© Revista de Matemática: Teoría y Aplicaciones 2019 **26**(2) : 299–318
cimpa – ucr issn: 1409-2433 (Print), 2215-3373 (Online)
doi: https://doi.org/10.15517/rmta.v26i2.38320

Grafo n-residual módulo m y su aplicación en la estructuración de residuos n-ádicos

n-residual module m graph and its application in structuring n-adic residuals

Iveth Martínez* René Solís†

Received: 19/Apr/2018; Revised: 25/Jun/2019;
Accepted: 28/Jun/2019

*Universidad de Panamá, Centro Regional Universitario de Panamá Oeste, Departamento de Matemática, Provincia de Panamá Oeste, Panamá. E-Mail: iveth.martinez@up.ac.pa
†Universidad Tecnológica de Panamá, Facultad de Ciencias y Tecnología, Departamento de Matemática, Ciudad de Panamá, Panamá. E-Mail: rene.solis@utp.ac.pa

Resumen

En este estudio analizamos el comportamiento de los residuos de un módulo elevado a una potencia n y su relación con los conjuntos n-*residuales*, los grafos de residuos de potencia, llamados grafos n-*residuales* y las raíces primitivas en el mismo módulo. Con los conjuntos obtenidos, los grafos reducidos y árboles complementarios, se establecieron algunas propiedades que se comprobaron en rutinas desarrolladas con *Mathematica*, brindando una interpretación visual de las estructuras, objeto del estudio, permitiendo realizar varias pruebas con distintos valores de número primo impar p. Con lo cual, se llegó a algunas conjeturas interesantes con posibles resultados formales.

Palabras clave: raíces primitivas; conjunto n-residual; residuos n-ádicos; n-grafos.

Abstract

In this study we analyze the behavior of the residuals of a module, raised to a power n and its relation with the n-*residual* sets, the graphs of residuals of power, called n-*residual* graphs and the primitive roots in the same module. With the obtained sets, the reduced graphs and complementary trees were established some properties that are analyzed in routines developed with *Mathematica*, providing a visual interpretation of the structures, object of the study, and allowing several tests with different values for odd prime number p. With obtained some interesting conjectures with possible formal results.

Keywords: primitive roots; n-residual set; n-adic residuals; n-graphs.

Mathematics Subject Classification: 11F33.

1 Introducción

Una de las herramientas más importantes en la teoría elemental de los números es la aritmética modular o congruencias, la cual relaciona dos cantidades que dividido por un tercero, llamado módulo, dejan el mismo resto. Estos restos o residuos pueden ser generados por raíces primitivas, el cual genera un conjunto de números coprimos al módulo.

La aritmética modular, proporciona ejemplos clave para la teoría de grupos, la teoría de anillo y el álgebra abstracta. Estos conceptos no solo se limitan a la teoría sino que también son de gran apoyo en diversas aplicaciones, como el cálculo de las sumas de verificación dentro de identificadores, en el caso de cuentas bancarias. En criptografía, esta teoría respalda directamente los sistemas de clave pública siendo la base de diversos algoritmos de clave simétrica. En informática, se aplica a menudo en operaciones *bitwise* y otras que involucran estructuras de datos cíclicos de ancho fijo. El último número de regisro CAS, que es un número único para cada compuesto químico, es de gran apoyo en la química. En general, también es utilizado en otras disciplinas como la complejidad computacional, la música, las leyes, la economía y otras áreas de las ciencias sociales donde la división proporcional y la asignación de recursos juega una parte importante del análisis.

En este trabajo se estudiarán los conjuntos n-residuales de módulo m, sus propiedades y su relación con el conjunto de raíces primitivas, con el apoyo de los grafos de residuos de potencia. Para su análisis, haremos uso del álgebra computacional, fundamentándonos en el software *Mathematica*, con el cual se mostrarán algunas de las rutinas diseñadas para tal fin. Iniciamos con algunos conceptos básicos importantes para el entendimiento y desarrollo sistemático de la teoría, hasta culminar con el establecimiento y comprobación de algunas propiedades, así como el estudio del comportamiento de las estructuras obtenidas.

2 Preliminares

Decimos que un entero b es divisible por un entero no nulo a, si existe un entero x tal que $b = ax$ y se denota $a|b$ ($a \nmid b$ es su negación). El máximo común divisor de dos números a y b, es el mayor entero c que divide a ambos y lo denotaremos $(a, b) = c$. Del mismo modo, el mínimo común múltiplo, es el menor entero d que contenga a a y b, denotado $[a, b] = d$. Recordemos que dos números enteros positivos a y b son primos relativos o coprimos si $(a, b) = 1$.

Los números enteros cumplen propiedades que se pueden revisar en [10], entre estas uno de los resultados importantes de esta teoría es el algoritmo de división que se enuncia a continuación.

Teorema 1 *Dados los enteros a positivo y b arbitrario, existe solamente una pareja de enteros q, r tales que se cumplen las condiciones:*

$$a = bq + r, \;\; 0 \leq r < b.$$

A q se le conoce como cociente y a r residuo, en caso que $r = 0$ se tiene que $a = bq$ y se dice que b divide a a, representándolo como $b|a$.

Otro concepto de mucha importancia es la congruencia, que según [3], “si un número m divide la diferencia de los números a y b, se dice que a y b son congruentes según el módulo m, si no lo son, se dice que son incongruentes; el número m se llama módulo”.

Lo anterior se escribe formalmente: sea $m \in \mathbb{N}$, se define sobre $\mathbb{Z}$ una relación como: $\forall a, b \in \mathbb{Z}$, $a \cong b \mod (m)$ si y solo si $m|(a-b)$, de lo contrario $a \ncong b \mod (m)$.

