que estos no **pertenecen** al exponente 18, ya que contradice la idea anterior ($(k, 18) = 1$); luego para determinar la no **pertenencia**, se realiza el siguiente procedimiento:

Se escoge al azar una de las soluciones 2^k, la cual cumple $(k, 18) \neq 1$, por ejemplo 2^{12}.

Se proporcionan todas las posibles opciones de escribir 12 como producto de dos números enteros positivos, esto es:

$$12 = 1 \times 12$$

$$12 = 2 \times 6$$

$$12 = 3 \times 4$$

$$12 = 4 \times 3$$

$$12 = 6 \times 2$$

$$12 = 12 \times 1$$

Con esto,

$$2^{12} = (2^1)^{12} = (2^2)^6 = (2^3)^4 = (2^4)^3 = (2^6)^2 = (2^{12})^1$$

Se buscan exponentes i que cumplan la congruencia $(2^{12})^i \equiv 1\ (mod\ 19)$; se recurre a distintas maneras de escribir 12 como producto de dos números *a* y *b*, en la forma ya señalada, esto es, $((2^a)^b)^i$ así:

$$((2^1)^{12})^i \equiv 1\ (mod\ 19)$$

$$((2^2)^6)^i \equiv 1\ (mod\ 19)$$

$$((2^3)^4)^i \equiv 1\ (mod\ 19)$$

$$((2^4)^3)^i \equiv 1\ (mod\ 19)$$

$$((2^6)^2)^i \equiv 1\ (mod\ 19)$$

$$((2^{12})^1)^i \equiv 1\ (mod\ 19)$$

Como $2^{18} \equiv 1\ (m\acute{o}d\ 19)$, entonces en las congruencias anteriores, se busca los *i* apropiados de manera que $ai = 18$, con $a, i \in \mathbb{N}$. Esto ya que, al tener la congruencia previa, para cualquiera de los *b* hallados, $(2^{ai})^b \equiv 1\ (m\acute{o}d\ 19)$ o lo que es igual, $(2^{ab})^i \equiv 1\ (m\acute{o}d\ 19)$, donde, como se ha dicho, *ab* = 12. Interesa conocer el menor valor de *i*. Veamos:

- ✓ $((2^1)^{12})^{i=18} = (2^{12})^{18} \equiv 1\ (mod\ 19)$
- ✓ $((2^2)^6)^{i=9} = (2^{12})^9 \equiv 1\ (mod\ 19)$
- ✓ $((2^3)^4)^{i=6} = (2^{12})^6 \equiv 1\ (mod\ 19)$
- ✓ $((2^6)^2)^{i=3} = (2^{12})^3 \equiv 1\ (mod\ 19)$

Como se evidencia, el menor *i* es 3, lo que significa que 2^{12} **pertenece** al exponente $i = 3$, es decir $(2^{12})^3 \equiv 1\ (mod\ 19)$, luego, 2^{12} no **pertenece** al exponente 18.

Para evidenciar la no **pertenencia** de las demás potencias 2^k (donde k comparte por lo menos un divisor con 18) se construyó la *Tabla 8*, que resume el procedimiento realizado anteriormente para la no **pertenencia** de 2^{12} , dicho procedimiento es análogo para estas potencias.

Para una mejor comprensión se describe la distribución de la *Tabla 8*:

- Columna 1: Se muestran las soluciones de la congruencia $(x)^{18} \equiv 1(mód\ 19)$, con $x = 2^k$: $2^2, 2^3, 2^4, 2^6, 2^8, 2^9, 2^{10}$, $2^{14}, 2^{15}, 2^{16}$ y 2^{18}
- Columna 2: Valores de k, donde k comparte divisores con 18.
- Columna 3: Factores de k, que cumple $k = a \times b$ donde exista un número entero positivo i que al ser operado por a de como resultado 18. Se excluyen todos aquellos factores que no cumplen dicha condición.
- Columna 4: Divisores en común entre 18 y k.
- Columna 5[III]: De la tercera columna se obtuvo las maneras de escribir k como producto de dos números a y b; e igualmente se mencionó el producto $ai = 18$, con $a, i \in Z^+$, luego se muestra el i que cumple lo anterior con el fin de representar a $(2^k)^i = (2^{a \times b})^i$
- Columna 6: De la columna anterior obtenemos todas las formas posibles para escribir $(2^k)^i$, luego se escogerá la expresión que tenga en su exponente el i menor.
- Columna 7: Se presenta los valores para cada i encontrado de la anterior columna.

2^k	k	$\boldsymbol{k = a \times b}$	Divisores	$((\mathbf{2^a})^{\mathbf{b}})^{\mathbf{i}}$	$(\mathbf{2^k})^{\mathbf{i}}$	$\boldsymbol{i}$
$\mathbf{2^2}$	2	1×2 2×1	$1, 2$	$((2^1)^2)^{18}$ $((2^2)^1)^9$	$(2^2)^9$	9
$\mathbf{2^3}$	3	1×3 3×1	$1, 3$	$((2^1)^3)^{18}$ $((2^3)^1)^6$	$(2^3)^6$	6
$\mathbf{2^4}$	4	1×4 2×2	$1, 2$	$((2^1)^4)^{18}$ $((2^2)^2)^9$	$(2^2)^9$	9
$\mathbf{2^6}$	6	1×6 2×3 3×2	$1, 2, 3\ y\ 6$	$((2^1)^6)^{18}$ $((2^2)^3)^9$ $((2^3)^2)^6$	$(2^6)^3$	3

[III] Como es sabido $2^{18} \equiv 1\ (mód\ 19)$, $(2^{18})^{\ n} \equiv 1\ (mód\ 19)$ y $ai = 18$ entonces se expresan como $(2^{ai})^b \equiv 1\ (mód\ 19)$ donde $b = n$, lo que es igual a $(2^{ab})^i \equiv 1\ (mód\ 19)$,

		6×1		$((2^6)^1)^3$		
$\mathbf{2^8}$	8	1×8 2×4	$1, 2$	$((2^1)^8)^{18}$ $((2^2)^4)^9$	$(2^8)^9$	9
$\mathbf{2^{10}}$	10	1×10 2×5	$1, 2$	$((2^1)^{10})^{18}$ $((2^2)^5)^9$	$(2^{10})^9$	9
$\mathbf{2^{12}}$	12	1×12 2×6 3×4 6×2	$1, 2, 3\ y\ 6$	$((2^1)^{12})^{18}$ $((2^2)^6)^9$ $((2^3)^4)^6$ $((2^6)^2)^3$	$(2^{12})^3$	3
$\mathbf{2^{14}}$	14	1×14 2×7	$1, 2$	$((2^1)^{14})^{18}$ $((2^2)^7)^9$	$(2^{14})^9$	9
$\mathbf{2^{15}}$	15	1×15 3×5	$1, 3$	$((2^1)^{15})^{18}$ $((2^3)^5)^6$	$(2^{15})^6$	6
$\mathbf{2^{16}}$	16	2×8	$1, 2$	$((2^2)^8)^9$	$(2^{16})^9$	9
$\mathbf{2^{18}}$	18	2×9 3×6 18×1	$1, 2, 3,$ $6, 9\ y\ 18$	$((2^2)^9)^9$ $((2^3)^6)^6$ $((2^{18})^1)^1$	$(2^{18})^1$	1

