Universidad Nacional Autónoma
de México

Facultad de Ciencias

Digráficas de congruencias cúbicas y sus propiedades.

T E S I S

QUE PARA OBTENER EL TÍTULO DE:

Matemática

PRESENTA:

Mariana Paola Vázquez García

TUTOR

M. en C. Gerardo Miguel Tecpa Galván

Ciudad de México 2021

1. Datos del alumno
Vázquez
García
Mariana Paola
5535689411
Universidad Nacional Autónoma de México
Matemáticas
312090384
2.Datos del tutor
M. en C.
Gerardo Miguel
Tecpa
Galván
3. Datos del sinodal 1
Mat.
Laura
Pastrana
Ramírez
4. Datos del sinodal 2
Dra.
María del Rocío
Sánchez
López
5. Datos del sinodal 3
Mat.
Julio César
Guevara
Bravo
6. Datos del sinodal 4
M. en C.
Fernando Esteban
Contreras
Mendoza
7. Datos del trabajo escrito
Digráficas de congruencias cúbicas y sus propiedades.
106 p
2021
Facultad de Ciencias

Agradecimientos

Primero que nada quiero agradecer a toda mi familia en general, por su apoyo y por siempre estar al pendiente de mí. A mis padres por alentarme a seguir adelante y ser una buena estudiante desde muy pequeña, por nunca soltarme y ser mis pilares. A mi hermana, que aunque siempre me tira de a loca, me inspira a ser un mejor ejemplo cada día para ella.

Quiero también agradecer a mis amigos por impulsarme a seguir mis sueños, aconsejarme y dejarme aprender un poquito de cada uno, se que siempre podré contar con ustedes. Un agradecimiento especial a Dany y Sam por hacer de esta etapa de la universidad y mi estancia en la facultad un momento único y especial, por incitarme todo el tiempo a hacer la tarea, estudiar, dar un poquito más de mi en cada momento, todas esas pláticas en nuestro tiempo libre que nos ayudaron a crecer, sin ustedes la carrera no hubiera sido lo mismo.

A la UNAM y la Facultad de Ciencias no tengo mas que palabras de agradecimiento por darme una gran formación académica y hacerme encontrar con personas y profesores dignos de admirar. A mis profesores les doy gracias por sus enseñanzas y por ser fuente de inspiración para mí. También toda mi gratitud a EMCI y a las personas que conocí ahí porque de igual manera han sido parte de este logro.

Por último, quiero hacer una mención especial para Laura pues de no ser por ella este trabajo no podría haber sido posible, por presentarme con Miguel y darme un poco de luz en algo que no creía que fuera posible (combinar la teoría de números y la teoría de gráficas). Gracias a Miguel por su interés en lo que quería trabajar dentro de la tesis, su gran ayuda y apoyo para el desarrollo de la misma, además de su paciencia y enseñanzas. A mis sinodales Rocío, César y Esteban les agradezco sus consejos y aportaciones para mejorar la presentación y redacción de ésta.

II

Índice general

Introducción

La teoría de gráficas tiene su origen en 1736, cuando Leonhard Euler resuelve *el problema de los puentes de Königsberg*. En esos años, la ciudad de Königsberg estaba separada en cuatro partes de tierra por el río Pregel, por lo que se construyeron 7 puentes sobre el río que permitieran el tránsito de los habitantes por estas cuatro zonas, tal como se muestra en la siguiente figura:

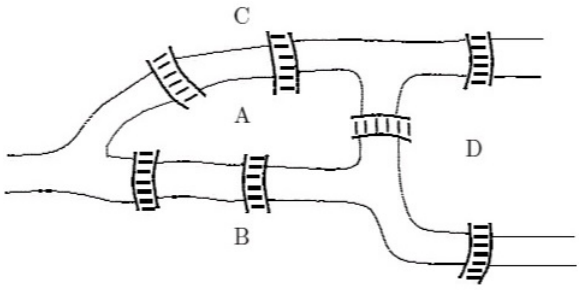

Figura 1: Puentes de Königsberg.

Algunos habitantes se preguntaban si era posible pasear por la ciudad pasando por cada puente exactamente una vez y volviendo al punto de inicio. Esto llamó la atención de Euler, quien presentó una solución general del problema de la siguiente forma: cada parte de tierra sería representada con un punto y cada puente mediante un segmento de línea entre dos puntos si dicho puente unía las dos partes de tierra respectivas. Dicha representación puede verse en la Figura 2.

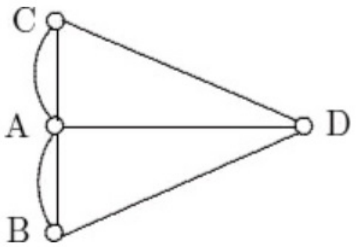

Figura 2: La gráfica de los puentes de Königsberg.

Lo que se buscaba era encontrar un camino que iniciara en algún punto, pasara por cada segmento una

única vez y regresara al punto inicial. Euler se dio cuenta que para que lo anterior fuera posible a cada uno de los puntos debía incidirle un número par de segmentos: un segmento para llegar al punto y otro distinto para salir. Con esa idea en mente y observando la Figura 2, podemos ver que no era posible para el caso de los puentes de Königsberg. Dicha idea fue publicada en [7]. A pesar de que ésto dio origen a lo que en la actualidad conocemos como teoría de gráficas, y en particular a los paseos eulerianos, el trabajo de Euler no incluía el concepto de gráfica.

Por otro lado, desde el siglo I d.C. el matemático chino Sun-Tsu trabajó buscando números que al ser divididos por $3, 5$ y 7 dieran como residuos $2, 3$ y 2 respectivamente, por lo que daría pie a lo que más tarde se conocería como el Teorema Chino del Residuo. Así, a lo largo de los años, muchos matemáticos trabajaron con esta idea en problemas específicos, como Fermat, quien mandó una carta a Frénicle de Bessy retándolo a demostrar la siguiente afirmación: p divide a $a^{p-1} - 1$ cuando p sea primo y a sea coprimo con p. Siendo esta proposición demostrada por Euler y posteriormente nombrado como *el pequeño Teorema de Fermat*. Además Euler, establece una generalización del pequeño teorema de Fermat, en la cual afirma que si a y n son dos enteros tales que son primos relativos, entonces n divide al entero $a^{\varphi(n)} - 1$, donde $\varphi(n)$ es la función de Euler definida como el número de enteros entre 1 y n tales que son primos relativos con n. Mientras que en 1770, Wilson enuncia otro teorema relacionado con divisibilidad y números primos, el cual nos dice que si p es un número primo, entonces $(p-1)! + 1$ es divisible por p; no obstante fue Lagrange quien un año después demuestra tal teorema. Sin embargo, no es hasta 1801 que el matemático Karl Friedrich Gauss, motivado por los trabajos de estos matemáticos, introduce una definición formal de la relación de congruencia y desarrolla sus propiedades. Además, establece el símbolo $\equiv$ para denotar tal relación, con el motivo de hacer una analogía al símbolo de igualdad. Lo anterior es publicado en su trabajo *Disquistiones Arithmeticae* donde presenta la teoría de congruencias como una rama de la teoría de divisibilidad.

Como podemos observar, tanto la teoría de gráficas como la teoría de números, en particular la teoría de congruencias, han jugado un papel muy importante en el desarrollo de las matemáticas a través de los años, así como en su relación y aplicación con otras ramas, como lo son la química en [16], la biología en [1] e informática en [15], por mencionar algunas. En el caso de la teoría de gráficas y para el caso de la teoría de congruencias podemos ver su aplicación en ramas como las criptografía en [10], usada incluso en la segunda guerra mundial, los relojes en [2], la música en [8] e incluso la astronomía en [13].

Así, desde hace algunos años, diversos investigadores han estado interesados en la conjunción de la Teoría de Gráficas y la Teoría de Números y podemos darnos idea al respecto en artículos como [9], [14] y [4], por mencionar algunos. En particular, existen algunos autores que han relacionado la Teoría de Gráficas y la Teoría de Congruencias.

En 1967, S. Bryant en [5] construye una digráfica asociando al conjunto de vértices con un grupo G, mientras que las flechas estarán dadas de la siguiente manera: si a y b son vértices de la digráfica, (a, b) es una flecha si y sólo si $b = a^2$. Por su parte, L. Szalay en [19], retomando las ideas propuestas por Bryant, trabaja el caso particular cuando el grupo es $\mathbb{Z}/n\mathbb{Z}$. Notemos que en este caso la relación de adyacencia propuesta por Bryant se reinterpreta de la siguiente manera: (a, b) es una flecha si y sólo si $a^2 \equiv b \mod n$. Además Szalay presenta diferentes propiedades estructurales de tal digráfica. Años más tarde, esta idea nuevamente es retomada por M. Křížek y L. Somer en [12], quienes estudian y muestran resultados relacionados con los

números de Fermat en términos de la digráfica definida en [19]. Posteriormente en 2007, estos mismos autores presentan una generalización natural de la digráfica trabajada por Szalay en [19] de la siguiente manera: los vértices de la digráfica son nuevamente los elementos del grupo $\mathbb{Z}/n\mathbb{Z}$ y (a, b) es una flecha de la digráfica si y sólo si $a^k \equiv b \mod n$. Dicha generalización puede ser encontrada en [18]. Cabe mencionar que los resultados mostrados en [18] son una generalización de los resultados mostrados en [12].

Siguiendo esta misma línea de investigación, en 2009 J. Skowronek-Kaziów en [17] trabaja con la siguiente digráfica: el conjunto de vértices de la digráfica es el conjunto $\mathbb{Z}/n\mathbb{Z}$ y (a, b) es una flecha de la digráfica si sólo si $a^3 \equiv b \mod n$, a dicha digráfica la nombraremos *digráfica de congruencias cúbicas de orden n*. A pesar de que la digráfica trabajada por J. Skowronek-Kaziów es un caso particular de las digráficas introducidas en [18], es importante mencionar que los resultados obtenidos por J. Skowronek-Kaziów tienen un enfoque diferente a los de M. Křížek y L. Somer.

A lo largo de esta tesis estudiaremos y desarrollaremos los resultados propuestos por J. Skowronek-Kaziów en [17] referentes a la digráfica de congruencias cúbicas. Además extenderemos algunos de estos resultados a las digráficas definidas por M. Křížek y L. Somer en [12].

En el capítulo 1 se hará una revisión de algunas definiciones, resultados y ejemplos que nos serán útiles para el desarrollo de esta tesis, tanto en el ámbito de la teoría de números, como en el de la teoría de gráficas.

En el capítulo 2, definiremos formalmente las digráficas de congruencias cúbicas y enunciaremos diversos lemas, teoremas y corolarios que nos muestran algunas propiedades de estas digráficas. Dichas propiedades están relacionadas con los exgrados de los vértices, existencia de lazos, isomorfismos entre las componentes conexas, condiciones de existencia de caminos dirigidos y condiciones de existencia de ciclos dirigidos.

El capítulo 3 estará dedicado al conteo de los lazos de las digráficas de congruencias cúbicas. Los teoremas de este capítulo nos dirán cuántos lazos tiene la digráfica, dependiendo del número de primos en la descomposición canónica del orden de la digráfica y la potencia de 2 en dicha descomposición. Es importante mencionar que el Teorema Chino del Residuo jugará un papel muy importante en las demostraciones de estos teoremas.

Finalmente en el capítulo 4, retomaremos las digráficas definidas por M. Křížek y L. Somer en [18] y trabajaremos en una generalización de los resultados dados en el capítulo 2 en términos de dichas digráficas.

Capítulo 1

Definiciones y resultados básicos

En este capítulo enunciaremos las definiciones y resultados básicos, tanto del área de Teoría de Números en la primera sección, como del área de Teoría de Gráficas en la segunda sección, que nos serán útiles a lo largo de este trabajo, algunos principales: como los son el concepto de digráfica y el concepto de congruencia; además, teoremas como el Teorema Fundamental de la Aritmética y el Teorema Chino del Residuo que nos servirán de apoyo en la demostración de diversos resultados posteriores.

1.1. Teoría de Números

Los números enteros cumplen con distintos axiomas, uno de ellos es **el principio del buen orden**, que nos dice que todo conjunto no vacío de enteros positivos tiene un elemento mínimo.

Sean a y b enteros, diremos que a divide a b si $b = ax$ para alguna $x \in \mathbb{Z}$ y será denotado como $a \mid b$. Además diremos que a es un **factor** de b y del mismo modo diremos que b es **divisible** entre a. De igual manera, diremos que a no divide a b si $b \neq ax$ para alguna $x \in \mathbb{Z}$ y será denotado como $a \nmid b$.

Observación 1.1.1. *Si a y b son enteros y $a \mid b$, entonces existe un único entero, digamos x, tal que $b = ax$. Dicho entero x lo denotaremos por $\frac{b}{a}$.*

Observación 1.1.2. *Si a y b son enteros y $a = 1$, entonces $\frac{b}{a} = b$.*

Lema 1.1.3. *Sean a y b enteros, si $a \mid b$, entonces $a\left(\frac{b}{a}\right) = b$.*

Demostración: Como $a \mid b$, por definición sabemos que $b = ax$ para algún $x \in \mathbb{Z}$, además por la observación anterior $x = \frac{b}{a}$, por lo que sustituyendo x tenemos que $b = a\left(\frac{b}{a}\right)$. □

Un entero positivo p, $p > 1$ es un **número primo** si sus únicos factores positivos son 1 y él mismo.

A continuación enunciaremos uno de los teoremas más importantes dentro de la teoría de números, el cual nos permitirá trabajar con los números enteros a manera de producto de números primos y sus potencias,

así como encontrar todos los divisores de algún número e incluso nos será útil en la definición de funciones aritméticas relacionadas con tales factores primos.

Teorema 1.1.4 (**Teorema Fundamental de la Aritmética**). *Todo entero positivo n, $n \geq 2$ puede ser expresado como productos de potencias de números primos. Este producto es único salvo por el orden de dichos primos. [11]*

Tomando en cuenta el teorema anterior, si n es un natural mayor que 1, entonces existen números primos, $p_1, p_2, \ldots, p_k$ distintos y enteros positivos $a_1, a_2, \ldots, a_k$ tales que $n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$. A esta factorización le llamaremos **descomposición canónica de** n. En lo que resta de este trabajo, si $n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$ podemos suponer, sin pérdida de generalidad, que $p_i < p_{i+1}$ para todo $i \in \{1, \ldots, k\}$.

Un entero positivo es **libre de cuadrados** si no es divisible por el cuadrado de algún entero positivo mayor a 1.

El **máximo común divisor** de dos enteros a y b, ambos distintos de cero, es el entero positivo más grande que divide a a y b simultáneamente y es denotado por $(a; b)$, es decir $(a; b) = \text{máx}\{d \in \mathbb{Z} : d \mid a \text{ y } d \mid b\}$.

Observación 1.1.5. $(a; -b) = (-a; b) = (-a; -b) = (a; b)$*, por lo que nos centraremos en el máximo común divisor sólo de enteros positivos.*

Dado lo anterior, observemos que a y b siempre tendrán un divisor común pues al menos $1 \mid a$ y $1 \mid b$, ahora bien, si d es un divisor común de a y b, entonces $d \leq a$ y $d \leq b$, por lo que $d \leq \text{mín}\{a, b\}$. De manera que el conjunto de factores comunes de a y b es finito, por lo tanto, para todo par de enteros distintos de cero, digamos a y b, el máximo común divisor de ambos siempre existe.

Dos enteros positivos a y b son **primos relativos** si su máximo común divisor es 1; esto es, si $(a; b) = 1$.

El **mínimo común múltiplo** de dos enteros a y b es el entero positivo más pequeño que es divisible por a y b simultáneamente y es denotado por $[a; b]$, es decir $[a; b] = \text{mín}\{c \in \mathbb{Z} : a \mid c \text{ y } b \mid c\}$. Notemos que éste siempre existe pues como ab es un múltiplo común de a y b, entonces el conjunto de múltiplos comunes de a y b siempre es no vacío, por lo que por el Principio del Buen Orden, el conjunto tiene un elemento mínimo, por lo tanto, para todo par de enteros distintos de cero, digamos a y b, el mínimo común múltiplo de ambos siempre existe.

Teorema 1.1.6. *Sean a y b enteros positivos distintos de cero. Si $(a; b) = d$, entonces* $\left(\frac{a}{d}; \frac{b}{d}\right) = 1$.

Demostración: Tomando en cuenta que $(a; b) = d$, por definición $d \mid a$ y $d \mid b$, esto es $a = dx$ y $b = dy$ y por la Observación 1.1.1 $x = \frac{a}{d}$ y $y = \frac{b}{d}$ son ambos enteros.

Sea $d' = \left(\frac{a}{d}; \frac{b}{d}\right)$. Demostraremos que $d' = 1$.

Dado que d' es un factor común de $\frac{a}{d}$ y $\frac{b}{d}$, entonces $\frac{a}{d} = ld'$ y $\frac{b}{d} = md'$ para algunos enteros l y m. Como $\frac{a}{d} = ld'$, entonces $d\left(\frac{a}{d}\right) = ld'd$ y por el Lema 1.1.3 tenemos que $a = ldd'$. De la misma manera como $\frac{b}{d} = md'$, entonces $d\left(\frac{b}{d}\right) = md'd$ y por el Lema 1.1.3 tenemos que $b = mdd'$, por lo que dd' es un factor común de a y b. Por definición de máximo común divisor, $dd' \leq d$ de manera que $d' \leq 1$. Así, d' es un entero

positivo tal que $d' \leq 1$, por lo tanto $d' = 1$. Podemos concluir que si $(a;b) = d$, entonces $\frac{a}{d}$ y $\frac{b}{d}$ son primos relativos. □

La siguiente definición nos será de gran ayuda para la demostración de las dos proposiciones posteriores, sobre el máximo común divisor y el mínimo común múltiplo de dos enteros, tomando en cuenta sus descomposiciones canónicas. Supongamos que $n > 1$ y sea $a_1^{\alpha_1} a_2^{\alpha_2} \cdots a_k^{\alpha_k}$ su descomposición canónica. Si $A = \{q_1, q_2, \ldots, q_m\}$ es un conjunto de números primos tal que $\{a_1, \ldots, a_k\} \subseteq A$, entonces $n = q_1^{\beta_1} q_2^{\beta_2} \cdots q_m^{\beta_m}$ donde para toda $i \in \{1, \ldots, m\}$, $\beta_i = \alpha_j$ si $q_i = a_j$ para algún $j \in \{1, \ldots, k\}$ y $\beta_i = 0$ si $q_i \neq a_j$ para todo $j \in \{1, \ldots, k\}$. A la expresión $n = q_1^{\beta_1} q_2^{\beta_2} \cdots q_m^{\beta_m}$ le llamaremos **pseudodescomposición prima de** n **respecto a** A.

Proposición 1.1.7. *Sea $\{a, b\} \subseteq \mathbb{Z}$ tal que $(a;b) \neq 1$ y $a = u_1^{\alpha_1} u_2^{\alpha_2} \cdots u_n^{\alpha_n}$ y $b = v_1^{\beta_1} v_2^{\beta_2} \cdots v_m^{\beta_m}$ son las descomposiciones canónicas de a y b respectivamente y sea B el conjunto de todos los primos en la descomposición canónica de a y b y supongamos que $B = \{p_1, p_2, \ldots, p_s\}$. Sean $a = p_1^{\gamma_1} p_2^{\gamma_2} \cdots p_s^{\gamma_s}$ y $b = p_1^{\eta_1} p_2^{\eta_2} \cdots p_s^{\eta_s}$ las pseudodescomposiciones primas de a y b respecto a B. Entonces:*

$$(a;b) = p_1^{\min\{\gamma_1, \eta_1\}} p_2^{\min\{\gamma_2, \eta_2\}} \cdots p_s^{\min\{\gamma_s, \eta_s\}}.$$

Demostración: Sea $d = p_1^{\min\{\gamma_1, \eta_1\}} p_2^{\min\{\gamma_2, \eta_2\}} \cdots p_s^{\min\{\gamma_s, \eta_s\}}$. Primero demostremos que d es un divisor común de a y b. Notemos que para cada $l \in \{1, \ldots, s\}$, $\gamma_l \geq \min\{\gamma_l, \eta_l\}$, por lo que $p_l^{\min\{\gamma_l, \eta_l\}} \mid p_l^{\gamma_l}$. Si $\gamma_l = 0$, $p_l^{\gamma_l} = 1$ y $1 \mid a$, si $\gamma_l \neq 1$, $p_l^{\gamma_l}$ es un factor de la descomposición canónica de a, por lo que $p_l^{\gamma_l} \mid a$, concluyendo que $d \mid a$. Análogamente $d \mid b$. Así, podemos ver que d es un divisor común de a y b.

Ahora veamos que d es el máximo de los divisores comunes de a y b. Sea c un divisor común de a y b distinto de d y 1, y $c = q_1^{\delta_1} q_2^{\delta_2} \cdots q_t^{\delta t}$ su descomposición canónica en primos. Luego, cada $q_k^{\delta_k}$ divide a a y b simultáneamente; por lo que cada $q_k = u_i$ para alguna $i \in \{1, \ldots, n\}$ y cada $q_k = v_j$ para alguna $j \in \{1, \ldots, m\}$, en particular cada $q_k = p_l$ para alguna $l \in \{1, \ldots, s\}$. Además, cada $\delta_k \leq \min\{\gamma_l, \eta_l\}$ para alguna $l \in \{1, \ldots, s\}$, por lo que cada $q_k^{\gamma_k} \leq p_l^{\min \gamma_l, \eta_l}$, así $c < d$, es decir cualquier divisor común de a y b distinto de d es menor que d, por lo tanto $(a;b) = d$. □

Proposición 1.1.8. *Sean $\{a, b\} \subseteq \mathbb{Z}$ tal que $a = u_1^{\alpha_1} u_2^{\alpha_2} \cdots u_n^{\alpha_n}$ y $b = v_1^{\beta_1} v_2^{\beta_2} \cdots v_m^{\beta_m}$ son las descomposiciones canónicas de a y b respectivamente y B el conjunto de todos los primos en la descomposición canónica de a y b y supongamos que $B = \{p_1, p_2, \ldots, p_s\}$. Sean $a = p_1^{\gamma_1} p_2^{\gamma_2} \cdots p_s^{\gamma_s}$ y $b = p_1^{\eta_1} p_2^{\eta_2} \cdots p_s^{\eta_s}$ las pseudodescomposiciones primas de a y b respecto a B. Entonces:*

$$[a;b] = p_1^{\max\{\gamma_1, \eta_1\}} p_2^{\max\{\gamma_2, \eta_2\}} \cdots p_s^{\max\{\gamma_s, \eta_s\}}.$$

Demostración: Sea $d = p_1^{\max\{\gamma_1, \eta_1\}} p_2^{\max\{\gamma_2, \eta_2\}} \cdots p_s^{\max\{\gamma_s, \eta_s\}}$. Primero demostraremos que d es un múltiplo común de a y b. Notemos que para cada $i \in \{1, \ldots, s\}$, $\gamma_i \leq \max\{\gamma_i, \eta_i\}$, por lo que $p_i^{\gamma_i} \mid p_i^{\max\{\gamma_i, \eta_i\}}$, concluyendo que $a \mid d$. Análogamente $b \mid d$. Así, podemos ver que d es un múltiplo común de a y b.

Ahora veamos que d es el mínimo de los múltiplos comunes de a y b. Sea c un múltiplo común de a y b distinto de d. Como $a \mid c$ y $b \mid c$, entonces $c = at$ para algún entero t, es decir $c = p_1^{\gamma_1} p_2^{\gamma_2} \cdots p_s^{\gamma_s} t$, análogamente

$c = br$ para algún entero r, es decir $c = p_1^{\eta_1} p_2^{\eta_2} \cdots p_s^{\eta_s} r$, por lo que para cada $i \in \{1, \ldots, s\}$, $p_i^{\gamma_i} \mid c$ y $p_i^{\eta_i} \mid c$, en particular $p_i^{\text{máx}\{\gamma_i, \eta_i\}} \mid c$, concluyendo que $d \mid c$, en particular $d < c$. Por lo tanto, $[a; b] = d$. □

Teorema 1.1.9. *Si a y b son dos enteros positivos, entonces*

$$[a; b] = \frac{ab}{(a; b)}.$$

Demostración: Sean $\{a, b\} \subseteq \mathbb{Z}$ tal que $a = u_1^{\alpha_1} u_2^{\alpha_2} \cdots u_n^{\alpha_n}$ y $b = v_1^{\beta_1} v_2^{\beta_2} \cdots v_m^{\beta_m}$ son las descomposiciones canónicas de a y b respectivamente y B el conjunto de todos los primos en la descomposición canónica de a y b y supongamos que $B = \{p_1, p_2, \ldots, p_s\}$. Además podemos suponer sin pérdida de generalidad que $p_1, \ldots, p_k$ son los divisores primos comunes de a y b para alguna $k \leq s$. Sean $a = p_1^{\gamma_1} p_2^{\gamma_2} \cdots p_s^{\gamma_s}$ y $b = p_1^{\eta_1} p_2^{\eta_2} \cdots p_s^{\eta_s}$ las pseudodescomposiciones primas de a y b respecto a B.

Dadas las Proposiciones 1.1.7 y 1.1.8 tenemos lo siguiente:

$$\begin{aligned}
(a; b) \cdot [a; b] &= \left(p_1^{\text{mín}\{\gamma_1, \eta_1\}} p_2^{\text{mín}\{\gamma_2, \eta_2\}} \cdots p_k^{\text{mín}\{\gamma_k, \eta_k\}}\right) \left(p_1^{\text{máx}\{\gamma_1, \eta_1\}} p_2^{\text{máx}\{\gamma_2, \eta_2\}} \cdots p_s^{\text{máx}\{\gamma_s, \eta_s\}}\right) \\
&= \left(p_1^{\text{mín}\{\gamma_1, \eta_1\} + \text{máx}\{\gamma_1, \eta_1\}} \cdots p_k^{\text{mín}\{\gamma_k, \eta_k\} + \text{máx}\{\gamma_k, \eta_k\}}\right) \left(p_{k+1}^{\text{máx}\{\gamma_{k+1}, \eta_{k+1}\}} \cdots p_s^{\text{máx}\{\gamma_s, \eta_s\}}\right) \\
&= \left(p_1^{\gamma_1 + \eta_1} \cdots p_k^{\gamma_k + \eta_k}\right) \left(p_{k+1}^{\text{máx}\{\gamma_{k+1}, \eta_{k+1}\}} \cdots p_s^{\text{máx}\{\gamma_s, \eta_s\}}\right).
\end{aligned}$$

Notemos que para $i \in \{k+1, \ldots, s\}$, $\gamma_i = 0$ o $\eta_i = 0$, en cuyo caso $p_i^{\text{máx}\{\gamma_i, \eta_i\}} = p_i^{\gamma_i + \eta_i}$. Dado lo anterior tenemos que:

$$\begin{aligned}
(a; b) \cdot [a; b] &= \left(p_1^{\gamma_1 + \eta_1} \cdots p_k^{\gamma_k + \eta_k}\right) \left(p_{k+1}^{\text{máx}\{\gamma_{k+1}, \eta_{k+1}\}} \cdots p_s^{\text{máx}\{\gamma_s, \eta_s\}}\right) \\
&= p_1^{\gamma_1 + \eta_1} p_2^{\gamma_2 + \eta_2} \cdots p_s^{\gamma_s + \eta_s} \\
&= \left(p_1^{\gamma_1} p_2^{\gamma_2} \cdots p_s^{\gamma_s}\right) \left(p_1^{\eta_1} p_2^{\eta_2} \cdots p_s^{\eta_s}\right) \\
&= ab.
\end{aligned}$$

Así, podemos ver que $(a; b) \cdot [a; b] = ab$ y por la Observación 1.1.1 concluimos que

$$[a; b] = \frac{ab}{(a; b)}.$$

□

Dado un conjunto de enteros, digamos $A = \{a_1, \ldots, a_n\}$, y un entero b diremos que b es **combinación lineal de** A si existen enteros $\alpha_1, \ldots, \alpha_n$ tales que $b = \alpha_1 a_1 + \cdots + \alpha_n a_n$. Cuando $n = 2$, omitiremos la notación conjuntista y diremos que b es **combinación lineal de los enteros** a_1 **y** a_2.

Teorema 1.1.10. *Sea $\{a, b, c, \alpha, \beta\} \subseteq \mathbb{Z}$. Si $a \mid b$ y $a \mid c$, entonces $a \mid (\alpha b + \beta c)$.*

Demostración: Como $a \mid b$ y $a \mid c$, entonces $b = ax$ y $c = ay$ para algunos x y y enteros. Sustituyendo b y c en $\alpha b + \beta c$ tenemos que $\alpha b + \beta c = \alpha ax + \beta ay$, factorizando a obtenemos que $\alpha b + \beta c = a(\alpha x + \beta y)$. Concluyendo así que $a \mid (\alpha b + \beta c)$. □

Teorema 1.1.11 (**El algoritmo de la división**). *Sean a un entero y b un entero positivo. Entonces existen enteros únicos q y r tal que $a = b \cdot q + r$, donde $r \in \{0, \ldots, b-1\}$.*

Demostración: Para demostrar lo anterior, primero debemos demostrar la existencia de q y r y luego la unicidad de los mismos.

Para demostrar la existencia de q y r consideremos el conjunto $S = \{x \in \mathbb{N} : x = a - bn \text{ y } n \in \mathbb{Z}\}$. Demostremos que S contiene un elemento mínimo. Para este fin, veamos primero que S es un subconjunto no vacío de $\{0, 1, 2, 3, \ldots\}$.

Caso 1. $a \geq 0$.

En este caso, $a = a - b \cdot 0$, de manera que $a \in S$. Así, S contiene un elemento.

Caso 2. $a < 0$.

En este caso, como b es un entero positivo, entonces $b \geq 1$. Así, $-ba \geq -a$, esto es $a - ba \geq 0$, por consiguiente $a - ba \in S$.

En ambos casos, S tiene al menos un elemento, por lo que S es un subconjunto no vacío de $\{0, 1, 2, 3, \ldots\}$. Por lo tanto, por el Principio del Buen Orden, S contiene un elemento mínimo r.

Como $r \in S$, existe un entero q tal que $r = a - bq$, donde $r \geq 0$.

Veamos que $r < b$, probemos esto por contradicción. Supongamos que $r \geq b$, entonces $r - b \geq 0$, pero $r - b = (a - bq) - b$, esto es $r - b = a - b(q + 1)$. Como $a - b(q + 1)$ es mayor o igual a cero, entonces $a - b(q + 1) \in S$, es decir, $r - b \in S$. Por otro lado, como $b > 0$, entonces $r - b < r$. Por lo tanto, $r - b$ es menor que r y pertenece a S, lo que contradice la elección de r, de manera que $r < b$.

Concluímos que existen enteros q y r tales que $a = bq + r$ donde $r \in \{0, \ldots, b-1\}$.

Para probar la unicidad de q y r, supongamos que existen enteros q' y r' tales que $a = bq + r$ y $a = bq' + r'$, donde $\{r, r'\} \subseteq \{0, \ldots, b-1\}$.

Dado lo anterior tenemos que $bq + r = bq' + r'$, esto es

$$b(q - q') = r' - r \tag{1.1}$$

Consideremos los siguientes casos sobre q y q':

Caso 1. $q = q'$.

En este caso, se sigue de la Ecuación 1.1 que $r = r'$.

Caso 2. $q \neq q'$.

En este caso podemos suponer, sin pérdida de generalidad, que $q > q'$, en particular $q - q' \geq 1$ y como b es un entero positivo, entonces $b(q - q') \geq b$, por lo que $r' - r \geq b$. Por otro lado, como $r' < b$, entonces $r' - r < b$, lo cual no es posible.

De los casos anteriores q y r son únicos. □

Llamamos **cociente** al número q y **residuo** al número r en la expresión del teorema anterior.

Teorema 1.1.12 (Euler). *El máximo común divisor de los enteros positivos a y b es una combinación lineal de a y b.*

Demostración: Sea S el conjunto de las combinaciones lineales positivas de a y b; esto es, $S = \{x \in \mathbb{N} \setminus \{0\} : x = ma + nb, \{m, n\} \subseteq \mathbb{Z}\}$.

Demostraremos que S tiene un elemento mínimo. Como $a > 0$, entonces $a \in S$, pues $a = 1 \cdot a + 0 \cdot b$, por lo que S es no vacío. De manera que, por el Principio del Buen Orden, S tiene un elemento mínimo d.

Para mostrar que $d = (a; b)$ veamos que como $d \in S$, entonces $d = \alpha a + \beta b$ para algunos enteros α y β.

Primero mostremos que $d \mid a$ y $d \mid b$:

Por el algoritmo de la división, existen enteros q y r tales que $a = dq + r$, donde $r \in \{0, \ldots, d - 1\}$. Despejando r tenemos $r = a - dq$, sustituyendo d en lo anterior

$$\begin{aligned} r &= a - (\alpha a + \beta b)q \\ &= (1 - \alpha q)a + (-\beta q)b. \end{aligned}$$

Si $r > 0$, entonces $r \in S$. Como $r < d$, entonces r es menor que el mínimo de S, lo cual es una contradicción, por lo que $r = 0$ y así, $a = dq$, de manera que $d \mid a$. Análogamente, $d \mid b$, por lo tanto d es un divisor común de a y b.

Ahora bien, para probar que cada divisor común positivo d' de a y b es menor o igual a d, si $d' \mid a$ y $d' \mid b$, entonces por el Teorema 1.1.10, $d' \mid (\alpha a + \beta b)$, esto es $d' \mid d$. Así $d' \leq d$. Dado lo anterior podemos concluir que $d = (a; b)$. □

Teorema 1.1.13. *Dos enteros positivos a y b son primos relativos si y sólo si existen enteros α y β tales que $\alpha a + \beta b = 1$.*

Demostración: Demostremos la parte suficiente. Como a y b son primos relativos, entonces $(a; b) = 1$. De manera que, por el Teorema 1.1.12, existen enteros α y β tal que $\alpha a + \beta b = 1$.

Veamos ahora la parte necesaria. Supongamos que $\alpha a + \beta b = 1$ y sea $d = (a; b)$, entonces, por el Teorema 1.1.10, $d \mid \alpha a + \beta b$, esto es $d \mid 1$, por lo que $d = 1$. Concluyendo que a y b son primos relativos. □

Corolario 1.1.14. *Sea $\{a, b, c\} \subseteq \mathbb{Z}$. Si $(a; b) = 1$ y $(a; c) = 1$, entonces $(a; bc) = 1$.*

Demostración: Como $(a; b) = 1$ y $(a; c) = 1$, entonces, por el Teorema 1.1.13, tenemos que existe $\{\alpha, \beta, \alpha', \gamma\} \subseteq \mathbb{Z}$ tal que

$$\begin{aligned} &(1)\ \alpha a + \beta b = 1 \\ &(2)\ \alpha' a + \gamma c = 1. \end{aligned}$$

Si multiplicamos (1) y (2) obtenemos

$$(\alpha a + \beta b)(\alpha' a + \gamma c) = 1.$$

Desarrollando nos queda

$$\alpha\alpha' a^2 + \alpha\gamma ac + \alpha'\beta ab + \beta\gamma bc = 1.$$

Factorizando a tenemos

$$a(\alpha\alpha' a + \alpha\gamma c + \alpha'\beta b) + bc(\beta\gamma) = 1.$$

Ahora bien, como tenemos una combinación lineal de a y bc igualada a 1, entonces, por el Teorema 1.1.13, a y bc son primos relativos, es decir $(a; bc) = 1$. □

Corolario 1.1.15. *Sea $\{a_1, \ldots, a_n\} \subseteq \mathbb{Z}$. Si $(a_i; b) = 1$ para todo $i \in \{1, \ldots, n\}$, entonces $(a_1 \cdots a_n; b) = 1$.*

Demostración: Demostraremos por inducción sobre n.

Base de inducción. Sea $\{a_1, a_2, b\} \subseteq \mathbb{Z}$ tal que $(a_1; b) = 1$ y $(a_2; b) = 1$, entonces por el Corolario 1.1.14, $(a_1 a_2; b) = 1$.

Hipótesis de inducción. Si $\{a_1, \ldots, a_{n-1}, b\} \subseteq \mathbb{Z}$ es tal que $(a_i, b) = 1$ para todo $i \in \{1, \ldots, n-1\}$, entonces $(a_1 \cdots a_{n-1}; b) = 1$.

Paso inductivo. Sea $\{a_1, \ldots, a_n, b\} \subseteq \mathbb{Z}$ tal que $(a_i; b) = 1$ para todo $i \in \{1, \ldots, n\}$. Veamos que $(a_1 \cdots a_n, b) = 1$.

Supongamos que $k = a_1 \cdots a_{n-1}$. Luego, por hipótesis de inducción $(a_1 \cdots a_{n-1}; b) = 1$, es decir $(k; b) = 1$, además $(a_n; b) = 1$ por lo que, por el Corolario 1.1.14, $(ka_n; b) = 1$, esto es $(a_1 \cdots a_n; b) = 1$. □

Corolario 1.1.16 (Euclides). *Sea $\{a, b, c\} \subseteq \mathbb{Z}$. Si a y b son primos relativos y $a \mid bc$, entonces $a \mid c$.*

Demostración: Como a y b son primos relativos, entonces, por el Teorema 1.1.13, existen enteros α y β tales que $\alpha a + \beta b = 1$. Multiplicando por c obtenemos $\alpha ac + \beta bc = c$. Podemos ver que $a \mid \alpha ac$ y $a \mid \beta bc$ por hipótesis, entonces, por el Teorema 1.1.10, $a \mid \alpha ac + \beta bc$ y dado que $\alpha ac + \beta bc = c$, entonces $a \mid c$. □

Definamos ahora, el máximo común divisor para 3 o más enteros de la siguiente manera, sea $\{a_1, a_2, \ldots a_n\} \subseteq \mathbb{N}$ con $n \geq 3$, entonces $(a_1; a_2; \ldots; a_n) = \text{máx}\{d \in \mathbb{Z} : d \mid a_i \text{ para todo } i \in \{1, \ldots, n\}\}$.

Podemos ver que algunas de las propiedades ya mencionadas anteriormente, pueden generalizarse bajo la definición del máximo común divisor de un conjunto $\{a_1, \ldots, a_n\}$, con $n \geq 3$. A continuación demostraremos dos teoremas que nos serán útiles en lo que resta de este trabajo.

Teorema 1.1.17. *Sea $\{a_1, \ldots, a_n, b\} \subseteq \mathbb{Z}$. Si $b \mid a_i$ para todo $i \in \{1, \ldots, n\}$, entonces para todo $\{\alpha_1, \ldots, \alpha_n\} \subseteq \mathbb{Z}$, $b \mid a_1\alpha_1 + \cdots + a_n\alpha_n$.*

Demostración: Demostremos por inducción sobre n.

Base de inducción. Sea $\{a_1, a_2, b\} \subseteq \mathbb{Z}$ tal que $b \mid a_1$ y $b \mid a_2$. Por el Teorema 1.1.10 para todo $\{\alpha_1, \alpha_2\} \subseteq \mathbb{Z}$, tenemos que $b \mid a_1\alpha_1 + a_2\alpha_2$.

Hipótesis de inducción. Si $\{a_1, \ldots, a_{n-1}, b\} \subseteq \mathbb{Z}$ es tal que $b \mid a_i$ para todo $i \in \{1, \ldots, n-1\}$, entonces para todo $\{\alpha_1, \ldots, \alpha_{n-1}\} \subseteq \mathbb{Z}$, $b \mid a_1\alpha_1 + \cdots + a_{n-1}\alpha_{n-1}$.

Paso inductivo. Sea $\{a_1, \ldots, a_n, b\} \subseteq \mathbb{Z}$ tal que $b \mid a_i$ para todo $i \in \{1, \ldots, n\}$. Veamos que para todo $\{\alpha_1, \ldots, \alpha_n\} \subseteq \mathbb{Z}$, $b \mid a_1\alpha_1 + \cdots + a_n\alpha_n$.

Sea $c = a_1\alpha_1 + \cdots + a_{n-1}\alpha_{n-1}$, por hipótesis de inducción, como $b \mid a_i$ para todo $i \in \{1, \ldots, n-1\}$, entonces $b \mid a_1\alpha_1 + \cdots + a_{n-1}\alpha_{n-1}$, es decir, $b \mid c$.

Luego, como en particular $b \mid a_n$ y $b \mid c$, entonces por el Teorema 1.1.10, $b \mid c + a_n\alpha_n$.

De manera que sustituyendo c, tenemos que $b \mid a_1\alpha_1 + \cdots + a_{n-1}\alpha_{n-1} + a_n\alpha_n$. □

Veamos ahora una generalización del Teorema de Euler para un conjunto de enteros positivos $\{a_1, \ldots, a_n\}$.

Teorema 1.1.18. *El máximo común divisor de los enteros positivos $a_1, \ldots, a_n$ es una combinación lineal del conjunto $\{a_1, \ldots, a_n\}$.*

Demostración: Sea S el conjunto de las combinaciones lineales positivas de $\{a_1, \ldots, a_n\}$, es decir, $S = \{x \in \mathbb{N} \setminus \{0\} : x = \alpha_1 a_1 + \cdots + \alpha_n a_n, \text{ y } \{\alpha_1, \ldots, \alpha_n\} \subseteq \mathbb{Z}\}$. Primero demostraremos que S tiene un elemento mínimo. Como $a_1 > 0$, entonces $a_1 \in S$ pues $a_1 = 1 \cdot a_1 + 0 \cdot a_2 + \cdots + 0 \cdot a_n$, por lo que S es no vacío. De manera que, por el Principio del Buen Orden, S tiene un elemento mínimo, digamos d.

Ahora demostraremos que $d = (a_1; \ldots; a_n)$. Como $d \in S$, entonces $d = \alpha_1 a_1 + \cdots + \alpha_n a_n$, para algunos enteros α_i, con $i \in \{1, \ldots, n\}$. Afirmamos que $d \mid a_i$ para todo $i \in \{1, \ldots, n\}$. Veremos que esto se cumple para $i = 1$ y una prueba análoga mostrará los casos $i \in \{2, \ldots, n\}$. Por el Algoritmo de la División, existen enteros q_1 y r_1 tales que $a_1 = dq_1 + r_1$, donde $r_1 \in \{0, \ldots, d-1\}$. Despejando r_1, tenemos $r_1 = a_1 - dq_1$, sustituyendo d en lo anterior:

$$\begin{aligned} r_1 &= a_1 - (\alpha_1 a_1 + \cdots + \alpha_n a_n) q_1 \\ &= (1 - \alpha_1 q_1) a_1 + (-\alpha_2 q_1) a_2 + \cdots + (-\alpha_n q_1) a_n. \end{aligned}$$

Si $r_1 > 0$, entonces $r_1 \in S$. Como $r_1 < d$, entonces r_1 es menor que el mínimo de S, lo cual es una contradicción, por lo que $r_1 = 0$ y así, $a_1 = dq_1$ por consiguiente $d \mid a_1$. De manera similar, $d \mid a_i$ para todo $i \in \{2, \ldots, n\}$, por lo tanto, d es un divisor común de a_i con $i \in \{1, \ldots, n\}$.

Por último demostraremos que d es el máximo de los divisores positivos, que tienen en común los enteros a_i, con $i \in \{1, \ldots, n\}$. Supongamos que $d' \mid a_i$ para toda $i \in \{1, \ldots, n\}$, por el Teorema 1.1.17, d' divide a cualquier combinación lineal de $\{a_1, \ldots, a_n\}$, en particular, $d' \mid (\alpha_1 a_1 + \cdots \alpha_n a_n)$, esto es $d' \mid d$. Así, $d' \leq d$. Dado lo anterior, podemos concluir que $d = (a_1; \ldots; a_n)$. □

Teorema 1.1.19. *Sean $a_1, a_2, \ldots, a_n$ enteros positivos con $n \geq 3$. Entonces:*

$$(a_1; a_2; \ldots; a_n) = ((a_1; a_2; \ldots; a_{n-1}); a_n).$$

Demostración: Sean $d = (a_1; a_2; \ldots; a_n)$, $d' = (a_1; a_2; \ldots; a_{n-1})$ y $d'' = (d'; a_n)$. Demostraremos que $d = d''$.