Cuando se trabaja con congruencias de módulo m, el conjunto de los enteros se convierte en m clases, las cuales se llaman clases residuales, tales que dos elementos cualesquiera de la misma clase son congruentes y dos elementos de dos clases diferentes son incongruentes. Las clases residuales son también llamadas progresiones aritméticas de diferencia m, lo que significa que las posibles soluciones se restringen a una cantidad finita de valores posibles.

Definición 1 *Un conjunto de enteros* $\{a_1, a_2, \ldots, a_n\}$ *se le conoce como sistema completo de residuo módulo* m*, si cumple:*

i) $a_i \neq a_j \mod (m)$ *para* $i \neq j$.

ii) Sea $n \in \mathbb{Z}$*, existe un índice* i*,* $1 \leq i \leq m$*, para el cual* $n \cong a_i \mod (m)$.

Así, el sistema completo de residuos está compuesto por m elementos, en cambio el sistema reducido de residuos está compuesto por todos los residuos coprimos con m. Esta medida, que depende de m, es conocida como la función de Euler y se denota $\varphi(m)$. Para $m > 1$, $\varphi(m)$ se puede definir como el número de enteros positivos menores que m y coprimos de m. La función de Euler cumple con propiedad multiplicativa (ver en [11]).

A partir de lo planteado, se puede deducir para un número primo p impar, que

$$\varphi(p^n) = p^n \left(1 - \frac{1}{p}\right)$$

y para determinar cuántas potencias hay, escribimos un número la función de Euler para un número n, $\alpha_i \in \mathbb{N}$ y p_i primo, de la forma

$$n = \prod_{i=1}^{k} p_i^{\alpha_i},$$

$$\varphi(n) = \varphi\left(\prod_{i=1}^{k} p_i^{\alpha_i}\right) = \prod_{i=1}^{k} \varphi\left(p_i^{\alpha_i}\right) = \prod_{i=1}^{k} p_i^{\alpha_i}\left(1 - \frac{1}{p_i}\right).$$

Si $f(x)$ es un polinomio no constante, se plantea encontrar todos los valores enteros u tales que

$$f(u) \cong 0 \mod (m),$$

entonces u será una solución de la congruencia. De manera que la cantidad de soluciones de una congruencia $f(x) \cong 0 \mod (m)$ es el número de soluciones de la congruencia en un sistema completo de resto. Para el caso de la congruencia lineal, que se expresa como $ax \cong b \mod (m)$, si existe un entero k tal que $ax \cong b + km$ y si la congruencia tiene una única solución, entonces $(m, a)|b$ dado en el siguiente teorema.

Teorema 2 *Una condición necesaria y suficiente para que la congruencia*

$$ax \cong b \mod (m)$$

tenga una única solución es que $(m, a)|b$. En caso contrario existirá exactamente (m, a) solución módulo m.

Es posible resolver un sistema de ecuaciones lineales módulo m, aplicando el Teorema Chino de los Restos (ver en [1]).

Para el estudio trabajaremos con secuencia que resulta cuando las potencias son todas reducidas a sus mínimos residuos módulo m, donde $(a, m) = 1$ y los módulos sean primos.

Definición 2 *El orden de a módulo m, denotado $ord_m a$, es el menor entero positivo n tal que*

$$a^n \cong 1 \mod (m).$$

Es posible verificar que la longitud del periodo estará determinado por $m - 1$. El siguiente teorema es una generalización del famoso pequeño Teorema de Fermat, (ver [4]), el cual introduce polinomios con un número máximo de raíces.

Teorema 3 *Si p es primo y $d|(p - 1)$, entonces existen exactamente d raíces de la congruencia*

$$x^d \cong 1 \mod (p).$$

Definición 3 *Si a es miembro del exponente $\varphi(m)$ módulo m, entonces a recibe el nombre de raíz primitiva módulo m.*

La rutina en la Figura 1 obtiene las raíces primitivas para un módulo n.

```
rpr[n_] :=
 (A={}; Table[If[MultiplicativeOrder[i, n] = EulerPhi[n],
  A = Append[A, i]], (i, n-1)]; A)
```

Figura 1: Rutina en *Mathematica* que calcula las raíces primitivas respecto a un módulo dado n.

La importancia de este concepto radica en que si g es una raíz primitiva, entonces sus potencias g, g^2, $\ldots$,$g^{\varphi(m)}$ son distintas módulo m, y además son coprimos con m. Esto constituye un sistema residual reducido módulo m, así presentado y analizado en [7]; existen exactamente $\varphi(\varphi(p))$ raíces primitivas de un número primo p y sin entrar en detalle, los números que tienen raíces primitivas son exactamente aquellos de la forma 2, 4, p^α y $2p^\alpha$ con α entero positivo y p primo impar.

Definición 4 *Sea g una raíz primitiva de q, entonces llamaremos índice de a a la potencia de g que genere a y lo denotaremos por $ind_g(a)$.*

En la Figura 2 se muestra la rutina que obtiene el índice de a a la potencia de g, y con la rutina de la Figura 3 se generan los índices de cada raíz primitiva.

```
indice[a_, n_] := (MultiplicativeOrder[PrimitiveRoot[n], n, a])]
```

Figura 2: Índice de a módulo n respecto a la primera raíz primitiva.

```
copin[n_] := (A = rpr[n];
 t = EulerPhi@EulerPhi[n];
 TableForm[Table[MultiplicativeOrder[A[[i]]], n, j], {j, n-1}, {i, t}]])
```

Figura 3: Código para generar los índices respecto a cada raíz primitiva.