Tabla 8. Procedimiento para la no pertenencia de las potencias $2^2, 2^3, 2^4, 2^6, 2^8, 2^9, 2^{10}, 2^{14}, 2^{15}, 2^{16}\ y\ 2^{18}$

Algo que se puede apreciar de la anterior tabla, es que al encontrar el menor i este siempre está relacionado con el mayor de los divisores en común encontrados entre 18 y k, esto es $(18, k)$; por esto una forma fácil de encontrar a i es buscar primero el máximo común divisor para que se cumpla $ai = 18$, todo esto para encontrar la menor potencia a la que se eleva la solución 2^kque es congruente con la unidad y así garantizar que esta no **pertenece** a 18, por ende se concluye que al no **pertenecer** 2^k a 18, entonces k y 18 no son primos relativos.

Es importante aclarar que para el desarrollo de los análisis previos, se partió de la idea general de la existencia de un número a que **pertenece** al exponente *d*, para este caso $a = 2$ y $d = 18$, luego, producto de la ejemplificación y visualización de la *Tabla 4*, se consigue deducir que no solamente existe un número sino que al contrario, para este caso en particular existen por lo menos 6, pero con el análisis de las potencia 2^k cuyos exponentes no son primos relativos a 18 se garantiza que son exactamente 6, lo que indica que es la misma cantidad de números menores y primos a 18 (para los demás divisores d ocurre lo mismo).

1.2 Resultados obtenidos a partir de la ejemplificación.

Llegado a este punto, se procederá a demostrar de manera formal las afirmaciones mencionadas anteriormente producto del análisis de ejemplos particulares, dichas afirmaciones son:

1. Si $(d, k) = 1$, entonces a^k **pertenece** a d.
2. Si $(d, k) \neq 1$, entonces a^k no **pertenece** a d.

El fundamento de la demostración de las afirmaciones 1 y 2 radica en la **pertenencia**, recordando la definición se tiene que:

- a **pertenece** al exponente d si solo si $a^d \equiv 1 (mód\ p)$, con d el menor entero positivo que cumple con esta congruencia.

Donde:

- $a \in R_p$, R_p conjunto conformado por los enteros positivos menores que $p - 1$
- $d \in D(p-1)$, donde $D(p-1)$ es el conjunto de los divisores de $p - 1$.

- p primo

1.2.1 Demostración de pertenencia

Sea p un número primo, d un divisor de $p-1$, a un entero positivo que **pertenece** al exponente d y k un número menor y primo con d ($(k,d)=1$)**,** entonces a^k **pertenece** a d**.**

Como a **pertenece** al exponente d, entonces $a^d \equiv 1\ (mód\ p)$ siendo d el menor entero que satisface esta relación, por otro lado $(a^d)^k \equiv 1\ (mód\ p)$ que es igual a $(a^k)^d \equiv 1\ (mód\ p)$ para todo $0 < k < d$, sin embargo, esto no garantiza que las potencias $a^1, a^2, \dots, a^{d-1}$ **pertenezcan** a d, ya que no se sabe si $\boldsymbol{d}$ sea el menor exponente que cumpla con esta congruencia. Por tanto, se pretende buscar cuáles de estas **pertenecen** a este exponente**.**

Algo que se puede inferir de lo anterior es que como a **pertenece** a d, entonces $a^e \not\equiv 1\ (mód\ p)$ donde $0 < e < d$, (ya que $e < d$ y d es el menor exponente entero positivo de a que cumple con la congruencia), además de esto por ser $\equiv$ una relación de equivalencia, entonces se tiene que $a \equiv a\ (mód\ p)$.

Como $(k,d)=1$ entonces existen enteros x, y tales que $kx + dy = 1$, equivalente a la expresión $dy = 1 - kx$, luego, d divide a $1 - kx$, que en términos de congruencia significa:

$$kx \equiv 1\ (mód\ d),$$

Utilizando las congruencias $a \equiv a\ (mód\ p)$, $kx \equiv 1\ (mód\ d)$ y la proposición 46 de Disquisiciones (Gauss, 1995) se afirma que $a^{kx} \equiv a\ (mód\ p)$; y como el interés es demostrar que a^k **pertenece** a d, entonces basta con demostrar que no existe un número e menor que d tal que, $(a^k)^e \equiv 1\ (mód\ p)$, para esto se procede por contradicción y se supone la existencia de un número e, por tanto, al elevar a ambos lados de la anterior congruencia por x tenemos que $((a^k)^e)^x \equiv 1^x \equiv 1\ (mód\ p)$, lo que es igual a $(a^{kx})^e \equiv 1\ (mód\ p)$ y como $a^{kx} \equiv a\ (mód\ p)$, entonces $a^e \equiv 1\ (mód\ p)$, lo que es una contradicción con la minimalidad de d; por lo cual no existe una potencia de a^k, cuyo exponente sea menor a d que sea congruente con la unidad módulo p y como $(a^k)^d \equiv 1\ (mód\ p)$, entonces, a^k **pertenece** a d en módulo p.

1.2.2 Demostración no pertenencia

Ahora, si se tiene el caso contrario de que algunos de los exponentes tienen divisores comunes, diferentes de 1, con d, entonces ¿alguna de esas potencias k serán congruentes con la unidad?, veamos:

Lo primero es descomponer al exponente en factores, esto es $k = a \times b$, con el fin de identificar el máximo común divisor δ de d y k. Entones, Sea $(d, k) = \delta$, con $\delta \neq 1$, se tiene $a^d \equiv 1\ (mód\ p)$, así $(a^d)^{\frac{k}{\delta}} \equiv 1\ (mód\ p)$, con lo que $(a^k)^{\frac{d}{\delta}} \equiv 1\ (mód\ p)$[IV]. Observemos que $\frac{d}{\delta} < d$, por tanto a^k **pertenece** a $\frac{d}{\delta}$. En conclusión, si $(d, k) \neq 1$ a^k no **pertenece** a d.

1.3 Función φ de Euler desde congruencias

Si se centra la atención en la cantidad de números n que pertenecen a un divisor d, se afirma que es igual a la cantidad de números primos menores e iguales a él, donde se conoce de antemano que por lo menos un número a **pertenece** a d; dicha relación se estableció a través de la función $\aleph: D(p-1) \rightarrow R_p$, así, el comportamiento que se ha estado estudiando lo describe el número asociado a $\aleph(d)$ lo que significa que $\aleph$ cuenta los números en relación con d que cumplen ser primos menores e iguales a d, lo que hace pensar en la similitud con la función φ de Euler.