Veamos primero que $d \leq d''$. Como $d' = (a_1; a_2; \ldots; a_{n-1})$, entonces por el Teorema 1.1.18 podemos escribir a d' como combinación lineal del conjunto $\{a_1, \ldots, a_{n-1}\}$, es decir, $d' = \beta_1 a_1 + \cdots + \beta_{n-1} a_{n-1}$ para algún $\{\beta_1, \ldots, \beta_{n-1}\} \subseteq \mathbb{Z}$.

Por otro lado, como $d = (a_1; a_2; \ldots; a_n)$, entonces $d \mid a_i$ para cada $i \in \{1, \ldots, n\}$, en particular $d \mid a_i$ para $i \in \{1, \ldots, n-1\}$, por lo que, por el Teorema 1.1.17, d divide a cualquier combinación lineal de $\{a_1, \ldots, a_n\}$, en particular $d \mid d'$. Luego, como $d \mid d'$ y $d \mid a_n$, entonces por definición de máximo común divisor $d \leq d''$.

Ahora veamos que $d'' \leq d$. Como $d'' = (d'; a_n)$ por definición $d'' \mid d'$ y $d'' \mid a_n$, pero $d'' \mid d'$ implica que $d'' \mid a_i$ para toda $i \in \{1, \ldots, n-1\}$. Por lo que, $d'' \mid a_i$ para toda $i \in \{1, \ldots, n\}$, por la definición de máximo común divisor, podemos concluir que $d'' \leq d$. Así, como $d \leq d''$ y $d'' \leq d$, entonces $d = d''$. □

Definamos ahora el mínimo común múltiplo para 3 o más enteros positivos de la siguiente manera: sea $\{a_1, a_2, \dots a_n\} \subseteq \mathbb{N} \setminus \{0\}$ con $n \geq 3$, entonces

$$[a_1; a_2; \dots; a_n] = \text{mín}\{c \in \mathbb{N} \setminus \{0\} : a_i \mid c \text{ para todo } i \in \{1, \dots, n\}\}$$

.

Proposición 1.1.20. *Sea $\{a_1, \dots, a_n\} \subseteq \mathbb{N} \setminus \{0\}$. Si $m = [a_1; \dots; a_n]$ y c es un múltiplo común de $a_1, \dots, a_n$, entonces $m \mid c$.*

Demostración: Demostraremos por contradicción. Supongamos que $m \nmid c$, entonces por el algoritmo de la división existen enteros q y r tales que $c = qm + r$ con $r \in \{0, \dots, m-1\}$. Como $a_i \mid c$ y $a_i \mid m$ para todo $i \in \{1, \dots, n\}$, entonces $a_i \mid c - qm$ para todo $i \in \{1, \dots, n\}$, pero $c - qm = r$, por lo que $a_i \mid r$ para todo $i \in \{1, \dots, n\}$, es decir, r es un múltiplo común de $a_1, \dots, a_n$, $r > 0$ y $r < m$, lo cual es una contradicción pues m es el mínimo de los múltiplos comunes de $a_1, \dots, a_n$. Por lo tanto, $m \mid c$. □

Proposición 1.1.21. *Si $a_1, a_2, \dots, a_n$ son enteros positivos con $n \geq 3$, entonces*

$$[[\, a_1; a_2; \dots; a_{n-1}\,]; a_n] = [a_1; a_2; \dots; a_n]\,.$$

Demostración: Supongamos que $c = [a_1; a_2; \dots; a_n]$ y $c' = [[\, a_1; a_2; \dots; a_{n-1}\,]; a_n]$. Demostraremos que $c = c'$.

Veamos primero que $c' \mid c$. Como $c = [a_1; a_2; \dots; a_n]$, $a_i \mid c$ para cada $i \in \{1, \dots, n\}$, en particular $a_i \mid c$ para todo $i \in \{1, \dots, n-1\}$, entonces por la Proposición 1.1.20 $[a_1; \dots; a_{n-1}] \mid c$; además $a_n \mid c$, entonces c es un múltiplo común de $[a_1; \dots; a_{n-1}]$ y a_n, por lo que de nuevo por la Proposición 1.1.20, $[[\, a_1; a_2; \dots; a_{n-1}\,]; a_n] \mid c$, esto es $c' \mid c$.

Ahora veamos que $c \mid c'$. Como $c' = [[\, a_1; a_2; \dots; a_{n-1}\,]; a_n]$, por definición de mínimo común múltiplo $[a_1; a_2; \dots; a_{n-1}] \mid c'$ y $a_n \mid c'$, luego $a_i \mid c'$ para cada $i \in \{1, \dots, n\}$, de manera que c' es un múltiplo común de $a_1, \dots, a_n$; en consecuencia, por la Proposición 1.1.20 $c \mid c'$.

Podemos concluir que como $c \mid c'$ y $c' \mid c$, entonces $c = c'$. □

Corolario 1.1.22. *Sean $a_1, a_2, \dots, a_n$ enteros positivos distintos y primos relativos por pares, entonces $[a_1; a_2; \dots; a_n] = a_1 a_2 \cdots a_{n-1} a_n$.*

Demostración: Demostraremos por inducción sobre n.

Base de inducción. Sea $\{a_1, a_2\} \subseteq \mathbb{N} \setminus \{0\}$ tal que $(a_1; a_2) = 1$, por el Teorema 1.1.9

$$[a_1; a_2] = \frac{a_1 a_2}{(a_1; a_2)} = a_1 a_2.$$

Hipótesis de inducción. Si $\{a_1, a_2, \dots, a_{n-1}\} \subseteq \mathbb{N} \setminus \{0\}$ es tal que $(a_i; a_j) = 1$ para todo $\{i, j\} \subseteq \{1, \dots, n-1\}$, $i \neq j$, entonces $[a_1; a_2; \dots; a_{n-1}] = a_1 \cdots a_{n-1}$.

Paso inductivo. Sea $\{a_1, a_2, \dots, a_n\} \subseteq \mathbb{N} \setminus \{0\}$ tal que $(a_i; a_j) = 1$ para todo $\{i, j\} \subseteq \{1, \dots, n\}$, $i \neq j$. Veamos que $[a_1; a_2; \dots; a_n] = a_1 a_2 \cdots a_n$.

Sabemos por la Proposición 1.1.21 que $[a_1; a_2; \dots; a_n] = [[\, a_1; a_2; \dots; a_{n-1}\,]; a_n]$ y por la hipótesis de inducción $[a_1; a_2; \dots; a_{n-1}] = a_1 a_2 \cdots a_{n-1}$, entonces $[a_1; a_2; \dots; a_n] = [a_1 a_2 \cdots a_{n-1}; a_n]$.

Como $(a_i; a_j) = 1$ para todo $\{i, j\} \subseteq \{1, \ldots, n\}$, en particular $(a_i; a_n) = 1$ para todo $i \in \{1, \ldots, n-1\}$, entonces por el Corolario 1.1.15 $(a_1 a_2 \cdots a_{n-1}; a_n) = 1$.

Por el Teorema 1.1.9:

$$\begin{aligned}[[\, a_1; a_2; \ldots; a_{n-1}\,]; a_n] &= [a_1 a_2 \cdots a_{n-1}; a_n] \\ &= \frac{(a_1 a_2 \cdots a_{n-1}) \cdot a_n}{(a_1 a_2 \cdots a_{n-1}; a_n)} \\ &= \frac{a_1 a_2 \cdots a_{n-1} \cdot a_n}{1} \\ &= a_1 a_2 \cdots a_n.\end{aligned}$$

Por lo tanto, $[a_1; a_2; \ldots; a_n] = a_1 a_2 \cdots a_n$. □

Las ecuaciones con coeficientes enteros son llamadas **ecuaciones diofantinas**. La clase más simple de ecuaciones diofantinas es la clase de las ecuaciones diofantinas lineales. Una **ecuación diofantina lineal de dos variables** x y y es una ecuación diofantina de la forma $ax + by = c$. Una pareja ordenada $(x_0, y_0) \in \mathbb{Z} \times \mathbb{Z}$ es una **solución** de la ecuación $ax + by = c$ si y sólo si $ax_0 + by_0 = c$.

Teorema 1.1.23. *La ecuación diofantina lineal $ax + by = c$ tiene solución si y sólo si $d \mid c$ donde $d = (a; b)$. Si (x_0, y_0) es una solución particular de la ecuación, entonces todas sus soluciones están dadas por*

$$x = x_0 + \left(\frac{b}{d}\right) t \qquad y \qquad y = y_0 - \left(\frac{a}{d}\right) t$$

donde t es un entero arbitrario.

Demostración: La prueba consiste de cuatro partes

- Si la ecuación tiene solución, entonces $d \mid c$.

  Supongamos que (α, β) es una solución de la ecuación, es decir, $a\alpha + b\beta = c$. Como $d = (a; b)$, entonces $d \mid a$ y $d \mid b$, entonces $d \mid (a\alpha + b\beta)$, de manera que $d \mid c$

- Si $d \mid c$, entonces la ecuación tiene solución.

  Supongamos que $d \mid c$. Entonces $c = de$ para algún entero e.

  Por otro lado, como $d = (a; b)$ existen enteros r y s tales que $ra + sb = d$. Multiplicando ambos lados de la ecuación por e tenemos $rae + sbe = de$, es decir $a(re) + b(se) = c$. Por lo que, (re, se) es una solución de la ecuación.

- Demostremos ahora que si (x_0, y_0) es una solución particular de la ecuación, entonces (x, y), donde $x = x_0 + \left(\frac{b}{d}\right) t$ y $y = y_0 - \left(\frac{a}{d}\right) t$, es una solución.

  Tenemos que

$$\begin{aligned}ax + by &= a\left[x_0 + \left(\frac{b}{d}\right) t\right] + b\left[y_0 - \left(\frac{a}{d}\right) t\right] \\ &= (ax_0 + by_0) + at\left(\frac{b}{d}\right) - bt\left(\frac{a}{d}\right).\end{aligned}$$

Como $d = (a;b)$, entonces $d \mid a$ y $d \mid b$ y por el Lema 1.1.3 sabemos que $a = d\left(\frac{a}{d}\right)$ y $b = d\left(\frac{b}{d}\right)$, sustituyendo estos valores en la ecuación anterior tenemos que

$$\begin{aligned}(ax_0 + by_0) + at\left(\frac{b}{d}\right) - bt\left(\frac{a}{d}\right) &= (ax_0 + by_0) + d\left(\frac{a}{d}\right)t\left(\frac{b}{d}\right) - d\left(\frac{b}{d}\right)t\left(\frac{a}{d}\right)\\ &= ax_0 + by_0\\ &= c.\end{aligned}$$

Concluyendo que (x, y) es una solución de la ecuación.

- Demostremos que cada solución (x', y') es de la forma

$$x' = x_0 + \left(\frac{b}{d}\right)t \qquad \text{y} \qquad y' = y_0 - \left(\frac{a}{d}\right)t.$$

Como (x_0, y_0) y (x', y') son soluciones de las ecuación, tenemos que $ax_0 + by_0 = ax' + by'$.

Así,

$$a(x' - x_0) = b(y_0 - y'). \tag{1.2}$$

Veamos que como $d = (a;b)$, entonces $d \mid a$ y $d \mid b$ y por el Lema 1.1.3 tenemos que $a = d\left(\frac{a}{d}\right)$ y $b = d\left(\frac{b}{d}\right)$, sustituyendo en la Ecuación 1.2 tenemos

$$d\left(\frac{a}{d}\right)(x' - x_0) = d\left(\frac{b}{d}\right)(y_0 - y')$$

y como $d \neq 0$, entonces por la ley de cancelación de los enteros se sigue que

$$\left(\frac{a}{d}\right)(x' - x_0) = \left(\frac{b}{d}\right)(y_0 - y').$$

En particular, $\frac{b}{d} \mid \left(\frac{a}{d}\right)(x' - x_0)$, luego, por el Teorema 1.1.6 se sigue que $\left(\frac{a}{d}, \frac{b}{d}\right) = 1$ y por el Corolario 1.1.16, concluimos que $\frac{b}{d} \mid (x' - x_0)$. Por lo tanto, $x' - x_0 = \left(\frac{b}{d}\right)t$ para algún entero t, esto es $x' = x_0 + \left(\frac{b}{d}\right)t$.

Ahora, sustituyendo $x' - x_0$ en la ecuación 1.2, tenemos

$$a\left(\frac{b}{d}\right)t = b(y_0 - y')$$

Por el Lema 1.1.3, como $d \mid a$, entonces $a = d\left(\frac{a}{d}\right)$ y sustituyéndolo en la ecuación anterior tenemos que

$$d\left(\frac{a}{d}\right)\left(\frac{b}{d}\right)t = b(y_0 - y')$$

y de nuevo por el Lema 1.1.3, como $d \mid b$, entonces $b = d\left(\frac{b}{d}\right)$, por lo que la ecuación anterior queda de la siguiente manera

$$\left(\frac{a}{d}\right)bt = b(y_0 - y')$$

y por la ley de la cancelación de los enteros, se sigue que

$$\left(\frac{a}{d}\right)t = y_0 - y', \text{es decir,}$$

$$y' = y_0 - \left(\frac{a}{d}\right)t.$$

De manera que cada solución de la ecuación es de la forma deseada.

□

Sea m un entero positivo. Un entero a es **congruente** a un entero b **módulo** m si $m \mid (a-b)$. Denotaremos esto como $a \equiv b \mod m$; diremos que m es el módulo de la congruencia.

Si a y b no son congruentes módulo m, entonces lo denotaremos como $a \not\equiv b \mod m$

Teorema 1.1.24. *Sea $\{a, b, c, m\} \subseteq \mathbb{Z}$. Lo siguiente se satisface:*

1. $a \equiv a \mod m$ *(propiedad reflexiva).*
2. *Si* $a \equiv b \mod m$, *entonces* $b \equiv a \mod m$ *(propiedad simétrica).*
3. *Si* $a \equiv b \mod m$ *y* $b \equiv c \mod m$, *entonces* $a \equiv c \mod m$ *(propiedad transitiva).*

Demostración:

1. Notemos que $(a - a) = 0$ y $m \mid 0$, por lo que $a \equiv a \mod m$.
2. Supongamos que $a \equiv b \mod m$, entonces $m \mid (a - b)$; o lo que es lo mismo, $m \mid -(b - a)$. De manera que $m \mid (b - a)$ y por definición $b \equiv a \mod m$.
3. Supongamos que $a \equiv b \mod m$ y $b \equiv c \mod m$. Se sigue de la definición de congruencia que $m \mid (a-b)$ y $m \mid (b - c)$, entonces por el Teorema 1.1.10, $m \mid [(a - b) + (b - c)]$; simplificando, $m \mid (a - c)$, por consecuencia, $a \equiv c \mod m$.

□

Corolario 1.1.25. *Si* $\{a,b,c,m\} \subseteq \mathbb{Z}$, *entonces* $a \equiv b \mod m$ *si y sólo si* $(a-c) \equiv (b-c) \mod m$.

Demostración: Demostremos la parte suficiente. Como $a \equiv b \mod m$, entonces $a-b = km$ para alguna $m \in \mathbb{Z}$. Ahora bien $(a-b)+(c-c) = km$, reagrupando, $(a-c)-(b-c) = km$ y por definición de congruencia, $(a-c) \equiv (b-c) \mod m$.

Demostremos ahora la parte necesaria. Como $(a-c) \equiv (b-c) \mod m$, entonces $(a-c)-(b-c) = lm$ para alguna $l \in \mathbb{Z}$, reagrupando, $(a-b)+(c-c) = lm$, por lo que $(a-b) = lm$. De manera que $a \equiv b \mod m$. □

Teorema 1.1.26. *Sea* $\{a,b,c,m\} \subseteq \mathbb{Z}$, *si* $ac \equiv bc \mod m$ *y* $(c;m) = d$, *entonces* $a \equiv b \mod \dfrac{m}{d}$.

Demostración: Supongamos que $ac \equiv bc \mod m$ donde $(c;m) = d$. Como $m \mid (ac-bc)$ tenemos que $ac-bc = km$ para algún entero k, factorizando c, $c(a-b) = km$. Como $d \mid c$ y $d \mid m$, entonces por el Lema 1.1.3, $c = d\left(\dfrac{c}{d}\right)$ y $m = d\left(\dfrac{m}{d}\right)$; sustituyendo en la ecuación anterior tenemos

$$d\left(\frac{c}{d}\right)(a-b) = kd\left(\frac{m}{d}\right)$$

y por la ley de la cancelación de los enteros, se sigue que

$$\left(\frac{c}{d}\right)(a-b) = k\left(\frac{m}{d}\right)$$

De lo anterior tenemos que, en particular, $\dfrac{m}{d} \mid \left(\dfrac{c}{d}\right)(a-b)$. Por el Teorema 1.1.6, $\left(\dfrac{c}{d};\dfrac{m}{d}\right) = 1$ y por el Corolario 1.1.16, $\dfrac{m}{d} \mid (a-b)$, de manera que, por definición, $a \equiv b \mod \dfrac{m}{d}$. □

Sea $\{a,b,m\} \subseteq \mathbb{Z}$. Una congruencia de la forma $ax \equiv b \mod m$ será llamada **congruencia lineal**. Diremos que un entero x_0 es **solución de la congruencia lineal** $ax \equiv b \mod n$ si $ax_0 \equiv b \mod n$. Sea $ax \equiv b \mod m$, diremos que x_1 y x_2 son **soluciones incongruentes** de la congruencia lineal si $ax_1 \equiv b \mod m$, $ax_2 \equiv b \mod m$ y $x_1 \not\equiv x_2 \mod m$.

Teorema 1.1.27. *La congruencia lineal* $ax \equiv b \mod m$ *tiene solución si y sólo si* $d \mid b$ *donde* $d = (a;m)$. *Si* $d \mid b$, *entonces la congruencia lineal tiene* d *soluciones incongruentes.*

Demostración: Como $ax \equiv b \mod m$, entonces $m \mid (ax-b)$,de este modo, $ax-b = my$ para alguna $y \in \mathbb{Z}$, por lo que la congruencia lineal es equivalente a la ecuación diofantina lineal $ax-my = b$; en consecuencia, la congruencia tiene solución si y sólo si la ecuación diofantina lineal tiene solución. Sin embargo, sabemos por el Teorema 1.1.23 que la ecuación diofantina lineal tiene solución si y sólo si $d \mid b$, donde $d = (a;m)$. De manera que $ax \equiv b \mod m$ tiene solución si y sólo si $d \mid b$.

Además, si (x_0, y_0) es una solución particular de la ecuación diofantina, entonces x_0 es solución de la congruencia lineal. Más aún, si z es solución de la congruencia lineal, entonces $az \equiv b \mod m$ y de la definición, $m \mid az-b$, es decir $az-b = my'$ para alguna $y' \in \mathbb{Z}$, como z satisface la ecuación diofantina para alguna y', entonces por el Teorema 1.1.23, z es de la forma $z = x_0 + \left(\dfrac{m}{d}\right)t$ con $t \in \mathbb{Z}$.

Si $d \mid b$, todas las soluciones de la ecuación diofantina lineal $ax-my = b$ son de la forma:

$$x = x_0 + \left(\frac{m}{d}\right)t, \quad y = y_0 + \left(\frac{a}{d}\right)t$$

con $t \in \mathbb{Z}$, por lo que los enteros de la forma $x = x_0 + \left(\frac{m}{d}\right) t$, son soluciones de la congruencia lineal, donde x_0 es una solución particular.

Veamos ahora que si $d \mid b$, entonces la congruencia tiene d soluciones incongruentes, supongamos que $x_1 = x_0 + \left(\frac{m}{d}\right) t_1$ y $x_2 = x_0 + \left(\frac{m}{d}\right) t_2$ son dos soluciones tales que $x_1 \equiv x_2 \mod m$, entonces

$$x_0 + \left(\frac{m}{d}\right) t_1 \equiv x_0 + \left(\frac{m}{d}\right) t_2 \mod m$$

y por el Corolario 1.1.25, restando x_0 de ambos lados tenemos

$$\left(\frac{m}{d}\right) t_1 \equiv \left(\frac{m}{d}\right) t_2 \mod m.$$

Como $\frac{m}{d} \mid m$, entonces $\left(\frac{m}{d}; m\right) = \frac{m}{d}$ y por el Teorema 1.1.26, $t_1 \equiv t_2 \mod d$. Así $x_1 \equiv x_2 \mod m$ si y sólo si $t_1 \equiv t_2 \mod d$; dicho de otro modo, si y sólo si t_1 y t_2 pertenecen a la misma clase de congruencia módulo d y sabemos que existen d clases incongruentes módulo d. Además, como t puede ser cualquier entero y sabemos que cada entero pertenece a una clase de congruencia módulo d, entonces existirán exactamente d soluciones incongruentes.

Podemos concluir que la congruencia lineal, cuando tiene solución, tiene exactamente d soluciones incongruentes dadas por $x = x_0 + \left(\frac{m}{d}\right) t$, donde $t \in \{0, \ldots, d-1\}$. □

A partir del enunciado anterior, cuando $b = 1$ en la congruencia lineal $ax \equiv b \mod m$, entonces ésta tendrá una única solución si y sólo si $(a; m) = 1$. Dado lo anterior, diremos que a es **invertible**; además x será llamado el **inverso de** a **módulo** m y será denotado por a^{-1}, de manera que $aa^{-1} \equiv 1 \mod m$.

Corolario 1.1.28. *La congruencia lineal $ax \equiv b \mod m$ tiene una única solución si y sólo si $(a, m) = 1$.*

Demostración: Demostremos la parte suficiente. Sabemos por el teorema anterior que si la congruencia $ax \equiv b \mod m$ tiene solución, entonces $d \mid b$ con $d = (a; m)$ y además tiene d soluciones incongruentes. Dado que, por hipótesis, la congruencia tiene solución única, entonces $d = 1$, es decir $(a; m) = 1$.

Demostremos la parte necesaria. Como $(a; m) = 1$ y $1 \mid b$, entonces por el teorema anterior sabemos que la congruencia $ax \equiv b \mod m$ tiene solución.

Además, tiene d soluciones incongruentes, puesto que $d = 1$, entonces la solución es única. □

Teorema 1.1.29. ***(Teorema Chino del Residuo)*** *Sea S un sistema de congruencias lineales $x \equiv a_i \mod m_i$ con $i \in \{1, \ldots, k\}$. Si $(m_i; m_j) = 1$ para todo $\{i, j\} \subseteq \{1, \ldots, k\}$ con $i \neq j$, entonces el sistema S tiene una solución única módulo $m_1 m_2 \cdots m_k$.*

Demostración: La demostración consiste en dos partes. Primero construiremos una solución y luego demostraremos que ésta es única módulo $m_1 m_2 \cdots m_k$.

Sea $M = m_1 m_2 \cdots m_k$ y $M_i = \frac{M}{m_i}$, con $i \in \{1, \ldots, k\}$. Notemos que $M_i = \prod_{\substack{j=1 \\ j \neq i}}^{k} m_j$ y como los módulos m_i son primos relativos por pares, entonces M_i y m_i no tienen divisores en común para cada $i \in \{1, \ldots, k\}$, esto es, $(M_i; m_i) = 1$. Además, $M_i \equiv 0 \mod m_j$ cuando $i \neq j$.

Como $(M_i; m_i) = 1$, por el Corolario 1.1.28 la congruencia $M_i y_i \equiv 1 \mod m_i$ tiene una única solución y_i. Además, notemos que y_i es el inverso de M_i módulo m_i. Sea $x = a_1M_1y_1 + a_2M_2y_2 + \cdots + a_kM_ky_k$.

Veamos que ésta es una solución para el sistema lineal. Consideremos $j \in \{1, \ldots, k\}$ arbitraria, tenemos

$$x = \left(\sum_{\substack{i=1 \\ i \neq j}}^{k} a_i M_i y_i \right) + a_j M_j y_j.$$

Sabemos que si $i \neq j$, entonces $M_i \equiv 0 \mod m_j$ por lo que:

$$x = rm_j + a_j M_j y_j$$

para alguna $r \in \mathbb{Z}$. En particular $(x - a_j M_j y_j) \equiv 0 \mod m_j$, o bien $x \equiv a_j M_j y_j \mod m_j$. Como $M_j y_j \equiv 1$ mód m_j, entonces $a_j M_j y_j \equiv a_j \mod m_j$, de lo anterior, podemos concluir que $x \equiv a_j \mod m_j$. Por lo que, x satisface cada congruencia del sistema, de esta manera, x es una solución para el sistema S.

Probemos que la solución es única módulo M.

Sean x_0 y x_1 dos soluciones del sistema. Demostraremos que $x_0 \equiv x_1 \mod M$.

Como $x_0 \equiv x_1 \mod m_j$ y $x_1 \equiv a_j \mod m_j$ para $1 \leq j \leq k$, $x_1 - x_0 \equiv 0 \mod m_j$; esto es, $m_j \mid (x_1 - x_0)$ para cada j. Por la Proposición 1.1.20, $[m_1, m_2, \ldots, m_k] \mid (x_1 - x_0)$ y por el Corolario 1.1.22, $[m_1, m_2, \ldots, m_k] = M$. De manera que $M \mid (x_1 - x_0)$, de la definición, $x_1 - x_0 \equiv 0 \mod M$; o lo que es lo mismo, $x_1 \equiv x_0 \mod M$. De este modo, cualesquiera dos soluciones del sistema lineal S son congruentes módulo M, por lo tanto, la solución es única módulo M. □

1.2. Teoría de Gráficas y Digráficas

Una **gráfica** G es una pareja ordenada (V, E) tal que V es un conjunto finito no vacío de objetos llamados **vértices** y E es un conjunto de subconjuntos de 2 elementos de V llamados **aristas**. Denotaremos por $V(G)$ al conjuntos de vértices de la gráfica G y por $E(G)$ al conjunto de aristas de la misma. Podemos además, tener una representación geométrica de la misma, donde los vértices serán puntos en el plano y las aristas serán un segmento de recta que une los puntos correspondientes a los extremos de la arista. Un ejemplo de lo anterior, es la Figura 1.1:

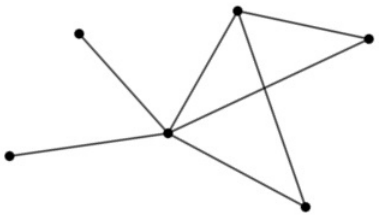

Figura 1.1: Gráfica G.

Si $\{u, v\} \in E(G)$, entonces diremos que los vértices u y v son **adyacentes**, tal arista será denotada como uv.

Una gráfica H es una **subgráfica** de una gráfica G si $V(H) \subseteq V(G)$ y $E(H) \subseteq E(G)$.

Sea G un gráfica y S un subconjunto no vacío de $V(G)$, la **subgráfica inducida por S**, denotada por $G[S]$, es la gráfica tal que su conjunto de vértices es S y dos vértices u y v en S son adyacentes en $G[S]$ si y sólo si u y v son adyacentes en G, es decir una subgráfica H de una gráfica G es llamada **subgráfica inducida** si existe un subconjunto S no vacío de $V(G)$ tal que $H = G[S]$.

Un **camino** W en G es una sucesión de vértices $W = (v_0, v_1, \ldots, v_k)$ en G tal que vértices consecutivos en W son adyacentes en G, dicho de otro modo, para $i \in \{0, \ldots, k-1\}$, $v_i v_{i+1} \in E(G)$. Diremos que v_0 es el **vértice inicial** de W y v_k el **vértice final** de W.

Un **camino cerrado** es un camino en el que sus vértices inicial y final son iguales.

Un camino $C = (x_1, \ldots, x_{k+1})$ es un **paseo** en G si no se repite ninguna arista, esto es, si $i \neq j$ con $\{i, j\} \subseteq \{0, \ldots, k\}$, entonces $x_i x_{i+1} \neq x_j x_{j+1}$. Diremos que C es una **trayectoria** en G si no repite ningún vértice, es decir, si $\{i, j\} \subseteq \{1, \ldots, k+1\}$ e $i \neq j$, entonces $x_i \neq x_j$.

Un **circuito** es un paseo cerrado. Un **ciclo** es un camino cerrado, digamos $C = (x_1, \ldots, x_{k+1})$, tal que no repite vértices salvo el inicial y final, dicho de otra manera, $x_i \neq x_j$ para todo $\{i, j\} \subseteq \{2, \ldots, k\}$ y $x_1 = x_{k+1}$.

Una gráfica G es **conexa** si para cada par de vértices x y y, existe al menos un camino que une a x con y.

Una subgráfica H de una gráfica G es una **componente conexa** de G si H es conexa y no es una subgráfica propia de una subgráfica conexa de G.

Un ejemplo de la definición anterior, es la gráfica siguiente en la que podemos observar que tiene dos componentes conexas, la primera es la inducida por el conjunto $\{1, 2, 3, 4\}$ y la segunda es la inducida por el conjunto $\{5, 6, 7\}$.

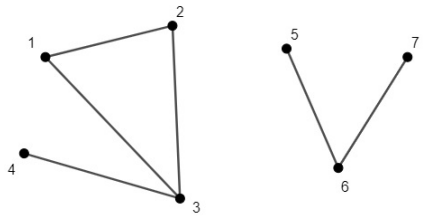

Figura 1.2: Gráfica de componentes conexas.

Una **digráfica** D es una pareja ordenada (V, F) tal que V es un conjunto finito no vacío de elementos llamados **vértices** y F es un conjunto finito de pares ordenados de vértices, llamados **flechas**. Denotamos por $V(D)$ al conjunto de vértices de la digráfica D y por $F(D)$ al conjunto de flechas de la misma.

Si $\{x, y\} \subseteq V(D)$ diremos que x es **adyacente a** y si $(x, y) \in F(D)$ o $(y, x) \in F(D)$. Diremos que x es **adyacente hacia** y si $(x, y) \in F(D)$. Al igual que la gráfica , la digráfica también tiene su representación geométrica, en este caso las flechas serán representadas como tal para indicar la dirección de la adyacencia entre los dos vértices.

Un ejemplo de la representación mencionada anteriormente es la Figura 1.3:

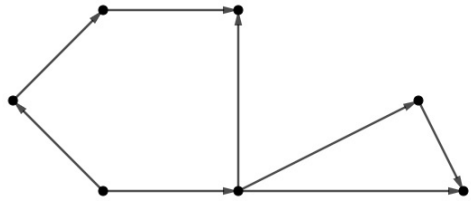

Figura 1.3: Digráfica D.

Una flecha de la forma (x, x) será llamada **lazo**. Diremos que el lazo $(x, x) \in F(D)$ es un **lazo aislado** si no existe $y \in V(D) \setminus \{x\}$ tal que $(x, y) \in F(D)$ y no existe $z \in V(D) \setminus \{x\}$ tal que $(z, x) \in F(D)$.

Sean D_1 y D_2 dos digráficas, diremos que la digráfica D es la **unión** de D_1 y D_2, si $V(D) = V(D_1) \cup V(D_2)$ y $F(D) = F(D_1) \cup F(D_2)$ y será denotada como $D_1 \cup D_2$.

Si v es un vértice en D, denotaremos al conjunto $\{u \in V \setminus \{ v \}: (v, u) \in F(D)\}$ por $N_D^+(v)$ y de manera análoga podemos denotar al conjunto $\{w \in V \setminus \{ v \}: (w, v) \in F(D)\}$ por $N_D^-(v)$. Los conjuntos $N_D^+(v)$ y $N_D^-(v)$ serán llamados **exvecindad** e **invecindad** de v, respectivamente. Así, el conjunto $N_D^+(v) \cup N_D^-(v)$, denotado por $N_D(v)$, es llamado la **vecindad** de v.

Además, los elementos del conjunto $N_D^+(v)$ serán llamados **exvecinos** de v y los elementos del conjunto $N_D^-(v)$ serán llamados **invecinos** de v; los elementos de $N_D(v)$ serán llamados **vecinos** de v.

El **exgrado** de v es $|N_D^+(v)|$ y es denotado por $d^+(v)$ y el **ingrado** de v es $|N_D^-(v)|$, denotado por $d^-(v)$. De manera que el **grado** de v es $d^+(v) + d^-(v)$ y se denota por $d(v)$. El **pseudoexgrado** del vértive v es el número de flechas que salen de v. El **pseudoingrado** del vértice v es el número de flechas que llegan a v.

Diremos que un vértice x es un **vértice aislado** si $d^+(x) = 0$ y $d^-(x) = 0$.

Observación 1.2.1. *Si (x, x) es un lazo aislado en una digráfica D, el pseudoingrado de x y el pseudoexgrado de x son ambos iguales a 1.*

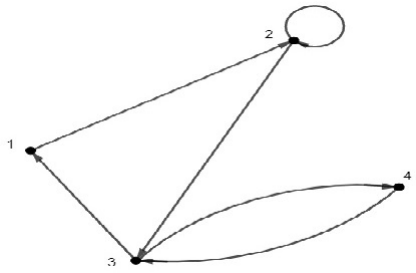

Figura 1.4: Digráfica D_1

Podemos observar que en la Figura 1.4 el conjunto de vértices de la digráfica D_1 es $\{1, 2, 3, 4\}$ y el conjunto de flechas es $\{(1, 2), (2, 3), (3, 1), (2, 2), (3, 4), (4, 3)\}$. Así, por ejemplo, podemos decir que el vértice

2 es adyacente hacia 3, el vértice 4 es adyancente hacia 3, etcétera. Además el vértice 2 tiene un lazo pues la flecha $(2, 2)$ pertenece al conjunto $F(D_1)$.

Por otro lado, si nos fijamos en el vértice 3, su exvecindad es $\{1, 4\}$, por lo que sus exvecinos son los vértices 1 y 4, mientras que su invecindad es $\{2, 4\}$ de manera que sus invecinos son los vértices 2 y 4 y su vecindad es $\{1, 2, 4\}$ de este modo, sus vecinos son los vértices 1, 2 y 4. De manera que el exgrado del vértice 3 es 2, el ingrado del vértice 3 es 2 y el grado es 4.

Notemos que en el caso del vértice 2 a pesar de tener un lazo, el mismo vértice 2, no pertenece ni a la exvecindad, ni a la invecindad, ni a la vecindad de si mismo, por lo que su exgrado es igual a 1 y su ingrado es igual a 1; sin embargo, podemos ver que su pseudoexgrado es igual a 2 y su pseudoingrado es 2.

Sean D y H dos digráficas. Diremos que H es una **subdigráfica** de D si $V(H) \subseteq V(D)$ y $F(H) \subseteq F(D)$. Si H es una subdigráfica de D, decimos que H es una **subdigráfica inducida** en D si y sólo si $F(H) = \{(u, v) \in F(D) : \{u, v\} \subseteq V(H)\}$. Si X es un subconjunto de D no vacío, la **subdigráfica inducida por X en D**, denotada por $D[X]$, es la digráfica tal que $V(D[X]) = X$ y si $\{u, v\} \subseteq X$, $(u, v) \in F(D[X])$ si y sólo si $(u, v) \in F(D)$.

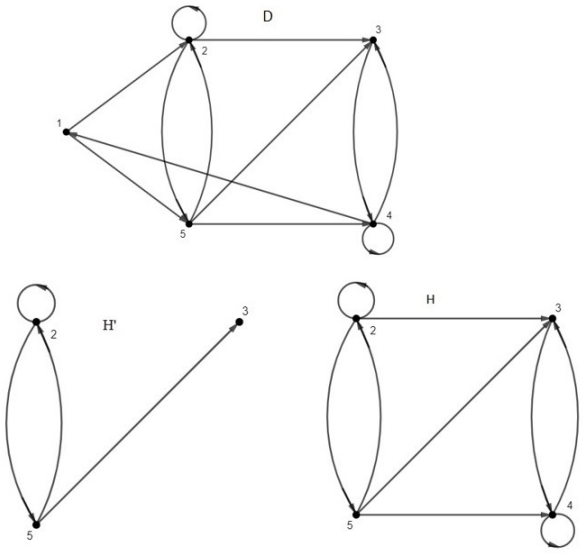

Figura 1.5: Digráfica D y algunas subdigráficas.

En la Figura 1.5 podemos ver que H' es una subdigráfica de la digráfica D. Mientras que la digráfica H es un subdigráfica inducida en D y también es la subdigráfica inducida por el conjunto X en D donde $X = \{2, 3, 4, 5\}$, esto es $H = D[X]$.

Un **camino** en una digráfica, es una sucesión de vértices, digamos $C = (x_1, x_2, \ldots, x_n)$, tal que para todo $i \in \{1, \ldots, n-1\}$, x_i es adyacente a x_{i+1}. Diremos que un camino C es **dirigido** si la flecha $(x_i, x_{i+1}) \in F(D)$ para toda $i \in \{1, \ldots, n-1\}$. Diremos que un camino C es **antidirigido** si no tiene subsucesiones que sean caminos dirigidos de longitud 2.

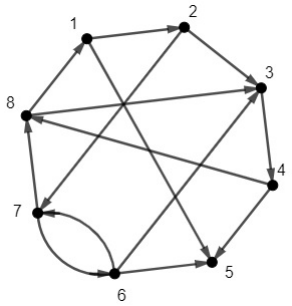

Figura 1.6: Digráfica D_2.

La sucesión de vértices $(3, 4, 5, 6, 7, 2, 1, 8)$ es un ejemplo de camino en la digráfica de la Figura 1.6. Mientras que la sucesión de vértices $(3, 4, 8, 1, 2, 7, 6)$ es un camino dirigido para tal digráfica. Luego, la sucesión $(4, 5, 6, 3, 2, 7)$ es un camino antidirigido de la misma.

Una **trayectoria dirigida** en una digráfica, es un camino dirigido $(x_1, \ldots, x_n)$, tal que si $\{i, j\} \subseteq \{1, \ldots, n\}$ e $i \neq j$, entonces $x_i \neq x_j$, es decir los vértices del camino son distintos.

Un camino dirigido en una digráfica, $(x_1, x_2, \ldots, x_k)$ es **cerrado** si $x_1 = x_k$. Un **ciclo dirigido** en una digráfica, es un camino dirigido cerrado, digamos $(x_1, \ldots, x_n, x_1)$, tal que no repite vértices salvo el primero y el último, es decir $x_i \neq x_j$ para todo $\{i, j\} \subseteq \{1, \ldots, n\}$.

Diremos que un ciclo dirigido γ es un **ciclo aislado** si no existe $y \in V(D) \setminus V(\gamma)$ tal que $(x, y) \in F(D)$ y no existe $z \in V(D) \setminus V(\gamma)$ tal que $(z, x) \in F(D)$.

Si C es un camino dirigido en una digráfica, digamos $C = (x_0, \ldots, x_n)$, entonces la **longitud** del camino es $\boldsymbol{n}$ y se denota por $l(C)$. Así, un $\boldsymbol{k}$**-ciclo** es un ciclo dirigido de longitud k.

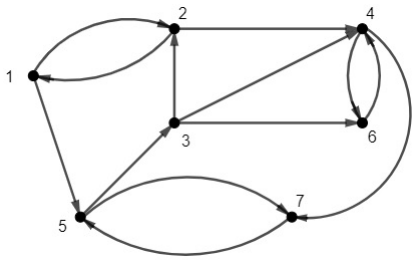

Figura 1.7: Digráfica D_3.

La sucesión de vértices $(1, 5, 3, 4, 7, 5, 3, 2, 1)$ es un ejemplo de camino cerrado en la digráfica D_3.

Un ejemplo de trayectoria en la digráfica D_3 de la Figura 1.7 es $(2, 1, 5, 3, 4, 7)$.

La sucesión de vértices $(5, 3, 6, 4, 7, 5)$ es un ejemplo de ciclo en la digráfica D_3 y diremos que es un 5-ciclo pues su longitud es 5.

Notemos que un camino dirigido $C = (x_1, x_2, \ldots, x_n)$, puede ser considerado como una digráfica, donde $F(C) = \{(x_i, x_{i+1}) : i \in \{0, \ldots, n-1\}\}$ y $V(W) = \{x_1, x_2, \ldots, x_n\}$.

Observación 1.2.2. *Si una digráfica D cumple que $d^+(x) = 1$ para todo vértice x en D y C es un camino de longitud al menos 3, entonces C no es antidirigido.*

Demostración: Demostremos la observación por contradicción, es decir, supongamos que $C = (\alpha_0, \alpha_1, \ldots, \alpha_n)$ es un camino de longitud al menos 3 y es antidirigido. Consideremos lo siguientes casos:

Caso 1: $(\alpha_0, \alpha_1) \in F(C)$.

En este caso, como $(\alpha_0, \alpha_1) \in F(C)$ y C es antidirigido, entonces $(\alpha_2, \alpha_1) \in F(C)$ y de igual manera $(\alpha_2, \alpha_3) \in F(C)$, de modo que $d^+(\alpha_2) \geq 2$ lo cual contradice la hipótesis.

Caso 2: $(\alpha_0, \alpha_1) \notin F(C)$.

En este caso, como $(\alpha_0, \alpha_1) \notin F(C)$, entonces $(\alpha_1, \alpha_0) \in F(C)$. Además, como C es antidirigido, $(\alpha_1, \alpha_2) \in F(C)$, lo que implica que, $d^+(\alpha_1) \geq 2$, lo cual es una contradicción.

Dados ambos casos, concluimos que C no puede ser antidirigido. □

Si D es una digráfica, la **gráfica subyacente de D**, denotada por $UG(D)$ es la gráfica tal que $V(UG(D)) = V(D)$ y $uv \in E(UG(D))$ si y sólo si u y v son adyacentes en D. Un ejemplo de esto se muestra en la Figura 1.8, donde $UG(D)$ es la gráfica subyacente de D.

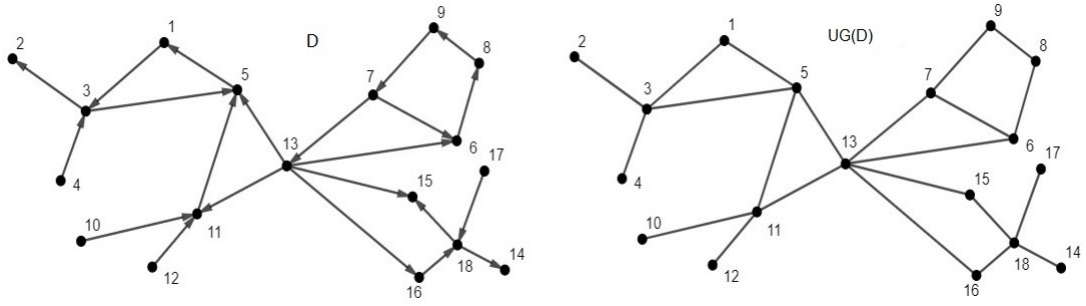

Figura 1.8: Digráfica D y su gráfica subyacente.

Lema 1.2.3. *Si H es una digráfica tal que para todo $v \in V(H)$, $d^+(v) = 1$, entonces H tiene al menos un ciclo dirigido.*

Demostración: Como para todo $v \in V(H)$, $d^+(v) = 1$, entonces podemos considerar una trayectoria dirigida, digamos $T = (x_1, \ldots, x_t)$, de longitud máxima. Al ser T de longitud máxima y como en particular $d^+(x_t) = 1$, existe x_i con $i \in \{1, \ldots, t\}$ tal que $(x_t, x_i) \in F(H)$. Concluyendo que $(x_i, x_{i+1}, \ldots, x_t, x_i)$ es un ciclo dirigido en H. □

Una digráfica D es **conexa** si $UG(D)$ es una gráfica conexa. Un ejemplo de una digráfica conexa se muestra nuevamente en la Figura 1.8.

Una digráfica D es **unilateralmente conexa** si para cada par de vértices x y y, existe algún camino dirigido de x hacia y o de y hacia x. Un ejemplo se presenta en la siguiente digráfica:

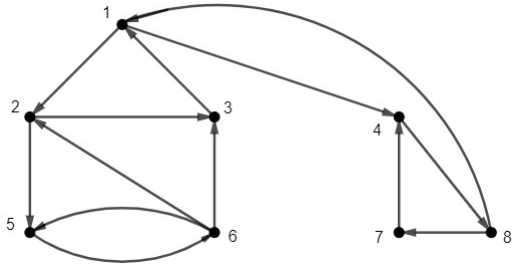

Figura 1.9: Digráfica unilateralmente conexa.

Una digráfica D es **fuertemente conexa** si para cada par de vértices x y y, existe un camino dirigido de x hacia y y un camino dirigido de y hacia x. Un ejemplo se presenta en la siguiente digráfica:

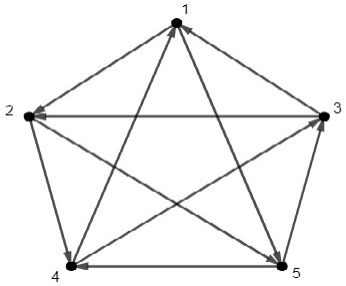

Figura 1.10: Digráfica fuertemente conexa.