Conociendo una raíz primitiva, es posible determinar los índices de los elementos de un sistema reducido y es útil para estudiar las congruencias de la forma $x^n \cong c \mod (p)$, pero por su complejidad, el Teorema 4 presenta una forma más conveniente del análisis del mismo.

Teorema 4 *Sea $(c, q) = 1$, entonces una condición necesaria y suficiente para que la congruencia*

$$x^n \cong c \mod (q)$$

tenga solución es que $c^{(\varphi(q)/d)} \cong 1 \mod (q)$, donde $d = (n, \varphi(q))$.

Definición 5 *Si $x^n \cong c \mod (m)$ tiene solución y $(m, c) = 1$, entonces se dice que c es una potencia n-ésima residual de m.*

3 Conjuntos n-residuales módulo m

Estudiamos algunas condiciones en que la ecuación $x^n \cong a \mod (m)$ admite solución, en este punto determinaremos cuáles y cuántas serán las soluciones, y además se analizarán como varían las mismas conforme a enteros positivos m y n dados. Dado el conjunto reducido de residuos módulo m, $\mathbb{Z}_m^*$, es fácil verificar que el mismo forma un grupo bajo el producto usual y es de orden $\varphi(m)$.

Definición 6 *Un conjunto n-residual módulo m o simplemente n conjunto de m, se define como:*

$$\psi_{m,n} = \{a \in \mathbb{Z}_m^* : x^n \cong a \mod (m)\}.$$

Para el caso de $m = 11$, consideremos $n = 1$, 3 y 10 se puede obtener, utilizando en conjunto las rutinas dada en las Figuras 4 y 5, se obtiene los conjuntos

$$\psi_{11,1} = \mathbb{Z}_{11}^*, \qquad \psi_{11,3} = \mathbb{Z}_{11}^*, \qquad \psi_{11,10} = \{1\}.$$

```
crn[m_, n_] := (A = {};
  Table[If[GCD[m, i] == 1, A = Append[A, PowerMod[i, n, m]]], {i, m-1}];
  DeleteDuplicates[A])
```

Figura 4: Código para generar el conjunto $\psi_{m,n}$ n-residual de módulo m.

```
crn[m_, n_] := (A = {};
  Table[If[GCD[m, i] == 1, A = Append[A, PowerMod[i, n, m]]], {i, m-1}];
  DeleteDuplicates[A])
```

Figura 5: Determina los valores que satisfacen $\psi_{m,n} = \mathbb{Z}_m^*$.

Realizando diversas pruebas con las rutinas mostradas, se verifica que $(\psi_{m,n}, \cdot)$ es un subgrupo de $(\mathbb{Z}_m^*, \cdot)$.

Teorema 5 *Sean p, q, m y $n \in \mathbb{N}$, entonces*

a) $\psi_{m,n} \subseteq \mathbb{Z}_m^*$.

b) $\psi_{m,\varphi(m)} = \{1\}$.

c) Si $p \cong q \mod \varphi(m)$ entonces $\psi_{m,p} = \psi_{m,q}$.

d) Si $a \in \psi_{m,n}$ entonces $a^k \in \psi_{m,n}$, para todo $k \in \mathbb{Z}^+$.

Demostración: a) Sea $a \in \psi_{m,n}$, por definición tenemos $\psi_{m,n} \subseteq \mathbb{Z}_m^*$.
b) Sabemos que si $(a, m) = 1$, entonces $a^{\varphi(m)} \cong 1 \mod m$, tenemos que para todo $b \in \mathbb{Z}_m^*$

$$b^{\varphi(m)} \cong 1(mod\ m),$$

entonces la ecuación

$$x^{\varphi(m)} \cong a(mod\ m)$$

admite solución si y solo si $a = 1$. Por lo que

$$\psi_{m,\varphi(n)} = \{1\}.$$

c) Sin perder generalidad, sea $p > q$, luego

$$p = n \cdot \varphi(m) + q,$$

para algún entero n. Ahora

$$\begin{aligned} \psi_{m,p} &= \{a \in \mathbb{Z}_m^* : x^p \cong a(mod\ m)\} \\ &= \{a \in \mathbb{Z}_m^* : x^{n\cdot\varphi(m)+q} \cong a(mod\ m)\} \\ &= \{a \in \mathbb{Z}_m^* : x^{n\cdot\varphi(m)} x^q \cong a(mod\ m)\} \\ &= \{a \in \mathbb{Z}_m^* : x^{\varphi(m)^n} x^q \cong a(mod\ m)\} \\ &= \{a \in \mathbb{Z}_m^* : x^q \cong a(mod\ m)\} = \psi_{m,q}. \end{aligned}$$

d) Sea $a \in \psi_{m,n}$, luego

$$x^n \cong a(mod\ m),$$

elevamos ambos términos a la t y se tiene

$$\begin{aligned} (x^n)^t &\cong a^t(mod\ m), \\ (x^t)^n &\cong a^t(mod\ m). \quad \blacksquare \end{aligned}$$

El recíproco de c) no es cierto, esto se puede verificar con los conjuntos $\psi_{m,n}$ para $m = 11$, específicamente si $\psi_{11,2} = \psi_{11,6} = \{1, 3, 4, 5, 9\}$, pero $2 \ncong 6 \mod (10)$. Como los n-conjuntos son subgrupos del sistema reducido de m, su cardinal será un divisor de $\varphi(m)$. Por lo que el recíproco de $d)$ igual no es cierto, ya que $4 \in \psi_{11,2}$, pero $4 = 2^2$ y $2 \notin \psi_{11,2}$.

La cardinalidad de los n-conjuntos se formalizará con el teorema que se presenta a continuación.