Por tanto, para este caso $\aleph(18) = 6$, $\aleph(9) = 6$, $\aleph(6) = 2$, $\aleph(3) = 2$, $\aleph(2) = 1$ y $\aleph(1) = 1$, lo que constata la igualdad entre $\aleph(d)$ y $\varphi\ (d)$ ya que: $\varphi(18) = 6$, $\varphi(9) = 6$, $\varphi(18) = 6$, $\varphi(6) = 2$, $\varphi(3) = 2$, $\varphi(2) = 1$ y $\varphi(1) = 1$.

[IV] $d\frac{k}{\delta} = k\frac{d}{\delta}$ ya que Si $(d, k) = \delta$, entonces: $\delta\ /\ d$ y $\delta\ /\ k$, lo que significa: $\delta q = d$ con $q = \frac{d}{\delta}$ y para $\delta\ /\ k$ se tiene que $\delta q' = k$ donde $q' = \frac{k}{\delta}$, luego:

$$d\frac{k}{\delta} = dq'$$
$$d\frac{k}{\delta} = (\delta q)q'$$
$$d\frac{k}{\delta} = q(\delta q')$$
$$d\frac{k}{\delta} = qk$$
$$d\frac{k}{\delta} = k\frac{d}{\delta}$$

Ahora bien, ¿Qué comportamiento tiene $\aleph(d)$ cuando se excluye la condición inicial, esto es, a **pertenece** al exponente d?

En el caso que se excluya esta condición, se tienen dos posibilidades: $\aleph(d) = \varphi\ (d)$ ó $\aleph(d) = 0$, ya que si se tiene por lo menos un número que pertenezca a d, se garantiza que $\aleph(d) = \varphi(d)$ y si no se tiene significa que $\aleph(d) = 0$.

A continuación se muestra la demostración que surge del análisis de los casos particulares mencionados con anterioridad:

Por el artículo 39 del libro disquisiciones (Gauss, 1995), si los divisores de $p-1$ son $d, d', d'', \dots, d^n, p-1$, entonces:

$$\varphi(d) + \varphi(d') + \varphi(d'') + (d''') + \cdots + \varphi(d^{n-1}) + \ \varphi(d^n) = p - 1 \qquad (1)$$

Además como se ha visto, $\sum_{d|p-1} \aleph(d) = p - 1$, se tiene:

$$\varphi(d) + \varphi(d') + \varphi(d'') + \varphi(d''') + \cdots = \aleph(d) + \aleph(d') + \aleph(d'') \ldots. \qquad (2)$$

Como el interés radica en determinar la igualdad entre las dos funciones $\aleph$ y φ, el procedimiento a seguir es comparar los valores que toma cada divisor dentro de cada función. Al comparar cada uno de los valores, se inicia con el supuesto de que para algún d^*, $\aleph(d^*) = 0$, luego el resultado de la suma de los $\aleph(d)$ se debe afectar y por ende llegar a una contradicción, veamos. Se escoge un $\varphi(d^*)$, luego se compara con $\aleph(d^*)$, así, puede ocurrir dos casos: 1) $\aleph(d^*) = 0$ o 2) $\aleph(d^*) = \varphi\ (d^*)$.

Caso1: $\aleph(d^*) = 0$

Sustituyendo $\aleph(d^*) = 0$ en (2) se tiene que:

$$\aleph(d') + \aleph(d'') + \aleph(d''') + \cdots + 0 + \cdots + \aleph(d^{n-1}) + \aleph(d^n) = \ \varphi(d') + \varphi(d'') + (d''') + \cdots + \varphi(d^*) + \cdots + \varphi(d^{n-1}) + \ \varphi(d^n) \qquad (3)$$

Se supone que de los $\aleph(d)$ el único igual a 0 es $\aleph(d^*)$ entonces ocurre:

$$\aleph(d') = \varphi\ (d')$$

$$\aleph(d'') = \varphi\ (d'')$$

$$\aleph(d''') = \varphi\ (d''')$$

$$\vdots$$

$$0 = \varphi\ (d^*)$$

$$\vdots$$

$$\aleph(d^{n-1}) = \varphi\ (d^{n-1})$$

$$\aleph(d^n) = \varphi\ (d^n)$$

Utilizando la propiedad cancelativa en (3) se tiene:

$$0 = \varphi(d^*)$$

Lo que es una contradicción pues $\varphi(d^*) > 0$, para cualquier $d \in D(p-1)$, análogamente ocurre lo mismo en el caso que existiera más de uno igual a cero ($\aleph(d^*) = 0, \aleph(d') = 0, \aleph(d'') = 0$ …), entonces $\aleph(d) \neq 0$, lo que significa que $\aleph(d) = \varphi(d)$.

Los procedimientos hasta aquí realizados permiten afirmar objetivamente, la existencia de otro camino para hallar la función de φ Euler, dicho camino fue la construcción de $\aleph(d)$ a partir de los residuos de la congruencia $a^d \equiv 1\ (mód\ p)$, lo que conllevó a relacionarla directamente con la función φ de Euler.

1.4 Estructura algebraica

Dada la función imagen recíproca de N:

$$N^!: \mathcal{P}\big(D(p-1)\big) \rightarrow\ \ \mathcal{P}\big(R_p\big),$$

se hace una restricción en el dominio tomando únicamente los conjuntos de la forma $\{d\}$, donde $d \in D(p-1)$, a esta función la notaremos N^*.

$$N^*: D(p-1) \rightarrow\ \ \mathcal{P}\big(R_p\big),$$

Se fija la atención en el rango de N^*, es decir:

$$\Re = \{N^*(\{d\})|\ d \in D(p-1)\},$$

Se define para todo $a, b \in \Re$,

$$a \preccurlyeq b \leftrightarrow \big(\exists\ d, d' \in D(p-1)\big)(N^*(\{d\}) = a\ \wedge\ N^*(\{d'\}) = b\ \wedge\ d \mid d')\ ,$$

Esta relación cumple ser una relación de orden, para esto se prueban propiedades que lo confirman: *Reflexiva, Antisimétrica y transitiva.*

1. *Reflexiva:*

Para todo $d \in D(p-1)$ se tiene que $d|d$, por otro lado $N^*(\{d\}) = N^*(\{d\}) = a$, luego $a \in \Re$ y por tanto $a \preccurlyeq a$.

2. *Antisimétrica*

Sean $a, b \in \Re$ de modo que $a \preccurlyeq b$ y $b \preccurlyeq a$, entonces existe un $d, d' \in D(p-1)$, donde $N^*(\{d\}) = a,\ N^*(\{d'\}) = b$, como $a \preccurlyeq b$ y $b \preccurlyeq a$ luego $d|d'$ y $d'|d,$, entonces $d = d'$ por lo tanto $a = b$.