Una **componente fuertemente conexa** de una digráfica D es una subdigráfica inducida maximal de D con la propiedad de ser fuertemente conexa.

Un ejemplo es la siguiente digráfica, en la que podemos observar que tiene tres componentes fuertemente conexas, la primera es la inducida por el conjunto $\{1, 2, 5\}$, la segunda es la inducida por el conjunto $\{6, 7\}$ y la tercera es la inducida por el conjunto $\{3, 4, 8\}$.

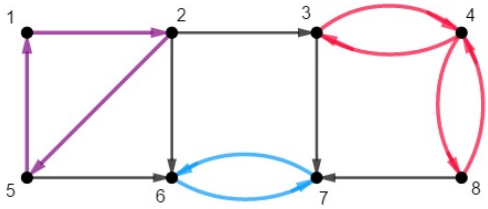

Figura 1.11: Ejemplo de una digráfica y sus componentes fuertemente conexas.

Capítulo 2

Digráficas de congruencias cúbicas

En este capítulo presentamos algunas propiedades básicas de las digráficas de congruencias cúbicas trabajadas en [17], tales como el exgrado de los vértices, el comportamiento de sus flechas, también propiedades sobre caminos dirigidos y ciclos dirigidos de la misma.

2.1. Propiedades de la digráfica de congruencias cúbicas de orden n

Sea n un natural distinto de 0, la **digráfica de congruencias cúbicas de orden n**, denotada por $\Gamma(n)$, es la digráfica cuyo conjunto de vértices es el conjunto $\{0, 1, \ldots, n-1\}$ y $(a, b) \in F(\Gamma(n))$ si y sólo si $a^3 \equiv b \mod n$. Dicha digráfica fue definida en [17] por J. Skowronek-Kaziów, quien demostró diversos resultados que han sido enunciados a lo largo del trabajo.

Para ejemplificar la construcción de la digráfica de congruencias cúbicas, consideremos la digráfica $\Gamma(13)$. En dicha digráfica, dos vértices a y b que satisfagan $a^3 \equiv b \mod 13$ tendrán una flecha de a hacia b. Podemos construir la representación geométrica de la digráfica obteniendo las flechas de la misma por medio de las congruencia de cada vértice, como se muestra a continuación:

$$
\begin{aligned}
0^3 = 0 \text{ y } 0 \equiv 0 \mod 13, &\text{ por lo que } (0,0) \in F(\Gamma(13)),\\
1^3 = 1 \text{ y } 1 \equiv 1 \mod 13, &\text{ por lo que } (1,1) \in F(\Gamma(13)),\\
2^3 = 8 \text{ y } 8 \equiv 8 \mod 13, &\text{ por lo que } (2,8) \in F(\Gamma(13)),\\
3^3 = 27 \text{ y } 27 \equiv 1 \mod 13, &\text{ por lo que } (3,1) \in F(\Gamma(13)),\\
4^3 = 64 \text{ y } 64 \equiv 12 \mod 13, &\text{ por lo que } (4,12) \in F(\Gamma(13)),\\
5^3 = 125 \text{ y } 125 \equiv 8 \mod 13, &\text{ por lo que } (5,8) \in F(\Gamma(13)),\\
6^3 = 216 \text{ y } 216 \equiv 8 \mod 13, &\text{ por lo que } (6,8) \in F(\Gamma(13)),\\
7^3 = 343 \text{ y } 343 \equiv 5 \mod 13, &\text{ por lo que } (7,5) \in F(\Gamma(13)),\\
8^3 = 512 \text{ y } 512 \equiv 5 \mod 13, &\text{ por lo que } (8,5) \in F(\Gamma(13)),\\
9^3 = 729 \text{ y } 729 \equiv 1 \mod 13, &\text{ por lo que } (9,1) \in F(\Gamma(13)),\\
10^3 = 1000 \text{ y } 1000 \equiv 12 \mod 13, &\text{ por lo que } (10,12) \in F(\Gamma(13)),
\end{aligned}
$$

$11^3 = 1331$ y $1331 \equiv 5 \mod 13$, por lo que $(11, 5) \in F(\Gamma(13))$,
$12^3 = 1728$ y $1728 \equiv 12 \mod 13$, por lo que $(12, 12) \in F(\Gamma(13))$.

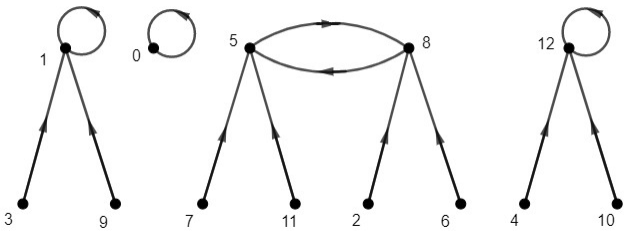

Figura 2.1: La digráfica $\Gamma(13)$.

En el ejemplo anterior podemos observar que todos los vértices tienen exgrado igual a 1, también podemos ver que los vértices $0, 1$ y 12 tienen un lazo. Demostraremos con los siguientes lemas, que esto no es una coincidencia y que por el contrario esta propiedad se conserva para cualquier $n \in \mathbb{N}$.

Lema 2.1.1. *Sea $\Gamma(n)$ una digráfica de congruencias cúbicas. Si n es un natural no nulo y $x \in V(\Gamma(n))$, entonces $d^+(x) = 1$.*

Demostración: Sea $x \in V(\Gamma(n))$. Como $\{[0], \ldots, [n-1]\}$ es una partición de $\mathbb{Z}$, entonces existe un único $l \in \{0, \ldots, n-1\}$ tal que $x^3 \in [l]$, es decir, $x^3 \equiv l \mod n$.

Por lo tanto, existe un único $l \in V(\Gamma(n))$ tal que $(x, l) \in F(\Gamma(n))$. Podemos concluir que $d^+(x) = 1$. □

La digráfica $\Gamma(n)$ suele tener lazos. En particular el siguiente lema nos demuestra que, para cualquier $n \geq 3$, existen al menos 3 vértices que siempre tienen lazo.

Sea $n \in \mathbb{N}$, diremos que n es **libre de cuadrados** si no existe $y \in \mathbb{Z}$ tal que $y^2 \mid n$.

Lema 2.1.2. *Sea $\Gamma(n)$ una digráfica de congruencias cúbicas. Los vértices 0, 1 y $n-1$ tienen un lazo en $\Gamma(n)$. Más aún, el vértice 0 es un vértice aislado con un lazo en $\Gamma(n)$ si y sólo si n es libre de cuadrados.*

Demostración: Es fácil ver que $0^3 \equiv 0 \mod n$, esto implica que $(0, 0) \in F(\Gamma(n))$, es decir el vértice 0 tiene un lazo. De igual manera $1^3 \equiv 1 \mod n$, por lo que $(1, 1) \in F(\Gamma(n))$, concluyendo que el vértice 1 tiene un lazo.

Demostremos ahora que $(n-1)^3 \equiv (n-1) \mod n$, esto es $(n-1)^3 - (n-1) = kn$ para algún $k \in \mathbb{Z}$.

Veamos que

$$\begin{aligned}(n-1)^3 - (n-1) &= n^3 - 3n^2 + 3n - 1 - n + 1 \\ &= n^3 - 3n^2 + 2n \\ &= n\left(n^2 - 3n + 2\right).\end{aligned}$$

De manera que $(n-1)^3 - (n-1) = kn$ para $k = \left(n^2 - 3n + 2\right)$, por lo que $(n-1)^3 \equiv (n-1) \mod n$. Concluyendo que el vértice $n-1$ tiene un lazo.

Por otro lado, falta demostrar que el vértice 0 es un vértice aislado con un lazo en $\Gamma(n)$ si y sólo si n es libre de cuadrados.

Demostraremos la condición suficiente por contradicción.

Supongamos que n no es libre de cuadrados, entonces existe un entero, en particular un primo p, tal que $p^2 \mid n$, es decir, $\frac{n}{p^2} \in \mathbb{N}$ y de igual manera $\frac{n}{p} \in \mathbb{N}$.

Así,

$$\left(\frac{n}{p}\right)^3 = n \cdot \frac{n}{p} \cdot \frac{n}{p^2} = na \qquad \text{para alguna } a \in \mathbb{Z},$$

por lo que $\left(\frac{n}{p}\right)^3 \equiv 0 \mod n$, es decir, $\left(\frac{n}{p}, 0\right) \in F(\Gamma(n))$. Notamos que lo anterior es una contradicción pues 0 es un vértice aislado, concluyendo que n es libre de cuadrados.

Ahora demostraremos la condición necesaria.

Supongamos que n es libre de cuadrados, es decir, $k^2 \nmid n$ para todo $k \in \{2, 3, \ldots, n-2\}$.

Como para todo $k \in \{2, 3, \ldots, n-2\}$, $k^2 \nmid n$, entonces $k^3 \nmid n$ pues si $k^3 \mid n$, implica que $n = k^3 u$ donde $u \in \mathbb{N}$, escribiéndolo de otra manera $n = k^2 \cdot k \cdot u$, por lo que $k^2 \mid n$, lo cual es una contradicción a la hipótesis. Además, vimos que el vértice $n-1$ tiene un lazo, de manera que $(n-1)^3 \not\equiv 0 \mod n$.

De lo anterior, $k^3 \not\equiv 0 \mod n$ para todo $k \in \{1, 2, \ldots, n-1\}$. Concluyendo que el vértice 0 es un vértice aislado con un lazo en $\Gamma(n)$. □

La digráfica $\Gamma(n)$ tiene un comportamiento espejo respecto al conjunto de vértices, es decir, la mitad de los vértices se comportan de la misma manera que la otra mitad, respecto a sus flechas. El siguiente lema nos enuncia esta y otras propiedades.

Lema 2.1.3. *Sea $\Gamma(n)$ una digráfica de congruencias cúbicas. Si n es un natural no nulo y $\{k, l\} \subseteq \{1, \ldots, n-1\}$, entonces lo siguiente se cumple:*

(*i*) $(k, 0) \in F(\Gamma(n))$ *si y sólo si* $(n-k, 0) \in F(\Gamma(n))$.

(*ii*) *Si $n = 2b$ para alguna $b \in \mathbb{N}$, entonces* $(k, b) \in F(\Gamma(n))$ *si y sólo si* $(n-k, b) \in F(\Gamma(n))$.

(*iii*) $(k, l) \in F(\Gamma(n))$ *si y sólo si* $(n-k, n-l) \in F(\Gamma(n))$.

(*iv*) $N(k) = \{k\}$ *si y sólo si* $N(n-k) = \{n-k\}$.

(*v*) *El vértice k pertenece a un t-ciclo aislado si y sólo si el vértice $n-k$ pertenece a algún t-ciclo aislado.*

Demostración:

(*i*) $(k, 0) \in F(\Gamma(n))$ si y sólo si $(n-k, 0) \in F(\Gamma(n))$. Demostraremos la condición suficiente. Sea $(k, 0) \in F(\Gamma(n))$, por definición de $\Gamma(n)$, $k^3 \equiv 0 \mod n$, o bien $k^3 = na$ para alguna $a \in \mathbb{N}$.

Por otro lado, notemos que

$$(n-k)^3 = n^3 - 3n^2k + 3nk^2 - k^3.$$

Dado que $k^3 = na$, entonces

$$(n-k)^3 = n^3 - 3n^2k + 3nk^2 - na.$$

Factorizando n, tenemos que $(n-k)^3 = n\left(n^2-3nk+3k^2-a\right)$, es decir, $(n-k)^3 \equiv 0 \mod n$. Concluyendo que $(n-k,0) \in F(\Gamma(n))$.

Ahora, demostremos la parte necesaria. Supongamos que $(n-k)^3 \equiv 0 \mod n$, es decir,

$$(n-k)^3 = nc \qquad \text{para alguna } c \in \mathbb{Z}. \tag{2.1}$$

Por otro lado, $(n-k)^3 = n^3 - 3n^2k + 3nk^2 - k^3$. Siguiendo de la Ecuación (2.1) que

$$n^3 - 3n^2k + 3nk^2 - k^3 = nc.$$

Despejando tenemos que

$$\begin{aligned} k^3 &= n^3 - 3n^2k + 3nk^2 - nc \\ &= n\left(n^2 - 3nk + 3k^2 - c\right), \end{aligned}$$

por lo que $k^3 = nb$, donde $b = n^2 - 3nk + 3k^2 - c$. Lo que implica que $k^3 \equiv 0 \mod n$. Concluyendo que $(k,0) \in F(\Gamma(n))$.

(ii) Si $n = 2b$ para alguna $b \in \mathbb{N}$, entonces $(k,b) \in F(\Gamma(n))$ si y sólo si $(n-k,b) \in F(\Gamma(n))$. Demostraremos la parte suficiente. Supongamos que $(k,b) \in F(\Gamma(n))$, por definición de $\Gamma(n)$, $k^3 \equiv b \mod n$, es decir,

$$k^3 - b = na \qquad \text{para alguna } a \in \mathbb{Z}. \tag{2.2}$$

Por otro lado,

$$(n-k)^3 - b = n^3 - 3n^2k + 3nk^2 - k^3 - b.$$

De la Ecuación (2.2), como $k^3 - b = na$, entonces $k^3 = na + b$, sustituyendo

$$n^3 - 3n^2k + 3nk^2 - k^3 - b = n^3 - 3n^2k + 3nk^2 - na - b - b.$$

De manera que $(n-k)^3 - b = n\left(n^2 - 3nk + 3k^2 - a - 1\right)$, es decir, $(n-k)^3 - b = na'$ para alguna $a' \in \mathbb{Z}$, por lo que $(n-k)^3 \equiv b \mod n$ y por definición de $\Gamma(n)$, $(n-k,b) \in F(\Gamma(n))$.

Ahora demostraremos la parte necesaria. Supongamos que $(n-k,b) \in F(\Gamma(n))$, por definición de $\Gamma(n)$, $(n-k)^3 \equiv b \mod n$, es decir,

$$(n-k)^3 - b = nc \qquad \text{para alguna } c \in \mathbb{Z}. \tag{2.3}$$

Por otro lado, $(n-k)^3 - b = n^3 - 3n^2k + 3nk^2 - k^3 - b$. Siguiendo de la Ecuación (2.3)

$$n^3 - 3n^2k + 3nk^2 - k^3 - b = nc.$$

Despejando

$$\begin{aligned} k^3 + b &= n^3 - 3n^2k + 3nk^2 - nc \\ &= n\left(n^2 - 3nk + 3k^2 - c\right). \end{aligned}$$

De manera que $\left(k^3+b\right) \equiv 0 \mod n$, o bien, $k^3 \equiv (-b) \mod n$. Notemos que como $n = 2b$, entonces $2b \equiv 0 \mod n$; ahora bien $2b = b-(-b)$, por lo que $b-(-b) \equiv 0 \mod n$, es decir, $b \equiv (-b) \mod n$.

Tenemos que, por la observación anterior, como $k^3 \equiv (-b) \mod n$ y $(-b) \equiv b \mod n$, entonces $k^3 \equiv b \mod n$. Concluyendo que $(k,b) \in F(\Gamma(n))$.

(iii) $(k,l) \in F(\Gamma(n))$ si y sólo si $(n-k, n-l) \in F(\Gamma(n))$. Primero demostraremos la parte suficiente. Supongamos que $(k,l) \in F(\Gamma(n))$, por definición de $\Gamma(n)$, se tiene que $k^3 \equiv l \mod n$, entonces

$$k^3 - l = na \qquad \text{para alguna } a \in \mathbb{Z}. \tag{2.4}$$

Por otro lado notemos que

$$\begin{aligned}(n-k)^3 - (n-l) &= n^3 - 3n^2k + 3nk^2 - k^3 - n + l \\ &= n^3 - 3n^2k + 3nk^2 - n - \left(k^3 - l\right).\end{aligned}$$

Dada la Ecuación (2.4)

$$n^3 - 3n^2k + 3nk^2 - n - \left(k^3 - l\right) = n^3 - 3n^2k + 3nk^2 - n - na.$$

Factorizando n, $(n-k)^3 - (n-l) = n\left(n^2 - 3nk + 3k^2 - 1 - a\right)$, por lo que, $(n-k)^3 \equiv (n-l) \mod n$. De manera que $(n-k, n-l) \in F(\Gamma(n))$.

Ahora demostraremos la parte necesaria. Supongamos que $(n-k, n-l) \in F(\Gamma(n))$, por definición de $\Gamma(n)$ se tiene que $(n-k)^3 \equiv (n-l) \mod n$, entonces

$$(n-k)^3 - (n-l) = nb \qquad \text{para alguna } b \in \mathbb{Z}. \tag{2.5}$$

Por otro lado $(n-k)^3 - (n-l) = n^3 - 3n^2k + 3nk^2 - k^3 - n + l$. Siguiendo de la Ecuación (2.5) que

$$n^3 - 3n^2k + 3nk^2 - k^3 - n + l = nb.$$

Despejando tenemos que

$$\begin{aligned}k^3 - l &= n^3 - 3n^2k + 3nk^2 - n - nb \\ &= n\left(n^2 - 3nk + 3k^2 - 1 - b\right).\end{aligned}$$

De este modo, $k^3 - l = nb'$ donde $b' = n^2 - 3nk + 3k^2 - 1 - b$, por lo que $k^3 \equiv l \mod n$. Concluyendo que $(k,l) \in F(\Gamma(n))$.

(iv) $N(k) = \{k\}$ si y sólo si $N(n-k) = \{n-k\}$. Para demostrar la parte suficiente basta ver que

a) Si $(n-k, a) \in F(\Gamma(n))$, entonces $a = n-k$.

Supongamos que $(n-k, a) \in F(\Gamma(n))$, entonces por el inciso *(iii)* tenemos que $(n-(n-k), n-a) \in F(\Gamma(n))$, esto es, $(k, n-a) \in F(\Gamma(n))$ y como $N(k) = \{k\}$, entonces $n-a = k$. Concluyendo que $a = n-k$. Por lo tanto, $N^+(n-k) = \{n-k\}$.

b) Si $(b, n-k) \in F(\Gamma(n))$, entonces $b = n-k$.

Supongamos que $(b, n-k) \in F(\Gamma(n))$, entonces por el inciso (iii) tenemos que $(n-b, n-(n-k)) \in F(\Gamma(n))$, esto es, $(n-b, k) \in F(\Gamma(n))$ y como $N(k) = \{k\}$, entonces $n-b = k$. Concluyendo que $b = n-k$. De esta manera, $N^-(n-k) = \{n-k\}$.

Por lo tanto, $N(n-k) = \{n-k\}$.

Para demostrar la parte necesaria basta ver que

(c) Si $(k, a) \in F(\Gamma(n))$, entonces $a = k$.

Supongamos que $(k, a) \in F(\Gamma(n))$, entonces por el inciso (iii) tenemos que $(n-k, n-a) \in F(\Gamma(n))$ y como $N(n-k) = \{n-k\}$, entonces $n-a = n-k$. Concluyendo que $a = k$. Por lo tanto, $N^+(k) = \{k\}$.

(d) Si $(b, k) \in F(\Gamma(n))$, entonces $b = k$.

Supongamos que $(b, k) \in F(\Gamma(n))$, entonces por el inciso (iii) tenemos que $(n-b, n-k) \in F(\Gamma(n))$ y como $N(n-k) = \{n-k\}$, entonces $n-b = n-k$. Concluyendo que $b = k$. De este modo, $N^-(k) = \{k\}$.

Por lo tanto, $N(k) = \{k\}$.

(v) El vértice k pertenece a un t-ciclo aislado si y sólo si el vértice $n-k$ pertenece a algún t-ciclo aislado. Demostraremos la parte suficiente. Supongamos que existe un ciclo aislado $\gamma_1 = (\alpha_1, \alpha_2, \ldots, \alpha_t, \alpha_1)$ tal que $\alpha_i = k$ para alguna $i \in \{1, \ldots, t\}$. Por el inciso (iii), $\gamma_2 = (n-\alpha_1, n-\alpha_2, \ldots, n-\alpha_t, n-\alpha_1)$ es un ciclo en $\Gamma(n)$; además, $n-\alpha_i = n-k$ para alguna $i \in \{1, \ldots, t\}$.

Veamos que γ_2 también es un ciclo aislado.

Supongamos, por contradicción, que el ciclo γ_2 no es aislado, entonces existe $(\alpha_s, n-\alpha_r) \in F(\Gamma(n))$ con $s \notin \{1, \ldots, t\}$ y $r \in \{1, \ldots, t\}$. Por el inciso (iii), $(n-\alpha_s, n-(n-\alpha_r)) \in F(\Gamma(n))$, es decir, $(n-\alpha_s, \alpha_r) \in F(\Gamma(n))$, lo cual es una contradicción, pues $\alpha_r \in V(\gamma_1)$ y γ_1 es un ciclo aislado. Por lo tanto, γ_2 es un ciclo aislado.

Ahora demostraremos la parte necesaria. Supongamos que existe un ciclo aislado $\gamma_3 = (\beta_1, \beta_2, \ldots, \beta_r, \beta_1)$ tal que $\beta_i = n-k$ para alguna $i \in \{1, \ldots, r\}$. De manera que, por el inciso (iii), $\gamma_4 = (n-\beta_1, n-\beta_2, \ldots, n-\beta_r, n-\beta_1)$ es un ciclo en $\Gamma(n)$ y $n-\beta_i = n-(n-k)$ para alguna $i \in \{1, \ldots, r\}$, esto es, $n-\beta_i = k$.

Veamos que γ_4 es un ciclo aislado.

Supongamos, por contradicción, que el ciclo γ_4 no es aislado, entonces existe $(\beta_s, n-\beta_l) \in F(\Gamma(n))$ con $s \notin \{1, \ldots, r\}$ y $l \in \{1, \ldots, r\}$. Por el inciso (iii), $(n-\beta_s, n-(n-\beta_l)) \in F(\Gamma(n))$, es decir, $(n-\beta_s, \beta_l) \in F(\Gamma(n))$, lo cual es una contradicción, pues $\beta_l \in V(\gamma_3)$ y γ_3 es un ciclo aislado. Por lo tanto, γ_4 es un ciclo aislado.

□

Definamos dos subdigráficas de $\Gamma(n)$. Sean $\Gamma_1(n)$ la subdigráfica de $\Gamma(n)$ inducida por el conjunto de vértices que son primos relativos con n y $\Gamma_2(n)$ la subdigráfica $\Gamma(n)$ inducida por los vértices que no son primos relativos con n. Veremos que una de las peculiaridades de estas dos subdigráficas es que son ajenas, es decir no comparten vértices ni flechas.

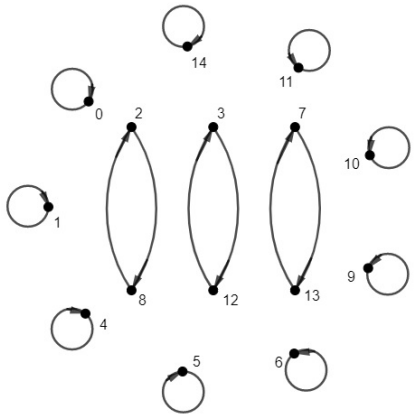

Figura 2.2: Digráfica $\Gamma(15)$.

Notemos que el conjunto de vértices $\{1, 2, 4, 7, 8, 11, 13, 14\}$ en la Figura 2.2 es el conjunto de vértices de la subdigráfica $\Gamma_1(15)$, mientras que el conjunto de vértices $\{0, 3, 5, 6, 9, 10, 12\}$ es el conjunto de vértices de la subdigráfica $\Gamma_2(15)$. Es claro que 0 siempre es un vértice de $\Gamma_2(n)$ y para $n > 1$ los números 1 y $n - 1$ están en $\Gamma_1(n)$.

Lema 2.1.4. *Sean $\Gamma(n)$ una digráfica de congruencias cúbicas, $n \geq 2$ y $\{x, z\} \subseteq V(\Gamma(n))$ tales que $(x, z) \in F(\Gamma(n))$. x y n son primos relativos si y sólo si z y n son primos relativos.*

Demostración: Demostremos la parte suficiente. Supongamos que $(x; n) = 1$ y veamos que $(z; n) = 1$.

Como $(x, z) \in F(\Gamma(n))$, tenemos que $x^3 = na + z$ para alguna $a \in \mathbb{Z}$ y, supongamos por contradicción que $(z; n) \neq 1$. Sea $(z; n) = d$ para algún $d \in \mathbb{Z}$ y sea p un primo tal que $d = pt$ para algún $t \in \mathbb{Z}$, de esta manera, $p \mid z$ y $p \mid n$, por lo que por el Teorema 1.1.10, $p \mid na + z$, es decir, $p \mid x^3$ y como p es un primo, entonces $p \mid x$, de modo que p es un divisor común de x y n. Esto es una contradicción, pues por hipótesis $(x; n) = 1$. Por lo tanto, $(z; n) = 1$.

Ahora demostremos la parte necesaria. Supongamos que $(z; n) = 1$ y veamos que $(x; n) = 1$.

Como $(x, z) \in F(\Gamma(n))$, tenemos que $z = x^3 - na$ para alguna $a \in \mathbb{Z}$ y, procediendo por contradicción, supongamos que $(x; n) \neq 1$. Sea $(x; n) = d$ para algún $d \in \mathbb{Z}$ y sea p un primo tal que $d = pt$ para algún $t \in \mathbb{Z}$, de esta manera, $p \mid x$ y $p \mid n$, por lo que por el Teorema 1.1.10, $p \mid x^3 - na$, es decir, $p \mid z$, de modo que p es un divisor común de z y n. Esto es una contradicción, pues por hipótesis $(z; n) = 1$. Por lo tanto, $(x; n) = 1$. □

Observación 2.1.5. *Sean $\Gamma(n)$ una digráfica de congruencias cúbicas, $n \geq 2$ y $\{x, z\} \subseteq V(\Gamma(n))$ tales que $(x, z) \in F(\Gamma(n))$. x y n no son primos relativos si y sólo si z y n no son primos relativos.*

Demostración: Se sigue inmediatamente del lema anterior. □

Proposición 2.1.6. *Sea $\Gamma(n)$ una digráfica de congruencias cúbicas. Si $n \geq 2$, entonces $V(\Gamma_1(n)) \cap V(\Gamma_2(n)) = \emptyset$ y $\Gamma(n) = \Gamma_1(n) \cup \Gamma_2(n)$.*

Demostración: Demostremos primero que $V(\Gamma_1(n)) \cap V(\Gamma_2(n)) = \emptyset$ por contradicción.

Supongamos que existe $l \in V(\Gamma_1(n)) \cap V(\Gamma_2(n))$. Como $l \in V(\Gamma_1(n))$, tenemos que $(n; l) = 1$ y como $l \in V(\Gamma_2(n))$, tenemos que $(n; l) = d$ para alguna $d \neq 1$, lo cual es una contradicción. Por lo tanto, $V(\Gamma_1(n)) \cap V(\Gamma_2(n)) = \emptyset$.

Para ver que $\Gamma(n) = \Gamma_1(n) \cup \Gamma_2(n)$ bastará demostrar que ambas digráficas coinciden en su conjunto de vértices y en su conjunto de flechas, respectivamente.

Tenemos que ver que $V(\Gamma(n)) = V(\Gamma_1(n) \cup \Gamma_2(n))$.

Sea $k \in V(\Gamma(n))$, entonces podemos ver que k es primo relativo con n o k no es primo relativo con n, es decir, $k \in V(\Gamma_1(n))$ o $k \in V(\Gamma_2(n))$. De manera que $k \in V(\Gamma_1(n) \cup \Gamma_2(n))$. Como k es un vértice cualquiera de $\Gamma(n)$, entonces podemos concluir que $V(\Gamma(n)) \subseteq V(\Gamma_1(n) \cup \Gamma_2(n))$.

Sea $l \in V(\Gamma_1(n) \cup \Gamma_2(n))$, entonces $l \in V(\Gamma_1(n))$ o $l \in V(\Gamma_2(n))$. Por la definición de $\Gamma_1(n)$ y $\Gamma_2(n)$ tenemos que $l \in V(\Gamma(n))$. Por lo que, $V(\Gamma_1(n) \cup \Gamma_2(n)) \subseteq V(\Gamma(n))$. Podemos concluir que $V(\Gamma(n)) = V(\Gamma_1(n) \cup \Gamma_2(n))$.

Por otro lado, veamos que $F(\Gamma(n)) = F(\Gamma_1(n) \cup \Gamma_2(n))$.

Sea $(u, v) \in F(\Gamma_1(n) \cup \Gamma_2(n))$, entonces $(u, v) \in F(\Gamma_1(n))$ o $(u, v) \in F(\Gamma_2(n))$. Por definición de ambas subdigráficas $(u, v) \in F(\Gamma(n))$. De esta manera $F(\Gamma_1(n) \cup \Gamma_2(n)) \subseteq F(\Gamma(n))$.

Ahora, sea $(u, v) \in F(\Gamma(n))$.

Caso 1: $(u; n) = 1$.

Por el Lema 2.1.4, $(v; n) = 1$, por lo que $\{u, v\} \subseteq V(\Gamma_1(n))$ y como $\Gamma_1(n)$ es una subdigráfica inducida, entonces $(u, v) \in F(\Gamma_1(n))$.

Caso 2: $(u; n) \neq 1$.

Por la Observación 2.1.5, $(v; n) \neq 1$, por lo que $\{u, v\} \subseteq V(\Gamma_2(n))$ y como $\Gamma_2(n)$ es una subdigráfica inducida, entonces $(u, v) \in F(\Gamma_2(n))$.

Dados ambos casos tenemos que $F(\Gamma(n)) \subseteq F(\Gamma_1(n) \cup \Gamma_2(n))$. Podemos concluir que $F(\Gamma(n)) = F(\Gamma_1(n) \cup \Gamma_2(n))$.

Por lo tanto, $\Gamma(n) = \Gamma_1(n) \cup \Gamma_2(n)$. □

2.2. Caminos dirigidos en $\Gamma(n)$

En esta sección presentaremos resultados relacionados con caminos dirigidos, trayectorias dirigidas y ciclos dirigidos dentro de la digráfica $\Gamma(n)$.

El siguiente lema nos demostrará la existencia de un ciclo en la digráfica $\Gamma(n)$, esto únicamente a través de la definición que se tiene para la construcción de la misma.

Lema 2.2.1. *Sean $\Gamma(n)$ una digráfica de congruencias cúbicas, $a_1, a_2, \ldots, a_t$ vértices distintos en $\Gamma(n)$ y $C = (a_1, a_2, \ldots, a_t, a_1)$ una sucesión de vértices. C es un ciclo dirigido de longitud t en $\Gamma(n)$ si y sólo si*

$$\begin{aligned} a_1^3 &\equiv a_2 \mod n, \\ a_2^3 &\equiv a_3 \mod n, \\ &\vdots \\ a_t^3 &\equiv a_1 \mod n. \end{aligned}$$

Demostración: Demostraremos la parte suficiente. Como $(a_1, a_2) \in F(\Gamma(n))$, entonces $a_1^3 \equiv a_2 \mod n$. De igual modo, como $(a_2, a_3) \in F(\Gamma(n))$, entonces $a_2^3 \equiv a_3 \mod n$. De esta manera, como para cada $i \in \{1, \ldots, t-1\}$, $(a_i, a_{i+1}) \in F(\Gamma(n))$, entonces $a_i^3 \equiv a_{i+1} \mod n$. Además, $(a_t, a_1) \in F(\Gamma(n))$, por lo que $a_t^3 \equiv a_1 \mod n$.

Por lo tanto, podemos concluir que un ciclo dirigido determina la secuencia de congruencias dada.

Ahora demostraremos la parte necesaria.

Como $a_1^3 \equiv a_2 \mod n$, entonces $(a_1, a_2) \in F(\Gamma(n))$. De igual modo, como $a_2^3 \equiv a_3 \mod n$, entonces $(a_2, a_3) \in F(\Gamma(n))$. En general tenemos que como $a_i^3 \equiv a_{i+1} \mod n$ con $i \in \{1, \ldots, t-1\}$, entonces $(a_i, a_{i+1}) \in F(\Gamma(n))$. De igual manera, como $a_t^3 \equiv a_1 \mod n$, entonces $(a_t, a_1) \in F(\Gamma(n))$, por lo que tenemos el ciclo dirigido $(a_1, a_2, \ldots, a_t, a_1)$. □

Por ejemplo, la digráfica $\Gamma(11)$ mostrada en la Figura 2.3 contiene dos 4-ciclos y tres lazos.

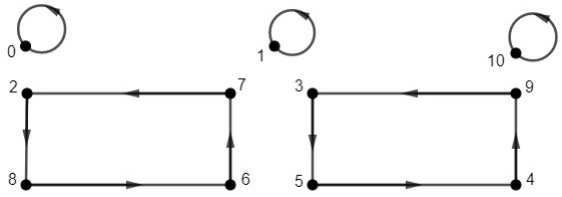

Figura 2.3: La digráfica $\Gamma(11)$.

Sea D una digráfica. Diremos que D es una **digráfica de componentes espejo** si existe una bipartición de sus componentes conexas, digamos $\{\mathscr{B}, \mathscr{D}\}$ y una función biyectiva $f : \mathscr{B} \to \mathscr{D}$ tal que para toda $H \in \mathscr{B}$, $f(H) \cong H$.

Por ejemplo, en la Figura 2.4 podemos ver que $\Gamma(14)$ es una digráfica de componentes espejo. Si $\mathscr{B} = \{H_1, H_2, H_3\}$ y $\mathscr{D} = \{H_4, H_5, H_6\}$, entonces la función $f : \mathscr{B} \to \mathscr{D}$, dada por $f(H_1) = H_4$, $f(H_2) = H_5$ y $f(H_3) = H_6$, satisface que para toda $H \in \mathscr{B}$, $f(H) \cong H$.

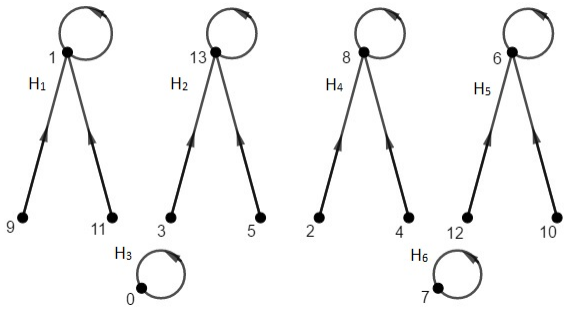

Figura 2.4: La digráfica $\Gamma(14)$.

Cabe mencionar que no todos los valores de n cumplen que $\Gamma(n)$ sea una digráfica de componentes espejo, tal es el caso de la digráfica $\Gamma(11)$ en la Figura 2.3, que al tener 5 componentes conexas no existe una bipartición de éstas, que nos genere una función biyectiva.

Proposición 2.2.2. *Sea $\Gamma(n)$ una digráfica de congruencias cúbicas. Toda componente conexa de $\Gamma(n)$ tiene exactamente un ciclo dirigido.*

Demostración: Demostremos primero que cada componente conexa tiene al menos un ciclo dirigido.

Sea H una componente conexa de $\Gamma(n)$. Por el Lema 2.1.1, para todo $v \in V(H)$, $d^+(v) = 1$, entonces por el Lema 1.2.3, H tiene al menos un ciclo dirigido.

Ahora veremos por contradicción que las componentes conexas tienen un único ciclo dirigido.

Supongamos que existen al menos dos ciclos dirigidos distintos en la componente H, digamos $C = (\alpha_1, \ldots, \alpha_r, \alpha_1)$ y $C' = (\beta_1, \ldots, \beta_t, \beta_1)$.

Entonces tenemos dos casos:

Caso 1: $V(C) \cap V(C') \neq \emptyset$.

Sea $\alpha_i \in V(C) \cap V(C')$ y supongamos que $\alpha_i = \beta_j$ para algún $j \in \{1, \ldots, t\}$, tal que $\alpha_{i+1} \notin V(C')$ y $\beta_{j+1} \notin V(C)$, como $\alpha_i \in V(H)$ y cada ciclo es dirigido, $d^+(\alpha_i) \geq 2$ lo cual, por el Lema 2.1.1, contradice el hecho de que $d^+(a) = 1$ para todo $a \in V(\Gamma(n))$.

Caso 2: $V(C) \cap V(C') = \emptyset$.

Como H es una componente conexa, entonces existe un $\alpha_i\beta_j$-camino no necesariamente dirigido, digamos $C_1 = (\alpha_i = x_0, x_1, \ldots, x_{r-1}, x_r = \beta_j)$ tal que $\alpha_i \in V(C)$ y $\beta_j \in V(C')$, es decir $V(C_1) \cap V(C) = \{\alpha_i\}$ y $V(C_1) \cap V(C') = \{\beta_j\}$.

Si $(\alpha_i, x_1) \in F(C_1)$, entonces $d^+(\alpha_i) \geq 2$ lo cual, por el Lema 2.1.1, es una contradicción. Esto quiere decir que $(x_1, \alpha_i) \in F(C_1)$.

Además, si $(\beta_j, x_{r-1}) \in F(C_1)$, entonces $d^+(\beta_j) \geq 2$ lo cual, por el Lema 2.1.1, es una contradicción, por lo que $(x_{r-1}, \beta_j) \in F(C_1)$.

De esta manera, definimos $\tau = \min\{i \in\{0, \ldots, r-1\}: (x_i, x_{i+1}) \in F(C_1)\}$.

Podemos ver que, por lo observado anteriormente, si $i = r-1$, $(x_{r-1}, x_r) \in F(C_1)$, entonces el conjunto $\{i \in\{0, \ldots, r-1\}: (x_i, x_{i+1}) \in F(C_1)\}$ es no vacío. Por otro lado, si $i = 0$, $(x_0, x_1) \notin F(C_1)$, entonces $\tau \geq 1$.

De manera que $(x_\tau, x_{\tau+1}) \in F(C_1)$ y como τ es mínimo, $(x_{\tau-1}, x_\tau) \notin F(C_1)$, por lo que $(x_\tau, x_{\tau-1}) \in F(C_1)$. Esto implica que $d^+(x_\tau) \geq 2$, lo cual, por el Lema 2.1.1, es una contradicción.

Dado que en ambos casos se llega a una contradicción, podemos concluir que C y C' son el mismo. Por lo tanto, H tiene un único ciclo dirigido. □

Corolario 2.2.3. *Sea $\Gamma(n)$ una digráfica de congruencias cúbicas. El número de componentes conexas de $\Gamma(n)$ es igual al número de ciclos dirigidos.*

Demostración: Sean

$$\mathscr{C} = \{C : C \text{ es un ciclo dirigido en } \Gamma(n)\} \text{ y}$$
$$\mathscr{H} = \{H : H \text{ es una componente conexa de } \Gamma(n)\}.$$

Consideremos la relación f de $\mathscr{H}$ en $\mathscr{C}$ dada por $(H, C) \in f$ si y sólo si C es un ciclo dirigido de H.

Veamos primero que f es una función.

Sea H una componente conexa cualquiera de $\mathscr{H}$, sabemos que cada componente conexa tiene un ciclo dirigido, por lo que existe $C \in \mathscr{C}$ tal que $(H, C) \in f$. Por lo anterior, $Dom(f) = \mathscr{C}$.

Por otro lado, sean $(H_1, C_1) \in f$, $(H_2, C_2) \in f$ y $H_1 = H_2$, demostremos que $C_1 = C_2$.

Vimos en la proposición anterior que cada componente tiene un único ciclo dirigido, por lo que si C_1 es un ciclo dirigido de H_1 y C_2 es un ciclo dirigido de H_2 y $H_1 = H_2$, entonces $C_1 = C_2$. Por lo tanto, la relación f es una función.

Ahora, demostraremos que f es inyectiva. Sean H y H' dos componentes conexas de $\Gamma(n)$ tales que $f(H) = f(H')$, veamos que $H = H'$. Sea $f(H) = C$, como $f(H) = f(H')$, entonces C es un ciclo dirigido de H y C es un ciclo dirigido de H'. Dada la definición de componente conexa, C no puede pertenecer a dos componentes distintas, de manera que $H = H'$. Por lo tanto, f es una función inyectiva.

Por último, demostraremos que f es una función suprayectiva. Sea $C \in \mathscr{C}$ un ciclo dirigido de alguna componente conexa de $\Gamma(n)$. Sabemos que $C \in H$ para alguna componente conexa $H \in \mathscr{H}$ y $C = f(H)$. Por lo tanto, f es suprayectiva.

Dado lo anterior, f es una función biyectiva y podemos concluir que el número de componentes conexas de la digráfica es igual al número de ciclos dirigidos de $\Gamma(n)$. □

Lema 2.2.4. *Sea $\Gamma(n)$ una digráfica de congruencias cúbicas. Si $(\alpha_0, \alpha_1, \ldots, \alpha_r)$ es una trayectoria dirigida de longitud r en $\Gamma(n)$, entonces $\alpha_0^{3^r} \equiv \alpha_r \mod n$.*

Demostración: Demostraremos por inducción sobre r que $(\alpha_0^{3^r}) \equiv \alpha_r \mod n$.

Base de inducción. Para $r = 1$, $\alpha_0^3 \equiv \alpha_1 \mod n$, lo cual es cierto, pues $(\alpha_0, \alpha_1) \in F(\Gamma(n))$.

Hipótesis de inducción. Si $(\alpha_0, \alpha_1, \ldots, \alpha_{r-1})$ es una trayectoria dirigida de longitud $r-1$, entonces $(\alpha_0^{3^{r-1}}) \equiv \alpha_{r-1} \mod n$.

Paso inductivo. Si $T = (\alpha_0, \alpha_1, \ldots, \alpha_r)$ es una trayectoria dirigida de longitud r, entonces $(\alpha_0^{3^r}) \equiv \alpha_r \mod n$.

Consideremos $T' = (\alpha_0, \alpha_1, \ldots, \alpha_{r-1})$ una subtrayectoria dirigida de T, entonces por hipótesis de inducción $(\alpha_0^{3^{r-1}}) \equiv \alpha_{r-1} \mod n$. Además, como $(\alpha_{r-1}, \alpha_r) \in F(\Gamma(n))$, tenemos que $\alpha_{r-1}^3 \equiv \alpha_r \mod n$, entonces $(\alpha_0^{3^{r-1}})^3 \equiv \alpha_r \mod n$, es decir, $\alpha_0^{3^r} \equiv \alpha_r \mod n$. □

Corolario 2.2.5. *Sea $\Gamma(n)$ una digráfica de congruencias cúbicas. Si $C = (\alpha_0, \alpha_1, \ldots, \alpha_r, \alpha_0)$ es un ciclo dirigido de $\Gamma(n)$, entonces $\alpha_0^{3^{r+1}} \equiv \alpha_0 \mod n$.*

Demostración: Como C es un ciclo dirigido de $\Gamma(n)$, consideremos la trayectoria dirigida $T = (\alpha_0, \alpha_1, \ldots, \alpha_r)$. Por el lema anterior, tenemos que $\alpha_0^{3^r} \equiv \alpha_r \mod n$ y sabemos que $\alpha_r^3 \equiv \alpha_0 \mod n$, entonces $(\alpha_0^{3^r})^3 \equiv \alpha_0 \mod n$, es decir, $\alpha_0^{3^{r+1}} \equiv \alpha_0 \mod n$. □

Lema 2.2.6. *Sean $\Gamma(n)$ una digráfica de congruencias cúbicas y $\{l, n\} \subseteq \mathbb{N}$ tal que $1 < l \leq n-1$. Si $s \leq \text{máx}\{r \in \mathbb{N} : l^{3^r} < n\}$, entonces existe una s-trayectoria dirigida cuyo vértice inicial es l.*

Demostración: Notemos que para cada $r \in \{t \in \mathbb{N} : l^{3^t} < n\}$, $(l^{3^r}, l^{3^{r+1}}) \in F(\Gamma(n))$, pues $(l^{3^r})^3 \equiv l^{3^{r+1}} \mod n$. De modo que podemos formar un camino dirigido con vértice inicial l de la siguiente manera:
$T = (l, l^3, l^{3^2}, \ldots, l^{3^r})$. Además, como $l > 1$, entonces para cada $\{t_1, t_2\} \subseteq \{t \in \mathbb{N} : l^{3^t} < n\}$, si $t_1 \neq t_2$, entonces $l^{3^{t_1}} \neq l^{3^{t_2}}$, concluyendo que T es una trayectoria dirigida.