Teorema 6

$$|\psi_{m,n}| = \frac{\varphi(m)}{d},$$

donde m admite raíz primitiva y $d = (\varphi(m), n)$.

Demostración: Se tiene que $x^n \cong c \mod (m)$ posee una solución única solo si $c^{\varphi(m)/d} \cong 1 \mod (m)$. Si $d = 1$, es obvio que $\varphi(m) = |\mathbb{Z}^*|$, en el caso de que $d > 1$ y $(\varphi(m))/d < \varphi(m)$, cada $c \in \mathbb{Z}_m^*$ deberá poseer como factor común a $\varphi(m)/d$. En caso contrario no se satisface la congruencia. Luego como $d|\varphi(m)$, se obtiene que

$$\sum_{k|\varphi(m)/d} k = \varphi(m)/d.$$

Por tanto

$$|\psi_{m,n}| = \frac{\varphi(m)}{d}. \qquad \blacksquare$$

Una propiedad adicional que se puede deducir de la parte d) del Teorema 5, es que

$$\psi_{m,pq} \subseteq \psi_{m,p},$$

de gran utilidad para la demostración del teorema, el cual formaliza la intersección entre estos conjuntos.

Teorema 7 *Se tiene $\psi_{m,p} \cap \psi_{m,q} = \psi_{m,r}$, donde $r = [p,q]$ y m admite una raíz primitiva.*

Demostración: Veamos primero que $\psi_{m,p} \cap \psi_{m,q} \subseteq \psi_{m,r}$. Como $r = [p,q]$, entonces $r = ap = bq$ para algún $a, b \in \mathbb{N}$. De esta manera

$$\psi_{m,r} = \psi_{m,ap} \subseteq \psi_{m,p},$$

$$\psi_{m,r} = \psi_{m,bq} \subseteq \psi_{m,q}.$$

Luego

$$\psi_{m,r} \subseteq \psi_{m,p} \cap \psi_{m,q}.$$

Ahora sea $a \in \psi_{m,p} \cap \psi_{m,q}$ y g una raíz primitiva de m, entonces:

$$\begin{aligned} a \in \psi_{m,p} \cap \psi_{m,q} \quad &\Rightarrow \quad a \in \psi_{m,p} \quad \wedge \quad a \in \psi_{m,q} \\ &\Rightarrow \quad a \cong g^{cp} \mod (m) \quad \wedge \quad a \cong g^{dq} \mod (m) \\ &\Rightarrow \quad a \cong g^{cp} \cong g^{dq} \mod (m) \\ &\Rightarrow \quad x \cong cp \cong dq \mod (\varphi(m)). \end{aligned}$$

Luego existe un x tal que tenga como factor a p y q de manera que $x = rz$, con $z \in \mathbb{N}$, nos queda

$$a \in \psi_{m,x} \Leftrightarrow a \in \psi_{m,rz} \Rightarrow a \in \psi_{m,r}. \quad \blacksquare$$

A pesar de esto, mediante cálculos computacionales es posible verificar la veracidad para todo número entero positivo menor que 100000, tengamos en cuenta, dado el caso de que $(p, q) = 1$ entonces $[p, q] = pq$, de esto deducimos lo siguiente: sea n un entero positivo, luego por el teorema fundamental de la aritmética, se tiene que

$$n = \prod_{i=1}^{k} p_i^{\alpha_i} \Rightarrow \bigcap_{i=1}^{k} \psi_{m,p_i^{\alpha_i}}.$$

De esta manera, sólo se revisarán los casos en que $(p_i, \varphi(m)) > 1$, conociendo que la intersección de un subconjunto con el conjunto, es igual al subconjunto propio.

4 Raíces primitivas y residuos n-ádicos

Una vez caracterizados los conjuntos n-residuales en el punto anterior, daremos otro enfoque que establezca su relación con las raíces primitivas. Los n-conjuntos contendrán a las potencias n-ésimas residuales de m, así para $n = 2, 3, 4$ se les conoce como cuadráticos, cúbicos y cuárticos, respectivamente y han sido objetos de muchos estudios, como se verá más adelante.

Definición 7 *Sea m un entero positivo, el conjunto de las raíces primitivas se define como:*

$$\chi_m = \{a \in \mathbb{Z}_m^* : a^\lambda \cong 1 \mod (m) \Leftrightarrow \varphi(m)|\lambda\}.$$

Las propiedades que cumple el conjunto de las raíces primitivas, se presentan en el siguiente teorema.

Teorema 8 *Sea $m \in \mathbb{Z}^+$, entonces:*

a) $\chi_m \neq \emptyset$ *si* $m =$ *2, 4,* p^α *y* $2p^\alpha$ *con* $\alpha \in \mathbb{N}$.

b) $|\chi_m| = \varphi(\varphi(m))$ *si* m *toma los valores en a).*

c) $\chi_m \subsetneqq \mathbb{Z}_m^*$.

Ejemplo 1 *Se quiere determinar χ_{11}. Es obvio que 1 y 10 no pueden pertenecer a χ_{11} pues su orden será 1 y 2, respectivamente. Por lo que tenemos.*

$$\begin{array}{ll} 2^2 \cong 4 & 2^5 \cong 10 \\ 3^2 \cong 9 & 3^5 \cong 1 \\ 4^2 \cong 5 & 4^5 \cong 1 \\ 5^2 \cong 3 & 5^5 \cong 1 \\ 6^2 \cong 3 & 6^5 \cong 10 \\ 7^2 \cong 5 & 7^5 \cong 10 \\ 8^2 \cong 9 & 8^5 \cong 10 \\ 9^2 \cong 4 & 9^5 \cong 1. \end{array}$$

Así que, $\chi_{11} = \{2, 6, 7, 5\}$.