3. *Transitiva*

Sean $a, b, c \in \Re$ de modo que $a \preccurlyeq b$ y $b \preccurlyeq c$ existen $d, d', d''' \in D(p-1)$, donde $d|d'$ y $d'|d''$ por lo tanto $d|d''$, entonces $a \preccurlyeq c$.

Luego $\Re$ queda parcialmente ordenado, ya que para cualquier $a, b \in \Re$ no se cumple $a \preccurlyeq b$ ó $b \preccurlyeq a$; además de esto se sabe que cualquier subconjunto finito de este tiene supremo e ínfimo, para probar este hecho se realiza el análisis siguiente:

Sea $A \subseteq \Re$, ya que A es un conjunto finito, pues $\Re$ lo es, entonces, $A = \{A_1, A_2, A_3 \dots, A_k\}$, donde existen $d_1, d_2, \dots, d_k$ divisores de $p-1$, tales que:

$$\begin{aligned} A_1 &= N^*(\{d_1\}) \\ A_2 &= N^*(\{d_2\}) \\ &\vdots \\ A_k &= N^*(\{d_k\}), \end{aligned}$$

Como se sabe que cualquier subconjunto de $D(p-1)$ tiene supremo, que en particular es el mínimo común múltiplo de los elementos del subconjunto, entonces, se garantiza la existencia de un $r \in \Re$ tal que $N^*(\{\text{mcm}(d_1, d_2, \dots, d_k)\}) = r$. Al $\text{mcm}(d_1, d_2, \dots, d_k)$ se denota d_{mcm}.

Al comparar cada uno de los elementos de A con r, se verifica que este es cota superior de todos los elementos de A, puesto que:

$A_1 \preccurlyeq r$ en razón que $\big(\exists\, d_1, d_{mcm} \in D(p-1)\big)(N^*(\{d_1\}) = A_1 \wedge N^*(\{d_{mcm}\}) = r \wedge d_1 \mid d_{mcm})$

$A_2 \preccurlyeq r$ en razón que $\big(\exists\, d_2, d_{mcm} \in D(p-1)\big)(N^*(\{d_2\}) = A_2 \wedge N^*(\{d_{mcm}\}) = r \wedge d_2 \mid d_{mcm})$

$\vdots$

$A_k \preccurlyeq r$ en razón que $\big(\exists\, d_k, d_{mcm} \in D(p-1)\big)(N^*(\{d_k\}) = A_k \wedge N^*(\{d_{mcm}\}) = r \wedge d_k \mid d_{mcm})$

Por ser r la imagen reciproca de d_{mcm}, se tiene que r es el menor elemento de las cotas superiores de A, por ende r es el supremo de A.

En cuanto a la existencia del ínfimo de A, según lo anterior se puede determinar que este es $N^*(\{\text{mcd}(d_1, d_2, \dots, d_k)\})$. Los procedimientos para verificar este hecho son análogos al procedimiento anterior.

En resumen, $\Re$ es parcialmente ordenado y todo subconjunto finito de este tiene supremo e ínfimo, por tanto $\Re$ es un *Retículo*.

Como $(\Re, \preccurlyeq)$ es un retículo (Garcia, 2005), se definen dos operaciones a partir del supremo e ínfimo de subconjuntos binarios, así, para todo $a, b \in \Re, a \vee b = \sup\{a, b\}$ y $a \wedge b = \inf\{a, b\}$. Estas operaciones satisfacen las siguientes propiedades (Garcia, 2005):

- Conmutativa $\begin{cases} a \vee b = b \vee a \\ a \wedge b = b \wedge a \end{cases}$
- Asociativa $\begin{cases} a \wedge (b \wedge c) = (a \wedge b) \wedge c \\ a \vee (b \vee c) = (a \vee b) \vee c \end{cases}$
- Absorción $\begin{cases} a \wedge (a \vee c) = a \\ a \vee (a \wedge c) = a \end{cases}$
- Idempotencia $\begin{cases} a \vee a = a \\ a \wedge a = a \end{cases}$

Para una mejor comprensión, se ejemplificará para $p = 19$:

A continuación se mostrará la función N^*:

$$N^*: \mathcal{P}\big(D(18)\big) \rightarrow \mathcal{P}(R_{19})$$

$$\{1\} \rightarrow \{1\}$$

$$\{2\} \rightarrow \{18\}$$

$$\{3\} \rightarrow \{7, 11\}$$

$$\{6\} \rightarrow \{8, 12\}$$

$$\{9\} \rightarrow \{4, 5, 6, 9, 16, 17\}$$

$$\{18\} \rightarrow \{2, 3, 10, 13, 14, 15\}$$

entonces, el retículo asociado a este caso se representará mediante el siguiente diagrama de Hasse (Garcia, 2005) como:

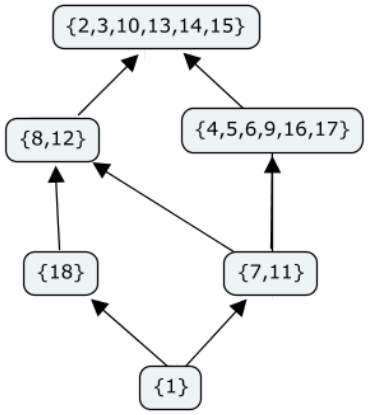

Figura 1. Diagrama de Hasse: Representación del retículo $(\mathfrak{R}, \preccurlyeq)$[v]

[v] $\mathfrak{R} = \{N^*(\{d\}) | \ d \in D(18)\}$

De la anterior representación, se puede evidenciar el orden de los elementos, por ejemplo, entre $\{18\}$ y $\{8,12\}$ se puede observar que el mayor es $\{8,12\}$, en razón que si se remite a la función N^* se identifica que la imagen inversa de $\{8,12\}$ es 6 y para $\{18\}$ es 2; donde $2/6$, lo cual cumple con la definición de $\preccurlyeq$. Análogo para los demás elementos.

Para claridad del concepto de ínfimo y supremo, se ejemplificará así:

Si se tiene $Y \subseteq \mathcal{P}(R_{19})$, en particular $Y = \{\{18\},\{18,12\}\}$, el conjunto de cotas superiores para este caso es $C_s = \{\{8,12\},\{2,3,10,13,14,15\}\}$; y como $\{8,12\} \preccurlyeq \{2,3,10,13,14,15\}$ entonces $\sup Y = \{8,12\}$.

Como el concepto de supremo e ínfimo cumplen ser operaciones, dichas operaciones se describen en las tablas 12 y 13.