Dada la definición de s, podemos ver que $l^{3^s} \leq n$; de manera que si $r = s$, entonces T es una s-trayectoria dirigida con vértice inicial l. □

Lema 2.2.7. *Sea $\Gamma(n)$ una digráfica de congruencias cúbicas. Si $\{n, k, t\} \subseteq \mathbb{N}$ es tal que $k^{3^{t-1}} \leq n$, entonces $n \mid k^{3^t} - k$ si y sólo si $\Gamma(n)$ tiene un t-ciclo dirigido que contiene a k.*

Demostración: Demostraremos la condición suficiente.

Como $n \mid k^{3^t} - k$, entonces $k^{3^t} \equiv k \mod n$, de modo que $(k^{3^{t-1}}, k) \in F(\Gamma(n))$.

Por otro lado, por el lema anterior tenemos que existe una trayectoria dirigida de longitud $t-1$ con vértice inicial k, digamos T. De esta manera, podemos definir $\gamma = T \cup (k^{3^{t-1}}, k)$ como un ciclo dirigido de longitud t que contiene al vértice k.

Demostraremos la condición necesaria.

Sea $C = (\alpha_0, \alpha_1, \ldots, \alpha_{t-1}, \alpha_0)$ un t-ciclo dirigido de $\Gamma(n)$ tal que, sin pérdida de generalidad, $\alpha_0 = k$, por el Corolario 2.2.5 tenemos que $n \mid \alpha_0^{3^t} - \alpha_0$. □

Como ejemplo del resultado anterior, $\Gamma(n)$ tiene un 3-ciclo dirigido que contiene al vértice 2 si y sólo si

$$n \mid 2^{3^3} - 2 = 2 \cdot (2^{13} - 1) \cdot (2^{13} + 1).$$

Sea $n = 2^{13} - 1 = 8191$. Entonces hay un 3-ciclo dirigido que contiene al vértice 2 en la digráfica $\Gamma(8191)$.

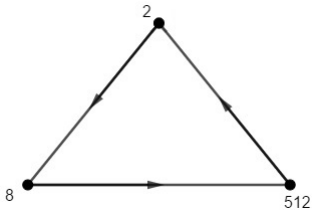

Figura 2.5: El 3-ciclo de la digráfica $\Gamma(n)$ con $n = 2^{13} - 1 = 8191$.

En general, tenemos que si $k \geq 2$, la digráfica $\Gamma(k^{3^t} - k)$ tiene un t-ciclo dirigido que contiene al vértice k.

Lema 2.2.8. *Sea $\Gamma(n)$ una digráfica de congruencias cúbicas y $\{\alpha_1, \alpha_2, \ldots, \alpha_k\} \subseteq \{0, \ldots, n-1\}$. Definimos:*

$$D_1 = \Gamma(n)\langle\{\alpha_1, \alpha_2, \ldots, \alpha_k\}\rangle \text{ y } D_2 = \Gamma(n)\langle\{n - \alpha_1, n - \alpha_2, \ldots, n - \alpha_k\}\rangle$$

entonces la función $\varphi : V(D_1) \to V(D_2)$ con regla de correspondencia $\varphi(\alpha_i) = n - \alpha_i$ es un isomorfismo.

Demostración: Notemos que por la definición de φ, ésta es biyectiva, por lo que resta demostrar que preserva adyacencias. Sea (α_r, α_s) alguna flecha de D_1, con $\{r, s\} \subseteq \{1, \ldots, k\}$.

Sabemos por el inciso (iii) del Lema 2.1.3 que $(n - \alpha_r, n - \alpha_s) \in F(\Gamma(n))$, además, $\{n - \alpha_r, n - \alpha_s\} \subseteq V(D_2)$, de manera que $(n - \alpha_r, n - \alpha_s) \in F(D_2)$, es decir, $(\varphi(a_r), \varphi(a_s)) \in F(D_2)$.

Análogamente, sea $(n - \alpha_r, n - \alpha_s)$ alguna flecha de D_2, con $\{r, s\} \subseteq \{1, \ldots, k\}$, por el inciso (iii) del Lema 2.1.3, $(\alpha_r, \alpha_s) \in F(\Gamma(n))$ y como $\{\alpha_r, \alpha_s\} \subseteq V(D_1)$, entonces $(\alpha_r, \alpha_s) \in F(D_1)$.

Dado lo anterior podemos concluir que $D_1 \cong D_2$. □

Corolario 2.2.9. *Sea $\Gamma(n)$ una digráfica de congruencias cúbicas y $k \in V(\Gamma(n))$. Si H es la componente conexa tal que $k \in V(H)$ y H' es la componente conexa tal que $n - k \in V(H')$, entonces $H \cong H'$.*

Demostración: Sea H la componente conexa tal que $k \in V(H)$. Supongamos que $V(H) = \{\alpha_1, \ldots, \alpha_r\}$. Por el lema anterior sabemos que $D = \Gamma(n)\langle\{n - \alpha_1, n - \alpha_2, \ldots, n - \alpha_r\}\rangle$ es isomorfa a H y D contiene al vértice $n - k$. Demostraremos que D es una componente conexa.

Dado que H es conexa, entonces D es conexa. Solo falta demostrar que D es conexa maximal. Procediendo por contradicción, supongamos que D' es conexa y D es una subdigráfica propia de D'. Si $V(D') = \{\beta_1, \ldots, \beta_t\}$, entonces $H_0 = \Gamma(n)\langle\{n - \beta_1, n - \beta_2, \ldots, n - \beta_t\}\rangle$ es isomorfa a D', por lo que H_0 es una subdigráfica conexa y H es una subdigráfica propia de H_0, lo cual no es posible, pues H es una componente conexa. Por lo tanto, $D = H'$ y en particular $H \cong H'$. □

Corolario 2.2.10. *Sean $\Gamma(n)$ una digráfica de congruencias cúbicas y $k \in \left\{\left\lceil \frac{n}{2} \right\rceil, \ldots, n\right\}$. Si H es la componente conexa de $\Gamma(n)$ tal que $k \in V(H)$ y H' es la componente conexa de $\Gamma(n)$ tal que $n-k \in V(H')$, entonces $H \cong H'$.*

Demostración: Notemos que si $k \in \left\{\left\lceil \frac{n}{2} \right\rceil, \ldots, n\right\}$, entonces $n-k \in \left\{1, \ldots, \left\lfloor \frac{n}{2} \right\rfloor\right\}$. Por el corolario anterior tenemos que $H \cong H'$. □

Lema 2.2.11. *Sea $\Gamma(n)$ una digráfica de congruencias cúbicas. Cada componente conexa de $\Gamma(n)$ es un ciclo dirigido si y sólo si para cada k tal que $2 \leq k \leq \left\lfloor \frac{1}{2}n \right\rfloor$, existe $t \geq 1$ que satisface que $k^{3^t} \equiv k \mod n$.*

Demostración: Demostraremos la parte suficiente. Sean $\alpha_1 \in \left\{2, \ldots, \left\lfloor \frac{1}{2}n \right\rfloor\right\}$ y H la componente conexa de $\Gamma(n)$ que contiene al vértice α_1. Por hipótesis H es un ciclo dirigido, digamos $\gamma = (\alpha_1, \alpha_2, \ldots, \alpha_r, \alpha_1)$.

Como γ es un ciclo dirigido, entonces por el Corolario 2.2.5 tenemos que $n \mid \alpha_1^{3^r} - \alpha_1$, esto es, $\alpha_1^{3^r} \equiv \alpha_1 \mod n$.

Notemos que r es la longitud del ciclo dirigido y la mínima longitud que puede tener un ciclo dirigido es 1, pues tomamos a los lazos como ciclos dirigidos de longitud 1, por lo que $r \geq 1$, lo cual cumple con las condiciones del lema. Por lo tanto, para toda k tal que $2 \leq k \leq \left\lfloor \frac{1}{2}n \right\rfloor$, existe $t \geq 1$, que satisface que $k^{3^t} \equiv k \mod n$.

Ahora demostraremos la parte necesaria. Primero veremos que todo vértice en $\Gamma(n)$ está en un ciclo dirigido. Notemos que como $k^{3^t} \equiv k \mod n$, entonces $n \mid k^{3^t} - k$; además, $(k^{3^{t-1}}, k) \in F(\Gamma(n))$, entonces $\Gamma(n)$ tiene un camino dirigido cerrado, digamos $C = (k, k^3, k^{3^2}, \ldots, k^{3^{t-1}}, k)$. Sabemos que todo camino dirigido cerrado contiene al menos un ciclo dirigido, digamos γ; si $V(C) \neq V(\gamma)$, entonces existe $x \in V(C) \cap V(\gamma)$ tal que $d^+(x) \geq 2$, lo cual es una contradicción, pues sabemos que para todo $v \in \Gamma(n)$, $d^+(v) = 1$, por lo que $V(C) = V(\gamma)$, de manera que C es un ciclo dirigido de longitud t que tiene al vértice k.

Por otro lado, como $(k^{3^{t-1}}, k) \in F(\Gamma(n))$ para cada $k \in \left\{2, \ldots, \left\lfloor \frac{1}{2}n \right\rfloor\right\}$, entonces cada $k \in \left\{2, \ldots, \left\lfloor \frac{1}{2}n \right\rfloor\right\}$ tiene un invecino.

Supongamos ahora que existe una componente conexa de $\Gamma(n)$, digamos H, tal que no es un ciclo dirigido y sea k un vértice de H. Por el Corolario 2.2.10 podemos suponer que $k \in \left\{2, \ldots, \left\lfloor \frac{1}{2}n \right\rfloor\right\}$ y por lo visto anteriormente k está en un ciclo dirigido, digamos γ. Notemos que γ es un ciclo de H.

Como H no es un ciclo dirigido, entonces $V(H) \neq V(\gamma)$ o $F(H) \neq F(\gamma)$.

Supongamos primero que $V(H) \neq V(\gamma)$. Podemos ver que si $x \in V(\gamma)$ y $z \in V(H) \setminus V(\gamma)$, entonces $(x, z) \notin F(\Gamma(n))$, pues en $\Gamma(n)$ todos los vértices tienen exgrado 1. Además, como $V(H) \neq V(\gamma)$ y H es conexa, entonces existe $x_1 \in V(H) \setminus V(\gamma)$ y $k' \in V(\gamma)$ tales que x_1 y k' son adyacentes. Por lo mencionado anteriormente $(x_1, k') \in F(H)$.

Sea T una trayectoria dirigida de longitud máxima cuyo vértice final es k' y no tenga vértices en común con γ, salvo k', dicha trayectoria dirigida existe, pues $(x_1, k') \in F(H)$. Sea w el vértice inicial de dicha trayectoria dirigida.

De esta manera, como cada vértice recibe una flecha, entonces en particular w recibe una flecha de algún vértice de H, pero por lo dicho anteriormente, tal vértice no puede ser un vértice de γ, entonces existe un

vértice en T, digamos x_i tal que $(x_i, w) \in F(H)$, por lo que $d^+(x_i) \geq 2$, lo cual es una contradicción. Por lo tanto, no es posible que $V(H) \neq V(\gamma)$.

Ahora supongamos que $V(H) = V(\gamma)$, como $H \neq \gamma$, entonces $F(H) \neq F(\gamma)$, esto es, para algún $\{u, v\} \subseteq V(\gamma)$, $(u, v) \in F(H) \setminus F(\gamma)$, pero como $u \in V(\gamma)$, entonces $d^+(u) \geq 2$, lo cual es una contradicción. Por lo tanto, la componente H es un ciclo dirigido. □

Por ejemplo, para $n = 10$ la digráfica $\Gamma\,(10)$ contiene sólo ciclos, pues para cada $k \in \{2, \ldots, 5\}$, existe $t \geq 1$ que satisface que $k^{3^t} \equiv k \mod n$, es decir,

para $k = 2$ tenemos que si $t = 2$, entonces $2^{3^2} \equiv 2 \mod 10$,
para $k = 3$ tenemos que si $t = 2$, entonces $3^{3^2} \equiv 3 \mod 10$,
para $k = 4$ tenemos que si $t = 1$, entonces $4^{3^1} \equiv 4 \mod 10$,
para $k = 5$ tenemos que si $t = 1$, entonces $5^{3^1} \equiv 5 \mod 10$.

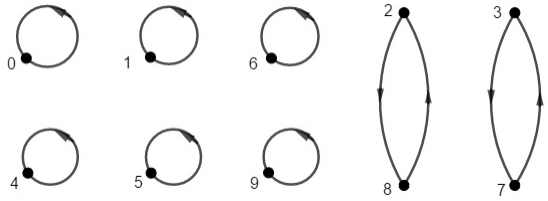

Figura 2.6: Digráfica $\Gamma(10)$.

A lo largo de este capítulo, estudiamos algunas propiedades de las digráficas de congruencias cúbicas, donde uno de los resultados más importantes es aquel donde notamos que basta con estudiar la mitad de la digráfica, respecto a los vértices, para conocer el comportamiento de la digráfica completa. De esta manera, podemos encontrar caminos dirigidos, ciclos dirigidos y componentes conexas que contengan a la primera mitad de los vértices y saber que existen isomorfismos dentro de la otra mitad de los vértices.

Capítulo 3

Número de lazos en $\Gamma(n)$

En este capítulo, enunciaremos y demostraremos una serie de teoremas que nos ayudarán en el conteo de los lazos de acuerdo con la factorización en primos del orden de la digráfica $\Gamma(n)$, mediante la definición de una función biyectiva que nos será útil para igualar el número de elementos de dos conjuntos, donde uno de ellos será el conjunto de lazos de la digráfica.

El siguiente teorema que enunciaremos establece el número de lazos de una digráfica $\Gamma(n)$, cuando n es impar. Antes de enunciar dicho teorema, veremos un ejemplo que nos dará una idea del método de la demostración de éste.

Sea $n = 2625$, consideremos su descomposición canónica en primos, es decir, $2625 = 3 \cdot 5^3 \cdot 7$. Los primos de dicha descomposición son considerados de forma ascendente. Ahora, nos fijamos en la digráfica $\Gamma(n)$, en particular en sus lazos. Por ejemplo, para $x = 126$, notemos que $(126)^3 = 2000376$ y $2000376 \equiv 126 \mod 2625$, por lo que 126 tiene un lazo en $\Gamma(2625)$.

Por otro lado, sabemos que para cualquier entero x se cumple que $x^3 - x = (x-1)(x)(x+1)$ y en particular $(126)^3 - 126 = (125)(126)(127)$. Además, como 126 tiene un lazo, $n \mid (126)^3 - 126$, es decir, $2625 \mid (125)(126)(127)$, equivalentemente $3 \cdot 5^3 \cdot 7 \mid (125)(126)(127)$.

Podemos observar que $3 \mid 126$, $3 \nmid 125$ y $3 \nmid 127$. De igual manera $5^3 \mid 125$, $5^3 \nmid 126$ y $5^3 \nmid 127$. Además, $7 \mid 126$, $7 \nmid 125$ y $7 \nmid 127$. De este modo, notamos que cada una de las potencias de los primos de la descomposición canónica de n divide a uno y sólo uno de los términos 125, 126 y 127.

Dado lo anterior, podemos asociar una triada ordenada $(\beta_1, \beta_2, \beta_3) \in \{-1, 0, 1\}^3$ al valor 126 de la siguiente manera:

Para el valor β_i vamos a considerar la potencia del i-ésimo primo en la descomposición canónica de n, digamos $p_i^{\alpha_i}$. Por lo antes visto, sabemos que $p_i^{\alpha_i}$ divide solamente a $126 - 1$ o a 126 o a $126 + 1$. De manera que, $\beta_i = -1$ si $p_i^{\alpha_i} \mid 126 - 1$ o $\beta_i = 0$ si $p_i^{\alpha_i} \mid 126$ o $\beta_i = 1$ si $p_i^{\alpha_i} \mid 126 + 1$.

Basándonos en ésto, para el valor $x = 126$ podemos asociarle la tercia ordenada $(0, -1, 0)$. Lo anterior, nos da la idea que es posible asociar los lazos de la digráfica $\Gamma(2625)$ con los elementos en el conjunto $\{-1, 0, 1\}^3$.

De manera similar, demostraremos que si tomamos una triada en el conjunto $\{-1, 0, 1\}^3$, entonces existe un lazo en $\Gamma(2625)$ que se puede asociar con dicha triada. Por ejemplo, si consideramos $(1, 0, 1)$ queremos

saber que existe un vértice $x \in V(\Gamma(2625))$ tal que el primer primo en la descomposición canónica de n divide a $x+1$, el segundo primo en la descomposición canónica divide a x y el tercer primo en la descomposición canónica divide a $x+1$. Es decir:

$$3 \mid x+1 \qquad 5^3 \mid x \qquad 7 \mid x+1.$$

Equivalentemente:

$$x \equiv -1 \mod 3 \qquad x \equiv 0 \mod 5^3 \qquad x \equiv -1 \mod 7.$$

De manera que podemos formar un sistema de congruencias de la siguiente manera:

$$\begin{aligned} x &\equiv -1 \mod 21 \\ x &\equiv 0 \mod 5^3. \end{aligned}$$

Notemos que $(21; 5^3) = 1$, por lo que, por el Teorema Chino del Residuo, tenemos que existe una única solución módulo $21 \cdot 5^3 = 2625$. Resolviendo el sistema de congruencias tenemos que $x = 125$ satisface cada una de las congruencias del sistema.

Ahora bien, veamos que $(125)^3 = 1953125$ y $1953125 \equiv 125 \mod 2625$, de manera que, efectivamente, $x = 125$ es un lazo en $\Gamma(2625)$.

El ejemplo anterior nos da la idea de que podemos asociar de manera biunivoca los lazos de $\Gamma(n)$ con s-adas ordenadas, donde s es el número de primos distintos en la descomposición canónica de n. Lo anterior es cierto y es la idea principal de la demostración del siguiente teorema.

Teorema 3.0.1. *Si n es un número natural no nulo, $p_1, p_2, \ldots, p_s$ son números primos distintos de 2 tales que $p_i < p_{i+1}$ para todo $i \in \{1, \ldots, s-1\}$ y $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s}$ es la factorización en primos de n, donde $\alpha_i \geq 1$ para todo $i \in \{1, \ldots, s\}$, entonces el número de lazos en $\Gamma(n)$ es 3^s.*

Demostración: Sean

$$\begin{aligned} B &= \{x \in V(\Gamma(n)) \backslash \{\, 0, 1, n-1 \,\}\colon (x,x) \in F(\Gamma(n))\} \text{ y} \\ D &= \{-1, 0, 1\}^s \setminus \{(0, \ldots, 0), (1, \ldots, 1), (-1, \ldots, -1)\}. \end{aligned}$$

Notemos que si $x \in B$, entonces $x^3 \equiv x \mod n$, es decir, $n \mid x^3 - x$, equivalentemente $x^3 - x = nk$ para algún $k \in \mathbb{N}$. Por otro lado, sabemos que $x^3 - x = (x-1)(x)(x+1)$, por lo que

$$(x-1)(x)(x+1) = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s} k. \tag{3.1}$$

Observemos que $(x-1)(x)(x+1) = 0$, implica que $x-1 = 0$ o $x = 0$ o $x+1 = 0$. Como $x \in B$, entonces no es posible que $x-1 = 0$ y $x = 0$. Además, como $x \geq 0$, no puede ser que $x+1 = 0$. De lo anterior $k \geq 1$.

De este modo, si $i \in \{1, \ldots, s\}$, entonces $p_i \mid x-1$ o $p_i \mid x$ o $p_i \mid x+1$. Asimismo, como para cada $i \in \{1, \ldots, s\}$, $p_i \neq 2$, se tiene que p_i divide exactamente a uno de los factores $x-1$, x o $x+1$. En tal caso, para cada $i \in \{1, \ldots, s\}$ se cumple que $p_i^{\alpha_i} \mid x-1$ o $p_i^{\alpha_i} \mid x$ o $p_i^{\alpha_i} \mid x+1$ y sólo a uno.

Definimos la relación η de B en D dada por $(x, (\beta_1, \ldots, \beta_s))$ donde para cada $i \in \{1, \ldots, s\}$

$$\beta_i = \begin{cases} -1 & \text{si} \quad p_i^{\alpha_i} \mid x-1 \\ 0 & \text{si} \quad p_i^{\alpha_i} \mid x \\ 1 & \text{si} \quad p_i^{\alpha_i} \mid x+1. \end{cases}$$

Afirmación 1. η es una función de B en D.

Primero demostraremos que $Dom(\eta) = B$. Claramente $Dom(\eta) \subseteq B$. Por otro lado, si $x \in B$ entonces $x^3 \equiv x \mod n$, por lo que $n \mid x^3 - x$. Podemos ver que cada $p_i^{\alpha_i}$ divide a $x-1$ o divide a x o divide a $x+1$, por lo que existe β_i para todo $i \in \{1, \ldots, s\}$. Dado que $x \notin \{0, 1, n-1\}$, entonces existe $\{i, j\} \subseteq \{1, \ldots, s\}$ tal que $\beta_i \neq \beta_j$, así tenemos que $(\beta_1, \beta_2, \ldots, \beta_s) \in D$ y es tal que $(x, (\beta_1, \beta_2, \ldots, \beta_s)) \in \eta$.

Por otro lado, sean $(x_1, (\beta_1, \beta_2, \ldots, \beta_s)) \in \eta$ y $(x_2, (\gamma_1, \gamma_2, \ldots, \gamma_s)) \in \eta$ y $x_1 = x_2$, demostremos que $(\beta_1, \ldots, \beta_s) = (\gamma_1, \ldots, \gamma_s)$. Sea $i \in \{1, \ldots, s\}$, consideremos los siguientes casos:

Caso 1. $\beta_i = -1$.

Como $\beta_i = -1$, entonces $p_i^{\alpha_i} \mid x_1 - 1$ y dado que $x_1 - 1 = x_2 - 1$ se tiene que $p_i^{\alpha_i} \mid x_2 - 1$. Por lo tanto, $\gamma_i = \beta_i$.

Caso 2. $\beta_i = 0$.

Como $\beta_i = 0$, entonces $p_i^{\alpha_i} \mid x_1$ y dado que $x_1 = x_2$ se tiene que $p_i^{\alpha_i} \mid x_2$. Por lo tanto $\gamma_i = \beta_1$.

Caso 3. $\beta_i = 1$.

Como $\beta_i = 1$, entonces $p_i^{\alpha_i} \mid x_1 + 1$ y dado que $x_1 + 1 = x_2 + 1$ se tiene que $p_i^{\alpha_i} \mid x_2 + 1$ por lo tanto $\gamma_i = \beta_i$.

Dados los casos anteriores, si $x_1 = x_2$, entonces $(\beta_1, \ldots, \beta_s) = (\gamma_1, \ldots, \gamma_s)$. Podemos concluir que η es función.

Afirmación 2. η es una función inyectiva.

Sea $\{x_1, x_2\} \subseteq B$ tal que $\eta(x_1) = \eta(x_2)$. Veamos que $x_1 = x_2$.

Supongamos que $\eta(x_1) = (\beta_1, \ldots, \beta_s)$ y definimos

$$I_1 = \{i \in \{1, \ldots, s\} : \beta_i = -1\},$$
$$I_2 = \{i \in \{1, \ldots, s\} : \beta_i = 0\}, \text{ y}$$
$$I_3 = \{i \in \{1, \ldots, s\} : \beta_i = 1\}.$$

Notemos que como $(\beta_1, \ldots, \beta_s) \notin \{(0, \ldots, 0), (1, \ldots, 1), (-1, \ldots, -1)\}$, entonces al menos dos de los conjuntos I_1, I_2, I_3 son no vacíos. Para cada $j \in \{1, 2, 3\}$, si $I_j \neq \emptyset$ definimos:

$$q_j = \prod_{i \in I_j} p_i^{\alpha_i}.$$

Procederemos con los siguientes casos:

Caso 1: $I_1 \neq \emptyset$, $I_2 \neq \emptyset$ e $I_3 = \emptyset$.

Observemos que:

$$p_i^{\alpha_i} \mid x_1 - 1 \text{ y } p_i^{\alpha_i} \mid x_2 - 1 \text{ para todo } i \in I_1, \text{ y}$$
$$p_i^{\alpha_i} \mid x_1 \text{ y } p_i^{\alpha_i} \mid x_2 \text{ para todo } i \in I_2.$$

Por lo que:

$$\begin{array}{cc} x_1 - 1 = q_1 k & x_2 - 1 = q_1 k' \\ x_1 = q_2 l & x_2 = q_2 l'. \end{array} \quad \text{y}$$

De esta manera, podemos obtener los siguientes sistemas de congruencias:

$$\left\{ \begin{array}{ll} x_1 \equiv 1 & \text{mód } q_1 \\ x_1 \equiv 0 & \text{mód } q_2 \end{array} \right. \quad \text{y} \quad \left\{ \begin{array}{ll} x_2 \equiv 1 & \text{mód } q_1 \\ x_2 \equiv 0 & \text{mód } q_2. \end{array} \right.$$

Ahora bien, podemos ver que q_1 y q_2 son primos relativos, de esta manera, por el Teorema Chino del Residuo, el sistema de congruencias anterior tiene una única solución módulo $q_1 q_2 = n$. Concluyendo que $x_1 = x_2$.

Caso 2: $I_2 \neq \emptyset$, $I_3 \neq \emptyset$ e $I_1 = \emptyset$.

Observemos que:

$$\begin{array}{c} p_i^{\alpha_i} \mid x_1 \text{ y } p_i^{\alpha_i} \mid x_2 \text{ para todo } i \in I_2, \text{ y} \\ p_i^{\alpha_i} \mid x_1 + 1 \text{ y } p_i^{\alpha_i} \mid x_2 + 1 \text{ para todo } i \in I_3. \end{array}$$

Por lo que:

$$\begin{array}{cc} x_1 = q_2 l & x_2 = q_2 l' \\ x_1 + 1 = q_3 t & x_2 + 1 = q_3 t'. \end{array} \quad \text{y}$$

De esta manera, podemos obtener los siguientes sistemas de congruencias:

$$\left\{ \begin{array}{ll} x_1 \equiv 0 & \text{mód } q_2 \\ x_1 \equiv -1 & \text{mód } q_3 \end{array} \right. \quad \text{y} \quad \left\{ \begin{array}{ll} x_2 \equiv 0 & \text{mód } q_2 \\ x_2 \equiv -1 & \text{mód } q_3. \end{array} \right.$$

Ahora bien, podemos ver que q_2 y q_3 son primos relativos, de esta manera, por el Teorema Chino del Residuo, el sistema de congruencias anterior tiene una única solución módulo $q_2 q_3 = n$. Concluyendo que $x_1 = x_2$.

Caso 3: $I_1 \neq \emptyset$, $I_3 \neq \emptyset$ e $I_2 = \emptyset$.

Observemos que:

$$\begin{array}{c} p_i^{\alpha_i} \mid x_1 - 1 \text{ y } p_i^{\alpha_i} \mid x_2 - 1 \text{ para todo } i \in I_1, \text{ y} \\ p_i^{\alpha_i} \mid x_1 + 1 \text{ y } p_i^{\alpha_i} \mid x_2 + 1 \text{ para todo } i \in I_3. \end{array}$$

Por lo que:

$$\begin{array}{cc} x_1 - 1 = q_1 k & x_2 - 1 = q_1 k' \\ x_1 + 1 = q_3 t & x_2 + 1 = q_3 t'. \end{array} \quad \text{y}$$

De esta manera, podemos obtener los siguientes sistemas de congruencias:

$$\left\{ \begin{array}{ll} x_1 \equiv 1 & \text{mód } q_1 \\ x_1 \equiv -1 & \text{mód } q_3 \end{array} \right. \quad \text{y} \quad \left\{ \begin{array}{ll} x_2 \equiv 1 & \text{mód } q_1 \\ x_2 \equiv -1 & \text{mód } q_3. \end{array} \right.$$

Ahora bien, podemos ver que q_1 y q_3 son primos relativos, de esta manera, por el Teorema Chino del Residuo, el sistema de congruencias anterior tiene una única solución módulo $q_1q_3 = n$. Concluyendo que $x_1 = x_2$.

Caso 4: $I_1 \neq \emptyset$, $I_2 \neq \emptyset$ e $I_3 \neq \emptyset$.

Observemos que:

$$\begin{gathered} p_i^{\alpha_i} \mid x_1 - 1 \text{ y } p_i^{\alpha_i} \mid x_2 - 1 \text{ para todo } i \in I_1, \\ p_i^{\alpha_i} \mid x_1 \text{ y } p_i^{\alpha_i} \mid x_2 \text{ para todo } i \in I_2, \text{ y} \\ p_i^{\alpha_i} \mid x_1 + 1 \text{ y } p_i^{\alpha_i} \mid x_2 + 1 \text{ para todo } i \in I_3. \end{gathered}$$

Por lo que:

$$\begin{array}{ccc} x_1 - 1 = q_1k & & x_2 - 1 = q_1k' \\ x_1 = q_2l & \text{y} & x_2 = q_2l' \\ x_1 + 1 = q_3t & & x_2 + 1 = q_3t'. \end{array}$$

De esta manera, podemos obtener los siguientes sistemas de congruencias:

$$\begin{cases} x_1 \equiv 1 \mod q_1 \\ x_1 \equiv 0 \mod q_2 \\ x_1 \equiv -1 \mod q_3 \end{cases} \quad \text{y} \quad \begin{cases} x_2 \equiv 1 \mod q_1 \\ x_2 \equiv 0 \mod q_2 \\ x_2 \equiv -1 \mod q_3 \end{cases}$$

Ahora bien, podemos ver que q_1, q_2 y q_3 son primos relativos por pares, de esta manera, por el Teorema Chino del Residuo, el sistema de congruencias anterior tiene una única solución módulo $q_1q_2q_3 = n$. Concluyendo que $x_1 = x_2$.

Dados los casos anteriores, η es una función inyectiva.

Afirmación 3. η es una función suprayectiva.

Sea $(\beta_1, \beta_2, \ldots, \beta_s) \in D$, demostremos que existe $x \in B$ tal que $\eta(x) = (\beta_1, \beta_2, \ldots, \beta_s)$.

Definamos

$$\begin{gathered} I_1 = \{i \in \{\, 1, \ldots, s \,\} \colon \beta_i = -1\}, \\ I_2 = \{i \in \{\, 1, \ldots, s \,\} \colon \beta_i = 0\}, \text{ y} \\ I_3 = \{i \in \{\, 1, \ldots, s \,\} \colon \beta_i = 1\}. \end{gathered}$$

Notemos que como $(\beta_1, \ldots, \beta_s) \notin \{(0, \ldots, 0), (1, \ldots, 1), (-1, \ldots, -1)\}$, entonces al menos dos de los conjuntos I_1, I_2, I_3 son no vacíos. Para cada $j \in \{1, 2, 3\}$, si $I_j \neq \emptyset$ definimos:

$$q_j = \prod_{i \in I_j} p_i^{\alpha_i}.$$

Procederemos con los siguientes casos:

Caso 1: $I_1 \neq \emptyset$, $I_2 \neq \emptyset$ e $I_3 = \emptyset$.

Consideremos el siguiente sistema de congruencias:

$$\begin{aligned} x &\equiv 1 \mod q_1 \\ x &\equiv 0 \mod q_2. \end{aligned}$$

Podemos ver que q_1 y q_2 son primos relativos y por el Teorema Chino del Residuo, el sistema tiene solución módulo $q_1q_2 = n$, digamos z, así $q_1 \mid z-1$ y $q_2 \mid z$, de manera que $q_1q_2 \mid (z-1)(z)$, más aún, $n \mid (z-1)(z)$. Asimismo, como $n \mid (z-1)(z)r$ para todo entero $r \geq 1$, en particular si $r = z+1$, entonces $n \mid (z-1)(z)(z+1)$, es decir, $n \mid z^3 - z$, esto es, $z^3 \equiv z \mod n$, por lo que, en z hay un lazo de $\Gamma(n)$. Se sigue además, de la elección de z, que $\eta(z) = (\beta_1, \ldots, \beta_s)$. Notemos que como $(\beta_1, \ldots, \beta_s) \notin \{(0, \ldots, 0), (1, \ldots, 1), (-1, \ldots, -1)\}$, entonces $z \notin \{0, 1, n-1\}$.

Caso 2: $I_2 \neq \emptyset$, $I_3 \neq \emptyset$ e $I_1 = \emptyset$.

Consideremos el siguiente sistema de congruencias:

$$\begin{aligned} x &\equiv 0 \mod q_2 \\ x &\equiv -1 \mod q_3. \end{aligned}$$

Podemos ver que q_2 y q_3 son primos relativos y por el Teorema Chino del Residuo, el sistema tiene solución módulo $q_2q_3 = n$, digamos z, así $q_2 \mid z$ y $q_3 \mid z+1$, de manera que $q_2q_3 \mid (z)(z+1)$, más aún, $n \mid (z)(z+1)$. Asimismo, como $n \mid (z)(z+1)r$ para todo entero $r \geq 1$, en particular si $r = z-1$, entonces $n \mid (z-1)(z)(z+1)$, es decir, $n \mid z^3 - z$, esto es, $z^3 \equiv z \mod n$, por lo que, en z hay un lazo de $\Gamma(n)$. Se sigue además, de la elección de z, que $\eta(z) = (\beta_1, \ldots, \beta_s)$. Notemos que como $(\beta_1, \ldots, \beta_s) \notin \{(0, \ldots, 0), (1, \ldots, 1), (-1, \ldots, -1)\}$, entonces $z \notin \{0, 1, n-1\}$.

Caso 3: $I_1 \neq \emptyset$, $I_3 \neq \emptyset$ e $I_2 = \emptyset$.

Consideremos el siguiente sistema de congruencias:

$$\begin{aligned} x &\equiv 1 \mod q_1 \\ x &\equiv -1 \mod q_3. \end{aligned}$$

Podemos ver que q_1 y q_3 son primos relativos y por el Teorema Chino del Residuo, el sistema tiene solución módulo $q_1q_3 = n$, digamos z, así $q_1 \mid z-1$ y $q_3 \mid z+1$, de manera que $q_1q_3 \mid (z-1)(z+1)$, más aún, $n \mid (z-1)(z+1)$. Asimismo, como $n \mid (z-1)(z+1)r$ para todo entero $r \geq 1$, en particular si $r = z$, entonces $n \mid (z-1)(z)(z+1)$, es decir, $n \mid z^3 - z$, esto es, $z^3 \equiv z \mod n$, por lo que, en z hay un lazo de $\Gamma(n)$. Se sigue además, de la elección de z, que $\eta(z) = (\beta_1, \ldots, \beta_s)$. Notemos que como $(\beta_1, \ldots, \beta_s) \notin \{(0, \ldots, 0), (1, \ldots, 1), (-1, \ldots, -1)\}$, entonces $z \notin \{0, 1, n-1\}$.

Caso 4: $I_1 \neq \emptyset$, $I_2 \neq \emptyset$ e $I_3 \neq \emptyset$.

Consideremos el siguiente sistema de congruencias:

$$\begin{aligned} x &\equiv 1 \mod q_1 \\ x &\equiv 0 \mod q_2 \\ x &\equiv -1 \mod q_3. \end{aligned}$$

Podemos ver que q_1, q_2 y q_3 son primos relativos por pares y por el Teorema Chino del Residuo, el sistema tiene solución módulo $q_1q_2q_3 = n$, digamos z, así $q_1 \mid z-1$, $q_2 \mid z$ y $q_3 \mid z+1$, de manera que $q_1q_2q_3 \mid (z-1)(z)(z+1)$, más aún, $n \mid (z-1)(z)(z+1)$. Tenemos entonces que $n \mid z^3 - z$, esto es, $z^3 \equiv z \mod n$, por lo que, en z hay un lazo de $\Gamma(n)$. Se sigue además, de la elección de z, que $\eta(z) = (\beta_1, \ldots, \beta_s)$. Notemos que como $(\beta_1, \ldots, \beta_s) \notin \{(0, \ldots, 0), (1, \ldots, 1), (-1, \ldots, -1)\}$, entonces $z \notin \{0, 1, n-1\}$.

Dadas las afirmaciones anteriores podemos concluir que η es una función biyectiva. Por lo tanto $|B|$ es igual a $|D| = 3^s - 3$ y demostramos anteriormente que en los vértices $0, 1$ y $n-1$ siempre hay un lazo, obteniendo que el número de lazos de $\Gamma(n)$ es igual a 3^s □

El siguiente teorema establece el número de lazos de $\Gamma(n)$, esta vez para n par y $\frac{n}{2}$ impar. Antes de enunciar dicho teorema, veremos un ejemplo en el que se mostrará que la demostración de éste es muy parecida a la anterior, pero tomando ahora en cuenta la paridad de los vértices que tienen un lazo.

Sea $n = 5250$ y consideremos su descomposición en primos, es decir, $5250 = 2 \cdot 3 \cdot 5^3 \cdot 7$. Los primos de dicha descomposición son considerados de forma ascendente. Ahora, nos fijamos en la digráfica $\Gamma(n)$, en particular en sus lazos. Por ejemplo, para $x = 125$, un entero impar, notemos que $(125)^3 = 1953125$ y $1953125 \equiv 125 \mod 5250$, por lo que 125 tiene un lazo en $\Gamma(5250)$.

Por otro lado, sabemos que para cualquier entero x se cumple que $x^3 - x = (x-1)(x)(x+1)$ y en particular $(125)^3 - 125 = (124)(125)(126)$. Además, como 125 tiene un lazo, $n \mid (125)^3 - 125$, es decir, $5250 \mid (124)(125)(126)$, equivalentemente $2 \cdot 3 \cdot 5^3 \cdot 7 \mid (124)(125)(126)$.

Podemos observar que $3 \mid 126$, $3 \nmid 124$ y $3 \nmid 125$. De igual manera $5^3 \mid 125$, $5^3 \nmid 124$ y $5^3 \nmid 126$. Además, $7 \mid 126$, $7 \nmid 124$ y $7 \nmid 125$. Esto es, cada una de las potencias de los primos distintos de 2 en la descomposición de n divide a uno y sólo uno de los términos $124, 125$ y 126; mientras que $2 \nmid 125$.

Consideremos ahora $x = 624$ un entero par, notemos que $(624)^3 = 242970624$ y $242970624 \equiv 624 \mod 5250$, por lo que 624 tiene un lazo en $\Gamma(5250)$.

Ahora bien, podemos ver que $(624)^3 - 624 = (623)(624)(625)$. Además, como 624 tiene un lazo, $n \mid (624)^3 - 624$, es decir, $5250 \mid (623)(624)(625)$, equivalentemente $2 \cdot 3 \cdot 5^3 \cdot 7 \mid (623)(624)(625)$.

Podemos observar que $3 \mid 624$ $3 \nmid 623$ y $3 \nmid 625$. De igual manera $5^3 \mid 625$, $5^3 \nmid 623$ y $5^3 \nmid 624$. Además, $7 \mid 623$, $7 \nmid 624$ y $7 \nmid 625$. Esto es, cada una de las potencias de los primos distintos de 2 en la descomposición de n divide a uno y sólo uno de los términos 623, 624 y 625; mientras que $2 \mid 624$.

Dado lo anterior, podemos asociar una cuarteta ordenada $(\beta_1, \beta_2, \beta_3, \beta_4)$ al valor 125 de la siguiente manera:

Para β_i con $i \in \{1, 2, 3\}$ vamos a considerar la potencia del i-ésimo primo distinto de dos en la descomposición canónica de n, digamos $p_i^{\alpha_i}$. Por lo antes visto, sabemos que $p_i^{\alpha_i}$ divide solamente a $125 - 1$ o a 125 o a $125 + 1$.

De manera que podemos definir $\beta_i = -1$ si $p_i^{\alpha_i} \mid 125 - 1$ o $\beta_i = 0$ si $p_i^{\alpha_i} \mid 125$ o $\beta_i = 1$ si $p_i^{\alpha_i} \mid 125 + 1$.

Por otro lado, para β_4 consideraremos el factor 2 en la descomposición canónica de n. Por lo antes visto, $2 \nmid 125$.

De modo que podemos definir $\beta_4 = 0$ si $2 \mid 125$ o $\beta_4 = 1$ si $2 \nmid 125$.

Basándonos en esto, para el valor $x = 125$ podemos asociarle la cuarteta ordenada $(1, 0, 1, 1)$. Lo anterior, nos da la idea que es posible asociar los lazos de la digráfica $\Gamma(5250)$ con los elementos en el conjunto

$$\{(\beta_1, \beta_2, \beta_3, \beta_4) : \beta_i \in \{-1, 0, 1\} \text{ para todo } i \in \{1, 2, 3\} \text{ y } \beta_4 \in \{0, 1\}\}.$$

De manera similar, demostraremos que si tomamos una cuarteta en el conjunto

$$\{(\beta_1, \beta_2, \beta_3, \beta_4) : \beta_i \in \{-1, 0, 1\} \text{ para todo } i \in \{1, 2, 3\} \text{ y } \beta_4 \in \{0, 1\}\},$$

entonces existe un lazo en $\Gamma(5250)$, que se puede asociar con dicha cuarteta. Por ejemplo, si consideramos $(0, -1, 0, 0)$ queremos saber si existe un vértice $x \in V(\Gamma(5250))$ tal que el primer primo distinto de dos en la descomposición canónica de n divide a x, el segundo primo distinto de dos en la descomposición canónica de n divide a $x - 1$ y el tercer primo distinto de dos en la descomposición canónica de n divide a x; además que 2 divide a x. Es decir:

$$3 \mid x \qquad 5^3 \mid x - 1 \qquad 7 \mid x \qquad 2 \mid x.$$

Equivalentemente

$$x \equiv 0 \mod 3 \qquad x \equiv 1 \mod 5^3 \qquad x \equiv 0 \mod 7 \qquad x \equiv 0 \mod 2.$$

De manera que podemos formar un sistema de congruencias de la siguiente manera:

$$\begin{aligned} x &\equiv 0 \mod 42 \\ x &\equiv 1 \mod 5^3. \end{aligned}$$

Notemos que $(42; 5^3) = 1$, por lo que, por el Teorema Chino del Residuo, tenemos que existe una única solución módulo $42 \cdot 5^3 = 5250$. Resolviendo el sistema de congruencias tenemos que $x = 126$ satisface cada una de las congruencias del sistema.

Ahora bien, veamos que $(126)^3 = 2000376$ y $2000376 \equiv 126 \mod 5250$, de manera que, efectivamente, $x = 126$ tiene un lazo en $\Gamma(5250)$.

El ejemplo anterior nos da la idea de que podemos asociar de manera biunivoca los lazos de $\Gamma(n)$ con $(s + 1)$-adas ordenadas, donde $s + 1$ es el número de primos distintos en la descomposición canónica de n tomando en cuenta el factor 2. Lo anterior es cierto y es la idea principal de la demostración del siguiente teorema.

Teorema 3.0.2. *Si n es un número natural no nulo, $p_1, p_2, \ldots, p_s$ son números primos distintos de 2 tales que $p_i < p_{i+1}$ para todo $i \in \{1, \ldots, s - 1\}$ y $n = 2p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s}$ es la factorización en primos de n, donde $\alpha_i \geq 1$ para todo $i \in \{1, \ldots, s\}$, entonces el número de lazos en $\Gamma(n)$ es $2 \cdot 3^s$.*

Demostración: Sean

$$B = \{x \in V(\Gamma(n)) \backslash \{0, 1, n - 1\} : (x, x) \in F(\Gamma(n))\} \text{ y}$$
$$D = \{(\beta_1, \ldots, \beta_{s+1}) : \beta_i \in \{-1, 0, 1\} \text{ para todo } i \in \{1 \ldots, s\} \text{ y } \beta_{s+1} \in \{0, 1\}\} \setminus \{(0, \ldots, 0), (1, \ldots, 1), (-1, \ldots, -1, 1)\}.$$

Notemos que si $x \in B$, entonces $x^3 \equiv x \mod n$, es decir, $n \mid x^3 - x$, equivalentemente $x^3 - x = nk$ para algún $k \in \mathbb{N}$. Por otro lado, sabemos que $x^3 - x = (x-1)(x)(x+1)$, por lo que

$$(x-1)(x)(x+1) = 2p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s} k. \tag{3.2}$$

Observemos que $(x-1)(x)(x+1) = 0$, implica que $x-1 = 0$ o $x = 0$ o $x+1 = 0$. Como $x \in B$, entonces no es posible que $x-1 = 0$ y $x = 0$. Además, como $x \geq 0$, entonces no puede ser que $x+1 = 0$. De lo anterior $k \geq 1$.