Se observa que el conjunto de raíces primitivas χ_m, por definición, se forman de aquellos conjuntos residuales de orden $\varphi(m)$. Sin embargo, el orden de los elementos de los n-conjuntos, tales que $(n, \varphi(m)) > 1$, será menor o igual que $\varphi(m)/(n, \varphi(m))$ [1].

Para aquellos que no pertenezcan, su orden será mayor a los que sí están contenidos, es decir

$$a \in \psi_{m,n} \quad \Rightarrow \quad ord_m(a) \leq \frac{\varphi(m)}{(n, \varphi(m))},$$

$$a \notin \psi_{m,n} \quad \Rightarrow \quad ord_m(a) > \frac{\varphi(m)}{(n, \varphi(m))}.$$

En el caso $(n, \varphi(m)) = 1$, tenemos que $\chi_m = \mathbb{Z}_m^*$, lo que origina la relación que se muestra en el teorema siguiente.

Teorema 9 *Se tiene* $\chi_m = \bigcap_{i=1}^k \psi_{m,p_i}^c$, *donde* $\varphi(m) = \prod_{i=1}^k p_i^{\alpha_i}$ *y* $\psi_{m,n}^c = \mathbb{Z}_m^* - \psi_{m,n}$.

Demostración: Para $(n, \varphi(m)) > 1$, cada elemento de $\psi_{m,n}$ es de orden menor que $\varphi(m)$, por lo tanto, una condición necesaria para que sea una raíz primitiva es que no pertenezca a ningún n-conjunto, de manera que $n/\varphi(m)$.

$$\chi_m = \bigcap_{t|\varphi(m)} \psi_{m,t}^c.$$

[1] Se debe al resultado "Si $ord_m a = t \Rightarrow ord_m a^n = t/(n, t)$" en [1].

Basta delimitar los divisores a los primos divisores de $\varphi(m)$, quedando

$$\chi_m = \bigcap_{i=1}^{k} \psi^c_{m,p_i},$$

donde $\varphi(m) = \prod_{i=1}^{k} p_i^{\alpha_i}$. ■

Teorema 10 *$(n, \varphi(m)) = 1$ si y solo si $\psi_{m,n} \cap \chi_m \neq \emptyset$, donde m admite raíz primitiva.*

Demostración:
$\Rightarrow$) Si $(n, \varphi(m)) = 1$, entonces $\psi_{m,n} = \mathbb{Z}^*_m$ y como m admite raíz primitiva, tenemos que $\chi_m \neq \emptyset$ y $\varphi_{m,n} \subsetneqq \mathbb{Z}^*_m$, por lo tanto

$$\chi_m \bigcap \psi_{m,n} = \chi_m \bigcap \mathbb{Z}^*_m = \chi_m \neq \emptyset.$$

$\Leftarrow$) Sea $a, g \in \chi_m$ entonces se puede expresar a a como una potencia de g, así $g^k \cong a \mod (m)$ con $(k, \varphi(m)) = 1$.

Como $a \in \psi_{m,n}$, entonces satisface la ecuación $x^n \cong a \mod (m)$, de manera que se puede expresar a x como potencia de g

$$g^{ny} \cong x^n \cong a \cong g^k \mod (m).$$

Por tanto, $ny \cong k \mod (\varphi(m))$, luego por las propiedades de congruencias y $(ny, \varphi(m)) = 1$, concluyendo que $(n, \varphi(m)) = 1$. ■

5 Los grafos n-residual en potencias de raíces primitivas

Ampliaremos algunas propiedades analizadas y la justificación de algunos resultados pueden ser representados por medio de grafos[2], pero en este caso nos apoyaremos en los grafos n-residuales. Nos adentraremos a desarrollar la teoría de grafo para el análisis que nos compete generalizando algunas definiciones y propiedades de la misma, con las que podamos sustentar el propósito del estudio.

Definición 8 *Un grafo n-residual de módulo m se define como:*

$$G_{m,n} = (V, E).$$

Donde $V = \mathbb{Z}_m$ es el conjunto de vértices y las aristas $E = \{\{a, a^n\} : a \in \mathbb{Z}_m\}$.

```
mata[m_, n_] :=
  Table[If[i == Mod[j^n, m], a[j, i] = 0], {j, 0, m - 1}, {i, 0, m-1}]

exprilm_,n_] := AdjacencyGraph[mata[m,n], VertexLabels->Table[i->i-1,
  {i,m}],DirectEdges -> True, EdgesStyle -> Arrowheads[Medium]]
```

Figura 6: La rutina *mata* genera la matriz adyacente del grafo de la iteración exponencial y la rutina *expri1* construye el grafo $G_{m,n}$.

Aclararemos el concepto dado de grafos n-residuales y sus representaciones en el siguiente ejemplo, desarrollado con el apoyo del software *Mathematica 8* (ver Figura 6).

Ejemplo 2 *En la Figura 7 se pueden ver las representaciones de los grafos* $G_{15,3}$ *y* $G_{13,2}$.