∨	$\{\mathbf{1}\}$	$\{\mathbf{18}\}$	$\{\mathbf{7,11}\}$	$\{\mathbf{8,12}\}$	$\{\mathbf{4,5,6,9,16,17}\}$	$\{\mathbf{2,3,10,13,14,15}\}$
$\{\mathbf{1}\}$	{1}	{18}	{7,11}	{8,12}	{4,5,6,9,16,17}	{2,3,10,13,14,15}
$\{\mathbf{18}\}$	{18}	{18}	{8,12}	{8,12}	{2,3,10,13,14,15}	{2,3,10,13,14,15}
$\{\mathbf{7,11}\}$	{7,11}	{8,12}	{7,11}	{8,12}	{4,5,6,9,16,17}	{2,3,10,13,14,15}
$\{\mathbf{8,12}\}$	{8,12}	{8,12}	{8,12}	{8,12}	{2,3,10,13,14,15}	{2,3,10,13,14,15}
$\{\mathbf{4,5,6,9,16,17}\}$	{4,5,6,9,16,17}	{2,3,10,13,14,15}	{4,5,6,9,16,17}	{2,3,10,13,14,15}	{4,5,6,9,16,17}	{2,3,10,13,14,15}
$\{\mathbf{2,3,10,13,14,15}\}$	{2,3,10,13,14,15}	{2,3,10,13,14,15}	{2,3,10,13,14,15}	{2,3,10,13,14,15}	{2,3,10,13,14,15}	{2,3,10,13,14,15}

Tabla 9. Operación Supremo

∧	$\{\mathbf{1}\}$	$\{\mathbf{18}\}$	$\{\mathbf{7,11}\}$	$\{\mathbf{8,12}\}$	$\{\mathbf{4,5,6,9,16,17}\}$	$\{\mathbf{2,3,10,13,14,15}\}$
$\{\mathbf{1}\}$	{1}	{1}	{1}	{1}	{1}	{1}
$\{\mathbf{18}\}$	{1}	{18}	{1}	{18}	{1}	{18}
$\{\mathbf{7,11}\}$	{1}	{1}	{7,11}	{7,11}	{7,11}	{7,11}
$\{\mathbf{8,12}\}$	{1}	{18}	{7,11}	{8,12}	{1}	{8,12}
$\{\mathbf{4,5,6,9,16,17}\}$	{1}	{1}	{7,11}	{1}	{4,5,6,9,16,17}	{4,5,6,9,16,17}
$\{\mathbf{2,3,10,13,14,15}\}$	{1}	{18}	{7,11}	{8,12}	{4,5,6,9,16,17}	{2,3,10,13,14,15}

Tabla 10. Operación ínfimo

Como se mostró en la *Tabla 9*, *Tabla 10* y con ayuda del programa Algebra finita (Ángel, 2011), se verifica que la operación ∧ cumple las mismas propiedades que la operación ∨, es decir:

- Conmutativa.
- Asociativa.
- Idempotencia.
- Absorción

En resumen, a partir del conjunto caracterizado y de las representaciones (tablas y diagrama) se mostraron propiedades y operaciones para determinar la estructura algebraica llamada retículo.

CAPÍTULO 2

2. Estudio y análisis sobre raíces primitivas, bases e índices[VI].

En el estudio del capítulo anterior se analizaron los residuos dejados por potencias de un número a al ser divididas entre un número p y en particular, se estudiaron congruencias del tipo $a^d \equiv 1\ (mód\ p)$ con p primo. Ahora se enfocará el presente estudio en las congruencias $a^d \equiv b\ (mód\ p)$. Como se observa, se redirigirá la atención al comportamiento de todas variables a, d, b y p; designando un valor para a y p, y variando a d (los valores para b se obtienen a partir de los valores de a, p y d). Así, para empezar, en la siguiente tabla se ha registrado algunos valores de b para diferentes a y d con p = 19:

Exponente d / Base a	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
2	2	4	8	16	13	7	14	9	18	17	15	11	3	6	12	5	10	1	2
3	3	9	8	5	15	7	2	6	18	16	10	11	14	4	12	17	13	1	3
4	4	16	7	9	17	11	6	5	1	4	16	7	9	17	11	6	5	1	4
5	5	6	11	17	9	7	16	4	1	5	6	11	17	9	7	16	4	1	5
6	6	17	7	4	5	11	9	16	1	6	17	7	4	5	11	9	16	1	6
7	7	11	1	7	11	1	7	11	1	7	11	1	7	11	1	7	11	1	7
8	8	7	18	11	12	1	8	7	18	11	12	1	8	7	18	11	12	1	8
9	9	5	7	6	16	11	4	17	1	9	5	7	6	16	11	4	17	1	9
10	10	5	12	6	3	11	15	17	18	9	14	7	13	16	8	4	2	1	10
11	11	7	1	11	7	1	11	7	1	11	7	1	11	7	1	11	7	1	11
12	12	11	18	7	8	1	12	11	18	7	8	1	12	11	18	7	8	1	12
13	13	17	12	4	14	11	10	16	18	6	2	7	15	5	8	9	3	1	13
14	14	6	8	17	10	7	3	4	18	5	13	11	2	9	12	16	15	1	14
15	15	16	12	9	2	11	13	5	18	4	3	7	10	17	8	6	14	1	15
16	16	9	11	5	4	7	17	6	1	16	9	11	55	4	7	17	6	1	16
17	17	4	11	16	6	7	5	9	1	17	4	11	16	6	7	5	9	1	17
18	18	1	18	1	18	1	18	1	18	1	18	1	18	1	18	1	18	1	18
19	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Tabla 11. Residuos que deja la congruencia $a^d \equiv b\ (mod\ 19)$ al reemplazar los valores de a y d.

[VI] Proposición 57 (Gauss, 1995)

Para esta tabla, cada número representa el residuo mínimo (Gauss, 1995) de la base a elevada al número d, con el módulo 19. Por ejemplo, $2^5 \equiv 13\ (mod\ 19)$ 2 y 5 de color rojo y 13 color rosado; lo mismo para $13^{10} \equiv 6\ (mod\ 19)$ como muestra la *Tabla 11*; y así para todos los demás números.

Acerca de los patrones encontrados. Los residuos generados por las potencias a^d (con a y d entre 0 y 19) en módulo 19, son todos diferentes y menores a 19, luego se comienzan a repetir después que uno de ellos es igual a 1, este análisis se evidenció anteriormente en la *Tabla 2*, a este comportamiento se llamó **periodo**; con esto se puede afirmar que los residuos que producen las potencias hasta cierto valor n de una base a son todas diferentes entre si (incongruentes).