De este modo, si $i \in \{1, \ldots, s\}$, entonces $p_i \mid x-1$ o $p_i \mid x$ o $p_i \mid x+1$. Asimismo, como para cada $i \in \{1, \ldots, s\}$, $p_i \neq 2$, entonces p_i divide exactamente a uno de los factores $x-1$, x o $x+1$. En tal caso para cada $i \in \{1, \ldots, s\}$ se cumple que $p_i^{\alpha_i} \mid x-1$ o $p_i^{\alpha_i} \mid x$ o $p_i^{\alpha_i} \mid x+1$ y sólo uno.

Por otro lado, si x es par, entonces $2 \mid x$ y si x es impar, entonces $2 \mid x-1$ y $2 \mid x+1$.

Definimos la relación μ de B en D dada por $(x, (\beta_1, \ldots, \beta_{s+1}))$ donde para cada $i \in \{1, \ldots, s\}$

$$\beta_i = \begin{cases} -1 & \text{si} \quad p_i^{\alpha_i} \mid x-1 \\ 0 & \text{si} \quad p_i^{\alpha_i} \mid x \\ 1 & \text{si} \quad p_i^{\alpha_i} \mid x+1 \end{cases}$$

y para $i = s+1$

$$\beta_i = \begin{cases} 0 & \text{si} \quad 2 \mid x \\ 1 & \text{si} \quad 2 \nmid x. \end{cases}$$

Afirmación 1. μ es una función de B en D.

Primero demostraremos que $Dom(\mu) = B$. Claramente $Dom(\mu) \subseteq B$. Por otro lado, si $x \in B$, entonces $x^3 \equiv x \mod n$, por lo que $n \mid x^3 - x$. Podemos ver que cada $p_i^{\alpha_i}$ divide a $x-1$ o divide a x o divide a $x+1$, por lo que existe β_i para todo $i \in \{1, \ldots, s\}$; además x es par o impar, por lo que $2 \mid x$ o $2 \nmid x$, de manera que existe β_{s+1}. Dado que $x \notin \{0, 1, n-1\}$, entonces existe $\{i, j\} \subseteq \{1, \ldots, s\}$ tal que $\beta_i \neq \beta_j$, así tenemos que $(\beta_1, \beta_2, \ldots, \beta_{s+1}) \in D$ y es tal que $(x, (\beta_1, \beta_2, \ldots, \beta_{s+1})) \in \mu$.

Por otro lado, sean $(x_1, (\beta_1, \beta_2, \ldots, \beta_{s+1})) \in \mu$ y $(x_2, (\gamma_1, \gamma_2, \ldots, \gamma_{s+1})) \in \mu$ y $x_1 = x_2$, demostremos que $(\beta_1, \ldots, \beta_{s+1}) = (\gamma_1, \ldots, \gamma_{s+1})$.

Observación 3.0.3. *Notemos que si $\beta_{s+1} = 0$, entonces $2 \mid x_1$ y como $x_1 = x_2$, entonces $2 \mid x_2$, por lo que $\gamma_{s+1} = \beta_{s+1}$. De igual manera si $\beta_{s+1} = 1$, entonces $2 \nmid x_1$ y como $x_1 = x_2$, entonces $2 \nmid x_2$, por lo que $\gamma_{s+1} = \beta_{s+1}$.*

Sea $i \in \{1, \ldots, s\}$, consideremos los siguientes casos:

Caso 1. $\beta_i = -1$.

Como $\beta_i = -1$, entonces $p_i^{\alpha_i} \mid x_1 - 1$ y dado que $x_1 - 1 = x_2 - 1$ se tiene que $p_i^{\alpha_i} \mid x_2 - 1$. Por lo tanto $\gamma_i = \beta_i$.

Caso 2. $\beta_i = 0$.

Como $\beta_i = 0$, entonces $p_i^{\alpha_i} \mid x_1$ y dado que $x_1 = x_2$ se tiene que $p_i^{\alpha_i} \mid x_2$. Por lo tanto $\gamma_i = \beta_1$.

Caso 3. $\beta_i = 1$.

Como $\beta_i = 1$, entonces $p_i^{\alpha_i} \mid x_1 + 1$ y dado que $x_1 + 1 = x_2 + 1$ se tiene que $p_i^{\alpha_i} \mid x_2 + 1$. Por lo tanto $\gamma_i = \beta_i$.

Dados los casos anteriores y la Observación 3.0.3, si $x_1 = x_2$ entonces $(\beta_1, \ldots, \beta_{s+1}) = (\gamma_1, \ldots, \gamma_{s+1})$. Podemos concluir que μ es función.

Afirmación 2. μ es una función inyectiva.

Sea $\{x_1, x_2\} \subseteq B$ tal que $\mu(x_1) = \mu(x_2)$. Veamos que $x_1 = x_2$.

Supongamos que $\mu(x_1) = (\beta_1, \ldots, \beta_{s+1})$ y definimos

$$I_1 = \{i \in \{1, \ldots, s\} : \beta_i = -1\},$$
$$I_2 = \{i \in \{1, \ldots, s\} : \beta_i = 0\}, \text{ y}$$
$$I_3 = \{i \in \{1, \ldots, s\} : \beta_i = 1\}.$$

Notemos que como $(\beta_1, \ldots, \beta_{s+1}) \notin \{(0, \ldots, 0), (1, \ldots, 1), (-1, \ldots, -1, 1)\}$, entonces al menos dos de los conjuntos I_1, I_2, I_3 son no vacíos. Para cada $j \in \{1, 2, 3\}$, si $I_j \neq \emptyset$ definimos:

$$q_j = \prod_{i \in I_j} p_i^{\alpha_i}.$$

Procederemos con los siguientes casos:

Caso 1: $I_1 \neq \emptyset$, $I_2 \neq \emptyset$ e $I_3 = \emptyset$.

Observemos que:

$$p_i^{\alpha_i} \mid x_1 - 1 \text{ y } p_i^{\alpha_i} \mid x_2 - 1 \text{ para todo } i \in I_1, \text{ y}$$
$$p_i^{\alpha_i} \mid x_1 \text{ y } p_i^{\alpha_i} \mid x_2 \text{ para todo } i \in I_2.$$

Por lo que:

$$\begin{array}{ccc} x_1 - 1 = q_1 k & & x_2 - 1 = q_1 k' \\ x_1 = q_2 l & \text{y} & x_2 = q_2 l'. \end{array}$$

Además, notemos que si $\beta_{s+1} = 0$, entonces $2 \mid x_1$ y $2 \mid x_2$ y por el contrario, si $\beta_{s+1} = 1$, entonces $2 \mid x_1 - 1$ y $2 \mid x_2 - 1$. Por lo que, tenemos alguno de los siguientes casos:

$$\begin{array}{ccccc} & x_1 = 2r & \text{y} & x_2 = 2r' & \\ \text{ó} & x_1 - 1 = 2u & \text{y} & x_2 - 1 = 2u'. & \end{array}$$

Así, podemos obtener los siguientes sistemas de congruencias. Si x_1 y x_2 son pares:

$$\begin{cases} x_1 \equiv 1 \mod q_1 \\ x_1 \equiv 0 \mod q_2 \\ x_1 \equiv 0 \mod 2 \end{cases} \quad \text{y} \quad \begin{cases} x_2 \equiv 1 \mod q_1 \\ x_2 \equiv 0 \mod q_2 \\ x_2 \equiv 0 \mod 2 \end{cases}$$

o si x_1 y x_2 son impares:

$$\begin{cases} x_1 \equiv 1 \mod q_1 \\ x_1 \equiv 0 \mod q_2 \\ x_1 \equiv 1 \mod 2 \end{cases} \quad \text{y} \quad \begin{cases} x_2 \equiv 1 \mod q_1 \\ x_2 \equiv 0 \mod q_2 \\ x_2 \equiv 1 \mod 2. \end{cases}$$

Ahora bien, podemos ver que q_1, q_2 y 2 son primos relativos por pares, de esta manera, por el Teorema Chino del Residuo, ambos sistemas de congruencias anteriores tienen una única solución módulo $2q_1q_2 = n$. Concluyendo que, para cualquiera de los dos sistemas, $x_1 = x_2$.

Caso 2: $I_2 \neq \emptyset$, $I_3 \neq \emptyset$ e $I_1 = \emptyset$.

Observemos que:

$$p_i^{\alpha_i} \mid x_1 \text{ y } p_i^{\alpha_i} \mid x_2 \text{ para todo } i \in I_2, \text{ y}$$
$$p_i^{\alpha_i} \mid x_1 + 1 \text{ y } p_i^{\alpha_i} \mid x_2 + 1 \text{ para todo } i \in I_3.$$

Por lo que:

$$\begin{matrix} x_1 = q_2 l \\ x_1 + 1 = q_3 t \end{matrix} \quad \text{y} \quad \begin{matrix} x_2 = q_2 l' \\ x_2 + 1 = q_3 t'. \end{matrix}$$

Además, notemos que si $\beta_{s+1} = 0$, entonces $2 \mid x_1$ y $2 \mid x_2$ y por el contrario, si $\beta_{s+1} = 1$, entonces $2 \mid x_1 - 1$ y $2 \mid x_2 - 1$. Por lo que, tenemos alguno de los siguientes casos:

$$\begin{matrix} x_1 = 2r & \text{y} & x_2 = 2r' \\ \text{ó} \quad x_1 - 1 = 2u & \text{y} & x_2 - 1 = 2u'. \end{matrix}$$

Así, podemos obtener los siguientes sistemas de congruencias. Si x_1 y x_2 son pares:

$$\begin{cases} x_1 \equiv 0 \mod q_2 \\ x_1 \equiv -1 \mod q_3 \\ x_1 \equiv 0 \mod 2 \end{cases} \quad \text{y} \quad \begin{cases} x_2 \equiv 0 \mod q_2 \\ x_2 \equiv -1 \mod q_3 \\ x_2 \equiv 0 \mod 2 \end{cases}$$

o si x_1 y x_2 son impares:

$$\begin{cases} x_1 \equiv 0 \mod q_2 \\ x_1 \equiv -1 \mod q_3 \\ x_1 \equiv 1 \mod 2 \end{cases} \text{ y } \begin{cases} x_2 \equiv 0 \mod q_2 \\ x_2 \equiv -1 \mod q_3 \\ x_2 \equiv 1 \mod 2. \end{cases}$$

Ahora bien, podemos ver que q_2, q_3 y 2 son primos relativos por pares, de esta manera, por el Teorema Chino del Residuo, ambos sistemas de congruencias anteriores tienen una única solución módulo $2q_2q_3 = n$. Concluyendo que, para cualquiera de los dos sistemas, $x_1 = x_2$.

Caso 3: $I_1 \neq \emptyset$, $I_3 \neq \emptyset$ e $I_2 = \emptyset$.

Observemos que:

$$p_i^{\alpha_i} \mid x_1 - 1 \text{ y } p_i^{\alpha_i} \mid x_2 - 1 \text{ para todo } i \in I_1, \text{ y}$$
$$p_i^{\alpha_i} \mid x_1 + 1 \text{ y } p_i^{\alpha_i} \mid x_2 + 1 \text{ para todo } i \in I_3.$$

Por lo que:

$$\begin{matrix} x_1 - 1 = q_1k \\ x_1 + 1 = q_3t \end{matrix} \text{ y } \begin{matrix} x_2 - 1 = q_1k' \\ x_2 + 1 = q_3t'. \end{matrix}$$

Además, notemos que si $\beta_{s+1} = 0$, entonces $2 \mid x_1$ y $2 \mid x_2$ y por el contrario, si $\beta_{s+1} = 1$, entonces $2 \mid x_1 - 1$ y $2 \mid x_2 - 1$. Por lo que, tenemos alguno de los siguientes casos:

$$\begin{matrix} x_1 = 2r & \text{y} & x_2 = 2r' \\ \text{ó} \quad x_1 - 1 = 2u & \text{y} & x_2 - 1 = 2u'. \end{matrix}$$

Así, podemos obtener los siguientes sistemas de congruencias. Si x_1 y x_2 son pares:

$$\begin{cases} x_1 \equiv 1 \mod q_1 \\ x_1 \equiv -1 \mod q_3 \\ x_1 \equiv 0 \mod 2 \end{cases} \text{ y } \begin{cases} x_2 \equiv 1 \mod q_1 \\ x_2 \equiv -1 \mod q_3 \\ x_2 \equiv 0 \mod 2 \end{cases}$$

ó si x_1 y x_2 son impares:

$$\begin{cases} x_1 \equiv 1 \mod q_1 \\ x_1 \equiv -1 \mod q_3 \\ x_1 \equiv 1 \mod 2 \end{cases} \text{ y } \begin{cases} x_2 \equiv 1 \mod q_1 \\ x_2 \equiv -1 \mod q_3 \\ x_2 \equiv 1 \mod 2. \end{cases}$$

Ahora bien, podemos ver que q_1, q_3 y 2 son primos relativos por pares, de esta manera, por el Teorema Chino del Residuo, ambos sistemas de congruencias anteriores tienen una única solución módulo $2q_1q_3 = n$. Concluyendo que, para cualquiera de los dos sistemas, $x_1 = x_2$.

Caso 4: $I_1 \neq \emptyset$, $I_2 \neq \emptyset$ e $I_3 \neq \emptyset$.

Observemos que:

$$p_i^{\alpha_i} \mid x_1 - 1 \text{ y } p_i^{\alpha_i} \mid x_2 - 1 \text{ para todo } i \in I_1,$$
$$p_i^{\alpha_i} \mid x_1 \text{ y } p_i^{\alpha_i} \mid x_2 \text{ para todo } i \in I_2, \text{ y}$$
$$p_i^{\alpha_i} \mid x_1 + 1 \text{ y } p_i^{\alpha_i} \mid x_2 + 1 \text{ para todo } i \in I_3.$$

Por lo que:

$$\begin{array}{ccc} x_1 - 1 = q_1 k & & x_2 - 1 = q_1 k' \\ x_1 = q_2 l & \text{y} & x_2 = q_2 l' \\ x_1 + 1 = q_3 t & & x_2 + 1 = q_3 t'. \end{array}$$

Además, notemos que si $\beta_{s+1} = 0$, entonces $2 \mid x_1$ y $2 \mid x_2$ y por el contrario, si $\beta_{s+1} = 1$, entonces $2 \mid x_1 - 1$ y $2 \mid x_2 - 1$. Por lo que, tenemos algunos de los siguientes casos:

$$\begin{array}{ccccc} & x_1 = 2r & \text{y} & x_2 = 2r' \\ \text{ó} & x_1 - 1 = 2u & \text{y} & x_2 - 1 = 2u'. \end{array}$$

Así, podemos obtener los siguientes sistemas de congruencias, Si x_1 y x_2 son pares:

$$\begin{cases} x_1 \equiv 1 \mod q_1 \\ x_1 \equiv 0 \mod q_2 \\ x_1 \equiv -1 \mod q_3 \\ x_1 \equiv 0 \mod 2 \end{cases} \text{ y } \begin{cases} x_2 \equiv 1 \mod q_1 \\ x_2 \equiv 0 \mod q_2 \\ x_2 \equiv -1 \mod q_3 \\ x_2 \equiv 0 \mod 2 \end{cases}$$

ó si x_1 y x_2 son impares:

$$\begin{cases} x_1 \equiv 1 \mod q_1 \\ x_1 \equiv 0 \mod q_2 \\ x_1 \equiv -1 \mod q_3 \\ x_1 \equiv 1 \mod 2 \end{cases} \text{ y } \begin{cases} x_2 \equiv 1 \mod q_1 \\ x_2 \equiv 0 \mod q_2 \\ x_2 \equiv -1 \mod q_3 \\ x_2 \equiv 1 \mod 2. \end{cases}$$

Ahora bien, podemos ver que q_1, q_2, q_3 y 2 son primos relativos por pares, de esta manera, por el Teorema Chino del Residuo, ambos sistemas de congruencias anteriores tienen una única solución módulo $2q_1q_2q_3 = n$. Concluyendo que, para cualquiera de los dos sistemas, $x_1 = x_2$.

Dados los casos anteriores, podemos concluir que μ es una función inyectiva.

Afirmación 3. μ es una función suprayectiva.

Sea $(\beta_1, \beta_2, \ldots, \beta_{s+1}) \in D$, demostremos que existe $x \in B$ tal que $\mu(x) = (\beta_1, \beta_2, \ldots, \beta_{s+1})$.

Definamos:

$$I_1 = \{i \in \{1, \ldots, s\} : \beta_i = -1\},$$
$$I_2 = \{i \in \{1, \ldots, s\} : \beta_i = 0\}, \text{ y}$$
$$I_3 = \{i \in \{1, \ldots, s\} : \beta_i = 1\}.$$

y $\beta_{s+1} = 0$ o $\beta_{s+1} = 1$.

Notemos que como $(\beta_1, \ldots, \beta_{s+1}) \notin \{(0, \ldots, 0), (1, \ldots, 1), (-1, \ldots, -1, 1)\}$, entonces al menos dos de los conjuntos I_1, I_2, I_3 son no vacíos. Para cada $j \in \{1, 2, 3\}$, si $I_j \neq \emptyset$ definimos:

$$q_j = \prod_{i \in I_j} p_i^{\alpha_i}.$$

Procederemos con los siguientes casos:

Caso 1: $I_1 \neq \emptyset$, $I_2 \neq \emptyset$ e $I_3 = \emptyset$.

Consideremos los siguientes sistemas de congruencias:

$$(1) \begin{cases} x \equiv 1 \mod q_1 \\ x \equiv 0 \mod q_2 \\ x \equiv 0 \mod 2 \end{cases} \quad \text{y} \quad (2) \begin{cases} x \equiv 1 \mod q_1 \\ x \equiv 0 \mod q_2 \\ x \equiv 1 \mod 2. \end{cases}$$

Podemos ver que q_1, q_2 y 2 son primos relativos por pares y por el Teorema Chino del Residuo, los sistemas (1) y (2) tienen solución módulo $2q_1q_2 = n$, digamos z y así:

- Para (1):
  $q_1 \mid z - 1$, $q_2 \mid z$ y $2 \mid z$, de manera que $2q_1q_2 \mid (z-1)(z)$.
- Para (2):
  $q_1 \mid z - 1$, $q_2 \mid z$ y $2 \mid z - 1$, de manera que $2q_1q_2 \mid (z-1)(z)$.

En cualquiera de los dos casos $n \mid (z-1)(z)$. Asimismo, como $n \mid (z-1)(z)r$ para todo entero $r \geq 1$, en particular si $r = z + 1$, entonces $n \mid (z-1)(z)(z+1)$, es decir, $n \mid z^3 - z$, esto es, $z^3 \equiv z \mod n$, de manera que, en z hay un lazo de $\Gamma(n)$. Se sigue además, de la elección de z, que $\mu(z) = (\beta_1, \ldots, \beta_{s+1})$. Notemos que como $(\beta_1, \ldots, \beta_s) \notin \{(0, \ldots, 0), (1, \ldots, 1), (-1, \ldots, -1, 1)\}$, entonces $z \notin \{0, 1, n-1\}$.

Caso 2: $I_2 \neq \emptyset$, $I_3 \neq \emptyset$ e $I_1 = \emptyset$.

Consideremos los siguientes sistemas de congruencias:

$$(1) \begin{cases} x \equiv 0 \mod q_2 \\ x \equiv -1 \mod q_3 \\ x \equiv 0 \mod 2 \end{cases} \quad \text{y} \quad (2) \begin{cases} x \equiv 0 \mod q_2 \\ x \equiv -1 \mod q_3 \\ x \equiv 1 \mod 2. \end{cases}$$

Podemos ver que q_2, q_3 y 2 son primos relativos por pares y por el Teorema Chino del Residuo, los sistemas (1) y (2) tienen solución módulo $2q_2q_3 = n$, digamos z y así:

- Para (1):
  $q_2 \mid z$, $q_3 \mid z+1$ y $2 \mid z$, de manera que $2q_2q_3 \mid (z)(z+1)$, más aún, $n \mid (z)(z+1)$. Asimismo, como $n \mid (z)(z+1)r$ para todo entero $r \geq 1$, en particular si $r = z-1$, entonces $n \mid (z-1)(z)(z+1)$, es decir, $n \mid z^3 - z$, esto es, $z^3 \equiv z \mod n$, por lo que, en z hay un lazo de $\Gamma(n)$. Se sigue además, de la elección de z, que $\mu(z) = (\beta_1, \ldots, \beta_{s+1})$.
- Para (2):
  $q_2 \mid z$, $q_3 \mid z+1$ y $2 \mid z-1$, de manera que $2q_1q_2 \mid (z-1)(z)(z+1)$, más aún, $n \mid (z-1)(z)(z+1)$. Tenemos entonces que $n \mid z^3 - z$, esto es, $z^3 \equiv z \mod n$, por lo que, en z hay un lazo de $\Gamma(n)$. Se sigue además, de la elección de z, que $\mu(z) = (\beta_1, \ldots, \beta_{s+1})$.

Notemos que para cualquier caso, como $(\beta_1, \ldots, \beta_s) \notin \{(0, \ldots, 0), (1, \ldots, 1), (-1, \ldots, -1, 1)\}$, entonces $z \notin \{0, 1, n-1\}$.

Caso 3: $I_1 \neq \emptyset$, $I_3 \neq \emptyset$ e $I_2 = \emptyset$.

Consideremos los siguientes sistemas de congruencias:

$$(1) \begin{cases} x \equiv 1 \mod q_1 \\ x \equiv -1 \mod q_3 \\ x \equiv 0 \mod 2 \end{cases} \quad \text{y} \quad (2) \begin{cases} x \equiv 1 \mod q_1 \\ x \equiv -1 \mod q_3 \\ x \equiv 1 \mod 2. \end{cases}$$

Podemos ver que q_1, q_3 y 2 son primos relativos por pares y por el Teorema Chino del Residuo, los sistemas (1) y (2) tienen solución módulo $2q_1q_3 = n$, digamos z y así:

- Para (1):
  $q_1 \mid z-1$, $q_3 \mid z+1$ y $2 \mid z$, de manera que $2q_1q_3 \mid (z-1)(z)(z+1)$, más aún, $n \mid (z-1)(z)(z+1)$. Tenemos entonces que $n \mid z^3 - z$, esto es, $z^3 \equiv z \mod n$, por lo que, en z hay un lazo de $\Gamma(n)$. Se sigue además, de la elección de z, que $\mu(z) = (\beta_1, \ldots, \beta_{s+1})$.
- Para (2):
  $q_1 \mid z-1$, $q_3 \mid z+1$ y $2 \mid z-1$, de manera que $2q_1q_3 \mid (z-1)(z+1)$, más aún, $n \mid (z-1)(z+1)$. Asimismo, como $n \mid (z-1)(z+1)r$ para todo entero $r \geq 1$, en particular si $r = z$, entonces $n \mid (z-1)(z)(z+1)$, es decir, $n \mid z^3 - z$, esto es, $z^3 \equiv z \mod n$, por lo que, en z hay un lazo de $\Gamma(n)$. Se sigue además, de la elección de z, que $\mu(z) = (\beta_1, \ldots, \beta_{s+1})$.

Notemos que para cualquier caso, como $(\beta_1, \ldots, \beta_s) \notin \{(0, \ldots, 0), (1, \ldots, 1), (-1, \ldots, -1, 1)\}$, entonces $z \notin \{0, 1, n-1\}$.

Caso 4: $I_1 \neq \emptyset$, $I_2 \neq \emptyset$ e $I_3 \neq \emptyset$.

Consideremos los siguientes sistemas de congruencias:

$$(1) \begin{cases} x \equiv 1 \mod q_1 \\ x \equiv 0 \mod q_2 \\ x \equiv -1 \mod q_3 \\ x \equiv 0 \mod 2 \end{cases} \quad \text{y} \quad (2) \begin{cases} x \equiv 1 \mod q_1 \\ x \equiv 0 \mod q_2 \\ x \equiv -1 \mod q_3 \\ x \equiv 1 \mod 2. \end{cases}$$

Podemos ver que q_1, q_2, q_3 y 2 son primos relativos por pares y por el Teorema Chino del Residuo, los sistemas (1) y (2) tienen solución módulo $2q_1q_2q_3 = n$, digamos z y así:

- Para (1):
  $q_1 \mid z-1$, $q_2 \mid z$, $q_3 \mid z+1$ y $2 \mid z$, de manera que $2q_1q_2q_3 \mid (z-1)(z)(z+1)$.
- Para (2):
  $q_1 \mid z-1$,$q_2 \mid z$, $q_3 \mid z+1$ y $2 \mid z-1$, de manera que $2q_1q_2q_3 \mid (z-1)(z)(z+1)$.

En cualquiera de los dos casos, tenemos que $n \mid z^3 - z$, esto es, $z^3 \equiv z \mod n$, de manera que, en z hay un lazo de $\Gamma(n)$. Se sigue además, de la elección de z, que $\mu(z) = (\beta_1, \ldots, \beta_{s+1})$. Notemos que como $(\beta_1, \ldots, \beta_s) \notin \{(0, \ldots, 0), (1, \ldots, 1), (-1, \ldots, -1, 1)\}$, entonces $z \notin \{0, 1, n-1\}$.

Dadas las afirmaciones anteriores podemos concluir que μ es una función biyectiva y por lo tanto, $|B|$ es igual a $|D| = (2 \cdot 3^s) - 3$. Demostramos anteriormente que en los vértices $0, 1$ y $n-1$ siempre hay un lazo, obteniendo que el número de lazos de $\Gamma(n)$ es igual a $2 \cdot 3^s$. □

El siguiente teorema establece el número de lazos de $\Gamma(n)$, esta vez para n par y $\frac{n}{4}$ impar. Antes de enunciar dicho teorema, veremos un ejemplo en el que se mostrará que la demostración de éste es muy parecida a la anterior pero ahora tomando en cuenta si el vértice que tiene un lazo es divisible entre 4 o no.

Sea $n = 540$ y consideremos su descomposición en primos, es decir, $540 = 2^2 \cdot 3^3 \cdot 5$. Los primos de dicha descomposición son considerados de forma ascendente. Ahora, nos fijamos en la digráfica $\Gamma(n)$, en particular en sus lazos. Por ejemplo, para $x = 55$, notemos que $(55)^3 = 166375$ y $166375 \equiv 55 \mod 540$, por lo que 55 tiene un lazo en $\Gamma(540)$.

Por otro lado, sabemos que para cualquier entero x se cumple que $x^3 - x = (x-1)(x)(x+1)$ y en particular $(55)^3 - 55 = (54)(55)(56)$. Además, como 55 tiene un lazo, $n \mid (55)^3 - 55$, es decir, $540 \mid (54)(55)(56)$, equivalentemente $2^2 \cdot 3^3 \cdot 5 \mid (54)(55)(56)$.

Podemos observar que $3^3 \mid 54$, $3^3 \nmid 55$ y $3^3 \nmid 56$. De igual manera $5 \mid 55$, $5 \nmid 54$ y $5 \nmid 56$. Esto es, cada una de las potencias de los primos distintos de 2 en la descomposición de n divide a uno y sólo uno de los términos $54, 55$ y 56; del mismo modo notemos que $2^2 \mid (54)(55)(56)$, por lo que $2^2 \mid 54$ o $2^2 \mid 55$ o $2^2 \mid 56$ y sólo a uno, en particular $2^2 \mid 56$.

Dado lo anterior, podemos asociar una tercia ordenada $(\beta_1, \beta_2, \beta_3)$ al valor 55 de la siguiente manera:

Para β_i con $i \in \{1, 2\}$ vamos a considerar la potencia del i-ésimo primo distinto de dos en la descomposición canónica de n, digamos $p_i^{\alpha_i}$. Por lo antes visto, sabemos que $p_i^{\alpha_i}$ divide solamente a $55-1$ o a 55 o a $55+1$.

De manera que podemos definir $\beta_i = -1$ si $p_i^{\alpha_i} \mid (55-1)$ o $\beta_i = 0$ si $p_i^{\alpha_i} \mid 55$ o $\beta_i = 1$ si $p_i^{\alpha_i} \mid (55+1)$.

Por otro lado, para β_3 consideraremos el factor 2^2 en la descomposición canónica de n. Por lo antes mencionado definiremos $\beta_3 = -1$ si $2^2 \mid 54$ o $\beta_3 = 0$ si $2^2 \mid 55$ o $\beta_3 = 1$ si $2^2 \mid 56$.

Basándonos en esto, para el valor $x = 55$ podemos asociarle la tercia ordenada $(-1, 0, 1)$. Lo anterior, nos da la idea que es posible asociar los lazos de la digráfica $\Gamma(540)$ con los elementos en el conjunto $\{-1, 0, 1\}^3$.

De manera similar, demostraremos que si tomamos una tercia en el conjunto $\{-1, 0, 1\}^3$, entonces existe un lazo en $\Gamma(540)$ que se puede asociar con dicha tercia. Por ejemplo, si consideramos $(1, 0, 0)$ queremos saber si existe un vértice $x \in V(\Gamma(540))$ tal que el primer primo distinto de dos en la descomposición canónica de

n divide a $x+1$, el segundo primo distinto de dos en la descomposición canónica de n divide a x; además que 2^2 divide a x. Es decir:

$$3^3 \mid x+1 \qquad 5 \mid x \qquad 2^2 \mid x.$$

Equivalentemente

$$x \equiv -1 \mod 3^3 \qquad x \equiv 0 \mod 5 \qquad x \equiv 0 \mod 2^2.$$

De manera que podemos formar un sistema de congruencias de la siguiente manera:

$$\begin{aligned} x &\equiv -1 \mod 3^3 \\ x &\equiv 0 \mod 20. \end{aligned}$$

Notemos que $(3^3; 20) = 1$, por lo que, por el Teorema Chino del Residuo, tenemos que existe una única solución módulo $3^3 \cdot 20 = 540$. Resolviendo el sistema de congruencias tenemos que $x = 80$ satisface cada una de las congruencias del sistema.

Ahora bien, veamos que $(80)^3 = 512000$ y $512000 \equiv 80 \mod 540$, de manera que, efectivamente, $x = 80$ tiene un lazo en $\Gamma(540)$.

El ejemplo anterior nos da la idea de que podemos asociar de manera biunivoca los lazos de $\Gamma(n)$ con $(s+1)$-adas ordenadas, donde $s+1$ es el número de primos distintos en la descomposición canónica de n tomando en cuenta el factor 2^2. Lo anterior es cierto y es la idea principal de la demostración del siguiente teorema.

Teorema 3.0.4. *Si n es un número natural no nulo, $p_1, p_2, \ldots, p_s$ son números primos distintos de 2 tales que $p_i < p_{i+1}$ para todo $i \in \{1, \ldots, s-1\}$ y $n = 2^2 p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s}$ es la factorización en primos de n, donde $\alpha_i \geq 1$ para todo $i \in \{1, \ldots, s\}$, entonces el número de lazos en $\Gamma(n)$ es $3 \cdot 3^s$.*

Demostración: Sean

$$\begin{aligned} B &= \{x \in V(\Gamma(n)) \backslash \{0, 1, n-1\} \colon (x, x) \in F(\Gamma(n))\} \text{ y} \\ D &= \{-1, 0, 1\}^{s+1} \setminus \{(0, \ldots, 0), (1, \ldots, 1), (-1, \ldots, -1)\}. \end{aligned}$$

Notemos que si $x \in B$, entonces $x^3 \equiv x \mod n$, es decir, $n \mid x^3 - x$, equivalentemente $x^3 - x = nk$ para algún $k \in \mathbb{N}$. Por otro lado, sabemos que $x^3 - x = (x-1)(x)(x+1)$, por lo que

$$(x-1)(x)(x+1) = 2^2 p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s} k. \tag{3.3}$$

Observemos que $(x-1)(x)(x+1) = 0$, implica que $x-1 = 0$ o $x = 0$ o $x+1 = 0$. Como $x \in B$, entonces no es posible que $x-1 = 0$ y $x = 0$. Además, como $x \geq 0$, entonces no puede ser que $x+1 = 0$. De lo anterior $k \geq 1$.

De este modo, si $i \in \{1, \ldots, s\}$, entonces $p_i \mid x-1$ o $p_i \mid x$ o $p_i \mid x+1$. Asimismo, como para cada $i \in \{1, \ldots, s\}$, $p_i \neq 2$, entonces p_i divide exactamente a uno de los factores $x-1$, x o $x+1$. En tal caso para cada $i \in \{1, \ldots, s\}$ se cumple que $p_i^{\alpha_i} \mid x-1$ o $p_i^{\alpha_i} \mid x$ o $p_i^{\alpha_i} \mid x+1$ y sólo uno.

Por otro lado, notemos que $2^2 \mid x$ o si $2^2 \nmid x$, como $2^2 \mid (x-1)(x)(x+1)$, entonces $2^2 \mid x-1$ o $2^2 \mid x+1$ y sólo a uno puesto que $x-1$ y $x+1$ son pares consecutivos y 2^2 no podría dividirlos a ambos.

Definimos la relación ν de B en D dada por $(x,(\beta_1,\ldots,\beta_{s+1}))$ donde para cada $i \in \{1,\ldots,s\}$

$$\beta_i = \begin{cases} -1 & \text{si} \quad p_i^{\alpha_i} \mid x-1 \\ 0 & \text{si} \quad p_i^{\alpha_i} \mid x \\ 1 & \text{si} \quad p_i^{\alpha_i} \mid x+1 \end{cases}$$

y para $i = s+1$

$$\beta_i = \begin{cases} -1 & \text{si} \quad 2^2 \mid x-1 \\ 0 & \text{si} \quad 2^2 \mid x \\ 1 & \text{si} \quad 2^2 \mid x+1. \end{cases}$$

Afirmación 1. ν es una función de B en D.

Primero demostraremos que $Dom(\nu) = B$. Claramente $Dom(\nu) \subseteq B$. Por otro lado, si $x \in B$, entonces $x^3 \equiv x \mod n$, por lo que $n \mid x^3 - x$. Podemos ver que cada $p_i^{\alpha_i}$ divide a $x-1$ o divide a x o divide a $x+1$, por lo que, existe β_i para todo $i \in \{1,\ldots,s\}$; además, 2^2 divide a $x-1$ o divide a x o divide a $x+1$, de manera que existe β_{s+1}. Dado que $x \notin \{0,1,n-1\}$, entonces existe $\{i,j\} \subseteq \{1,\ldots,s\}$ tal que $\beta_i \neq \beta_j$, así tenemos que $(\beta_1,\beta_2,\ldots,\beta_{s+1}) \in D$ y es tal que $(x,(\beta_1,\beta_2,\ldots,\beta_{s+1})) \in \nu$.

Por otro lado, sean $(x_1,(\beta_1,\beta_2,\ldots,\beta_{s+1})) \in \nu$ y $(x_2,(\gamma_1,\gamma_2,\ldots,\gamma_{s+1})) \in \nu$ y $x_1 = x_2$, demostremos que $(\beta_1,\ldots,\beta_{s+1}) = (\gamma_1,\ldots,\gamma_{s+1})$.

Observación 3.0.5. *Notemos que si $\beta_{s+1} = -1$, entonces $2^2 \mid x_1 - 1$ y como $x_1 = x_2$, entonces $2^2 \mid x_2 - 1$, por lo que $\gamma_{s+1} = \beta_{s+1}$. De igual manera si $\beta_{s+1} = 0$, entonces $2^2 \mid x_1$ y como $x_1 = x_2$, entonces $2^2 \mid x_2$, por lo que $\gamma_{s+1} = \beta_{s+1}$. Así mismo, si $\beta_{s+1} = 1$, entonces $2^2 \mid x+1$, por lo que $\gamma_{s+1} = \beta_{s+1}$.*

Sea $i \in \{1,\ldots,s\}$, consideremos los siguientes casos:

Caso 1. $\beta_i = -1$.

Como $\beta_i = -1$, entonces $p_i^{\alpha_i} \mid x_1 - 1$ y dado que $x_1 - 1 = x_2 - 1$ se tiene que $p_i^{\alpha_i} \mid x_2 - 1$. Por lo tanto $\gamma_i = \beta_i$.

Caso 2. $\beta_i = 0$.

Como $\beta_i = 0$, entonces $p_i^{\alpha_i} \mid x_1$ y dado que $x_1 = x_2$ se tiene que $p_i^{\alpha_i} \mid x_2$. Por lo tanto $\gamma_i = \beta_1$.

Caso 3. $\beta_i = 1$.

Como $\beta_i = 1$, entonces $p_i^{\alpha_i} \mid x_1 + 1$ y dado que $x_1 + 1 = x_2 + 1$ se tiene que $p_i^{\alpha_i} \mid x_2 + 1$. Por lo tanto $\gamma_i = \beta_i$.

Dados los casos anteriores y la Observación 3.0.5 si $x_1 = x_2$, entonces $(\beta_1,\ldots,\beta_{s+1}) = (\gamma_1,\ldots,\gamma_{s+1})$. Podemos concluir que ν es función.

Afirmación 2. ν es una función inyectiva.

Sea $\{x_1, x_2\} \subseteq B$ tal que $\nu(x_1) = \nu(x_2)$. Veamos que $x_1 = x_2$.

Supongamos que $\nu(x_1) = (\beta_1, \ldots, \beta_{s+1})$ y definimos

$$I_1 = \{i \in \{\, 1, \ldots, s \,\}: \beta_i = -1\},$$
$$I_2 = \{i \in \{\, 1, \ldots, s \,\}: \beta_i = 0\}, \text{ y}$$
$$I_3 = \{i \in \{\, 1, \ldots, s \,\}: \beta_i = 1\}.$$

Notemos que como $(\beta_1, \ldots, \beta_{s+1}) \notin \{(0, \ldots, 0), (1, \ldots, 1), (-1, \ldots, -1)\}$, entonces al menos dos de los conjuntos I_1, I_2, I_3 son no vacíos. Para cada $j \in \{1, 2, 3\}$, si $I_j \neq \emptyset$ definimos:

$$q_j = \prod_{i \in I_j} p_i^{\alpha_i}.$$

Procederemos con los siguientes casos:

Caso 1: $I_1 \neq \emptyset$, $I_2 \neq \emptyset$ e $I_3 = \emptyset$.

En este caso observemos que:

$$p_i^{\alpha_i} \mid x_1 - 1 \text{ y } p_i^{\alpha_i} \mid x_2 - 1 \text{ para todo } i \in I_1, \text{ y}$$
$$p_i^{\alpha_i} \mid x_1 \text{ y } p_i^{\alpha_i} \mid x_2 \text{ para todo } i \in I_2.$$

Por lo que:

$$\begin{array}{ccc} x_1 - 1 = q_1 k & & x_2 - 1 = q_1 k' \\ x_1 = q_2 l & \text{y} & x_2 = q_2 l'. \end{array}$$

Además, notemos que si $\beta_{s+1} = -1$, entonces $2^2 \mid x_1 - 1$ y $2^2 \mid x_2 - 1$, si $\beta_{s+1} = 0$, entonces $2^2 \mid x_1$ y $2^2 \mid x_2$ y por otro lado, si $\beta_{s+1} = 1$, entonces $2^2 \mid x_1 + 1$ y $2^2 \mid x_2 + 1$. Por lo que, tenemos alguno de los siguientes casos:

$$\begin{array}{ccccc} x_1 - 1 = 2^2 u & & \text{y} & & x_2 - 1 = 2^2 u' \\ \text{ó} \quad x_1 = 2^2 r & & \text{y} & & x_2 = 2^2 r' \\ \text{ó} \quad x_1 + 1 = 2^2 v & & \text{y} & & x_2 + 1 = 2^2 v'. \end{array}$$

Así, podemos obtener los siguientes sistemas de congruencias. Si $x_1 - 1 = 2^2 u$ y $x_2 - 1 = 2^2 u'$:

$$\begin{cases} x_1 \equiv 1 \mod q_1 \\ x_1 \equiv 0 \mod q_2 \\ x_1 \equiv 1 \mod 2^2 \end{cases} \quad \text{y} \quad \begin{cases} x_2 \equiv 1 \mod q_1 \\ x_2 \equiv 0 \mod q_2 \\ x_2 \equiv 1 \mod 2^2 \end{cases}$$

ó si $x_1 = 2^2 r$ y $x_2 = 2^2 r'$:

$$\begin{cases} x_1 \equiv 1 \mod q_1 \\ x_1 \equiv 0 \mod q_2 \\ x_1 \equiv 0 \mod 2^2 \end{cases} \text{ y } \begin{cases} x_2 \equiv 1 \mod q_1 \\ x_2 \equiv 0 \mod q_2 \\ x_2 \equiv 0 \mod 2^2 \end{cases}$$

ó si $x_1 + 1 = 2^2 v$ y $x_2 + 1 = 2^2 v'$:

$$\begin{cases} x_1 \equiv 1 \mod q_1 \\ x_1 \equiv 0 \mod q_2 \\ x_1 \equiv -1 \mod 2^2 \end{cases} \text{ y } \begin{cases} x_2 \equiv 1 \mod q_1 \\ x_2 \equiv 0 \mod q_2 \\ x_2 \equiv -1 \mod 2^2. \end{cases}$$

Ahora bien, podemos ver que en cualquier caso, q_1, q_2 y 2^2 son primos relativos por pares, de esta manera, por el Teorema Chino del Residuo, los sistemas de congruencias anteriores tienen una única solución módulo $2^2 q_1 q_2 = n$. Concluyendo que, para cualquiera de los sistemas, $x_1 = x_2$.

Caso 2: $I_2 \neq \emptyset$, $I_3 \neq \emptyset$ e $I_1 = \emptyset$.

En este caso observemos que:

$$\begin{gathered} p_i^{\alpha_i} \mid x_1 \text{ y } p_i^{\alpha_i} \mid x_2 \text{ para todo } i \in I_2, \text{ y} \\ p_i^{\alpha_i} \mid x_1 + 1 \text{ y } p_i^{\alpha_i} \mid x_2 + 1 \text{ para todo } i \in I_3. \end{gathered}$$

Por lo que:

$$\begin{matrix} x_1 = q_2 l \\ x_1 + 1 = q_3 t \end{matrix} \quad \text{y} \quad \begin{matrix} x_2 = q_2 l' \\ x_2 + 1 = q_3 t'. \end{matrix}$$

Además, notemos que si $\beta_{s+1} = -1$, entonces $2^2 \mid x_1 - 1$ y $2^2 \mid x_2 - 1$, si $\beta_{s+1} = 0$, entonces $2^2 \mid x_1$ y $2^2 \mid x_2$ y por otro lado, si $\beta_{s+1} = 1$, entonces $2^2 \mid x_1 + 1$ y $2^2 \mid x_2 + 1$. Por lo que, tenemos alguno de los siguientes casos:

$$\begin{matrix} x_1 - 1 = 2^2 u & \text{y} & x_2 - 1 = 2^2 u' \\ \text{ó} \quad x_1 = 2^2 r & \text{y} & x_2 = 2^2 r' \\ \text{ó} \quad x_1 + 1 = 2^2 v & \text{y} & x_2 + 1 = 2^2 v'. \end{matrix}$$

Así, podemos obtener los siguientes sistemas de congruencias. Si $x_1 - 1 = 2^2 u$ y $x_2 - 1 = 2^2 u'$:

$$\begin{cases} x_1 \equiv 0 \mod q_2 \\ x_1 \equiv -1 \mod q_3 \\ x_1 \equiv 1 \mod 2^2 \end{cases} \text{ y } \begin{cases} x_2 \equiv 0 \mod q_2 \\ x_2 \equiv -1 \mod q_3 \\ x_2 \equiv 1 \mod 2^2 \end{cases}$$

ó si $x_1 = 2^2 r$ y $x_2 = 2^2 r'$:

$$\begin{cases} x_1 \equiv 0 \mod q_2 \\ x_1 \equiv -1 \mod q_3 \\ x_1 \equiv 0 \mod 2^2 \end{cases} \text{ y } \begin{cases} x_2 \equiv 0 \mod q_2 \\ x_2 \equiv -1 \mod q_3 \\ x_2 \equiv 0 \mod 2^2 \end{cases}$$

ó $x_1 + 1 = 2^2 v$ y $x_2 + 1 = 2^2 v'$:

$$\begin{cases} x_1 \equiv 0 \mod q_2 \\ x_1 \equiv -1 \mod q_3 \\ x_1 \equiv -1 \mod 2^2 \end{cases} \text{ y } \begin{cases} x_2 \equiv 0 \mod q_2 \\ x_2 \equiv -1 \mod q_3 \\ x_2 \equiv -1 \mod 2^2. \end{cases}$$

Ahora bien, podemos ver que para cualquier caso q_2, q_3 y 2^2 son primos relativos por pares, de esta manera, por el Teorema Chino del Residuo, los sistemas de congruencias anteriores tienen una única solución módulo $2^2 q_2 q_3 = n$. Concluyendo que, para cualquiera de los dos sistemas, $x_1 = x_2$.