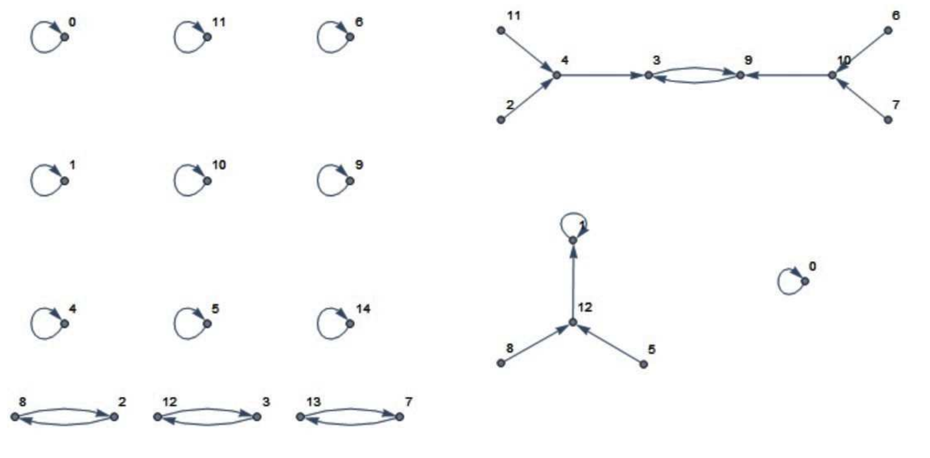

Figura 7: Grafo $G_{15,3}$ y $G_{13,2}$.

[2]La teoría de grafos y sus propiedades, que no se desarrollan en este contexto, se puede encontrar en [9].

Podemos observar en la Figura 7 que el grafo $G_{15,3}$ mantiene un patrón que, comparándolo con el grafo $G_{13,2}$, se puede establecer lo siguiente:

1. El grado[3] de salida de cada vértice es 1.

2. Los vértices del grafo $G_{13,2}$, que pertenecen al conjunto $\psi_{13,2} = \{1, 3, 4, 9, 10, 12\}$ tienen grado de llegada 2 y 0 en los vértices que son raíces primitivas de 13, como 2, 6, 7 y 11.

3. En el grafo $G_{13,2}$, se puede observar que la suma de los vértices que tiene dos aristas de llegadas, da un número m, que en este caso es 13 o suplementario de 13. Como el caso de los vértices 4 y 9 que llegan a 3, resulta que $9 + 4 = 13$.

Antes de revisar con mayor detalle lo analizado en el Ejemplo 1, es importante observar que el cardinal del conjunto de las aristas y de los vértices será igual al módulo, es decir

$$|V| = |E| = m.$$

Esto se puede verificar, ya que como vimos, el sistema completo de residuos posee m elementos y además que $gr(a)^- = 1$ para todo $a \in \mathbb{Z}_m$ y por las propiedades de la matriz de adyacencia, se sigue que $|E| = m$.

Definición 9 *Se llama a* $G^*_{m,n} = (\mathbb{Z}^*_m, E^*)$ *el grafo* n*-residual reducido de* m*, donde* $E^* = \{\{a, a^n\} : a \in \mathbb{Z}^*_m\}$.

Es evidente que $G^*_{m,n}$ es un subgrafo de $G_{m,n}$ y a partir del Ejemplo 1, se tienen los subgrafos $G^*_{15,3}$ y $G^*_{13,2}$.

Definición 10 *La representación de los grafos reducidos, se obtiene al suprimir aquellos vértices que no forman parte del sistema reducido de residuos,* $G^*_{15,3}$ *y* $G^*_{13,2}$ *(ver Figura 8).*

---

[3]El grado de un vértice u es el número de aristas que se conectan al vértice dado, de ser un grafo no dirigido, lo denotaremos por $gr(u)$, de lo contrario se denotará por $gr^-(u)$ a los que parten de u y $gr^+(u)$ a los que llegan a u.

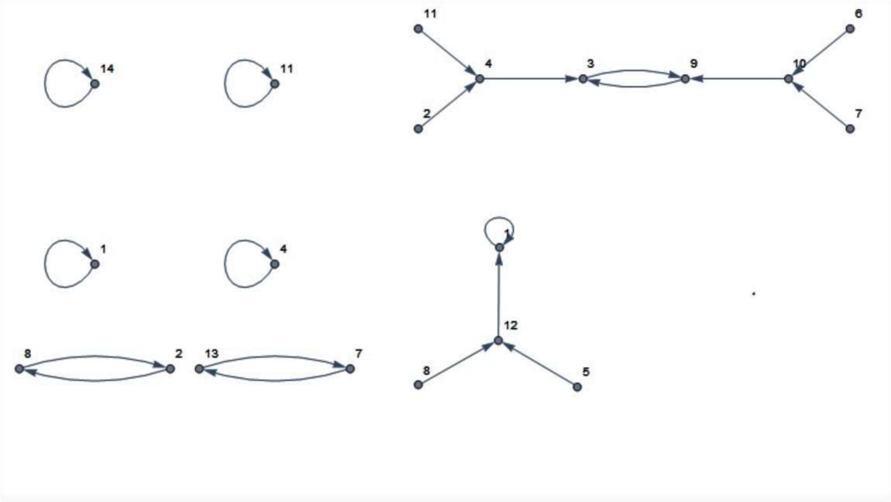

Figura 8: Grafo $G^*_{15,3}$ y $G^*_{13,2}$.

Ahora introduciremos la incidencia de un ciclo, suponiendo que cada residuo coprimo se eleva a un entero n tal que $(n, \varphi(m)) = 1$, entonces por definición se tiene que

$$x^n \cong r \mod (m),$$

donde las aristas tiene dirección de x a r. Sea g una raíz primitiva de m, entonces $y = ind_g(x)$ y $b = ind_g(r)$, por lo que

$$\begin{aligned} g^{yn} &\cong g^b \mod (m) \\ g^{y^n} &\cong g^b \mod (m) \\ n^y &\cong b \mod (\varphi(m)). \end{aligned}$$