Exponente d / Base a	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
2	2	4	8	16	13	7	14	9	18	17	15	11	3	6	12	5	10	1	2
3	3	9	8	5	15	7	2	6	18	16	10	11	14	4	12	17	13	1	3
4	4	16	7	9	17	11	6	5	1	4	16	7	9	17	11	6	5	1	4
5	5	6	11	17	9	7	16	4	1	5	6	11	17	9	7	16	4	1	5
6	6	17	7	4	5	11	9	16	1	6	17	7	4	5	11	9	16	1	6
7	7	11	1	7	11	1	7	11	1	7	11	1	7	11	1	7	11	1	7
8	8	7	18	11	12	1	8	7	18	11	12	1	8	7	18	11	12	1	8
9	9	5	7	6	16	11	4	17	1	9	5	7	6	16	11	4	17	1	9
10	10	5	12	6	3	11	15	17	18	9	14	7	13	16	8	4	2	1	10
11	11	7	1	11	7	1	11	7	1	11	7	1	11	7	1	11	7	1	11
12	12	11	18	7	8	1	12	11	18	7	8	1	12	11	18	7	8	1	12
13	13	17	12	4	14	11	10	16	18	6	2	7	15	5	8	9	3	1	13
14	14	6	8	17	10	7	3	4	18	5	13	11	2	9	12	16	15	1	14
15	15	16	12	9	2	11	13	5	18	4	3	7	10	17	8	6	14	1	15
16	16	9	11	5	4	7	17	6	1	16	9	11	55	4	7	17	6	1	16
17	17	4	11	16	6	7	5	9	1	17	4	11	16	6	7	5	9	1	17
18	18	1	18	1	18	1	18	1	18	1	18	1	18	1	18	1	18	1	18
19	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Tabla 12. Muestra las propiedades de la congruencia $a^d \equiv b\ (mod\ 19)$ *como el periodo y las raíces primitivas a* 19

Por ejemplo, en la *Tabla 12* las potencias de $4, 5, 6, 9, 16$ y 17 (color rosado) se repiten después de que llegan a la novena potencia, pero los de 7 y 11 (color azul) no se repiten hasta

después de la tercera potencia. Para las demás potencias ocurre lo mismo, haciendo la salvedad que no ocurre con la misma frecuencia (distinto periodo) como se mostró en la *Tabla 12* (cada color agrupa las potencias con el mismo número de residuos).

El interés del presente estudio se centra en las bases a que muestran los números de color rojo en la anterior tabla, ya que para estos, los números *b*, se repiten después del exponente $p - 1$. Esto hace referencia a la **pertenencia** que se mencionó en la anterior proposición, lo que significa que $2, 3, 10, 13, 14$ y 15 **pertenecen** a 18. Gauss llamó a estas bases, *raíces primitivas* de 19, precisando, se dirá que la base *a* es ***una raíz primitiva*** de *p*, si y solo si *a* **pertenece** al exponente $p - 1$. Esto implica que si a es una raíz primitiva de p, entonces todas las potencias de *a* desde 1 y hasta $p - 1$, son diferentes entre sí y por tanto, allí se distribuirán los números desde el 1 y hasta el $p - 1$. Así por ejemplo, las potencias de 3: $3^1, 3^2, 3^3, 3^4, 3^5, 3^6, 3^7, 3^8, 3^9, 3^{10}, 3^{11}, 3^{12}, 3^{13}, 3^{14}, 3^{15}, 3^{16}, 3^{17}$ y 3^{18} producen los siguientes residuos respectivamente, 3, 9, 8, 5, 15, 7, 2, 6, 18, 16, 10, 11, 14, 4, 12, 17, 13 y 1 donde se ve que todos los residuos son diferentes entre sí, además estos residuos son los números entre 0 y 19.

Ahora, si fijamos la atención en las raíces no primitivas y observamos la *Tabla 15*, se observa que algunas de ellas son congruentes a 1 en el noveno exponente (color rosado), en el tercero (azul claro), segundo (azul) y en el sexto (color verde). Como puede apreciarse todos estos exponentes son divisores de 18 (Gauss, 1995). Las raíces primitivas tienen la característica especial de que todos los residuos mínimos son congruentes a algunas de sus potencias. Así, para las potencias de 2, dentro del periodo se encuentra cada número entre 0 y 19 distribuidos de la siguiente forma:

$2^1 \equiv 2\ (mod\ 19)$	$2^7 \equiv 14\ (mod\ 19)$	$2^{13} \equiv 3\ (mod\ 19)$
$2^2 \equiv 4\ (mod\ 19)$	$2^8 \equiv 9\ (mod\ 19)$	$2^{14} \equiv 6\ (mod\ 19)$
$2^3 \equiv 8\ (mod\ 19)$	$2^9 \equiv 18\ (mod\ 19)$	$2^{15} \equiv 12\ (mod\ 19)$
$2^4 \equiv 16\ (mod\ 19)$	$2^{10} \equiv 17\ (mod\ 19)$	$2^{16} \equiv 5\ (mod\ 19)$
$2^5 \equiv 13\ (mod\ 19)$	$2^{11} \equiv 15\ (mod\ 19)$	$2^{17} \equiv 10\ (mod\ 19)$
$2^6 \equiv 7\ (mod\ 19)$	$2^{12} \equiv 11\ (mod\ 19)$	$2^{18} \equiv 1\ (mod\ 19)$

Tabla 13. Congruencias de las potencias de 2 (raíz primitiva) con los elementos del periodo entre 0 y 19.

En este caso se tiene $2^e \equiv b\ (mód\ 19)$, entonces a cada residuo b le corresponde una potencia de 2 (2 raíz primitiva de 19), es decir, existe un exponente (e) relacionado con 2 que cumple ser congruente a b. En general Sea a una raíz primitiva de p, entonces para cada $b \in R_p$ existe $e \in R_p$ de modo que $a^e \equiv b\ (mód\ p)$. El elemento e recibe el nombre de índice de b.

En el caso particular $2^e \equiv b\ (mód\ 19)$, dichas correspondencias son:

b	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**	**17**	**18**
$\boldsymbol{e}$	0	1	13	2	16	14	6	3	8	17	12	15	5	7	11	4	10	9

Tabla 14. Correspondencia entre los residuos b y los índices e en la congruencia $2^e \equiv b\ (mód\ 19)$.

Por ser b un elemento del periodo, se puede garantizar que cada b está relacionado con infinitos valores para e, de la misma manera cada e está relacionado con infinitos valores de b, todos estos en módulo $p - 1$ (para este caso 18).

Por ejemplo: $2^e \equiv 4\ (mód\ 19)$, como se muestra en la tabla $e = 2$, pero también puede ser $20, 38, \dots, 18q + 2$, para mayor claridad ver *Tabla 2*, lo que indica los infinitos valores que puede tomar e con respecto un b. Ahora si se tiene $2^2 \equiv b\ (mód\ 19)$, se ve que b puede tomar los valores $4, 22, 40, \dots, 18q + 4$, por ende b no tiene un valor fijo.