Caso 3: $I_1 \neq \emptyset$, $I_3 \neq \emptyset$ e $I_2 = \emptyset$.

En este caso observemos que:

$$p_i^{\alpha_i} \mid x_1 - 1 \text{ y } p_i^{\alpha_i} \mid x_2 - 1 \text{ para todo } i \in I_1, \text{ y}$$
$$p_i^{\alpha_i} \mid x_1 + 1 \text{ y } p_i^{\alpha_i} \mid x_2 + 1 \text{ para todo } i \in I_3.$$

Por lo que:

$$\begin{matrix} x_1 - 1 = q_1 k \\ x_1 + 1 = q_3 t \end{matrix} \quad \text{y} \quad \begin{matrix} x_2 - 1 = q_1 k' \\ x_2 + 1 = q_3 t'. \end{matrix}$$

Además, notemos que si $\beta_{s+1} = -1$, entonces $2^2 \mid x_1 - 1$ y $2^2 \mid x_2 - 1$, si $\beta_{s+1} = 0$, entonces $2^2 \mid x_1$ y $2^2 \mid x_2$ y por otro lado, si $\beta_{s+1} = 1$, entonces $2^2 \mid x_1 + 1$ y $2^2 \mid x_2 + 1$. Por lo que, tenemos algunos de los siguientes casos:

$$\begin{matrix} x_1 - 1 = 2^2 u & \text{y} & x_2 - 1 = 2^2 u' \\ \text{ó} \quad x_1 = 2^2 r & \text{y} & x_2 = 2^2 r' \\ \text{ó} \quad x_1 + 1 = 2^2 v & \text{y} & x_2 + 1 = 2^2 v'. \end{matrix}$$

Así, podemos obtener los siguientes sistemas de congruencias. Si $x_1 - 1 = 2^2 u$ y $x_2 - 1 = 2^2 u'$:

$$\begin{cases} x_1 \equiv 1 \mod q_1 \\ x_1 \equiv -1 \mod q_3 \\ x_1 \equiv 1 \mod 2^2 \end{cases} \text{ y } \begin{cases} x_2 \equiv 1 \mod q_1 \\ x_2 \equiv -1 \mod q_3 \\ x_2 \equiv 1 \mod 2^2 \end{cases}$$

ó si $x_1 = 2^2 r$ y $x_2 = 2^2 r'$:

$$\begin{cases} x_1 \equiv 1 \mod q_1 \\ x_1 \equiv -1 \mod q_3 \\ x_1 \equiv 0 \mod 2^2 \end{cases} \text{ y } \begin{cases} x_2 \equiv 1 \mod q_1 \\ x_2 \equiv -1 \mod q_3 \\ x_2 \equiv 0 \mod 2^2 \end{cases}$$

ó si $x_1 + 1 = 2^2 v$ y $x_2 + 1 = 2^2 v'$:

$$\begin{cases} x_1 \equiv 1 \mod q_1 \\ x_1 \equiv -1 \mod q_3 \\ x_1 \equiv -1 \mod 2^2 \end{cases} \text{ y } \begin{cases} x_2 \equiv 1 \mod q_1 \\ x_2 \equiv -1 \mod q_3 \\ x_2 \equiv -1 \mod 2^2. \end{cases}$$

Ahora bien, podemos ver que en cualquiera de los casos anteriores q_1, q_3 y 2^2 son primos relativos por pares, de esta manera, por el Teorema Chino del Residuo, ambos sistemas de congruencias anteriores tienen una única solución módulo $2^2q_1q_3 = n$. Concluyendo que, para cualquiera de los dos sistemas, $x_1 = x_2$.

Caso 4: $I_1 \neq \emptyset$, $I_2 \neq \emptyset$ e $I_3 \neq \emptyset$.

En este caso observemos que:

$$\begin{gathered} p_i^{\alpha_i} \mid x_1 - 1 \text{ y } p_i^{\alpha_i} \mid x_2 - 1 \text{ para todo } i \in I_1, \\ p_i^{\alpha_i} \mid x_1 \text{ y } p_i^{\alpha_i} \mid x_2 \text{ para todo } i \in I_2, \text{ y} \\ p_i^{\alpha_i} \mid x_1 + 1 \text{ y } p_i^{\alpha_i} \mid x_2 + 1 \text{ para todo } i \in I_3. \end{gathered}$$

Por lo que:

$$\begin{array}{ccc} x_1 - 1 = q_1k & & x_2 - 1 = q_1k' \\ x_1 = q_2l & \text{y} & x_2 = q_2l' \\ x_1 + 1 = q_3t & & x_2 + 1 = q_3t'. \end{array}$$

Además, notemos que si $\beta_{s+1} = -1$, entonces $2^2 \mid x_1 - 1$ y $2^2 \mid x_2 - 1$, si $\beta_{s+1} = 0$, entonces $2^2 \mid x_1$ y $2^2 \mid x_2$ y por otro lado, si $\beta_{s+1} = 1$, entonces $2^2 \mid x_1 + 1$ y $2^2 \mid x_2 + 1$. Por lo que, tenemos alguno de los siguientes casos:

$$\begin{array}{ccccc} x_1 - 1 = 2^2u & & \text{y} & & x_2 - 1 = 2^2u' \\ \text{ó} \quad x_1 = 2^2r & & \text{y} & & x_2 = 2^2r' \\ \text{ó} \quad x_1 + 1 = 2^2v & & \text{y} & & x_2 + 1 = 2^2v'. \end{array}$$

Así, podemos obtener los siguientes sistemas de congruencias. Si $x_1 - 1 = 2^2u$ y $x_2 - 1 = 2^2u'$:

$$\begin{cases} x_1 \equiv 1 \mod q_1 \\ x_1 \equiv 0 \mod q_2 \\ x_1 \equiv -1 \mod q_3 \\ x_1 \equiv 1 \mod 2^2 \end{cases} \text{y} \begin{cases} x_2 \equiv 1 \mod q_1 \\ x_2 \equiv 0 \mod q_2 \\ x_2 \equiv -1 \mod q_3 \\ x_2 \equiv 1 \mod 2^2 \end{cases}$$

ó si $x_1 = 2^2r$ y $x_2 = 2^2r'$:

$$\begin{cases} x_1 \equiv 1 \mod q_1 \\ x_1 \equiv 0 \mod q_2 \\ x_1 \equiv -1 \mod q_3 \\ x_1 \equiv 0 \mod 2^2 \end{cases} \text{y} \begin{cases} x_2 \equiv 1 \mod q_1 \\ x_2 \equiv 0 \mod q_2 \\ x_2 \equiv -1 \mod q_3 \\ x_2 \equiv 0 \mod 2^2 \end{cases}$$

ó si $x_1 + 1 = 2^2v$ y $x_2 + 1 = 2^2v'$:

$$\begin{cases} x_1 \equiv 1 \mod q_1 \\ x_1 \equiv 0 \mod q_2 \\ x_1 \equiv -1 \mod q_3 \\ x_1 \equiv -1 \mod 2^2 \end{cases} \text{y} \begin{cases} x_2 \equiv 1 \mod q_1 \\ x_2 \equiv 0 \mod q_2 \\ x_2 \equiv -1 \mod q_3 \\ x_2 \equiv -1 \mod 2^2. \end{cases}$$

Ahora bien, podemos ver que para cualquiera de los casos anteriores q_1, q_2, q_3 y 2^2 son primos relativos por pares, de esta manera, por el Teorema Chino del Residuo, los sistemas de congruencias anteriores tienen una única solución módulo $2^2q_1q_2q_3 = n$. Concluyendo que, para cualquiera de los dos sistemas, $x_1 = x_2$.

Dados los casos anteriores, podemos concluir que μ es una función inyectiva.

Afirmación 3. ν es una función suprayectiva.

Sea $(\beta_1, \beta_2, \ldots, \beta_{s+1}) \in D$, demostremos que existe $x \in B$ tal que $\nu(x) = (\beta_1, \beta_2, \ldots, \beta_{s+1})$.

Definamos:

$$I_1 = \{i \in\{\, 1, \ldots, s\,\}\colon \beta_i = -1\},$$
$$I_2 = \{i \in\{\, 1, \ldots, s\,\}\colon \beta_i = 0\}, \text{ y}$$
$$I_3 = \{i \in\{\, 1, \ldots, s\,\}\colon \beta_i = 1\}.$$

Notemos que como $(\beta_1, \ldots, \beta_{s+1}) \notin \{(0, \ldots, 0), (1, \ldots, 1), (-1, \ldots, -1)\}$, entonces al menos dos de los conjuntos I_1, I_2, I_3 son no vacíos. Para cada $j \in \{1, 2, 3\}$, si $I_j \neq \emptyset$ definimos:

$$q_j = \prod_{i \in I_j} p_i^{\alpha_i}.$$

Procederemos con los siguientes casos:

Caso 1: $I_1 \neq \emptyset$, $I_2 \neq \emptyset$ e $I_3 = \emptyset$.

En este caso consideremos el siguiente sistema de congruencias:

$$(1)\begin{cases} x \equiv 1 \mod q_1 \\ x \equiv 0 \mod q_2 \\ x \equiv 1 \mod 2^2 \end{cases} \text{ y } (2)\begin{cases} x \equiv 1 \mod q_1 \\ x \equiv 0 \mod q_2 \\ x \equiv 0 \mod 2^2 \end{cases} \text{ y } (3)\begin{cases} x \equiv 1 \mod q_1 \\ x \equiv 0 \mod q_2 \\ x \equiv -1 \mod 2^2. \end{cases}$$

Podemos ver que q_1, q_2 y 2^2 son primos relativos por pares y por el Teorema Chino del Residuo, los sistemas (1), (2) y (3) tienen solución módulo $2^2q_1q_2 = n$, digamos z y así:

- Para (1):
  $q_1 \mid z-1$, $q_2 \mid z$ y $2^2 \mid z-1$, de manera que $2^2q_1q_2 \mid (z-1)(z)$, en particular $n \mid (z-1)(z)(z+1)$.
- Para (2):
  $q_1 \mid z-1$, $q_2 \mid z$ y $2^2 \mid z$, de manera que $2^2q_1q_2 \mid (z-1)(z)$, en particular $n \mid (z-1)(z)(z+1)$.
- Para (3):
  $q_1 \mid z-1$, $q_2 \mid z$ y $2^2 \mid z+1$, de manera que $2^2q_1q_2 \mid (z-1)(z)(z+1)$, es decir, $n \mid (z-1)(z)(z+1)$.

De los casos anteriores, $n \mid z^3 - z$, esto es, $z^3 \equiv z \mod n$, por lo que, en z hay un lazo de $\Gamma(n)$. Además, como $(\beta_1, \ldots, \beta_{s+1}) \notin \{(0, \ldots, 0), (1, \ldots, 1), (-1, \ldots, -1)\}$, entonces $z \notin \{0, 1, n-1\}$, es decir, $z \in Dom(\nu)$. Se sigue, de la elección de z, que $\nu(z) = (\beta_1, \ldots, \beta_{s+1})$.

Caso 2: $I_2 \neq \emptyset$, $I_3 \neq \emptyset$ e $I_1 = \emptyset$.

En este caso consideremos el siguiente sistema de congruencias:

$$(1)\begin{cases} x \equiv 0 \mod q_2 \\ x \equiv -1 \mod q_3 \\ x \equiv 1 \mod 2^2 \end{cases} \text{ y } (2)\begin{cases} x \equiv 0 \mod q_2 \\ x \equiv -1 \mod q_3 \\ x \equiv 0 \mod 2^2 \end{cases} \text{ y } (3)\begin{cases} x \equiv 0 \mod q_2 \\ x \equiv -1 \mod q_3 \\ x \equiv -1 \mod 2^2. \end{cases}$$

Podemos ver que q_2, q_3 y 2^2 son primos relativos por pares y por el Teorema Chino del Residuo, los sistemas (1), (2) y (3) tienen solución módulo $2^2 q_2 q_3 = n$, digamos z y así:

- Para (1):
  $q_2 \mid z$, $q_3 \mid z+1$ y $2^2 \mid z-1$, de manera que $2^2 q_2 q_3 \mid (z-1)(z)(z+1)$, es decir, $n \mid (z-1)(z)(z+1)$.
- Para (2):
  $q_2 \mid z$, $q_3 \mid z+1$ y $2^2 \mid z$, de manera que $2^2 q_1 q_2 \mid (z)(z+1)$, en particular $n \mid (z-1)(z)(z+1)$.
- Para (3)
  $q_2 \mid z$, $q_3 \mid z+1$ y $2^2 \mid z+1$, de manera que $2^2 q_1 q_2 \mid (z)(z+1)$, en particular $n \mid (z-1)(z)(z+1)$.

En cualquiera de los casos anteriores, $n \mid z^3 - z$, esto es, $z^3 \equiv z \mod n$, por lo que, en z hay un lazo de $\Gamma(n)$. Además, como $(\beta_1, \ldots, \beta_{s+1}) \notin \{(0, \ldots, 0), (1, \ldots, 1), (-1, \ldots, -1)\}$, entonces $z \notin \{0, 1, n-1\}$, es decir, $z \in Dom(\nu)$. Se sigue, de la elección de z, que $\nu(z) = (\beta_1, \ldots, \beta_{s+1})$.

Caso 3: $I_1 \neq \emptyset$, $I_3 \neq \emptyset$ e $I_2 = \emptyset$.

En este caso consideremos el siguiente sistema de congruencias:

$$(1)\begin{cases} x \equiv 1 \mod q_1 \\ x \equiv -1 \mod q_3 \\ x \equiv 1 \mod 2^2 \end{cases} \text{ y } (2)\begin{cases} x \equiv 1 \mod q_1 \\ x \equiv -1 \mod q_3 \\ x \equiv 0 \mod 2^2 \end{cases} \text{ y } (3)\begin{cases} x \equiv 1 \mod q_1 \\ x \equiv -1 \mod q_3 \\ x \equiv -1 \mod 2^2. \end{cases}$$

Podemos ver que q_1, q_3 y 2^2 son primos relativos por pares y por el Teorema Chino del Residuo, los sistemas (1), (2) y (3) tienen solución módulo $2^2 q_1 q_3 = n$, digamos z y así:

- Para (1):
  $q_1 \mid z-1$, $q_3 \mid z+1$ y $2^2 \mid z-1$, de manera que $2^2 q_1 q_3 \mid (z-1)(z+1)$, en particular $n \mid (z-1)(z)(z+1)$.
- Para (2):
  $q_1 \mid z-1$, $q_3 \mid z+1$ y $2^2 \mid z$, de manera que $2^2 q_1 q_3 \mid (z-1)(z)(z+1)$, es decir, $n \mid (z-1)(z)(z+1)$.
- Para (3):
  $q_1 \mid z-1$, $q_3 \mid z+1$ y $2^2 \mid z+1$, de manera que $2^2 q_1 q_3 \mid (z-1)(z+1)$, en particular $n \mid (z-1)(z)(z+1)$.

En cualquiera de los casos anteriores, $n \mid z^3 - z$, esto es, $z^3 \equiv z \mod n$, por lo que, en z hay un lazo de $\Gamma(n)$. Además, como $(\beta_1, \ldots, \beta_{s+1}) \notin \{(0, \ldots, 0), (1, \ldots, 1), (-1, \ldots, -1)\}$, entonces $z \notin \{0, 1, n-1\}$, es decir, $z \in Dom(\nu)$. Se sigue, de la elección de z, que $\nu(z) = (\beta_1, \ldots, \beta_{s+1})$.

Caso 4: $I_1 \neq \emptyset$, $I_2 \neq \emptyset$ e $I_3 \neq \emptyset$.

En este caso consideremos el siguiente sistema de congruencias:

$$(1)\begin{cases} x \equiv 1 \mod q_1 \\ x \equiv 0 \mod q_2 \\ x \equiv -1 \mod q_3 \\ x \equiv 1 \mod 2^2 \end{cases} \text{ y } (2)\begin{cases} x \equiv 1 \mod q_1 \\ x \equiv 0 \mod q_2 \\ x \equiv -1 \mod q_3 \\ x \equiv 0 \mod 2^2 \end{cases} \text{ y } (3)\begin{cases} x \equiv 1 \mod q_1 \\ x \equiv 0 \mod q_2 \\ x \equiv -1 \mod q_3 \\ x \equiv -1 \mod 2^2. \end{cases}$$

Podemos ver que q_1, q_2, q_3 y 2^2 son primos relativos por pares y por el Teorema Chino del Residuo, los sistemas (1), (2) y (3) tienen solución módulo $2^2q_1q_2q_3 = n$, digamos z y así:

- Para (1):
  $q_1 \mid z-1$, $q_2 \mid z$, $q_3 \mid z+1$ y $2^2 \mid z-1$, de manera que $2^2q_1q_2q_3 \mid (z-1)(z)(z+1)$, es decir, $n \mid (z-1)(z)(z+1)$.
- Para (2):
  $q_1 \mid z-1$,$q_2 \mid z$, $q_3 \mid z+1$ y $2^2 \mid z$, de manera que $2^2q_1q_2q_3 \mid (z-1)(z)(z+1)$, es decir, $n \mid (z-1)(z)(z+1)$.
- Para (3):
  $q_1 \mid z-1$,$q_2 \mid z$, $q_3 \mid z+1$ y $2^2 \mid z+1$, de manera que $2^2q_1q_2q_3 \mid (z-1)(z)(z+1)$, es decir, $n \mid (z-1)(z)(z+1)$.

En cualquiera de los casos anteriores, $n \mid z^3 - z$, esto es, $z^3 \equiv z \mod n$, por lo que, en z hay un lazo de $\Gamma(n)$. Además, como $(\beta_1, \ldots, \beta_{s+1}) \notin \{(0,\ldots,0),(1,\ldots,1),(-1,\ldots,-1)\}$, entonces $z \notin \{0, 1, n-1\}$, es decir, $z \in Dom(\nu)$. Se sigue, de la elección de z, que $\nu(z) = (\beta_1, \ldots, \beta_{s+1})$.

Dados los casos anteriores, podemos concluir que ν es una función biyectiva y por lo tanto, $|B|$ es igual a $|D| = 3 \cdot 3^s - 3$. Demostramos anteriormente que en los vértices $0, 1$ y $n-1$ siempre hay un lazo, obteniendo así que el número de lazos de $\Gamma(n)$ es igual a $3 \cdot 3^s$. □

Antes de enunciar el último teorema relacionado con los lazos de la digráfica $\Gamma(n)$ demostraremos dos lemas que nos serán útiles para tal teorema.

Lema 3.0.6. *Sean x y m dos enteros positivos tales que $m > 1$. Los siguientes enunciados se satisfacen:*

1. *Si $x \equiv 1 \mod 2^{m-1}$, entonces $x \equiv 2^{m-1} + 1 \mod 2^m$.*
2. *Si $x \equiv -1 \mod 2^{m-1}$, entonces $x \equiv 2^{m-1} - 1 \mod 2^m$.*

Demostración:

1. Como $x \equiv 1 \mod 2^{m-1}$, entonces $2^{m-1} \mid x-1$, esto es ,

$$x - 1 = 2^{m-1}u \qquad \text{para algún } u \in \mathbb{Z}. \tag{3.4}$$

Ahora bien multiplicamos la Ecuación (3.4) por 2, es decir, $2x - 2 = 2^m u$. De manera que tenemos la congruencia lineal $2x \equiv 2 \mod 2^m$. Notemos que $(2; 2^m) = 2$ y $2 \mid 2$, por lo que, por el Teorema 1.1.27 tenemos 2 soluciones incongruentes, en particular $x \equiv 2^{m-1} + 1 \mod 2^m$.

2. Como $x \equiv -1 \mod 2^{m-1}$, entonces $2^{m-1} \mid x+1$, esto es,

$$x + 1 = 2^{m-1}v \qquad \text{para algún } v \in \mathbb{Z}. \tag{3.5}$$

Ahora bien podemos multiplicar la Ecuación (3.5) por 2, es decir, $2x+2 = 2^m v$. De manera que tenemos la congruencia lineal $2x \equiv -2 \mod 2^m$. Notemos que $(2; 2^m) = 2$ y $2 \mid -2$, por lo que por el Teorema 1.1.27 tenemos 2 soluciones incongruentes, en particular $x \equiv 2^{m-1} - 1 \mod 2^m$.

□

Lema 3.0.7. *Sean x y m dos enteros positivos tales que $m > 1$. Los siguientes enunciados se satisfacen:*

1. *Si $x \equiv 2^{m-1} + 1 \mod 2^m$, entonces $x \equiv 1 \mod 2^{m-1}$. Además $x \not\equiv 1 \mod 2^m$.*
2. *Si $x \equiv 2^{m-1} - 1 \mod 2^m$, entonces $x \equiv -1 \mod 2^{m-1}$. Además $x \not\equiv -1 \mod 2^m$.*

Demostración:

1. Como $x \equiv 2^{m-1} + 1 \mod 2^m$, entonces $2^m \mid x - 2^{m-1} - 1$, más aún, $x - 1 - 2^{m-1} = 2^m k$ para algún $k \in \mathbb{Z}$. Despejando $x-1$, tenemos que $x - 1 = 2^m k + 2^{m-1}$, o lo que es lo mismo, $x - 1 = 2^{m-1}(2k+1)$. Si $2k + 1 = l$, entonces $x - 1 = 2^{m-1}l$, es decir, $2^{m-1} \mid x - 1$. Por lo tanto, $x \equiv 1 \mod 2^{m-1}$.

   Por otro lado, podemos ver que $2^{m-1} + 1 \not\equiv 1 \mod 2^m$, pues de lo contrario $2^m \mid 2^{m-1}$, esto es, $2^{m-1} = 2^m t$ para alguna $t \in \mathbb{Z}$, lo cual no es posible, de manera que podemos concluir que $x \not\equiv 1 \mod 2^m$.

2. Como $x \equiv 2^{m-1} - 1 \mod 2^m$, entonces $2^m \mid x - 2^{m-1} + 1$, más aún, $x + 1 - 2^{m-1} = 2^m k'$ para algún $k' \in \mathbb{Z}$. Despejando $x+1$, tenemos que $x + 1 = 2^m k' + 2^{m-1}$, o lo que es lo mismo, $x + 1 = 2^{m-1}(2k'+1)$. Si $2k' + 1 = l'$, entonces $x + 1 = 2^{m-1}l'$, es decir, $2^{m-1} \mid x + 1$. Por lo tanto, $x \equiv -1 \mod 2^{m-1}$.

   Por otro lado, podemos ver que $2^{m-1} - 1 \not\equiv -1 \mod 2^m$, pues de lo contrario $2^m \mid 2^{m-1}$, esto es, $2^{m-1} = 2^m t'$ para alguna $t' \in \mathbb{Z}$ lo cual no es posible, de manera que podemos concluir que $x \not\equiv -1 \mod 2^m$.

□

El siguiente teorema establece el número de lazos de $\Gamma(n)$, esta vez cuando $2^m \mid n$ y $m \geq 3$. Antes de enunciar dicho teorema, veremos un ejemplo en el que se mostrará que la demostración de éste es parecida a las demostraciones antes realizadas.

Sea $n = 120$ y consideremos su descomposición en primos, es decir, $120 = 2^3 \cdot 3 \cdot 5$. Los primos de dicha descomposición serán considerados de forma ascendente. Ahora, fijémonos en la digráfica $\Gamma(n)$, en particular en sus lazos. Por ejemplo, para $x = 21$, notemos que $(21)^3 = 9261$ y $9261 \equiv 21 \mod 120$, por lo que, 21 tiene un lazo en $\Gamma(120)$.

Por otro lado, sabemos que para cualquier entero x se cumple que $x^3 - x = (x-1)(x)(x+1)$ y en particular $(21)^3 - 21 = (20)(21)(22)$. Además, como 21 tiene un lazo, $n \mid (21)^3 - 21$, es decir, $120 \mid (20)(21)(22)$, equivalentemente $2^3 \cdot 3 \cdot 5 \mid (20)(21)(22)$.

Podemos observar que $3 \mid 21$, $3 \nmid 20$ y $3 \nmid 22$. De igual manera $5 \mid 20$, $5 \nmid 21$ y $5 \nmid 22$. Esto es, cada una de las potencias de los primos distintos de 2 en la descomposición de n divide a uno y sólo uno de los términos $20, 21$ y 22; del mismo modo notemos que $2^3 \mid (20)(21)(22)$, es decir, 2^3 divide al producto de tres número consecutivos, lo cual nos brinda varios casos: un primer caso en el que 2^3 divide a alguno de los tres factores, y un segundo caso en el que 2^3 no divida a ninguno de los factores. En esta última situación, veremos posteriormente que 2^2 debe dividir al antecesor o sucesor del lazo, para el caso que estamos tratando, 2^2 debe dividir a 20 o a 22. En este caso particular, $2^2 \mid 20$. Así, podemos asociar una tercia ordenada $(\beta_1, \beta_2, \beta_3)$ al valor 21 de la siguiente manera:

Para β_i con $i \in \{1, 2\}$ vamos a considerar la potencia del i-ésimo primo distinto de dos en la descomposición canónica de n, digamos $p_i^{\alpha_i}$. Por lo antes visto, sabemos que $p_i^{\alpha_i}$ divide solamente a $21 - 1$ o 21 o $21 + 1$.

De manera que podemos definir $\beta_i = -1$ si $p_i^{\alpha_i} \mid (21 - 1)$ o $\beta_i = 0$ si $p_i^{\alpha_i} \mid 21$ o $\beta_i = 1$ si $p_i^{\alpha_i} \mid (21 + 1)$.

Por otro lado, para β_3 consideraremos el factor 2^3 en la descomposición canónica de n. Definiremos $\beta_3 = -1$ si $2^3 \mid 20$ o $\beta_3 = 0$ si $2^3 \mid 21$ o $\beta_3 = 1$ si $2^3 \mid 22$ o $\beta_3 = -2$ si $2^3 \nmid 20$, pero $2^2 \mid 20$ o $\beta_3 = 2$ si $2^3 \nmid 22$, pero $2^2 \mid 22$.

Así, para el valor $x = 21$ podemos asociarle la tercia ordenada $(0, -1, -2)$. Lo anterior, nos da la idea que es posible asociar los lazos de la digráfica $\Gamma(120)$ con los elementos en el conjunto

$$\{(\beta_1, \ldots, \beta_{s+1}) : \beta_i \in \{-1, 0, 1\} \text{ para todo } i \in \{1 \ldots, s\} \text{ y } \beta_{s+1} \in \{-2, 1, 0, 1, 2\}\} \setminus \{(0, \ldots, 0), (1, \ldots, 1), (-1, \ldots, -1)\}.$$

De manera similar, demostraremos que si tomamos una tercia en el conjunto

$$\{(\beta_1, \ldots, \beta_{s+1}) : \beta_i \in \{-1, 0, 1\} \text{ para todo } i \in \{1 \ldots, s\} \text{ y } \beta_{s+1} \in \{-2, 1, 0, 1, 2\}\} \setminus \{(0, \ldots, 0), (1, \ldots, 1), (-1, \ldots, -1)\},$$

entonces existe un lazo en $\Gamma(120)$ que se puede asociar con dicha tercia. Por ejemplo, si consideramos $(1, 0, 2)$ queremos saber si existe un vértice $x \in V(\Gamma(120))$ tal que el primer primo distinto de dos en la descomposición canónica de n divide a $x + 1$, el segundo primo distinto de dos en la descomposición canónica de n divide a x; además que 2^2 divide a $x + 1$ y $2^3 \nmid x + 1$. Es decir:

$$3 \mid x + 1 \qquad 5 \mid x \qquad 2^2 \mid x + 1.$$

Equivalentemente

$$x \equiv -1 \mod 3 \qquad x \equiv 0 \mod 5 \qquad x \equiv -1 \mod 2^2.$$

Ahora bien, por el Lema 3.0.6, sabemos que si $x \equiv -1 \mod 2^2$, entonces $x \equiv 2^2 - 1 \mod 2^3$. De manera que podemos formar un sistema de congruencias de la siguiente manera:

$$\begin{aligned} x &\equiv -1 \mod 3 \\ x &\equiv 0 \mod 5 \\ x &\equiv 2^2 - 1 \mod 2^3. \end{aligned}$$

Notemos que $3, 5$ y 2^3 son primos relativos por pares, por lo que, por el Teorema Chino del Residuo, tenemos que existe una única solución módulo $2^3 \cdot 3 \cdot 5 = 120$. Resolviendo el sistema de congruencias tenemos que $x = 35$ satisface cada una de las congruencias del sistema.

Ahora bien, veamos que $(35)^3 = 42875$ y $42875 \equiv 35 \mod 120$, de manera que, efectivamente, $x = 35$ tiene un lazo en $\Gamma(120)$.

El ejemplo anterior nos da la idea de que podemos asociar de manera biunivoca los lazos de $\Gamma(n)$ con $(s+1)$-adas ordenadas, donde $s+1$ es el número de primos distintos en la descomposición canónica de n tomando en cuenta el factor 2^m, con $m \geq 3$. Lo anterior es cierto y es la idea principal de la demostración del siguiente teorema.

Teorema 3.0.8. *Si n es un número natural no nulo, $p_1, p_2, \ldots, p_s$ son números primos distintos de 2 tales que $p_i < p_{i+1}$ para todo $i \in \{1, \ldots, s-1\}$ y $n = 2^m p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s}$ es la factorización en primos de n con $m \geq 3$, donde $\alpha_i \geq 1$ para todo $i \in \{1, \ldots, s\}$, entonces el número de lazos en $\Gamma(n)$ es $5 \cdot 3^s$.*

Demostración: Sean

$$B = \{x \in V(\Gamma(n)) \backslash \{0, 1, n-1\} : (x, x) \in F(\Gamma(n))\} \text{ y}$$
$$D = \{(\beta_1, \ldots, \beta_{s+1}) : \beta_i \in \{-1, 0, 1\} \text{ para todo } i \in \{1 \ldots, s\} \text{ y } \beta_{s+1} \in \{-2, 1, 0, 1, 2\}\} \setminus$$
$$\{(0, \ldots, 0), (1, \ldots, 1), (-1, \ldots, -1)\}.$$

Notemos que si $x \in B$, entonces $x^3 \equiv x \mod n$, es decir, $n \mid x^3 - x$, equivalentemente $x^3 - x = nk$ para algún $k \in \mathbb{N}$. Por otro lado, sabemos que $x^3 - x = (x-1)(x)(x+1)$, por lo que

$$(x-1)(x)(x+1) = 2^m p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s} k. \tag{3.6}$$

Observemos que $(x-1)(x)(x+1) = 0$, implica que $x - 1 = 0$ o $x = 0$ o $x + 1 = 0$. Como $x \in B$, entonces no es posible que $x - 1 = 0$ y $x = 0$. Además, como $x \geq 0$, entonces no puede ser que $x + 1 = 0$. De lo anterior $k \geq 1$.

De este modo, si $i \in \{1, \ldots, s\}$, entonces $p_i \mid x - 1$ o $p_i \mid x$ o $p_i \mid x + 1$. Asimismo, como para cada $i \in \{1, \ldots, s\}$, $p_i \neq 2$, entonces p_i divide exactamente a uno de los factores $x - 1$, x o $x + 1$. En tal caso para cada $i \in \{1, \ldots, s\}$ se cumple que $p_i^{\alpha_i} \mid x - 1$ o $p_i^{\alpha_i} \mid x$ o $p_i^{\alpha_i} \mid x + 1$ y sólo a uno.

Afirmación 3.0.9. *Si $2^i \mid x - 1$ para algún $i \in \{2, \ldots, m\}$, entonces $2^{m-1} \mid x - 1$ o $2^m \mid x - 1$ y análogamente si $2^i \mid x + 1$ para algún $i \in \{2, \ldots, m\}$, entonces $2^{m-1} \mid x + 1$ o $2^m \mid x + 1$.*

Si $2^i \mid x - 1$ para algún $i \geq 2$, entonces de la Ecuación (3.6) se sigue que $2^{m-i} \mid x + 1$ y como $x - 1$ y $x + 1$ son pares consecutivos, entonces $2^{m-1} \mid x - 1$ o $2^m \mid x - 1$. De manera análoga si $2^i \mid x + 1$, entonces $2^{m-1} \mid x + 1$ o $2^m \mid x + 1$.

Por otro lado, si x es par, entonces $2 \nmid x - 1$ y $2 \nmid x + 1$ y de la Ecuación (3.6), se sigue que $2^m \mid x$. Si x es impar, entonces $x - 1$ y $x + 1$ son pares, por lo que de la Ecuacion (3.6), $2^m \mid (x-1)(x+1)$. Por la Afirmación 3.0.9, tenemos los siguientes casos:

(a) $2 \mid x-1$ y $2^i \nmid x-1$ para todo $i \neq 1$ o (b) $2^{m-1} \mid x-1$ y $2^m \nmid x-1$ o (c) $2^m \mid x-1$, o bien (d) $2 \mid x+1$ y $2^i \nmid x+1$ para todo $i \neq 1$ o (e) $2^{m-1} \mid x+1$ y $2^m \nmid x+1$ o (f) $2^m \mid x+1$. Sin embargo, como $2^m \mid (x-1)(x+1)$, en particular $2^i \mid x-1$ y $2^{m-i} \mid x+1$ para algún $i \in \{0, \ldots, m\}$, entonces el caso (a) y el caso (e) son equivalentes y el caso (b) y (d) también lo son. Dado lo anterior, tenemos solamente los siguientes casos a considerar:

Caso 1. $2^m \mid x$.

Caso 2. $2^{m-1} \mid x-1$ y $2^m \nmid x-1$.

Caso 3. $2^m \mid x-1$.

Caso 4. $2^{m-1} \mid x+1$ y $2^m \nmid x+1$.

Caso 5. $2^m \mid x+1$.

Definimos la relación φ de B en D dada por $(x, (\beta_1, \ldots, \beta_{s+1}))$ donde para cada $i \in \{1, \ldots, s\}$:

$$\beta_i = \begin{cases} -1 & \text{si} \quad p_i^{\alpha_i} \mid x-1 \\ 0 & \text{si} \quad p_i^{\alpha_i} \mid x \\ 1 & \text{si} \quad p_i^{\alpha_i} \mid x+1 \end{cases}$$

y para $i = s+1$

$$\beta_i = \begin{cases} -2 & \text{si} \quad 2^{m-1} \mid x-1 \quad \text{y} \quad 2^m \nmid x-1 \\ -1 & \text{si} \quad 2^m \mid x-1 \\ 0 & \text{si} \quad 2^m \mid x \\ 1 & \text{si} \quad 2^m \mid x+1 \\ 2 & \text{si} \quad 2^{m-1} \mid x+1 \quad \text{y} \quad 2^m \nmid x+1. \end{cases}$$

Afirmación 1. φ es una función de B en D.

Primero demostraremos que $Dom(\varphi) = B$. Claramente $Dom(\varphi) \subseteq B$. Por otro lado, si $x \in B$ entonces $x^3 \equiv x \mod n$, por lo que $n \mid x^3 - x$. Podemos ver que cada $p_i^{\alpha_i} \mid x-1$ o $p_i^{\alpha_i} \mid x$ o $p_i^{\alpha_i} \mid x+1$, por lo que, existe β_i para todo $i \in \{1, \ldots, s\}$; además, $2^m \mid x-1$ o $2^m \mid x$ o $2^m \mid x+1$, o $2^{m-1} \mid x-1$ o $2^{m-1} \mid x+1$ de manera que existe β_{s+1}. Dado que $x \notin \{0, 1, n-1\}$, entonces existe $\{i, j\} \subseteq \{1, \ldots, s\}$ tal que $\beta_i \neq \beta_j$, así tenemos que $(\beta_1, \beta_2, \ldots, \beta_{s+1}) \in D$ y es tal que $(x, (\beta_1, \beta_2, \ldots, \beta_{s+1})) \in \varphi$.

Por otro lado, sean $(x_1, (\beta_1, \beta_2, \ldots, \beta_{s+1})) \in \varphi$ y $(x_2, (\gamma_1, \gamma_2, \ldots, \gamma_{s+1})) \in \varphi$ y $x_1 = x_2$, demostremos que $(\beta_1, \ldots, \beta_{s+1}) = (\gamma_1, \ldots, \gamma_{s+1})$.

Observación 3.0.10. *Notemos que si* $\beta_{s+1} = -2$, *entonces* $2^{m-1} \mid x_1 - 1$ *y dado que* $x_1 = x_2$, *se tiene que* $2^{m-1} \mid x-1$ *por lo que,* $\gamma_{s+1} = \beta_{s+1}$.

Si $\beta_{s+1} = -1$, *entonces* $2^m \mid x_1 - 1$ *y dado que* $x_1 = x_2$, *se tiene que* $2^m \mid x_2 - 1$ *por lo que,* $\gamma_{s+1} = \beta_{s+1}$.

Si $\beta_{s+1} = 0$, *entonces* $2^m \mid x_1$ *y dado que* $x_1 = x_2$, *se tiene que* $2^m \mid x_2$ *por lo que,* $\gamma_{s+1} = \beta_{s+1}$.

Si $\beta_{s+1} = 1$, *entonces* $2^m \mid x+1$ *y dado que* $x_1 = x_2$, *se tiene que* $2^m \mid x_2+1$ *por lo que,* $\gamma_{s+1} = \beta_{s+1}$.

Si $\beta_{s+1} = 2$, *entonces* $2^{m-1} \mid x_1+1$ *y dado que* $x_1 = x_2$, *se tiene que* $2^{m-1} \mid x_2+1$ *por lo que,* $\gamma_{s+1} = \beta_{s+1}$.

Sea $i \in \{1, \ldots, s\}$, consideremos los siguientes casos:

Caso 1. $\beta_i = -1$.

Como $\beta_i = -1$, entonces $p_i^{\alpha_i} \mid x_1 - 1$ y dado que $x_1 - 1 = x_2 - 1$ se tiene que $p_i^{\alpha_i} \mid x_2 - 1$. Por lo tanto $\gamma_i = \beta_i$.

Caso 2. $\beta_i = 0$.

Como $\beta_i = 0$, entonces $p_i^{\alpha_i} \mid x_1$ y dado que $x_1 = x_2$ se tiene que $p_i^{\alpha_i} \mid x_2$. Por lo tanto $\gamma_i = \beta_1$.

Caso 3. $\beta_i = 1$.

Como $\beta_i = 1$, entonces $p_i^{\alpha_i} \mid x_1 + 1$ y dado que $x_1 + 1 = x_2 + 1$ se tiene que $p_i^{\alpha_i} \mid x_2 + 1$. Por lo tanto $\gamma_i = \beta_i$.

Dado lo anterior, si $x_1 = x_2$, entonces $(\beta_1, \ldots, \beta_{s+1}) = (\gamma_1, \ldots, \gamma_{s+1})$. Podemos concluir que φ es función.

Afirmación 2. φ es una función inyectiva.

Sea $\{x_1, x_2\} \subseteq B$ tal que $\varphi(x_1) = \varphi(x_2)$. Veamos que $x_1 = x_2$.

Supongamos que $\varphi(x_1) = (\beta_1, \ldots, \beta_{s+1})$ y definimos

$$I_1 = \{i \in \{1, \ldots, s\} : \beta_i = -1\},$$
$$I_2 = \{i \in \{1, \ldots, s\} : \beta_i = 0\}, \text{ y}$$
$$I_3 = \{i \in \{1, \ldots, s\} : \beta_i = 1\}.$$

Notemos que como $(\beta_1, \ldots, \beta_{s+1}) \notin \{(0, \ldots, 0), (1, \ldots, 1), (-1, \ldots, -1)\}$, entonces al menos dos de los conjuntos I_1, I_2, I_3 son no vacíos. Para cada $j \in \{1, 2, 3\}$, si $I_j \neq \emptyset$ definimos:

$$q_j = \prod_{i \in I_j} p_i^{\alpha_i}.$$

Procederemos con los siguientes casos:

Caso 1: $I_1 \neq \emptyset$, $I_2 \neq \emptyset$ e $I_3 = \emptyset$.

En este caso observemos que:

$$p_i^{\alpha_i} \mid x_1 - 1 \text{ y } p_i^{\alpha_i} \mid x_2 - 1 \text{ para todo } i \in I_1, \text{ y}$$
$$p_i^{\alpha_i} \mid x_1 \text{ y } p_i^{\alpha_i} \mid x_2 \text{ para todo } i \in I_2.$$

Por lo que:

$$\begin{array}{ccc} x_1 - 1 = q_1 k & & x_2 - 1 = q_1 k' \\ x_1 = q_2 l & \text{y} & x_2 = q_2 l'. \end{array}$$

Además, notemos los siguientes casos de acuerdo a β_{s+1}:

Caso 1. Si $\beta_{s+1} = -2$, entonces $2^{m-1} \mid x_1 - 1$ y $2^{m-1} \mid x_2 - 1$, es decir, $x_1 \equiv 1 \mod 2^{m-1}$ y $x_2 \equiv 1 \mod 2^{m-1}$. Por el Lema 3.0.6 se sigue que $x_1 \equiv 2^{m-1} + 1 \mod 2^m$ y $x_2 \equiv 2^{m-1} + 1 \mod 2^m$.

Caso 2. Si $\beta_{s+1} = -1$, entonces $2^m \mid x_1 - 1$ y $2^m \mid x_2 - 1$, en particular $x_1 \equiv 1 \mod 2^m$ y $x_2 \equiv 1 \mod 2^m$.

Caso 3. Si $\beta_{s+1} = 0$, entonces $2^m \mid x_1$ y $2^m \mid x_2$, en particular $x_1 \equiv 0 \mod 2^m$ y $x_2 \equiv 0 \mod 2^m$.

Caso 4. Si $\beta_{s+1} = 1$, entonces $2^m \mid x_1 + 1$ y $2^m \mid x_2 + 1$, en particular $x_1 \equiv -1 \mod 2^m$ y $x_2 \equiv -1 \mod 2^m$.

Caso 5. Si $\beta_{s+1} = 2$, entonces $2^{m-1} \mid x_1 + 1$ y $2^{m-1} \mid x_2 + 1$, es decir, $x_1 \equiv -1 \mod 2^{m-1}$ y $x_2 \equiv -1 \mod 2^{m-1}$. Por el Lema 3.0.6 se sigue que $x_1 \equiv 2^{m-1} - 1 \mod 2^m$ y $x_2 \equiv 2^{m-1} - 1 \mod 2^m$.

Así, podemos obtener los siguientes sistemas de congruencias:

Para el caso 1:

$$\begin{cases} x_1 \equiv 1 \mod q_1 \\ x_1 \equiv 0 \mod q_2 \\ x_1 \equiv 2^{m-1} + 1 \mod 2^m \end{cases} \quad \text{y} \quad \begin{cases} x_2 \equiv 1 \mod q_1 \\ x_2 \equiv 0 \mod q_2 \\ x_2 \equiv 2^{m-1} + 1 \mod 2^m \end{cases}$$

ó en el caso 2:

$$\begin{cases} x_1 \equiv 1 \mod q_1 \\ x_1 \equiv 0 \mod q_2 \\ x_1 \equiv 1 \mod 2^m \end{cases} \quad \text{y} \quad \begin{cases} x_2 \equiv 1 \mod q_1 \\ x_2 \equiv 0 \mod q_2 \\ x_2 \equiv 1 \mod 2^m \end{cases}$$

ó en el caso 3:

$$\begin{cases} x_1 \equiv 1 \mod q_1 \\ x_1 \equiv 0 \mod q_2 \\ x_1 \equiv 0 \mod 2^m \end{cases} \quad \text{y} \quad \begin{cases} x_2 \equiv 1 \mod q_1 \\ x_2 \equiv 0 \mod q_2 \\ x_2 \equiv 0 \mod 2^m \end{cases}$$

ó en el caso 4:

$$\begin{cases} x_1 \equiv 1 \mod q_1 \\ x_1 \equiv 0 \mod q_2 \\ x_1 \equiv -1 \mod 2^m \end{cases} \text{ y } \begin{cases} x_2 \equiv 1 \mod q_1 \\ x_2 \equiv 0 \mod q_2 \\ x_2 \equiv -1 \mod 2^m \end{cases}$$

ó en el caso 5:

$$\begin{cases} x_1 \equiv 1 \mod q_1 \\ x_1 \equiv 0 \mod q_2 \\ x_1 \equiv 2^{m-1} - 1 \mod 2^m \end{cases} \text{ y } \begin{cases} x_2 \equiv 1 \mod q_1 \\ x_2 \equiv 0 \mod q_2 \\ x_2 \equiv 2^{m-1} - 1 \mod 2^m. \end{cases}$$

Ahora bien, podemos ver que q_1, q_2 y 2^m son primos relativos por pares, por lo que, en cualquiera de los casos anteriores, por el Teorema Chino del Residuo, los sistemas de congruencias tienen una única solución módulo $2^m q_1 q_2 = n$. Concluyendo que, para cualquiera de los sistemas, $x_1 = x_2$.