Pero $(n^y, \varphi(m)) = 1$, por tanto $(b, \varphi(m)) = 1$, los que nos lleva a que x y r posean el mismo exponente. Si existen caminos $a_1 \to a_2 \to a_3 \to \ldots \to a_n$, obteniendo

$$\begin{aligned} &a_1^n \cong a_2 \mod (m) \\ &a_2^n \cong a_3 \mod (m) \quad \Rightarrow \quad a_1^{n^2} \cong a_3 \mod (m) \\ &a_3^n \cong a_4 \mod (m) \quad \Rightarrow \quad a_1^{n^3} \cong a_4 \mod (m). \end{aligned}$$

Luego, por inducción obtenemos

$$a_1^{n^i} \cong a_{i+1} \mod (m).$$

Evidentemente se cumple para $i=1$, asumamos que se cumple para $i=k$ de manera que se probará para $k+1$

$$\begin{aligned} a_{k+2} &\cong (a_{k+1})^n \mod (m) \\ &\cong (a_1^{n^k})^n \mod (m) \\ &\cong a_1^{n^{k+1}} \mod (m). \end{aligned}$$

Determinamos la longitud de los ciclos, así consideremos k como el exponente de a_1 y sabemos que $a_1|\varphi(m)$ y que m admite raíz primitiva. Tomemos g tal que, $g^{\varphi(m)/k} \cong a_1 \mod (m)$, resulta

$$(g^{\varphi(m)/k})^{n^i} \cong a_1^{n^i} \mod (m).$$

Por lo que se tiene que

$$(g^{\varphi(m)/k})^{n^i} \cong a_{i+1} \mod (m).$$

Como $(n,\varphi(m))=1$, se tiene que $(n,k)=1$, por lo que el período del ciclo estará dado por el exponente de n módulo k. Esto nos indica que los ciclos de los n-grafos cuando m admite raíces primitivas, serán divisibles por $\varphi(\varphi(m))$. Por lo tanto, los ciclos son de longitud divisible por $\varphi(\varphi(m))$.

Se evidencia que la longitud máxima posible de un ciclo es $\varphi(\varphi(m))$, pero para que esto se cumpla, n debe tener exponente $\varphi(\varphi(m))$, lo que indica que n debe ser una raíz primitiva de $\varphi(m)$ de la forma 2, 4, p ó $2p$, donde p es un primo de la forma $2q^\alpha+1$ con q primo impar y α entero no negativo.

El número de ciclos para 2 será 1, para el caso 4 será 2, en cambio para los primos impares está dado por el número de divisores de la forma $\varphi(p)=2q^\alpha$, lo que nos da $2(\alpha+1)$. Por lo que existirá un número par de ciclos en grafos respectivos. Sea w un número primo impar de la forma $2q^\alpha+1$, donde q es primo impar, α entero no negativo y n una raíz primitiva de $\varphi(w)$, entonces si

$$\begin{aligned} a^{n^i} &\cong a \mod (m) \\ n^i &\cong 1 \mod (\varphi(m)), \end{aligned}$$

se tiene que $\varphi(\varphi(m))|i$, por tanto admite ciclos de longitud máxima $\varphi(\varphi(m))$. Otras propiedades de los n-grafos con nuevas condiciones son los pares de ciclos, sus longitudes serán dos de $\varphi(q^\alpha)$, uno que contendrá a los elementos de orden q^α y $2q^\alpha$, dos de $\varphi(q^{\alpha-1})$, uno que contendrá a los elementos de orden $q^{\alpha-1}$ y $2q^{\alpha-1}$ y así respectivamente hasta obtener a los de orden 1 y 2. Esto se ilustrará con los grafos del ejemplo, a continuación.

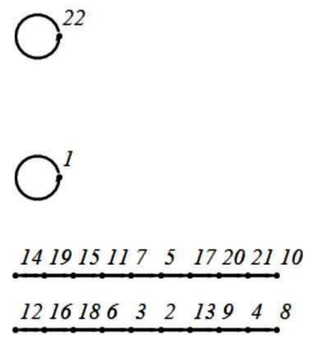

Figura 9: Grafo $G^*_{23,7}$.

Ejemplo 3 *Consideremos el módulo 23, de manera que* $\varphi(23) = 22 = 2 \cdot 11$, *que a su vez admite raíz primitiva, seleccionando* $n = 7$. *El grafo correspondiente se presenta en la Figura 9.*

Ejemplo 4 *Tomemos el módulo 251 y* $n = 3$, *después de realizar los cálculos correspondientes se obtiene el esquema mostrado en la Figura 10, en que se omitieron los vértices para no saturar el diagrama.*

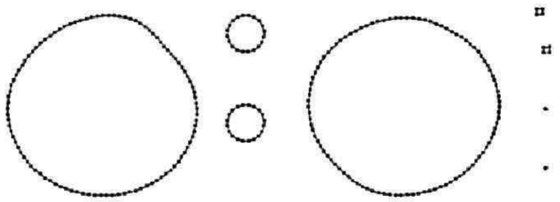

Figura 10: Grafo $G^*_{251,3}$.

En las Figuras 9 y 10 se observa que un ciclo de determinada longitud tiene cierto orden de elementos, el otro ciclo estará compuesto de los complementos suplementarios de los elementos del otro ciclo en el mismo orden.

Teorema 11 *Sea* $G^*_{m,n}$, *con* n *coprimo de* $\varphi(m)$, *entonces para cada ciclo de longitud* k, *existirá otro de igual longitud donde el orden posicional de cada elemento será suplementario al primer grafo. Es decir, si el ciclo es de la forma* $\langle a_1, a_2, \ldots, a_k \rangle$, *entonces el otro será* $\langle -a_1, -a_2, \ldots, -a_k \rangle$.