CAPÍTULO 3

3. Algoritmos de los índices[VII]

Con las raíces primitivas no solamente se busca la congruencia entre ciertos números, también facilitan y dan la posibilidad de generar propiedades con respecto a los índices, para facilidad se designa al índice de un número b como $IND(b)$. Luego, de manera particular se continua con el caso $a = 2$, raíz primitiva de 19, en el estudio de casos y propiedades; teniendo como punto de partida la *Tabla 14*. Es importante aclarar que todas las congruencias que se trabajan son de la forma $IND(b) \equiv e\ (mód\ p)$, pero en adelante se omitirán los módulos.

3.1 Procedimientos algorítmicos para el cálculo de índices.

A continuación se muestran conjuntos previamente seleccionados de acuerdo a una caracterización entre sus elementos, con el fin de analizarlos desde una perspectiva algorítmica y así determinar y evidenciar regularidades en la obtención del índice de dichos elementos, para esto se nombraron los siguientes casos:

Caso 1: Conjunto M en el cual sus elementos se obtienen como el producto de dos primos diferentes:

$$M = \{6, 10, 14, 15\}$$

Según la *Tabla 14*:

$$IND(b) \equiv e$$
$$IND(6) \equiv 14$$
$$IND(10) \equiv 17$$
$$IND(14) \equiv 7$$
$$IND(15) \equiv 11$$

[VII] Proposición 58 (Gauss, 1995): Los teoremas que tratan sobre los índices son completamente análogos a los que se refieren a los logaritmos.

Se expresa los elementos de M de tal forma que se muestren como producto de factores, por ejemplo: $6 = 2 \times 3$; al observar la *Tabla 14* se visualiza que el índice de los factores individuales encontrados son respectivamente 1 y 13, los que suman 14, luego este cumple ser el índice asociado con 6 (Número compuesto).

De manera análoga se muestra a continuación esta particularidad para los demás elementos:

$$IND(10) \equiv 17$$
$$IND(10) \equiv IND(2 \times 5)$$
$$IND(10) \equiv IND(2) + IND(5)$$
$$IND(10) \equiv 1 + 16 = 17$$

$$IND(14) \equiv 7$$
$$IND(14) \equiv IND(2 \times 7)$$
$$IND(14) \equiv IND(2) + IND(7)$$
$$IND(14) \equiv 1 + 6 = 7$$

Ejemplo "especial"

$$IND(15) \equiv 11$$
$$IND(15) \equiv IND(3 \times 5)$$
$$IND(15) \equiv IND(3) + IND(5)$$
$$IND(15) \equiv 13 + 16 = 29$$
$$11 \equiv 29 \ (mód\ 18)$$
$$IND(15) \equiv 11$$

Se llamó "especial" porque su verificación no es la misma con respecto a los anteriores ejemplos, como se puede observar, la suma de los índices es mayor a 18, de forma general mayor que $p - 1$, entonces para comprobar la veracidad del resultado, se busca su entero congruente en módulo 18, pues como se ha visto, a un índice le corresponden varios números b.

En conclusión, con este patrón es posible ver que el índice de un número compuesto será igual a la suma de los índices de cada uno de sus factores en módulo $p-1$, la cual tiene una estrecha relación con la propiedad de los logaritmos: $\log(ab) = \log(a) + \log(b)$.

Caso 2: Conjunto P en el cual sus elementos son potencias cuyas bases son números primos.

$$P = \{4,8,9,16\}$$

Según la *Tabla 14*:

$$IND(b) \equiv e$$
$$IND(4) \equiv 2$$
$$IND(8) \equiv 3$$
$$IND(9) \equiv 8$$
$$IND(16) \equiv 4$$

Se expresan los b como potencias de números primos, por ejemplo $4 = 2^2$, según la *Tabla 14* se puede ver que el índice de 2 es 1, y al multiplicar este por su exponente 2 da como resultado el índice del número compuesto, para este caso 2.

Para mayor claridad a continuación se muestra el procedimiento para los otros elementos de P:

$$IND(4) \equiv 2$$
$$IND(4) \equiv IND(2^2)$$
$$IND(4) \equiv 2 \times IND(2)$$
$$IND(4) \equiv 2 \times 1 = 2$$

$$IND(8) \equiv 3$$
$$IND(8) \equiv IND(2^3)$$
$$IND(8) \equiv 3 \times IND(2)$$
$$IND(8) \equiv 3 \times 1 \equiv 3$$

$$IND(16) \equiv 4$$
$$IND(16) \equiv IND(2^4)$$
$$IND(16) \equiv 4 \times IND(2)$$
$$IND(16) \equiv 4 \times 1 = 4$$

Similar al ejemplo "especial" de la Caso 1:

$$IND(9) \equiv 8$$
$$IND(9) \equiv IND(3^2)$$
$$IND(9) \equiv 2 \times IND(3)$$
$$IND(9) \equiv 2 \times 13 = 26$$
$$8 \equiv 26(mód\ 18)$$
$$IND(9) \equiv 8$$

En resumen, el índice de un número compuesto por las potencias de un número primo es igual al producto del índice de la base y el exponente de la potencia en módulo $p - 1$. Al igual que en el Caso 1, aquí se puede nombrar y relacionar a otra propiedad presente en los logaritmos:

$$\log(\ a^b) = b\ \times log\ (a).$$

Al tener estos casos, la idea es facilitar procedimientos para adquirir $IND(b)$ de cada b, a continuación se muestran ejemplos de cómo se pueden utilizar:

$$IND(12) \equiv 15$$
$$IND(18) \equiv 9$$

Teniendo en cuenta los algoritmos para los casos 1 y 2, se tiene:

$$12 = 2^2 \times 3$$

El $\mathrm{IND}(12)$ es igual a la suma de los índices de sus factores (caso 1), es decir:

$$IND(3) + \mathrm{IND}(2^2),$$

pero como uno de los factores es una potencia de un numero primo (2^2), se utiliza el caso 2, que indica que es igual al índice de la base por su exponente:

$$IND(2) \times 2,$$

de lo que se obtiene: $IND(3) + IND(2^2) \equiv 13 + (1 \times 2) = 15$, donde se puede verificar la igualdad con $IND(12)$.

Se verifica lo anterior para $b = 18$:

$$IND(18) \equiv 9$$
$$IND(18) \equiv IND(2 \times 3^2)$$
$$IND(18) \equiv IND(2) + IND(3^2)$$
$$IND(18) \equiv 1 + [2 \times IND(3)]$$
$$IND(18) \equiv 1 + (2 \times 13) = 27$$
$$9 \equiv 27 \ (mód\ 18)$$
$$IND(18) \equiv 9$$

3.2 Teoremas de índices.

Con el anterior análisis se encuentra el índice para cualquier número; lo primero es conocer los índices de los primos menores a p; y luego, identificar si dicho índice se encuentra entre los números mayores, menores o múltiplos de p; con el fin de realizar los procedimientos que a continuación de muestran:

- Índices de números menores a p: en el caso que el número sea un entero positivo menor a p y compuesto, se puede utilizar el Caso 1, el Caso 2 o la combinación de los dos casos.
- Índices de números mayores a p (diferentes a múltiplos de p): si el número es mayor a p, entonces debe existir un b congruente a este número en módulo p, se debe analizar si el número es primo o si es compuesto.