Caso 2: $I_2 \neq \emptyset$, $I_3 \neq \emptyset$ e $I_1 = \emptyset$.

En este caso observemos que:

$$p_i^{\alpha_i} \mid x_1 \text{ y } p_i^{\alpha_i} \mid x_2 \text{ para todo } i \in I_2, \text{ y}$$
$$p_i^{\alpha_i} \mid x_1 + 1 \text{ y } p_i^{\alpha_i} \mid x_2 + 1 \text{ para todo } i \in I_3.$$

Por lo que:

$$\begin{matrix} x_1 = q_2 l \\ x_1 + 1 = q_3 t \end{matrix} \text{ y } \begin{matrix} x_2 = q_2 l' \\ x_2 + 1 = q_3 t'. \end{matrix}$$

Además, notemos los siguientes casos de acuerdo a β_{s+1}:

Caso 1. Si $\beta_{s+1} = -2$, entonces $2^{m-1} \mid x_1 - 1$ y $2^{m-1} \mid x_2 - 1$, es decir, $x_1 \equiv 1 \mod 2^{m-1}$ y $x_2 \equiv 1 \mod 2^{m-1}$. Por el Lema 3.0.6 se sigue que $x_1 \equiv 2^{m-1} + 1 \mod 2^m$ y $x_2 \equiv 2^{m-1} + 1 \mod 2^m$.

Caso 2. Si $\beta_{s+1} = -1$, entonces $2^m \mid x_1 - 1$ y $2^m \mid x_2 - 1$, en particular $x_1 \equiv 1 \mod 2^m$ y $x_2 \equiv 1 \mod 2^m$.

Caso 3. Si $\beta_{s+1} = 0$, entonces $2^m \mid x_1$ y $2^m \mid x_2$, en particular $x_1 \equiv 0 \mod 2^m$ y $x_2 \equiv 0 \mod 2^m$.

Caso 4. Si $\beta_{s+1} = 1$, entonces $2^m \mid x_1 + 1$ y $2^m \mid x_2 + 1$, en particular $x_1 \equiv -1 \mod 2^m$ y $x_2 \equiv -1 \mod 2^m$.

Caso 5. Si $\beta_{s+1} = 2$, entonces $2^{m-1} \mid x_1 + 1$ y $2^{m-1} \mid x_2 + 1$, es decir, $x_1 \equiv -1 \mod 2^{m-1}$ y $x_2 \equiv -1 \mod 2^{m-1}$. Por el Lema 3.0.6 se sigue que $x_1 \equiv 2^{m-1} - 1 \mod 2^m$ y $x_2 \equiv 2^{m-1} - 1 \mod 2^m$.

Así, podemos obtener los siguientes sistemas de congruencias:

Para el caso 1:

$$\begin{cases} x_1 \equiv 0 \mod q_2 \\ x_1 \equiv -1 \mod q_3 \\ x_1 \equiv 2^{m-1}+1 \mod 2^m \end{cases} \text{ y } \begin{cases} x_2 \equiv 0 \mod q_2 \\ x_2 \equiv -1 \mod q_3 \\ x_2 \equiv 2^{m-1}+1 \mod 2^m \end{cases}$$

ó para el caso 2:

$$\begin{cases} x_1 \equiv 0 \mod q_2 \\ x_1 \equiv -1 \mod q_3 \\ x_1 \equiv 1 \mod 2^m \end{cases} \text{ y } \begin{cases} x_2 \equiv 0 \mod q_2 \\ x_2 \equiv -1 \mod q_3 \\ x_2 \equiv 1 \mod 2^m \end{cases}$$

ó para el caso 3:

$$\begin{cases} x_1 \equiv 0 \mod q_2 \\ x_1 \equiv -1 \mod q_3 \\ x_1 \equiv 0 \mod 2^m \end{cases} \text{ y } \begin{cases} x_2 \equiv 0 \mod q_2 \\ x_2 \equiv -1 \mod q_3 \\ x_2 \equiv 0 \mod 2^m \end{cases}$$

ó para el caso 4:

$$\begin{cases} x_1 \equiv 0 \mod q_2 \\ x_1 \equiv -1 \mod q_3 \\ x_1 \equiv -1 \mod 2^m \end{cases} \text{ y } \begin{cases} x_2 \equiv 0 \mod q_2 \\ x_2 \equiv -1 \mod q_3 \\ x_2 \equiv -1 \mod 2^m \end{cases}$$

ó para el caso 5:

$$\begin{cases} x_1 \equiv 0 \mod q_2 \\ x_1 \equiv -1 \mod q_3 \\ x_1 \equiv 2^{m-1}-1 \mod 2^m \end{cases} \text{ y } \begin{cases} x_2 \equiv 0 \mod q_2 \\ x_2 \equiv -1 \mod q_3 \\ x_2 \equiv 2^{m-1}-1 \mod 2^m. \end{cases}$$

Ahora bien, podemos ver que q_2, q_3 y 2^m son primos relativos por pares, por lo que, en cualquiera de los casos anteriores, por el Teorema Chino del Residuo, los sistemas de congruencias tienen una única solución módulo $2^m q_2 q_3 = n$. Concluyendo que, para cualquiera de los dos sistemas, $x_1 = x_2$.

Caso 3: $I_1 \neq \emptyset$, $I_3 \neq \emptyset$ e $I_2 = \emptyset$.

En este caso observemos que:

$$p_i^{\alpha_i} \mid x_1 - 1 \text{ y } p_i^{\alpha_i} \mid x_2 - 1 \text{ para todo } i \in I_1, \text{ y}$$
$$p_i^{\alpha_i} \mid x_1 + 1 \text{ y } p_i^{\alpha_i} \mid x_2 + 1 \text{ para todo } i \in I_3.$$

Por lo que:

$$\begin{array}{ccc} x_1 - 1 = q_1 k & & x_2 - 1 = q_1 k' \\ x_1 + 1 = q_3 t & \text{y} & x_2 + 1 = q_3 t'. \end{array}$$

Además, notemos los siguientes casos de acuerdo a β_{s+1}:

Caso 1. Si $\beta_{s+1} = -2$, entonces $2^{m-1} \mid x_1 - 1$ y $2^{m-1} \mid x_2 - 1$, es decir, $x_1 \equiv 1 \mod 2^{m-1}$ y $x_2 \equiv 1 \mod 2^{m-1}$. Por el Lema 3.0.6 se sigue que $x_1 \equiv 2^{m-1} + 1 \mod 2^m$ y $x_2 \equiv 2^{m-1} + 1 \mod 2^m$.

Caso 2. Si $\beta_{s+1} = -1$, entonces $2^m \mid x_1 - 1$ y $2^m \mid x_2 - 1$, en particular $x_1 \equiv 1 \mod 2^m$ y $x_2 \equiv 1 \mod 2^m$.

Caso 3. Si $\beta_{s+1} = 0$, entonces $2^m \mid x_1$ y $2^m \mid x_2$, en particular $x_1 \equiv 0 \mod 2^m$ y $x_2 \equiv 0 \mod 2^m$.

Caso 4. Si $\beta_{s+1} = 1$, entonces $2^m \mid x_1 + 1$ y $2^m \mid x_2 + 1$, en particular $x_1 \equiv -1 \mod 2^m$ y $x_2 \equiv -1 \mod 2^m$.

Caso 5. Si $\beta_{s+1} = 2$, entonces $2^{m-1} \mid x_1 + 1$ y $2^{m-1} \mid x_2 + 1$, es decir, $x_1 \equiv -1 \mod 2^{m-1}$ y $x_2 \equiv -1 \mod 2^{m-1}$. Por el Lema 3.0.6 se sigue que $x_1 \equiv 2^{m-1} - 1 \mod 2^m$ y $x_2 \equiv 2^{m-1} - 1 \mod 2^m$.

Así, podemos obtener los siguientes sistemas de congruencias:

Para el caso 1:

$$\begin{cases} x_1 \equiv 1 \mod q_1 \\ x_1 \equiv -1 \mod q_3 \\ x_1 \equiv 2^{m-1} + 1 \mod 2^m \end{cases} \text{ y } \begin{cases} x_2 \equiv 1 \mod q_1 \\ x_2 \equiv -1 \mod q_3 \\ x_2 \equiv 2^{m-1} + 1 \mod 2^m \end{cases}$$

ó para el caso 2:

$$\begin{cases} x_1 \equiv 1 \mod q_1 \\ x_1 \equiv -1 \mod q_3 \\ x_1 \equiv 1 \mod 2^m \end{cases} \text{ y } \begin{cases} x_2 \equiv 1 \mod q_1 \\ x_2 \equiv -1 \mod q_3 \\ x_2 \equiv 1 \mod 2^m \end{cases}$$

ó para el caso 3:

$$\begin{cases} x_1 \equiv 1 \mod q_1 \\ x_1 \equiv -1 \mod q_3 \\ x_1 \equiv 0 \mod 2^m \end{cases} \text{ y } \begin{cases} x_2 \equiv 1 \mod q_1 \\ x_2 \equiv -1 \mod q_3 \\ x_2 \equiv 0 \mod 2^m \end{cases}$$

ó para el caso 4:

$$\begin{cases} x_1 \equiv 1 \mod q_1 \\ x_1 \equiv -1 \mod q_3 \\ x_1 \equiv -1 \mod 2^m \end{cases} \text{ y } \begin{cases} x_2 \equiv 1 \mod q_1 \\ x_2 \equiv -1 \mod q_3 \\ x_2 \equiv -1 \mod 2^m \end{cases}$$

ó para el caso 5:

$$\begin{cases} x_1 \equiv 1 \mod q_1 \\ x_1 \equiv -1 \mod q_3 \\ x_1 \equiv 2^{m-1}-1 \mod 2^m \end{cases} \text{ y } \begin{cases} x_2 \equiv 1 \mod q_1 \\ x_2 \equiv -1 \mod q_3 \\ x_2 \equiv 2^{m-1}-1 \mod 2^m. \end{cases}$$

Ahora bien, podemos ver que q_1, q_3 y 2^m son primos relativos por pares, por lo que, en cualquiera de los casos anteriores, por el Teorema Chino del Residuo, los sistemas de congruencias tienen una única solución módulo $2^m q_1 q_3 = n$. Concluyendo que, para cualquiera de los dos sistemas, $x_1 = x_2$.

Caso 4: $I_1 \neq \emptyset$, $I_2 \neq \emptyset$ e $I_3 \neq \emptyset$.

En este caso observemos que:

$$\begin{gathered} p_i^{\alpha_i} \mid x_1 - 1 \text{ y } p_i^{\alpha_i} \mid x_2 - 1 \text{ para todo } i \in I_1, \\ p_i^{\alpha_i} \mid x_1 \text{ y } p_i^{\alpha_i} \mid x_2 \text{ para todo } i \in I_2, \text{ y} \\ p_i^{\alpha_i} \mid x_1 + 1 \text{ y } p_i^{\alpha_i} \mid x_2 + 1 \text{ para todo } i \in I_3. \end{gathered}$$

Por lo que:

$$\begin{array}{ccc} x_1 - 1 = q_1 k & & x_2 - 1 = q_1 k' \\ x_1 = q_2 l & \text{y} & x_2 = q_2 l' \\ x_1 + 1 = q_3 t & & x_2 + 1 = q_3 t'. \end{array}$$

Además, notemos los siguientes casos de acuerdo a β_{s+1}:

Caso 1. Si $\beta_{s+1} = -2$, entonces $2^{m-1} \mid x_1 - 1$ y $2^{m-1} \mid x_2 - 1$, es decir, $x_1 \equiv 1 \mod 2^{m-1}$ y $x_2 \equiv 1 \mod 2^{m-1}$. Por el Lema 3.0.6 se sigue que $x_1 \equiv 2^{m-1} + 1 \mod 2^m$ y $x_2 \equiv 2^{m-1} + 1 \mod 2^m$.

Caso 2. Si $\beta_{s+1} = -1$, entonces $2^m \mid x_1 - 1$ y $2^m \mid x_2 - 1$, en particular $x_1 \equiv 1 \mod 2^m$ y $x_2 \equiv 1 \mod 2^m$.

Caso 3. Si $\beta_{s+1} = 0$, entonces $2^m \mid x_1$ y $2^m \mid x_2$, en particular $x_1 \equiv 0 \mod 2^m$ y $x_2 \equiv 0 \mod 2^m$.

Caso 4. Si $\beta_{s+1} = 1$, entonces $2^m \mid x_1 + 1$ y $2^m \mid x_2 + 1$, en particular $x_1 \equiv -1 \mod 2^m$ y $x_2 \equiv -1 \mod 2^m$.

Caso 5. Si $\beta_{s+1} = 2$, entonces $2^{m-1} \mid x_1 + 1$ y $2^{m-1} \mid x_2 + 1$, es decir, $x_1 \equiv -1 \mod 2^{m-1}$ y $x_2 \equiv -1 \mod 2^{m-1}$. Por el Lema 3.0.6 se sigue que $x_1 \equiv 2^{m-1} - 1 \mod 2^m$ y $x_2 \equiv 2^{m-1} - 1 \mod 2^m$.

Así, podemos obtener los siguientes sistemas de congruencias:

Para el caso 1:

$$\begin{cases} x_1 \equiv 1 \mod q_1 \\ x_1 \equiv 0 \mod q_2 \\ x_1 \equiv -1 \mod q_3 \\ x_1 \equiv 2^{m-1} + 1 \mod 2^m \end{cases} \text{ y } \begin{cases} x_2 \equiv 1 \mod q_1 \\ x_2 \equiv 0 \mod q_2 \\ x_2 \equiv -1 \mod q_3 \\ x_2 \equiv 2^{m-1} + 1 \mod 2^m \end{cases}$$

ó para el caso 2:

$$\begin{cases} x_1 \equiv 1 \mod q_1 \\ x_1 \equiv 0 \mod q_2 \\ x_1 \equiv -1 \mod q_3 \\ x_1 \equiv 1 \mod 2^m \end{cases} \text{ y } \begin{cases} x_2 \equiv 1 \mod q_1 \\ x_2 \equiv 0 \mod q_2 \\ x_2 \equiv -1 \mod q_3 \\ x_2 \equiv 1 \mod 2^m \end{cases}$$

ó para el caso 3:

$$\begin{cases} x_1 \equiv 1 \mod q_1 \\ x_1 \equiv 0 \mod q_2 \\ x_1 \equiv -1 \mod q_3 \\ x_1 \equiv 0 \mod 2^2 \end{cases} \text{ y } \begin{cases} x_2 \equiv 1 \mod q_1 \\ x_2 \equiv 0 \mod q_2 \\ x_2 \equiv -1 \mod q_3 \\ x_2 \equiv 0 \mod 2^2 \end{cases}$$

ó para el caso 4:

$$\begin{cases} x_1 \equiv 1 \mod q_1 \\ x_1 \equiv 0 \mod q_2 \\ x_1 \equiv -1 \mod q_3 \\ x_1 \equiv -1 \mod 2^m \end{cases} \text{ y } \begin{cases} x_2 \equiv 1 \mod q_1 \\ x_2 \equiv 0 \mod q_2 \\ x_2 \equiv -1 \mod q_3 \\ x_2 \equiv -1 \mod 2^m \end{cases}$$

ó para el caso 5:

$$\begin{cases} x_1 \equiv 1 \mod q_1 \\ x_1 \equiv 0 \mod q_2 \\ x_1 \equiv -1 \mod q_3 \\ x_1 \equiv 2^{m-1} - 1 \mod 2^m \end{cases} \text{ y } \begin{cases} x_2 \equiv 1 \mod q_1 \\ x_2 \equiv 0 \mod q_2 \\ x_2 \equiv -1 \mod q_3 \\ x_2 \equiv 2^{m-1} - 1 \mod 2^m. \end{cases}$$

Ahora bien, podemos ver que q_1, q_2, q_3 y 2^m son primos relativos por pares, por lo que, en cualquiera de los casos anteriores, por el Teorema Chino del Residuo, los sistemas de congruencias anteriores tienen una única solución módulo $2^m q_1 q_2 q_3 = n$. Concluyendo que, para cualquiera de los dos sistemas, $x_1 = x_2$.

Dados los casos anteriores, podemos concluir que μ es una función inyectiva.

Afirmación 3. φ es una función suprayectiva.

Sea $(\beta_1, \beta_2, \ldots, \beta_{s+1}) \in D$, demostremos que existe $x \in B$ tal que $\varphi(x) = (\beta_1, \beta_2, \ldots, \beta_{s+1})$.

Definamos

$$I_1 = \{i \in \{1, \ldots, s\} : \beta_i = -1\},$$
$$I_2 = \{i \in \{1, \ldots, s\} : \beta_i = 0\}, \text{ y}$$
$$I_3 = \{i \in \{1, \ldots, s\} : \beta_i = 1\}.$$

Notemos que como $(\beta_1, \ldots, \beta_{s+1}) \notin \{(0, \ldots, 0), (1, \ldots, 1), (-1, \ldots, -1)\}$, entonces al menos dos de los conjuntos I_1, I_2, I_3 son no vacíos. Para cada $j \in \{1, 2, 3\}$, si $I_j \neq \emptyset$ definimos:

$$q_j = \prod_{i \in I_j} p_i^{\alpha_i}.$$

Procederemos con los siguientes casos:

Caso 1: $I_1 \neq \emptyset$, $I_2 \neq \emptyset$ e $I_3 = \emptyset$.

En este caso consideremos los siguientes sistemas de congruencias:

$$(1) \begin{cases} x \equiv 1 \mod q_1 \\ x \equiv 0 \mod q_2 \\ x \equiv 2^{m-1} + 1 \mod 2^m \end{cases} \quad \text{y} \quad (2) \begin{cases} x \equiv 1 \mod q_1 \\ x \equiv 0 \mod q_2 \\ x \equiv 1 \mod 2^m \end{cases} \quad \text{y} \quad (3) \begin{cases} x \equiv 1 \mod q_1 \\ x \equiv 0 \mod q_2 \\ x \equiv 0 \mod 2^m \end{cases}$$

$$\text{y} \quad (4) \begin{cases} x \equiv 1 \mod q_1 \\ x \equiv 0 \mod q_2 \\ x \equiv -1 \mod 2^m \end{cases} \quad \text{y} \quad (5) \begin{cases} x \equiv 1 \mod q_1 \\ x \equiv 0 \mod q_2 \\ x \equiv 2^{m-1} - 1 \mod 2^m. \end{cases}$$

Podemos ver que q_1, q_2 y 2^m son primos relativos por pares y por el Teorema Chino del Residuo, los sistemas (1), (2), (3), (4) y (5) tienen solución módulo $2^m q_1 q_2 = n$, digamos z y así:

- Para (1):
  Notemos que como $z \equiv 2^{m-1} + 1 \mod 2^m$, entonces por el Lema 3.0.7, tenemos que $z \equiv 1 \mod 2^{m-1}$ y $z \not\equiv 1 \mod 2^m$, por lo que, $2^{m-1} \mid z - 1$ y $2^m \nmid z - 1$.
  Por otro lado, podemos ver que $q_1 \mid z - 1$, $q_2 \mid z$ y $2^{m-1} \mid z - 1$, de manera que $2^{m-1} q_1 q_2 \mid (z-1)(z)$. Además, como $2^{m-1} \mid z - 1$, entonces $2 \mid z + 1$, por lo que, $2^m q_1 q_2 \mid (z-1)(z)(z+1)$, esto es, $n \mid (z-1)(z)(z+1)$.

- Para (2):
  $q_1 \mid z-1$, $q_2 \mid z$ y $2^m \mid z-1$, de manera que $2^m q_1 q_2 \mid (z-1)(z)$, en particular, $n \mid (z-1)(z)(z+1)$.
- Para (3):
  $q_1 \mid z-1$, $q_2 \mid z$ y $2^m \mid z$, de manera que $2^m q_1 q_2 \mid (z-1)(z)$, en particular, $n \mid (z-1)(z)(z+1)$.
- Para (4):
  $q_1 \mid z-1$, $q_2 \mid z$ y $2^m \mid z+1$, de manera que $2^m q_1 q_2 \mid (z-1)(z)(z+1)$, es decir, $n \mid (z-1)(z)(z+1)$.
- Para (5):
  Notemos que como $z \equiv 2^{m-1} - 1 \mod 2^m$, entonces por el Lema 3.0.7, tenemos que $z \equiv -1 \mod 2^{m-1}$ y $z \not\equiv -1 \mod 2^m$, por lo que, $2^{m-1} \mid z+1$ y $2^m \nmid z+1$.
  Por otro lado, podemos ver que $q_1 \mid z-1$, $q_2 \mid z$ y $2^{m-1} \mid z+1$, de manera que $2^{m-1} q_1 q_2 \mid (z-1)(z)(z+1)$. Además, como $2^{m-1} \mid z+1$, entonces $2 \mid z-1$, por lo que, $2^m q_1 q_2 \mid (z-1)(z)(z+1)$, esto es, $n \mid (z-1)(z)(z+1)$.

En cualquiera de los casos anteriores $n \mid z^3 - z$, esto es, $z^3 \equiv z \mod n$, por lo que, en z hay un lazo de $\Gamma(n)$. Además, como $(\beta_1, \ldots, \beta_{s+1}) \notin \{(0, \ldots, 0), (1, \ldots, 1), (-1, \ldots, -1)\}$, entonces $z \notin \{0, 1, n-1\}$, es decir, $z \in Dom(\varphi)$. Se sigue, de la elección de z, que $\varphi(z) = (\beta_1, \ldots, \beta_{s+1})$.

Caso 2: $I_2 \neq \emptyset$, $I_3 \neq \emptyset$ e $I_1 = \emptyset$.

En este caso consideremos el siguiente sistema de congruencias:

$$(1)\begin{cases} x \equiv 0 \mod q_2 \\ x \equiv -1 \mod q_3 \\ x \equiv 2^{m-1}+1 \mod 2^m \end{cases} \text{ y } (2)\begin{cases} x \equiv 0 \mod q_2 \\ x \equiv -1 \mod q_3 \\ x \equiv 1 \mod 2^m \end{cases} \text{ y } (3)\begin{cases} x \equiv 0 \mod q_2 \\ x \equiv -1 \mod q_3 \\ x \equiv 0 \mod 2^m \end{cases}$$

$$\text{y } (4)\begin{cases} x \equiv 0 \mod q_2 \\ x \equiv -1 \mod q_3 \\ x \equiv -1 \mod 2^m \end{cases} \text{ y } (5)\begin{cases} x \equiv 0 \mod q_2 \\ x \equiv -1 \mod q_3 \\ x \equiv 2^{m-1}-1 \mod 2^m. \end{cases}$$

Podemos ver que q_2, q_3 y 2^m son primos relativos por pares y por el Teorema Chino del Residuo, los sistemas (1), (2), (3), (4) y (5) tienen solución módulo $2^m q_2 q_3 = n$, digamos z y así:

- Para (1):
  Notemos que como $z \equiv 2^{m-1} + 1 \mod 2^m$, entonces por el Lema 3.0.7, tenemos que $z \equiv 1 \mod 2^{m-1}$ y $z \not\equiv 1 \mod 2^m$, por lo que, $2^{m-1} \mid z-1$ y $2^m \nmid z-1$.
  Por otro lado, podemos ver que $q_2 \mid z$, $q_3 \mid z+1$ y $2^{m-1} \mid z-1$, de manera que $2^{m-1} q_2 q_3 \mid (z-1)(z)(z+1)$. Además, como $2^{m-1} \mid z-1$, entonces $2 \mid z+1$, por lo que, $2^m q_2 q_3 \mid (z-1)(z)(z+1)$, esto es, $n \mid (z-1)(z)(z+1)$.
- Para (2):
  $q_2 \mid z$, $q_3 \mid z+1$ y $2^m \mid z-1$, de manera que $2^m q_1 q_2 \mid (z-1)(z)(z+1)$, es decir, $n \mid (z-1)(z)(z+1)$.

- Para (3)
  $q_2 \mid z$, $q_3 \mid z+1$ y $2^m \mid z$, de manera que $2^m q_1 q_2 \mid (z)(z+1)$, en particular, $n \mid (z-1)(z)(z+1)$.
- Para (4)
  $q_2 \mid z$, $q_3 \mid z+1$ y $2^m \mid z+1$, de manera que $2^m q_1 q_2 \mid (z)(z+1)$, en particular, $n \mid (z-1)(z)(z+1)$.
- Para (5):
  Notemos que como $z \equiv 2^{m-1} - 1 \mod 2^m$, entonces por el Lema 3.0.7, tenemos que $z \equiv -1 \mod 2^{m-1}$ y $z \not\equiv -1 \mod 2^m$, por lo que, $2^{m-1} \mid z+1$ y $2^m \nmid z+1$.
  Por otro lado, podemos ver que $q_2 \mid z$, $q_3 \mid z+1$ y $2^{m-1} \mid z+1$, de manera que $2^{m-1} q_2 q_3 \mid (z)(z+1)$. Además, como $2^{m-1} \mid z+1$, entonces $2 \mid z-1$, por lo que, $2^m q_2 q_3 \mid (z-1)(z)(z+1)$, esto es, $n \mid (z-1)(z)(z+1)$.

En cualquiera de los casos anteriores $n \mid z^3 - z$, esto es, $z^3 \equiv z \mod n$, por lo que, en z hay un lazo de $\Gamma(n)$. Además, como $(\beta_1, \ldots, \beta_{s+1}) \notin \{(0,\ldots,0),(1,\ldots,1),(-1,\ldots,-1)\}$, entonces $z \notin \{0, 1, n-1\}$, es decir, $z \in Dom(\varphi)$. Se sigue, de la elección de z, que $\varphi(z) = (\beta_1, \ldots, \beta_{s+1})$.

Caso 3: $I_1 \neq \emptyset$, $I_3 \neq \emptyset$ e $I_2 = \emptyset$.

En este caso consideremos el siguiente sistema de congruencias:

$$(1)\begin{cases} x \equiv 1 \mod q_1 \\ x \equiv -1 \mod q_3 \\ x \equiv 2^{m-1}+1 \mod 2^m \end{cases} \text{ y } (2)\begin{cases} x \equiv 1 \mod q_1 \\ x \equiv -1 \mod q_3 \\ x \equiv 1 \mod 2^m \end{cases} \text{ y } (3)\begin{cases} x \equiv 1 \mod q_1 \\ x \equiv -1 \mod q_3 \\ x \equiv 0 \mod 2^m \end{cases}$$

$$\text{y } (4)\begin{cases} x \equiv 1 \mod q_1 \\ x \equiv -1 \mod q_3 \\ x \equiv -1 \mod 2^m \end{cases} \text{ y } (5)\begin{cases} x \equiv 1 \mod q_1 \\ x \equiv -1 \mod q_3 \\ x \equiv 2^{m-1}-1 \mod 2^m. \end{cases}$$

Podemos ver que q_1, q_3 y 2^m son primos relativos y por el Teorema Chino del Residuo, los sistemas (1), (2), (3), (4) y (5) tienen solución módulo $2^m q_1 q_3 = n$, digamos z y así:

- Para (1):
  Notemos que como $z \equiv 2^{m-1} + 1 \mod 2^m$, entonces por el Lema 3.0.7, tenemos que $z \equiv 1 \mod 2^{m-1}$ y $z \not\equiv 1 \mod 2^m$, por lo que, $2^{m-1} \mid z-1$ y $2^m \nmid z-1$.
  Por otro lado, podemos ver $q_1 \mid z-1$, $q_3 \mid z+1$ y $2^{m-1} \mid z-1$, de manera que $2^{m-1} q_1 q_3 \mid (z-1)(z+1)$. Además, como $2^{m-1} \mid z-1$, entonces $2 \mid z+1$, por lo que, $2^m q_2 q_3 \mid (z-1)(z+1)$, en particular, $n \mid (z-1)(z)(z+1)$.
- Para (2):
  $q_1 \mid z-1$, $q_3 \mid z+1$ y $2^m \mid z-1$, de manera que $2^m q_1 q_3 \mid (z-1)(z+1)$, en particular, $n \mid (z-1)(z)(z+1)$.
- Para (3):
  $q_1 \mid z-1$, $q_3 \mid z+1$ y $2^m \mid z$, de manera que $2^m q_1 q_3 \mid (z-1)(z)(z+1)$, es decir, $n \mid (z-1)(z)(z+1)$.

- Para (4):
  $q_1 \mid z-1$, $q_3 \mid z+1$ y $2^m \mid z+1$, de manera que $2^m q_1 q_3 \mid (z-1)(z+1)$, en particular, $n \mid (z-1)(z)(z+1)$.
- Para (5):
  Notemos que como $z \equiv 2^{m-1}-1 \mod 2^m$, entonces por el Lema 3.0.7, tenemos que $z \equiv -1 \mod 2^{m-1}$ y $z \not\equiv -1 \mod 2^m$, por lo que, $2^{m-1} \mid z+1$ y $2^m \nmid z+1$.
  Por otro lado, podemos ver $q_1 \mid z-1$, $q_3 \mid z+1$ y $2^{m-1} \mid z+1$, de manera que $2^{m-1} q_1 q_3 \mid (z-1)(z+1)$. Además, como $2^{m-1} \mid z+1$, entonces $2 \mid z-1$, por lo que, $2^m q_2 q_3 \mid (z-1)(z+1)$, en particular, $n \mid (z-1)(z)(z+1)$.

En cualquiera de los casos anteriores, $n \mid z^3 - z$, esto es, $z^3 \equiv z \mod n$, por lo que, en z hay un lazo de $\Gamma(n)$. Además, como $(\beta_1, \ldots, \beta_{s+1}) \notin \{(0,\ldots,0),(1,\ldots,1),(-1,\ldots,-1)\}$, entonces $z \notin \{0, 1, n-1\}$, es decir, $z \in Dom(\varphi)$. Se sigue, de la elección de z, que $\varphi(z) = (\beta_1, \ldots, \beta_{s+1})$.

Caso 4: $I_1 \neq \emptyset$, $I_2 \neq \emptyset$ e $I_3 \neq \emptyset$.

En este caso consideremos el siguiente sistema de congruencias:

$$(1)\begin{cases} x \equiv 1 \mod q_1 \\ x \equiv 0 \mod q_2 \\ x \equiv -1 \mod q_3 \\ x \equiv 2^{m-1}+1 \mod 2^m \end{cases} \text{ y } (2)\begin{cases} x \equiv 1 \mod q_1 \\ x \equiv 0 \mod q_2 \\ x \equiv -1 \mod q_3 \\ x \equiv 1 \mod 2^m \end{cases} \text{ y } (3)\begin{cases} x \equiv 1 \mod q_1 \\ x \equiv 0 \mod q_2 \\ x \equiv -1 \mod q_3 \\ x \equiv 0 \mod 2^m \end{cases}$$

$$\text{y } (4)\begin{cases} x \equiv 1 \mod q_1 \\ x \equiv 0 \mod q_2 \\ x \equiv -1 \mod q_3 \\ x \equiv -1 \mod 2^m \end{cases} \text{ y } (5)\begin{cases} x \equiv 1 \mod q_1 \\ x \equiv 0 \mod q_2 \\ x \equiv -1 \mod q_3 \\ x \equiv 2^{m-1}-1 \mod 2^m. \end{cases}$$

Podemos ver que q_1, q_2, q_3 y 2^m son primos relativos por pares y por el Teorema Chino del Residuo, los sistemas (1), (2), (3), (4) y (5) tienen solución módulo $2^m q_1 q_2 q_3 = n$, digamos z y así:

- Para (1):
  Notemos que como $z \equiv 2^{m-1}+1 \mod 2^m$, entonces por el Lema 3.0.7, tenemos que $z \equiv 1 \mod 2^{m-1}$ y $z \not\equiv 1 \mod 2^m$, por lo que, $2^{m-1} \mid z-1$ y $2^m \nmid z-1$.
  Por otro lado, podemos ver $q_1 \mid z-1$, $q_2 \mid z$, $q_3 \mid z+1$ y $2^{m-1} \mid z-1$, de manera que $2^{m-1} q_1 q_2 q_3 \mid (z-1)(z)(z+1)$. Además, como $2^{m-1} \mid z-1$, entonces $2 \mid z+1$, por lo que, $2^m q_1 q_2 q_3 \mid (z-1)(z)(z+1)$, es decir, $n \mid (z-1)(z)(z+1)$.
- Para (2):
  $q_1 \mid z-1$, $q_2 \mid z$, $q_3 \mid z+1$ y $2^m \mid z-1$, de manera que $2^m q_1 q_2 q_3 \mid (z-1)(z)(z+1)$, es decir, $n \mid (z-1)(z)(z+1)$.

- Para (3):
  $q_1 \mid z-1$, $q_2 \mid z$, $q_3 \mid z+1$ y $2^m \mid z$, de manera que $2^m q_1 q_2 q_3 \mid (z-1)(z)(z+1)$, es decir, $n \mid (z-1)(z)(z+1)$.
- Para (4):
  $q_1 \mid z-1$, $q_2 \mid z$, $q_3 \mid z+1$ y $2^m \mid z+1$, de manera que $2^m q_1 q_2 q_3 \mid (z-1)(z)(z+1)$, es decir, $n \mid (z-1)(z)(z+1)$.
- Para (5):
  Notemos que como $z \equiv 2^{m-1}-1 \mod 2^m$, entonces por el Lema 3.0.7, tenemos que $z \equiv -1 \mod 2^{m-1}$ y $z \not\equiv -1 \mod 2^m$, por lo que, $2^{m-1} \mid z+1$ y $2^m \nmid z+1$.
  Por otro lado, podemos ver $q_1 \mid z-1$,$q_2 \mid z$, $q_3 \mid z+1$ y $2^{m-1} \mid z+1$, de manera que $2^{m-1} q_1 q_2 q_3 \mid (z-1)(z)(z+1)$. Además, como $2^{m-1} \mid z+1$, entonces $2 \mid z-1$, por lo que, $2^m q_1 q_2 q_3 \mid (z-1)(z)(z+1)$, es decir, $n \mid (z-1)(z)(z+1)$.

En cualquiera de los casos anteriores, $n \mid z^3 - z$, esto es $z^3 \equiv z \mod n$, por lo que, en z hay un lazo de $\Gamma(n)$. Además, como $(\beta_1, \ldots, \beta_{s+1}) \notin \{(0,\ldots,0),(1,\ldots,1),(-1,\ldots,-1)\}$, entonces $z \notin \{0, 1, n-1\}$, es decir, $z \in Dom(\varphi)$. Se sigue, de la elección de z, que $\varphi(z) = (\beta_1, \ldots, \beta_{s+1})$.

Dados los casos anteriores, podemos concluir que φ es una función biyectiva y por lo tanto, $|B|$ es igual a $|D| = 5 \cdot 3^s - 3$. Demostramos anteriormente que en los vértices $0, 1$ y $n-1$ siempre hay un lazo, obteniendo así que el número de lazos de $\Gamma(n)$ es igual a $5 \cdot 3^s$.

□

Como pudimos ver a lo largo del capítulo, existe una manera relativamente fácil de calcular el número de lazos que tendrá una digráfica $\Gamma(n)$, únicamente conociendo el orden de la misma y su factorización en primos. Dados los detalles de cada una de las demostraciones propuestas, no fue posible conservar el enunciado original que se muestra en [17] el cuál engloba los cuatro teoremas estudiados en este capítulo.

Capítulo 4

La digráfica de congruencias de potencias m de orden n

Mientras desarrollábamos los resultados del capítulo dos, nos dimos cuenta que en algunas de las propiedades que se trabajaron, sus demostraciones no tomaban en cuenta directamente el exponente de la congruencia que define la construcción de la digráfica $\Gamma(n)$, por lo que nos surgió la idea de que una generalización de ésta, respecto al exponente, conservaría dichas propiedades, es decir, que trabajáramos con la congruencia $a^m \equiv b \mod n$, donde m ahora sería cualquier entero.

De este modo, definimos esta nueva digráfica de la siguiente manera:

Sean n y m dos números naturales distintos de 0, la **digráfica de congruencias de potencias m de orden n**, denotada por $\Gamma(n, m)$, es aquella cuyo conjunto de vértices es el conjunto $\{0, 1, \ldots, n-1\}$ y $(a, b) \in F(\Gamma(n, m))$ si y sólo si:

$$a^m \equiv b \mod n$$

Como ejemplo, para $n = 13$ y $m = 4$, tenemos la digráfica $\Gamma(13, 4)$, cuyas flechas son mostradas a continuación, así como su representación geométrica en la Figura 4.1:

$0^4 = 0$ y $0 \equiv 0 \mod 13$, por lo que $(0,0) \in F(\Gamma(13,4))$,
$1^4 = 1$ y $1 \equiv 1 \mod 13$, por lo que $(1,1) \in F(\Gamma(13,4))$,
$2^4 = 16$ y $16 \equiv 3 \mod 13$, por lo que $(2,3) \in F(\Gamma(13,4))$,
$3^4 = 81$ y $81 \equiv 3 \mod 13$, por lo que $(3,3) \in F(\Gamma(13,4))$,
$4^4 = 256$ y $256 \equiv 9 \mod 13$, por lo que $(4,9) \in F(\Gamma(13,4))$,
$5^4 = 625$ y $625 \equiv 1 \mod 13$, por lo que $(5,1) \in F(\Gamma(13,4))$,
$6^4 = 1296$ y $1296 \equiv 9 \mod 13$, por lo que $(6,9) \in F(\Gamma(13,4))$,
$7^4 = 2401$ y $2401 \equiv 9 \mod 13$, por lo que $(7,9) \in F(\Gamma(13,4))$,
$8^4 = 4096$ y $4096 \equiv 1 \mod 13$, por lo que $(8,1) \in F(\Gamma(13,4))$,
$9^4 = 6561$ y $6561 \equiv 9 \mod 13$, por lo que $(9,9) \in F(\Gamma(13,4))$,
$10^4 = 1000$ y $10000 \equiv 3 \mod 13$, por lo que $(10,3) \in F(\Gamma(13,4))$,

$11^4 = 14641$ y $14641 \equiv 3 \mod 13$, por lo que $(11, 3) \in F(\Gamma(13, 4))$,
$12^4 = 20736$ y $20736 \equiv 1 \mod 13$, por lo que $(12, 1) \in F(\Gamma(13, 4))$.

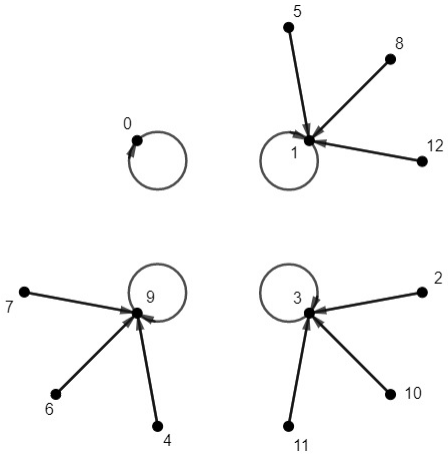

Figura 4.1: Digráfica $\Gamma(13, 4)$.

Dada la definición anterior, a lo largo de este capítulo trabajaremos algunos de los resultados vistos en el capítulo dos, adaptándolos a esta nueva digráfica.

4.1. Propiedades básicas de la digráfica $\Gamma(n, m)$

En el capítulo dos, uno de los resultados más importantes es el del Lema 2.1.1, donde demostramos que todos los vértices de la digráfica $\Gamma(n)$ tienen exgrado igual a 1, esta propiedad la preserva la digráfica $\Gamma(n, m)$, lo cual será demostrado en el siguiente lema.

Lema 4.1.1. *Sea $\Gamma(n, m)$ una digráfica de congruencias de potencias m de orden n. Si n es un natural no nulo y $x \in V(\Gamma(n, m))$, entonces $d^+(x) = 1$.*

Demostración: Sea $x \in V(\Gamma(n, m))$. Como $\{[0], \ldots, [n-1]\}$ es una partición de $\mathbb{Z}$, entonces existe un único $l \in \{0, \ldots, n-1\}$ tal que $x^m \in [l]$, es decir, $x^m \equiv l \mod n$.

Por lo tanto, existe un único $l \in V(\Gamma(n, m))$ tal que $(x, l) \in F(\Gamma(n, m))$. De este modo, podemos concluir que $d^+(x) = 1$. □

Notamos que, aún cuando hay propiedades que se pueden generalizar de forma natural, existen algunas otras obtenidas a partir de la paridad del exponente m con el que trabajemos. Dado esto, en algunos casos, los resultados vistos en el capítulo dos tuvieron que trabajarse de manera separada, dando como resultado que, para los exponentes impares, su generalización fuera similar, mientras que para los exponentes pares se obtuvieran propiedades análogas de acuerdo al comportamiento de la digráfica.

Lema 4.1.2. *Sea $\Gamma(n, m)$ una digráfica de congruencias de potencias m de orden n, tal que n y m son naturales no nulos, con $m \geq 2$. Los siguientes enunciados se satisfacen:*

1. *Los vértices 0 y 1 tienen un lazo en $\Gamma(n, m)$.*
2. *Si m es par, entonces $(n-1, 1) \in F(\Gamma(n, m))$.*
3. *Si m es impar, entonces $n-1$ tiene un lazo en $\Gamma(n, m)$.*
4. *El vértice 0 es un vértice aislado con un lazo en $\Gamma(n, m)$ si y sólo si n es libre de cuadrados.*

Demostración:

1. Es fácil ver que $0^m \equiv 0 \mod n$, esto implica que $(0, 0) \in F(\Gamma(n, m))$, es decir, el vértice 0 tiene un lazo. De igual manera $1^m \equiv 1 \mod n$, esto es, $(1, 1) \in F(\Gamma(n, m))$, por lo que el vértice 1 tiene un lazo.

2. Basta demostrar que $(n-1)^m \equiv 1 \mod n$, es decir, $(n-1)^m - 1 = nk$ para algún $k \in \mathbb{Z}$.

   Veamos que por el binomio de Newton

   $$(n-1)^m - 1 = \left(\sum_{i=0}^{m} (-1)^i \binom{m}{i} n^{m-i} \right) - 1.$$

   Como m es par

   $$(n-1)^m - 1 = \left(\sum_{i=0}^{m-1} (-1)^i \binom{m}{i} n^{m-i} \right) + 1 - 1.$$

   A partir de lo anterior

   $$(n-1)^m - 1 = n \left(\sum_{i=0}^{m-1} (-1)^i \binom{m}{i} n^{m-i-1} \right).$$

   De manera que $(n-1)^m - 1 = nk$ para algún $k \in \mathbb{N}$, por lo que $(n-1)^m \equiv 1 \mod n$. Concluyendo que si m es par, entonces $(n-1, 1) \in F(\Gamma(n, m))$.

3. Demostremos ahora que si m es impar, entonces $(n-1)^m \equiv (n-1) \mod n$, esto es, $(n-1)^m - (n-1) = nk$ para algún $k \in \mathbb{Z}$.

   Veamos que por el binomio de Newton

   $$(n-1)^m - (n-1) = \left(\sum_{i=0}^{m} (-1)^i \binom{m}{i} n^{m-i} \right) - (n-1).$$

   Como m es impar

   $$(n-1)^m - (n-1) = \left(\sum_{i=0}^{m-1} (-1)^i \binom{m}{i} n^{m-i} \right) - 1 - (n-1).$$

Por lo cual

$$(n-1)^m-(n-1)=\left(\sum_{i=0}^{m-1}(-1)^i\binom{m}{i}n^{m-i}\right)-n.$$

Por lo que

$$(n-1)^m-(n-1)=n\left(\left(\sum_{i=0}^{m-1}(-1)^i\binom{m}{i}n^{m-i-1}\right)-1\right).$$

De manera que $(n-1)^m-(n-1)=nk$ para algún $k\in\mathbb{N}$, por lo que, $(n-1)^m\equiv(n-1) \mod n$. Concluyendo que si m es impar, entonces el vértice $n-1$ tiene un lazo.