Demostración: Sea r un elemento de orden k en m, luego r^n es de orden k y a su vez, para cada potencia de n, por lo que el ciclo contendrá a cada elemento de orden k. Consideremos $-r$, entonces como n es impar, $(-r)^n = -r^n$, por ende el vértice $-r$ llegará al opuesto aditivo del $n-$ésimo residuo de r, que era lo que se quería demostrar y además contendrá de igual forma al resto. ■

El Teorema 11 se cumple para el caso de que n sea coprimo, la pregunta que surge es, ¿qué sucede si n no es coprimo?, es decir, si $(n, \varphi(m)) = d > 1$. Sabemos que si m admite raíz primitiva, el grado de llegada estará determinado por d, cuando admite solución, evidentemente existirán vértices que tendrán grado de llegada cero.

Ejemplo 5 *Consideremos el módulo 19 y la potencia 3, se obtiene el esquema de la Figura 11.*

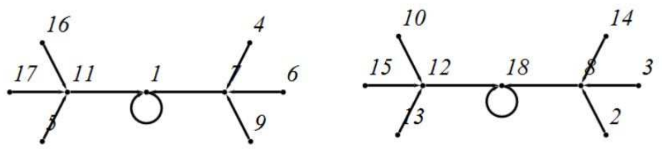

Figura 11: Grafo $G^*_{19,3}$.

Observemos en la Figura 11 que los vértices que admiten solución son: 11, 1, 7, 12, 18 y 8, donde cada uno tiene un grado de llegada de 3. El hecho relevante reside en que los valores de cada uno y su suma, es congruente al módulo del grafo, es decir, la suma de los vértices 5, 16 y 17 que se conectan al vértice 11 es igual a 38, que resulta ser el doble de 19. Revisando cada una de las 6 soluciones, se verifica que el comportamiento es el mismo.

Con lo analizado en la Figura 11 y aplicando la misma metodología demostrada en el Teorema 11 a los grafos $G^*_{m,n}$, n-residuales, cumpliendo la condición del que $(n, \varphi(m)) = d > 1$ con r un residuo que admita solución para la ecuación de la forma

$$x^n \cong r \mod (m),$$

implica que la suma de las raíces es congruente a cero módulo m.

Un resultado muy interesante que se verificó por medio de diversas pruebas computacionales en *Mathematica*, que nos permitió observar el comportamiento de este conjunto de residuos y la relación con el módulo, la cual requiere como todo resultado de la formalidad matemática.

6 Conclusiones

Al estudiar los conjuntos n-residuales de un módulo m, donde m admite una raíz primitiva de la forma 2, 4 , p^α, $2p^\alpha$ con p primo impar y $\alpha \in \mathbb{N}$, se pudo establecer un procedimiento más preciso para calcularlos por medio de su relación con el conjunto de potencias de raíces primitivas, dado el Teorema 9 y el Teorema 10, proporcionando una condición necesaria y suficiente para que el módulo m admita una raíz primitiva. Al incluir un instrumento matemático como los grafos y en especial los grafos n-residuales, nos permitió representar esquemáticamente algunos conceptos, fundamentados en el software *Mathematica*, obteniendo resultados interesantes sobre diversas corridas.

Para un grafo $G_{m,n}$, la cantidad de vértices y aristas coinciden con el módulo, dando como número de aristas de salida 1 (grado del vértice de salida). Esto tiene relación con el sistema completo de residuos y al utilizar el sistema reducido de residuos, se puede construir el subgrafo $G^*_{m,n}$.

Dado un ciclo donde $(n, \varphi(m)) = 1$, que contenga raíces primitivas de una determinada longitud, con una cantidad de elementos, se originará otro ciclo compuesto por el complemento suplementario con la misma cantidad de elementos del original y cuando $(n, \varphi(m)) > 1$ produce árboles complementarios, lo cual nos permite observar y establecer las condiciones para obtener una solución única de las sumas de las raíces para una ecuación polinomial de congruencia m con residuo r. Todas las condiciones y construcciones se limitaron a potencias de números enteros positivos, sería interesante el análisis para el caso de potencias de funciones con coeficientes enteros.

Agradecimientos

Nuestro agradecimiento es para la Escuela de Matemática de la Universidad de Panamá, donde se presentó el trabajo de investigación y para el Dr. Jaime Gutiérrez por sus sugerencias para mejorarlo, del cual se originó este artículo.

Referencias

[1] D. M. Burton, *Elementary Number Theory*, revised printing, Allyn and Bacon Inc, Estados Unidos, 1980.

[2] R. D. Carmichael, *The Theory of Numbers*, John Wiley & Sons Inc, New York, 1914.

[3] C. F. Gauss, *Disquisitiones Arithmeticae*, traducción en español, Universidad de Costa Rica, Costa Rica, 1995.

[4] F. Lemmermeyer, *Introduction to Number Theory*, manuscript, 2000.

[5] F. Lemmermeyer, *Reciprocity Laws: From Euler to Eisenstein*, Springer-Verlag, Berlín Heidelberg, 2000.

[6] W. J. Leveque, *Teoría Elemental de los Números*, Centro Regional de Ayuda Técnica, México, 1968.

[7] Math Pages. *Number theory*, `https://www.mathpages.com/home/inumber.htm`

[8] I, Niven, H. Zuckerman, *Introducción a la Teoría de Números*, Editorial Limusa, México, 1969.

[9] F. A. Toranzos, *Introducción a la Teoría de Grafos*, Secretaría General de la OEA, Washington, DC, 1976.

[10] I. Vinográdov, *Fundamentos de la Teoría de los Números*, 2nd ed., Editorial Mir, Moscú, 1977.

[11] D. R. Wilkins, *Course 311: Michaelmas term 2005, part I: topics in number theory*, David R. Wilkins, 1997-2005.