- Índices de números múltiplos a p: No existen, ya que no existe una raíz primitiva que se eleve a cualquier exponente y de como residuo a 0.

De la proposición 58 (Gauss, 1995)[VIII] y de la ejemplificación anterior surgen tres teoremas importantes sobre índices, es por esto que a continuación se demuestran de manera formal cada uno de ellos:

Sea:

1. $a^e \equiv b\ (mód\ p)$ con a raíz primitiva de p donde $a^{p-1} \equiv 1\ (mód\ p)$, $p-1$ menor entero positivo que cumple la congruencia.
2. $IND(b) \equiv e$, escrito de otra forma es $a^e \equiv b\ (mód\ p)$.

Teorema 1:

El índice de una potencia de a (raíz primitiva asociada al módulo p) es congruente al exponente de la potencia en módulo $p-1$.

Para esto, se parte de:

$$IND(a^x) \equiv y$$

Utilizando a (2) se reescribes lo anterior:

$$a^y \equiv a^x (mód\ p)$$

Por la proposición 48 (Gauss, 1995) y de la anterior congruencia se obtiene:

$$y \equiv x (mód\ p-1)$$

Luego el índice (y) es congruente con el exponente de la potencia (x), es decir:

$$IND(a^x) \equiv x\ (mód\ p-1)$$

Teorema 2:

El índice del producto compuesto de cualquier número de factores es congruente, según el módulo p − 1, a la suma de los índices de los factores individuales.

[VIII] Los teoremas que tratan sobre los índices son completamente análogos a los que se refieren a los logaritmos.

Sea

$$IND(A) \equiv w$$

y

$$IND(B) \equiv u$$

Por (2) se tiene que:

$$a^w \equiv A(\text{mód } p)$$

y

$$a^u \equiv B(\text{mód } p)$$

Al multiplicar las dos congruencias anteriores se tiene:

$$a^w a^u \equiv AB(\text{mód } p)$$

Reescrito queda:

$$a^{w+u} \equiv AB(\text{mód } p)$$

Luego por Teorema 1 y reemplazando se tiene:

$$w + u \equiv IND(A) + IND(B)(\text{mód } p - 1)$$

Lo que significa

$$IND(AB) \equiv \big(IND(A) + \ IND(B)\big)\ (\text{mód } p - 1)$$

Teorema 3:

El índice de la potencia de un número cualquiera es congruente, según el módulo p −1, al producto del índice del número dado por el exponente de la potencia.

Al tener

$$IND(A) \equiv y$$

Se sabe que:

$$a^y \equiv A$$

Si se tiene un índice de la siguiente forma: $IND(A^n) \equiv y$, entonces:

$$IND(A^n) \equiv IND((a^y)^n) \equiv IND(a^{yn})$$

Por el teorema 1:

$$IND(a^{yn}) \equiv yn \ (m\acute{o}d\ p-1)$$

Reescribiendo y reemplazando a y:

$$IND(a^{yn}) \equiv n\ IND(A)(m\acute{o}d\ p-1)$$

Conclusiones

A lo largo del presente estudio logró demostrarse un campo amplio de exploración y comprobación de ideas expuestas por el matemático Gauss. Esto implicó un uso extensivo y reflexivo de conocimientos previos, argumentos, reglas y algoritmos lo que conllevó a la elaboración de hipótesis y conjeturas; procesos que posibilitaron una mejor comprensión e interpretación de los resultados.

Las afirmaciones y resultados encontrados fueron sometidos a pruebas de las cuales algunos se refutaron, juzgando su validez y otros se aceptaron bajo argumentos lógicos, como es el caso específico de la construcción de la función $\aleph: D(p-1) \rightarrow R_p$, función que en principio tiene un comportamiento similar a la función φ de Euler y cuyo proceso de construcción permite probar la igualdad de estas dos funciones a partir de los residuos de la congruencia $a^d \equiv 1\ (mód\ p)$; así, a través de la solución de un problema se obtiene un camino alternativo para estudiar la función φ de Euler.

De otro lado, los procesos de estudio posibilitaron la construcción de estructuras algebraicas como el grupo $\mathbb{Z}_{18}$ a partir de una partición en el conjunto de todas las potencias de 2 obtenida al evaluar los residuos que estas dejan al ser divididas entre 19. Ahora bien, la otra estructura algebraica construida, fue la de un retículo, el cual surgió al restringir el dominio de la función $\aleph$, donde se estudiaron los elementos de la forma $\Re = \{N^*(\{d\}) |\ d \in D(p-1)\}$. Con ayuda de tablas y de software matemático se definió operaciones y estudio su estructura. En general, las dos estructuras algebraicas son aportes que dinamizan la estructura del trabajo, pues como se evidenció, la teoría de números es el eje principal del estudio, luego la creación de estructuras algebraicas es uno de los productos finales de este trabajo aprovechando los resultados obtenidos.

En cuanto a nuestra formación como docentes, consideramos que la propuesta de trabajo de grado genera en nuestro quehacer diario la habilidad de saber y juzgar el porqué de ciertas realidades matemáticas. Así mismo, nos direcciona hacia la implementación de procesos donde se vea la enseñanza impartida como la acción de guiar y facilitar el descubrimiento y el pensamiento crítico, claro está sin olvidar todo el sistema conceptual previo.

Bibliografía

Ángel, J. Software Álgebra finita 1.0. [CD-ROM]: Windows 95 o posterior. Bogotá, Colombia: Universidad Pedagógica Nacional, 2011.

Ávila, J. C. (2011). *Actividades matemáticas para formular teoremas en teoría de números y grupos*. Bogotá: Universidad Pedagógica Nacional.

García, J. (2005). Capítulo 3. Recuperado el junio de 2015, de Conjuntos ordenados. Retículos y álgebra de Boole.: http://www.ugr.es/~jesusgm/Curso%202005-2006/Matematica%20Discreta/Ordenes.pdf

Gauss, C. F. (1995). Disquisitiones Arithmeticae. (M. J. Hugo Barrantes, Trad.) Costa Rica: Universidad de Costa Rica.

Leveque, W. (1968). Teoría elemental de los números. (C. E. Gortari, Trad.) México: Herreros Hermanos, sucesores S.A.

Luque, C., Mora, L., Torres, J. (2014). Actividades matemáticas para el desarrollo de procesos lógicos: Clasificar, medir e invertir. Bogotá: Universidad Pedagógica Nacional.

Moreno, N., Fernández, J., Beltrán, Y., & García, J. (2014). Residuos de potencias: estudio de casos. Bogotá: Universidad Pedagógica Nacional.