4. Demostraremos la condición suficiente por contradicción.

   Supongamos que n no es libre de cuadrados, entonces existe un primo p tal que $p^2\mid n$, es decir, $\frac{n}{p^2}\in\mathbb{N}$ y de igual manera $\frac{n}{p}\in\mathbb{N}$.

   Así, si m es impar

   $$\left(\frac{n}{p}\right)^m=\left(n^t\right)\cdot\frac{n}{p}\cdot\underbrace{\frac{n}{p^2}\cdots\frac{n}{p^2}}_{t}=na \qquad \text{para alguna } a\in\mathbb{Z}$$

   donde $t=\dfrac{m-1}{2}$.

   Si m es par

   $$\left(\frac{n}{p}\right)^m=\left(n^t\right)\cdot\underbrace{\frac{n}{p^2}\cdots\frac{n}{p^2}}_{t}=na \qquad \text{para alguna } a\in\mathbb{Z}$$

   donde $t=\dfrac{m}{2}$.

   Por lo que, en cualquiera de los dos casos, $\left(\frac{n}{p}\right)^m\equiv 0 \mod n$, es decir, $\left(\dfrac{n}{p},0\right)\in F(\Gamma(n,m))$. Notamos que esto es una contradicción, pues 0 es un vértice aislado, concluyendo que n es libre de cuadrados.

   Ahora demostraremos la condición necesaria.

   Supongamos que n es libre de cuadrados, es decir, $k^2\nmid n$ para todo $k\in\{0,1,\ldots,n-1\}$.

   Como para todo $k\in\{0,1,\ldots,n-1\}$, $k^2\nmid n$, entonces $k^m\nmid n$ pues si $k^m\mid n$ tenemos que $n=k^mu$, donde $u\in\mathbb{N}$, esto es, $n=k^2\cdot k^{m-2}\cdot u$, por lo que $k^2\mid n$, lo cual es una contradicción a la hipótesis. Además, vimos que si m es impar, el vértice $n-1$ tiene un lazo y si m es par $(n-1)^m\equiv 1 \mod n$, de manera que, en cualquiera de los dos casos, $(n-1)^m\not\equiv 0 \mod n$.

   De este modo, $k^m\not\equiv 0 \mod n$ para todo $k\in\{1,2,\ldots,n-1\}$. Concluyendo que el vértice 0 es un vértice aislado con un lazo en $\Gamma(n,m)$.

□

Lema 4.1.3. *Sea $\Gamma(n,m)$ una digráfica de congruencias de potencias m de orden n. Si m y n son naturales no nulos y $\{k,l\} \subseteq \{1,\ldots,n-1\}$, entonces lo siguiente se cumple:*

(i) $(k,0) \in F(\Gamma(n,m))$ *si y sólo si* $(n-k,0) \in F(\Gamma(n,m))$.

(ii) Si $n = 2b$ para alguna $b \in \mathbb{N}$, entonces $(k,b) \in F(\Gamma(n,m))$ si y sólo si $(n-k,b) \in F(\Gamma(n,m))$.

Demostración:

(i) $(k,0) \in F(\Gamma(n,m))$ si y sólo si $(n-k,0) \in F(\Gamma(n,m))$. Demostraremos la condición suficiente. Sea $(k,0) \in F(\Gamma(n,m))$, por definición de $\Gamma(n,m)$, $k^m \equiv 0 \mod n$, o bien, $k^m = na$ para alguna $a \in \mathbb{N}$.

Por otro lado, notemos que

$$\begin{aligned}(n-k)^m &= \left(\sum_{i=0}^{m}(-1)^i\binom{m}{i}n^{m-i}k^i\right)\\ &= \left(\sum_{i=0}^{m-1}(-1)^i\binom{m}{i}n^{m-i}k^i\right)+(-1)^m k^m.\end{aligned}$$

Dado que $k^m = na$, entonces

$$(n-k)^m = \left(\sum_{i=0}^{m-1}(-1)^i\binom{m}{i}n^{m-i}k^i\right)+(-1)^m na$$

$$(n-k)^m = n\left(\left(\sum_{i=0}^{m-1}(-1)^i\binom{m}{i}n^{m-i-1}k^i\right)+(-1)^m a\right).$$

De este modo, $(n-k)^m \equiv 0 \mod n$. Concluyendo que $(n-k,0) \in F(\Gamma(n,m))$.

Ahora, demostremos la parte necesaria. Supongamos que $(n-k)^m \equiv 0 \mod n$, es decir,

$$(n-k)^m = nc \qquad \text{para alguna } c \in \mathbb{Z}. \tag{4.1}$$

Por otro lado

$$(n-k)^m = \left(\sum_{i=0}^{m}(-1)^i\binom{m}{i}n^{m-i}k^i\right).$$

Siguiendo de la Ecuación (4.1), para m impar

$$\begin{aligned}nc &= \left(\sum_{i=0}^{m}(-1)^i\binom{m}{i}n^{m-i}k^i\right)\\ &= \left(\sum_{i=0}^{m-1}(-1)^i\binom{m}{i}n^{m-i}k^i\right)-k^m.\end{aligned}$$

Despejando k^m, tenemos que,

$$\begin{aligned}k^m &= \left(\sum_{i=0}^{m-1}(-1)^i\binom{m}{i}n^{m-i}k^i\right)-nc\\ &= n\left(\left(\sum_{i=0}^{m-1}(-1)^i\binom{m}{i}n^{m-i-1}k^i\right)-c\right),\end{aligned}$$

es decir, $k^m = nb$, donde $b = \left(\sum_{i=0}^{m-1}(-1)^i\binom{m}{i}n^{m-i-1}k^i\right) - c$. Lo que implica que $k^m \equiv 0 \mod n$.

Para m par

$$\begin{aligned} nc &= \left(\sum_{i=0}^{m}(-1)^i\binom{m}{i}n^{m-i}k^i\right) \\ &= \left(\sum_{i=0}^{m-1}(-1)^i\binom{m}{i}n^{m-i}k^i\right) + k^m. \end{aligned}$$

Despejando tenemos que,

$$\begin{aligned} k^m &= nc - \left(\sum_{i=0}^{m-1}(-1)^i\binom{m}{i}n^{m-i}k^i\right) \\ &= n\left(c - \left(\sum_{i=0}^{m-1}(-1)^i\binom{m}{i}n^{m-i-1}k^i\right)\right), \end{aligned}$$

es decir, $k^m = nb$, donde $b = c - \left(\sum_{i=0}^{m-1}(-1)^i\binom{m}{i}n^{m-i-1}k^i\right)$. Lo que implica que $k^m \equiv 0 \mod n$.

En ambos casos podemos concluir que $(k, 0) \in F(\Gamma(n, m))$.

(ii) Si $n = 2b$ para alguna $b \in \mathbb{N}$, entonces $(k, b) \in F(\Gamma(n, m))$ si y sólo si $(n - k, b) \in F(\Gamma(n, m))$. Demostraremos la parte suficiente. Supongamos que $(k, b) \in F(\Gamma(n, m))$, por definición de $\Gamma(n, m)$, $k^m \equiv b \mod n$, es decir,

$$k^m - b = na \qquad \text{para alguna } a \in \mathbb{Z}. \tag{4.2}$$

Por otro lado,

$$(n-k)^m - b = \left(\sum_{i=0}^{m}(-1)^i\binom{m}{i}n^{m-i}k^i\right) - b.$$

De la Ecuación (4.2), como $k^m - b = na$, entonces $k^m = na + b$, por lo que, para m impar

$$\begin{aligned} \left(\sum_{i=0}^{m}(-1)^i\binom{m}{i}n^{m-i}k^i\right) - b &= \left(\sum_{i=0}^{m-1}(-1)^i\binom{m}{i}n^{m-i}k^i\right) - k^m - b \\ &= \left(\sum_{i=0}^{m-1}(-1)^i\binom{m}{i}n^{m-i}k^i\right) - na - b - b \\ &= \left(\sum_{i=0}^{m-1}(-1)^i\binom{m}{i}n^{m-i}k^i\right) - na - n. \end{aligned}$$

De manera que

$$(n-k)^m - b = n\left(\left(\sum_{i=0}^{m-1}(-1)^i\binom{m}{i}n^{m-i-1}k^i\right) - a - 1\right),$$

es decir, $(n-k)^m - b = na'$ para alguna $a' \in \mathbb{Z}$, por lo que, $(n-k)^m \equiv b \mod n$.

Para m par

$$\left(\sum_{i=0}^{m}(-1)^i\binom{m}{i}n^{m-i}k^i\right)-b=\left(\sum_{i=0}^{m-1}(-1)^i\binom{m}{i}n^{m-i}k^i\right)+k^m-b$$
$$=\left(\sum_{i=0}^{m-1}(-1)^i\binom{m}{i}n^{m-i}k^i\right)+na+b-b.$$

De manera que

$$(n-k)^m-b=n\left(\left(\sum_{i=0}^{m-1}(-1)^i\binom{m}{i}n^{m-i-1}k^i\right)+a\right),$$

es decir, $(n-k)^m-b=na'$ para alguna $a'\in\mathbb{Z}$, por lo que $(n-k)^m\equiv b \mod n$.

En cualquiera de los dos casos, por definición de $\Gamma(n,m)$, $(n-k,b)\in F(\Gamma(n,m))$.

Ahora demostraremos la parte necesaria. Supongamos que $(n-k,b)\in F(\Gamma(n,m))$, por definición de $\Gamma(n,m)$, $(n-k)^m\equiv b \mod n$, es decir,

$$(n-k)^m-b=nc \qquad \text{para alguna } c\in\mathbb{Z}. \tag{4.3}$$

Por otro lado,

$$(n-k)^m-b=\left(\sum_{i=0}^{m}(-1)^i\binom{m}{i}n^{m-i}k^i\right)-b.$$

Siguiendo de la Ecuación (4.3), para m impar

$$nc=\left(\sum_{i=0}^{m}(-1)^i\binom{m}{i}n^{m-i}k^i\right)-b$$
$$=\left(\sum_{i=0}^{m-1}(-1)^i\binom{m}{i}n^{m-i}k^i\right)-k^m-b.$$

Despejando

$$k^m+b=\left(\sum_{i=0}^{m-1}(-1)^i\binom{m}{i}n^{m-i}k^i\right)-nc$$
$$=n\left(\left(\sum_{i=0}^{m-1}(-1)^i\binom{m}{i}n^{m-i-1}k^i\right)-c\right).$$

De manera que $(k^m+b)\equiv 0 \mod n$, o bien, $k^m\equiv(-b) \mod n$. Notemos que como $n=2b$, entonces $2b\equiv 0 \mod n$; ahora bien $2b=b-(-b)$ por lo que $b-(-b)\equiv 0 \mod n$, es decir, $b\equiv(-b) \mod n$.

Tenemos que, por la observación anterior, como $k^3\equiv(-b) \mod n$ y $(-b)\equiv b \mod n$, entonces $k^3\equiv b \mod n$.

Para m par

$$\begin{aligned} nc &= \left(\sum_{i=0}^{m}(-1)^i\binom{m}{i}n^{m-i}k^i\right) - b \\ &= \left(\sum_{i=0}^{m-1}(-1)^i\binom{m}{i}n^{m-i}k^i\right) + k^m - b. \end{aligned}$$

Despejando

$$\begin{aligned} k^m - b &= nc - \left(\sum_{i=0}^{m-1}(-1)^i\binom{m}{i}n^{m-i}k^i\right) \\ &= n\left(c - \left(\sum_{i=0}^{m-1}(-1)^i\binom{m}{i}n^{m-i-1}k^i\right)\right). \end{aligned}$$

De manera que $(k^m - b) \equiv 0 \mod n$, esto es, $k^m \equiv b \mod n$.

Dados los casos anteriores, podemos concluir que $(k, b) \in F(\Gamma(n, m))$.

□

Como hemos visto en los resultados anteriores, ha sido necesario tratar por aparte el exponente de acuerdo a su paridad, por lo que al trabajar con la generalización del Lema 2.1.3, nos dimos cuenta que para los exponentes pares, la digráfica $\Gamma(n, m)$ no tenía el mismo comportamiento que para los exponentes impares. De esta manera, los incisos (iii) a (v) del lema antes mencionado se generalizaron únicamente para los exponentes impares y son demostrados en el siguiente lema.

Lema 4.1.4. *Sea $\Gamma(n, m)$ una digráfica de congruencias de potencias m de orden n. Si m y n son naturales no nulos con m impar y $\{k, l\} \subseteq \{1, \ldots, n-1\}$, lo siguiente se cumple:*

(i) *$(k, l) \in F(\Gamma(n, m))$ si y sólo si $(n-k, n-l) \in F(\Gamma(n, m))$.*

(ii) *$N(k) = \{k\}$ si y sólo si $N(n-k) = \{n-k\}$.*

(iii) *El vértice k pertenece a un t-ciclo aislado si y sólo si el vértice $n-k$ pertenece a algún t-ciclo aislado.*

Demostración:

(i) $(k, l) \in F(\Gamma(n, m))$ si y sólo si $(n-k, n-l) \in F(\Gamma(n, m))$. Primero demostraremos la parte suficiente. Supongamos que $(k, l) \in F(\Gamma(n, m))$, por definición de $\Gamma(n, m)$ se tiene que $k^m \equiv l \mod n$, entonces:

$$k^m - l = na \qquad \text{para alguna } a \in \mathbb{Z}. \tag{4.4}$$

Por otro lado notemos que

$$\begin{aligned}(n-k)^m-(n-l) &= \left(\sum_{i=0}^{m}(-1)^i\binom{m}{i}n^{m-i}k^i\right)-n+l\\ &= \left(\sum_{i=0}^{m-1}(-1)^i\binom{m}{i}n^{m-i}k^i\right)-k^m-n+l\\ &= \left(\sum_{i=0}^{m-1}(-1)^i\binom{m}{i}n^{m-i}k^i\right)-n-(k^m-l).\end{aligned}$$

Dada la Ecuación (4.4):

$$\left(\sum_{i=0}^{m-1}(-1)^i\binom{m}{i}n^{m-i}k^i\right)-n-(k^m-l)=\left(\sum_{i=0}^{m-1}(-1)^i\binom{m}{i}n^{m-i}k^i\right)-n-na.$$

Factorizando n,

$$(n-k)^m-(n-l)=n\left(\left(\sum_{i=0}^{m-1}(-1)^i\binom{m}{i}n^{m-i-1}k^i\right)-1-a\right),$$

por lo que, $(n-k)^m\equiv(n-l) \mod n$. De manera que $(n-k,n-l)\in F\left(\Gamma\left(n,m\right)\right)$.

Ahora demostraremos la parte necesaria. Supongamos que $(n-k,n-l)\in F(\Gamma(n,m))$, por definición de $\Gamma(n,m)$ se tiene que $(n-k)^m\equiv(n-l) \mod n$, entonces:

$$(n-k)^m-(n-l)=nb \qquad \text{para alguna } b\in\mathbb{Z}. \tag{4.5}$$

Por otro lado

$$\begin{aligned}(n-k)^m-(n-l) &= \left(\sum_{i=0}^{m}(-1)^i\binom{m}{i}n^{m-i}k^i\right)-n+l\\ &= \left(\sum_{i=0}^{m-1}(-1)^i\binom{m}{i}n^{m-i}k^i\right)-k^m-n+l.\end{aligned}$$

Siguiendo de la Ecuación (4.5)

$$\left(\sum_{i=0}^{m-1}(-1)^i\binom{m}{i}n^{m-i}k^i\right)-k^m-n+l=nb.$$

Despejando tenemos que

$$\begin{aligned}k^m-l &= \left(\sum_{i=0}^{m-1}(-1)^i\binom{m}{i}n^{m-i}k^i\right)-n-nb\\ &= n\left(\left(\sum_{i=0}^{m-1}(-1)^i\binom{m}{i}n^{m-i-1}k^i\right)-1-b\right).\end{aligned}$$

De este modo, $k^m - l = nb'$ donde $b' = \left(\sum_{i=0}^{m-1}(-1)^i\binom{m}{i}n^{m-i-1}k^i\right) - 1 - b$, por lo que $k^m \equiv l \mod n$. Concluyendo que $(k,l) \in F(\Gamma(n,m))$.

(ii) $N(k) = \{k\}$ si y sólo si $N(n-k) = \{n-k\}$. Para demostrar la parte suficiente basta ver que:

$a)$ Si $(n-k, a) \in F(\Gamma(n,m))$, entonces $a = n-k$.

Supongamos que $(n-k, a) \in F(\Gamma(n,m))$, entonces por el inciso (i) tenemos que $(n-(n-k), n-a) \in F(\Gamma(n,m))$, esto es, $(k, n-a) \in F(\Gamma(n,m))$ y como $N(k) = \{k\}$, entonces $n - a = k$. Concluyendo que $a = n-k$. Por lo tanto, $N^+(n-k) = \{n-k\}$.

$b)$ Si $(b, n-k) \in F(\Gamma(n))$, entonces $b = n-k$.

Supongamos que $(b, n-k) \in F(\Gamma(n,m))$, entonces por el inciso (i) tenemos que $(n-b, n-(n-k)) \in F(\Gamma(n,m))$, esto es, $(n-b, k) \in F(\Gamma(n,m))$ y como $N(k) = \{k\}$, entonces $n - b = k$. Concluyendo que $b = n-k$. De esta manera, $N^-(n-k) = \{n-k\}$.

Por lo tanto, $N(n-k) = \{n-k\}$.

Para demostrar la parte necesaria basta ver que:

(c) Si $(k, a) \in F(\Gamma(n,m))$, entonces $a = k$.

Supongamos que $(k, a) \in F(\Gamma(n,m))$, entonces por el inciso (i) tenemos que $(n-k, n-a) \in F(\Gamma(n,m))$ y como $N(n-k) = \{n-k\}$, entonces $n - a = n - k$. Concluyendo que $a = k$. Por lo tanto, $N^+(k) = \{k\}$.

(d) Si $(b, k) \in F(\Gamma(n,m))$, entonces $b = k$.

Supongamos que $(b, k) \in F(\Gamma(n,m))$, entonces por el inciso (i) tenemos que $(n-b, n-k) \in F(\Gamma(n,m))$ y como $N(n-k) = \{n-k\}$, entonces $n - b = n - k$. Concluyendo que $b = k$. De este modo, $N^-(k) = \{k\}$.

Por lo tanto, $N(k) = \{k\}$.

(iii) El vértice k pertenece a un t-ciclo aislado si y sólo si el vértice $n-k$ pertenece a algún t-ciclo aislado. Demostraremos la parte suficiente. Supongamos que existe un ciclo aislado $\gamma_1 = (\alpha_1, \alpha_2, \ldots, \alpha_t, \alpha_1)$ tal que $\alpha_i = k$ para alguna $i \in \{1, \ldots, t\}$. Por el inciso (i), $\gamma_2 = (n-\alpha_1, n-\alpha_2, \ldots, n-\alpha_t, n-\alpha_1)$ es un ciclo en $\Gamma(n,m)$; además, $n - \alpha_i = n - k$ para alguna $i \in \{1, \ldots, t\}$.

Veamos que γ_2 también es un ciclo aislado.

Supongamos, por contradicción, que el ciclo γ_2 no es aislado, entonces existe $(\alpha_s, n-\alpha_r) \in F(\Gamma(n,m))$ con $s \notin \{1, \ldots, t\}$ y $r \in \{1, \ldots, t\}$. Por el inciso (i), $(n-\alpha_s, n-(n-\alpha_r)) \in F(\Gamma(n,m))$, es decir, $(n-\alpha_s, \alpha_r) \in F(\Gamma(n,m))$, lo cual es una contradicción, pues $\alpha_r \in F(\gamma_1)$ y γ_1 es un ciclo aislado. Por lo tanto, γ_2 es un ciclo aislado.

Ahora demostraremos la parte necesaria. Supongamos que existe un ciclo aislado $\gamma_3 = (\beta_1, \beta_2, \ldots, \beta_r, \beta_1)$ tal que $\beta_i = n - k$ para alguna $i \in \{1, \ldots, r\}$. De manera que, por el inciso (i), $\gamma_4 = (n-\beta_1, n-\beta_2, \ldots, n-\beta_r, n-\beta_1)$ es un ciclo en $\Gamma(n,m)$ y $n - \beta_i = n - (n-k)$ para alguna $i \in \{1, \ldots, r\}$, esto es, $n - \beta_i = k$.

Veamos que γ_4 es un ciclo aislado.

Supongamos, por contradicción, que el ciclo γ_4 no es aislado, entonces existe $(\beta_s, n-\beta_l) \in F(\Gamma(n,m))$ con $s \notin \{1,\ldots,r\}$ y $l \in \{1,\ldots,r\}$. Por el inciso (i), $(n-\beta_s, n-(n-\beta_l)) \in F(\Gamma(n,m))$, es decir, $(n-\beta_s, \beta_l) \in F(\Gamma(n,m))$, lo cual es una contradicción, pues $\beta_l \in \gamma_3$ y γ_3 es un ciclo aislado. Por lo tanto, γ_4 es un ciclo aislado.

□

Podemos ver en la digráfica $\Gamma(11,5)$ de la siguiente figura un ejemplo del resultado anterior, donde si $k=3$, $(3,1) \in F(\Gamma(11,5))$, por lo que $l=1$. De este modo, de acuerdo al lema anterior, la flecha $(11-3, 11-1) \in F(\Gamma(11,5))$, es decir, $(8,10) \in F(\Gamma(11,5))$, lo cual de acuerdo a la representación de la digráfica es cierto. De igual manera, si $k=9$, $(9,1) \in F(\Gamma(11,5))$ por lo que $l=1$. De esta manera, de acuerdo al lema anterior, la flecha $(11-3, 11-1) \in F(\Gamma(11,5))$, esto es, $(8,10) \in F(\Gamma(11,5))$.

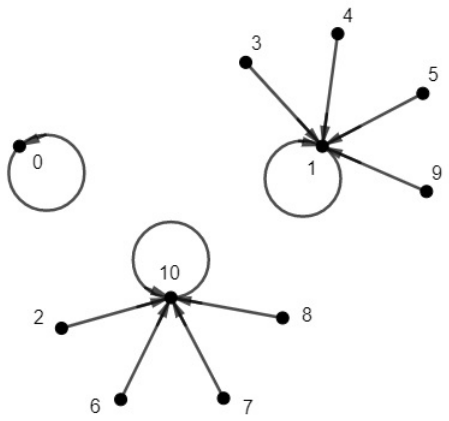

Figura 4.2: Digráfica $\Gamma(11,5)$.

Dado que el lema anterior solo fue posible generalizarlo para los exponentes impares, nos dimos cuenta que las digráficas $\Gamma(n,m)$ con m par tenía un comportamiento parecido a las digráficas con m impar, por lo que, estas nuevas propiedades fueron enunciadas en el siguiente lema.

Lema 4.1.5. *Sea $\Gamma(n,m)$ una digráfica de congruencias de potencias m de orden n. Si m y n son naturales no nulos con m par y $\{k,l\} \subseteq \{1,\ldots,n-1\}$, lo siguiente se cumple:*

(i) $(k,l) \in F(\Gamma(n,m))$ si y sólo si $(n-k,l) \in F(\Gamma(n,m))$.

(ii) Si $n=2b$ y n es libre de cuadrados, entonces $(b,b) \in F(\Gamma(n,m))$.

Demostración:

(i) Demostremos la parte suficiente. Supongamos que $(k,l) \in F(\Gamma(n,m))$, entonces $k^m \equiv l \mod n$, es decir,

$$k^m - l = ns \qquad \text{para alguna } s \in \mathbb{Z}. \tag{4.6}$$

Por otro lado

$$(n-k)^m - l = \left(\sum_{i=0}^{m}(-1)^i\binom{m}{i}n^{m-i}k^i\right) - l.$$

De la Ecuación (4.6) tenemos que

$$\begin{aligned}\left(\sum_{i=0}^{m}(-1)^i\binom{m}{i}n^{m-i}k^i\right) - l &= \left(\sum_{i=0}^{m-1}(-1)^i\binom{m}{i}n^{m-i}k^i\right) + k^m - l \\ &= \left(\sum_{i=0}^{m-1}(-1)^i\binom{m}{i}n^{m-i}k^i\right) + ns.\end{aligned}$$

De manera que

$$(n-k)^m - l = n\left(\left(\sum_{i=0}^{m-1}(-1)^i\binom{m}{i}n^{m-i-1}k^i\right) + s\right),$$

es decir, $(n-k)^m - l = na'$ para alguna $a' \in \mathbb{Z}$,por lo que, $(n-k)^m \equiv l \mod n$. Concluyendo que $(n-k,l) \in F(\Gamma(n,m))$.

Ahora demostraremos la parte necesaria. Supongamos que $(n-k,l) \in F(\Gamma(n,m))$, por definición de $\Gamma(n,m)$ se tiene que $(n-k)^m \equiv l \mod n$, entonces:

$$(n-k)^m - l = nb \qquad \text{para alguna } b \in \mathbb{Z}. \tag{4.7}$$

Por otro lado:

$$\begin{aligned}(n-k)^m - l &= \left(\sum_{i=0}^{m}(-1)^i\binom{m}{i}n^{m-i}k^i\right) - l \\ &= \left(\sum_{i=0}^{m-1}(-1)^i\binom{m}{i}n^{m-i}k^i\right) + k^m - l.\end{aligned}$$

Siguiendo de la Ecuación (4.7):

$$\left(\sum_{i=0}^{m-1}(-1)^i\binom{m}{i}n^{m-i}k^i\right) + k^m - l = nb.$$

Despejando tenemos que

$$\begin{aligned}k^m - l &= nb - \left(\sum_{i=0}^{m-1}(-1)^i\binom{m}{i}n^{m-i}k^i\right) \\ &= n\left(b - \left(\sum_{i=0}^{m-1}(-1)^i\binom{m}{i}n^{m-i-1}k^i\right)\right).\end{aligned}$$

De este modo, $k^m - l = nb'$ para alguna $b' \in \mathbb{Z}$, por lo que, $k^m \equiv l \mod n$. Concluyendo que $(k,l) \in F(\Gamma(n,m))$.

(ii) Para ver que $(b, b) \in F(\Gamma(n, m))$, basta ver que $b^m - b = na$ para algún $a \in \mathbb{Z}$.

Veamos que $b^m - b = b(b^{m-1} - 1)$. Notemos que como n es libre de cuadrados $2^k \nmid n$ para $k \geq 2$, entonces b es impar, por lo que, b^{m-1} es impar y por consecuencia $b^{m-1} - 1$ es par.

De manera que

$$\begin{aligned} b(b^{m-1} - 1) &= \frac{n}{2}(b^{m-1} - 1) \\ &= n\left(\frac{b^{m-1} - 1}{2}\right). \end{aligned}$$

y, por lo antes mencionado, $\dfrac{b^{m-1} - 1}{2} \in \mathbb{Z}$, de modo que $b^m - b = na$ para $a = \dfrac{b^{m-1} - 1}{2}$. Por lo tanto, $(b, b) \in F(\Gamma(n, m))$.

□

Podemos ver en la digráfica $\Gamma(14, 4)$ de la siguiente figura un ejemplo del resultado anterior, donde si $k = 10$, $(10, 4) \in F(\Gamma(14, 4))$, por lo que $l = 4$. De este modo, de acuerdo al lema anterior, la flecha $(14 - 10, 4) \in F(\Gamma(11, 5))$, es decir, $(4, 4) \in F(\Gamma(14, 4))$, lo cual de acuerdo a la representación de la digráfica es cierto. De igual manera, como $n = 14$, $b = 7$; además, 14 es libre de cuadrados, por lo que, de acuerdo al lema anterior, la flecha $(7, 7) \in F(\Gamma(14, 4))$.

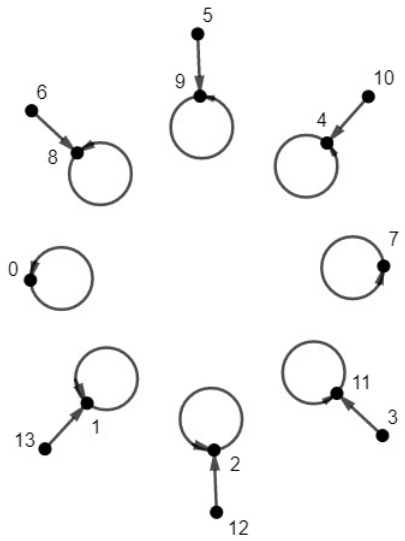

Figura 4.3: Digráfica $\Gamma(14, 4)$.

Recordemos que en el capítulo 2 se trabajó un resultado con respecto a dos subdigráficas inducidas de la digráfica $\Gamma(n)$, el cual para su demostración utiliza únicamente la propiedad directa que define tales subdigráficas, por lo cual fue posible una generalización tanto de las subdigráficas como del propio resultado. Para lo cual definamos estas dos subdigráficas de $\Gamma(n, m)$ de la siguiente manera. Sean $\Gamma_1(n, m)$ la subdigráfica

inducida por el conjunto de vértices que son primos relativos con n y $\Gamma_2(n,m)$ la subdigráfica inducida por los vértices que no son primos relativos con n.

Lema 4.1.6. *Sean $\Gamma(n,m)$ una digráfica de congruencias de potencias m de orden n, $n \geq 2$, $m \geq 1$ y $\{x,z\} \subseteq V(\Gamma(n,m))$ tales que $(x,z) \in F(\Gamma(n,m))$. x y n son primos relativos si y sólo si z y n son primos relativos.*

Demostración: Demostremos la parte suficiente. Supongamos que $(x;n) = 1$ y veamos que $(z;n) = 1$.

Como $(x,z) \in F(\Gamma(n,m))$, tenemos que $x^m = na + z$ para alguna $a \in \mathbb{Z}$ y, supongamos por contradicción, que $(z;n) \neq 1$. Sea $(z;n) = d$ para algún $d \in \mathbb{Z}$ y sea p un primo tal que $d = pt$ para algún $t \in \mathbb{Z}$, de esta manera, $p \mid z$ y $p \mid n$, por lo que, por el Teorema 1.1.10, $p \mid na + z$, es decir, $p \mid x^m$ y como p es un primo, entonces $p \mid x$, de modo que p es un divisor común de x y n. Esto es una contradicción, pues por hipótesis $(x;n) = 1$. Por lo tanto, $(z;n) = 1$.

Ahora demostremos la parte necesaria. Supongamos que $(z;n) = 1$ y veamos que $(x;n) = 1$.

Como $(x,z) \in F(\Gamma(n,m))$, tenemos que $z = x^m - na$ para alguna $a \in \mathbb{Z}$ y, procediendo por contradicción, supongamos que $(x;n) \neq 1$. Sea $(x;n) = d$ para algún $d \in \mathbb{Z}$ y sea p un primo tal que $d = pt$ para algún $t \in \mathbb{Z}$, de esta manera, $p \mid x$ y $p \mid n$, por lo que, por el Teorema 1.1.10, $p \mid x^m - na$, es decir, $p \mid z$ de modo que$p$ es un divisor común de z y n. Esto es una contradicción, pues por hipótesis $(z;n) = 1$. Por lo tanto, $(x;n) = 1$. □

Observación 4.1.7. *Sean $\Gamma(n,m)$ una digráfica de congruencias de potencias m de orden n, $n \geq 2$, $m \geq 1$ y $\{x,z\} \subseteq V(\Gamma(n,m))$ tales que $(x,z) \in F(\Gamma(n,m))$. x y n no son primos relativos si y sólo si z y n no son primos relativos.*

Demostración: Se sigue inmediatamente del lema anterior. □

Proposición 4.1.8. *Sea $\Gamma(n,m)$ una digráfica de congruencias de potencias m de orden n. Si $n \geq 2$ y $m \geq 1$, entonces $V(\Gamma_1(n,m)) \cap V(\Gamma_2(n,m)) = \emptyset$ y $\Gamma(n,m) = \Gamma_1(n,m) \cup \Gamma_2(n,m)$.*

Demostración: Demostremos primero que $V(\Gamma_1(n,m)) \cap V(\Gamma_2(n,m)) = \emptyset$ por contradicción.

Supongamos que existe $l \in V(\Gamma_1(n,m)) \cap V(\Gamma_2(n,m))$. Como $l \in V(\Gamma_1(n,m))$, tenemos que $(n;l) = 1$ y como $l \in V(\Gamma_2(n,m))$, tenemos que $(n;l) = d$ para alguna $d \neq 1$, lo cual es una contradicción. Por lo tanto, $V(\Gamma_1(n,m)) \cap V(\Gamma_2(n,m)) = \emptyset$.

Para ver que $\Gamma(n,m) = \Gamma_1(n,m) \cup \Gamma_2(n,m)$ bastará demostrar que ambas digráficas coinciden en su conjunto de vértices y en su conjunto de flechas respectivamente.

Tenemos que ver que $V(\Gamma(n,m)) = V(\Gamma_1(n,m) \cup \Gamma_2(n,m))$.

Sea $k \in V(\Gamma(n,m))$, entonces podemos ver que k es primo relativo con n o k no es primo relativo con n, es decir, $k \in V(\Gamma_1(n,m))$ o $k \in V(\Gamma_2(n,m))$. De manera que $k \in V(\Gamma_1(n,m) \cup \Gamma_2(n,m))$. Como k es un vértice cualquiera de $\Gamma(n,m)$, entonces podemos concluir que $V(\Gamma(n,m)) \subseteq V(\Gamma_1(n,m) \cup \Gamma_2(n,m))$.

Sea $l \in V(\Gamma_1(n,m) \cup \Gamma_2(n,m))$, entonces $l \in V(\Gamma_1(n,m))$ o $l \in V(\Gamma_2(n,m))$. Por la definición de $\Gamma_1(n,m)$ y $\Gamma_2(n,m)$ tenemos que $l \in V(\Gamma(n,m))$. Por lo que, $V(\Gamma_1(n,m) \cup \Gamma_2(n,m)) \subseteq V(\Gamma(n))$. Podemos concluir que $V(\Gamma(n,m)) = V(\Gamma_1(n,m) \cup \Gamma_2(n,m))$.

Por otro lado, veamos que $F(\Gamma(n,m)) = F(\Gamma_1(n,m) \cup \Gamma_2(n,m))$.

Sea $(u, v) \in F(\Gamma_1(n, m) \cup \Gamma_2(n, m))$, entonces $(u, v) \in F(\Gamma_1(n, m))$ o $(u, v) \in F(\Gamma_2(n, m))$. Por definición de ambas subdigráficas $(u, v) \in F(\Gamma(n, m))$. De esta manera $F(\Gamma_1(n, m) \cup \Gamma_2(n, m)) \subseteq F(\Gamma(n))$.

Ahora, sea $(u, v) \in F(\Gamma(n, m))$.

Caso 1: $(u; n) = 1$.

Por el Lema 4.1.6, $(v; n) = 1$, por lo que $\{u, v\} \subseteq V(\Gamma_1(n, m))$ y como $\Gamma_1(n, m)$ es una subdigráfica inducida, entonces $(u, v) \in F(\Gamma_1(n, m))$.

Caso 2: $(u; n) \neq 1$.

Por la Observación 4.1.7, $(v; n) \neq 1$, por lo que $\{u, v\} \subseteq V(\Gamma_2(n, m))$ y como $\Gamma_2(n, m)$ es una subdigráfica inducida, entonces $(u, v) \in F(\Gamma_2(n, m))$.

Dados ambos casos tenemos que $F(\Gamma(n, m)) \subseteq F(\Gamma_1(n, m) \cup \Gamma_2(n, m))$. Podemos concluir que $F(\Gamma(n, m)) = F(\Gamma_1(n, m) \cup \Gamma_2(n, m))$.

Por lo tanto, $\Gamma(n, m) = \Gamma_1(n, m) \cup \Gamma_2(n, m)$. □

4.2. Caminos dirigidos en $\boldsymbol{\Gamma(n, m)}$

Esta sección, al igual que en el capítulo 2, tratará algunos resultados generalizados relacionados con caminos dirigidos, trayectorias dirigidas y ciclos dirigidos, en la digráfica $\Gamma(n, m)$.

Lema 4.2.1. *Sean $\Gamma(n, m)$ una digráfica de congruencias de potencias m de orden n, $a_1, a_2, \ldots, a_t$ vértices distintos en $\Gamma(n, m)$ y $C = (a_1, a_2, \ldots, a_t, a_1)$ una sucesión de vértices. C es un ciclo dirigido de longitud t en $\Gamma(n, m)$ si y sólo si*

$$\begin{aligned} a_1^m &\equiv a_2 \mod n, \\ a_2^m &\equiv a_3 \mod n, \\ &\vdots \\ a_t^m &\equiv a_1 \mod n. \end{aligned}$$

Demostración: Demostraremos la parte suficiente. Como $(a_1, a_2) \in F(\Gamma(n, m))$, entonces $a_1^m \equiv a_2 \mod n$. De igual modo, como $(a_2, a_3) \in F(\Gamma(n, m))$, entonces $a_2^m \equiv a_3 \mod n$. De esta manera como para cada $i \in \{1, \ldots, t-1\}$, $(a_i, a_{i+1}) \in F(\Gamma(n, m))$, entonces $a_i^m \equiv a_{i+1} \mod n$. Además, $(a_t, a_1) \in F(\Gamma(n, m))$, por lo que $a_t^m \equiv a_1 \mod n$.

Por lo tanto, podemos concluir que un ciclo dirigido determina la secuencia de congruencias dada.

Ahora demostremos la parte necesaria.

Como $a_1^m \equiv a_2 \mod n$, entonces $(a_1, a_2) \in F(\Gamma(n, m))$. De igual modo, como $a_2^m \equiv a_3 \mod n$, entonces $(a_2, a_3) \in F(\Gamma(n, m))$. En general tenemos que como $a_i^m \equiv a_{i+1} \mod n$ con $i \in \{1, \ldots, t-1\}$, entonces $(a_i, a_{i+1}) \in F(\Gamma(n, m))$. De igual manera, como $a_t^m \equiv a_1 \mod n$, entonces $(a_t, a_1) \in F(\Gamma(n, m))$, por lo que tenemos el ciclo dirigido $(a_1, a_2, \ldots, a_t, a_1)$. □

Proposición 4.2.2. *Sea $\Gamma(n,m)$ una digráfica de congruencias de potencias m de orden n. Toda componente conexa de $\Gamma(n,m)$ tiene exactamente un ciclo dirigido.*

Demostración: Demostremos primero que cada componente conexa tiene al menos un ciclo dirigido.

Sean H una componente conexa de $\Gamma(n,m)$. Por el Lema 4.1.1, para todo $v \in V(H)$, $d^+(v) = 1$, entonces por el Lema 1.2.3, H tiene al menos un ciclo dirigido.

Ahora, veremos por contradicción que las componentes conexas tiene un único ciclo dirigido.

Supongamos que existen al menos dos ciclos dirigidos distintos en la componente H, $C = (\alpha_1, \ldots, \alpha_s, \alpha_1)$ y $C' = (\beta_1, \ldots, \beta_t, \beta_1)$.

Entonces tenemos dos casos:

Caso 1: $V(C) \cap V(C') \neq \emptyset$.

Sea $\alpha_i \in V(C) \cap V(C')$ y supongamos que $\alpha_i = \beta_j$ para algún $j \in \{1, \ldots, t\}$, tal que $\alpha_{i+1} \notin V(C')$ y $\beta_{j+1} \notin V(C)$, como $\alpha_i \in V(H)$ y cada ciclo es dirigido, $d^+(\alpha_i) \geq 2$ lo cual, por el Lema 4.1.1, contradice el hecho de que $d^+(a) = 1$ para todo $a \in V(\Gamma(n,m))$.

Caso 2: $V(C) \cap V(C') = \emptyset$.

Como H es una componente conexa, entonces existe un $\alpha_i\beta_j$-camino no necesariamente dirigido, digamos $C_1 = (\alpha_i = x_0, x_1, \ldots, x_{r-1}, x_r = \beta_j)$ tal que $\alpha_i \in V(C)$ y $\beta_j \in V(C')$, es decir, $V(C_1) \cap V(C) = \{\alpha_i\}$ y $V(C_1) \cap V(C') = \{\beta_j\}$.

Si $(\alpha_i, x_1) \in F(C_1)$, entonces $d^+(\alpha_i) \geq 2$ lo cual, por el Lema 4.1.1, es una contradicción. Esto quiere decir que $(x_1, \alpha_i) \in F(C_1)$.

Además, si $(\beta_j, x_{r-1}) \in F(C_1)$, entonces $d^+(\beta_j) \geq 2$ lo cual, por el Lema 4.1.1, es una contradicción, por lo que $(x_{r-1}, \beta_j) \in F(C_1)$.

De esta manera, definimos $\tau = \text{mín}\,\{i \in\{\, 0, \ldots, r-1\,\}\colon (x_i, x_{i+1}) \in F(C_1)\}$.

Podemos ver que, por lo observado anteriormente, si $i = r-1$, $(x_{r-1}, x_r) \in F(C_1)$, entonces el conjunto $\{i \in\{\, 0, \ldots, r-1\,\}\colon (x_i, x_{i+1}) \in F(C_1)\}$ es no vacío. Por otro lado, si $i = 0$, $(x_0, x_1) \notin F(C_1)$, entonces $\tau \geq 1$.

De manera que $(x_\tau, x_{\tau+1}) \in F(C_1)$ y como τ es mínimo, $(x_{\tau-1}, x_\tau) \notin F(C_1)$, por lo que $(x_\tau, x_{\tau-1}) \in F(C_1)$. Esto implica que $d^+(x_\tau) \geq 2$, lo cual, por el Lema 4.1.1, es una contradicción.

Dado que en ambos casos se llega a una contradicción, podemos concluir que C y C' son el mismo. Por lo tanto, H tiene un único ciclo dirigido. □

Corolario 4.2.3. *Sea $\Gamma(n, m)$ una digráfica de congruencias de potencias m de orden n. El número de componentes conexas de $\Gamma(n, m)$ es igual al número de ciclos dirigidos.*

Demostración: Sean

$$\mathscr{C} = \{C : C \text{ es un ciclo dirigido en } \Gamma(n, m)\} \text{ y}$$
$$\mathscr{H} = \{H : H \text{ es una componente conexa de } \Gamma(n, m)\}.$$

Consideremos la relación f de $\mathscr{H}$ en $\mathscr{C}$ dada por $(H, C) \in f$ si y sólo si C es un ciclo de H.

Veamos primero que f es una función.

Sea H una componente cualquiera de $\mathscr{H}$, sabemos que cada componente conexa tiene un ciclo dirigido, por lo que existe $C \in \mathscr{C}$ tal que $(H, C) \in f$. Por lo anterior, $Dom(f) = \mathscr{C}$.

Por otro lado, sean $(H_1, C_1) \in f$, $(H_2, C_2) \in f$ y $H_1 = H_2$, demostraremos que $C_1 = C_2$.

Vimos en la proposición anterior que cada componente tiene un único ciclo dirigido, por lo que si C_1 es un ciclo dirigido de H_1 y C_2 es un ciclo dirigido de H_2 y $H_1 = H_2$, entonces $C_1 = C_2$. Por lo tanto, la relación f es una función.

Ahora, demostraremos que f es inyectiva. Sean H y H' dos componentes conexas de $\Gamma(n, m)$ tales que $f(H) = f(H')$ y veamos que $H = H'$. Sea $f(H) = C$, como $f(H) = f(H')$, entonces C es un ciclo dirigido de H y C es un ciclo dirigido de H'. Dada la definición de componente conexa, C no puede pertenecer a dos componentes distintas, de manera que $H = H'$. Por lo tanto, f es una función inyectiva.

Por último, demostraremos que f es una función suprayectiva. Sea C un ciclo dirigido de alguna componente conexa de $\Gamma(n, m)$. Sabemos que $C \in H$ para alguna componente conexa $H \in \mathscr{H}$ y $C = f(H)$. Por lo tanto, f es suprayectiva.

Dado lo anterior, f es una función biyectiva y podemos concluir que el número de componentes conexas de la digráfica es igual al número de ciclos dirigidos de $\Gamma(n, m)$. □

Lema 4.2.4. *Sea $\Gamma(n, m)$ una digráfica de congruencias de potencias m de orden n. Si $(\alpha_0, \alpha_1, \ldots, \alpha_r)$ es una trayectoria dirigida de longitud r en $\Gamma(n, m)$, entonces $\alpha_0^{m^r} \equiv \alpha_r \mod n$.*

Demostración: Demostraremos por inducción sobre r que $(\alpha_0^{m^r}) \equiv \alpha_r \mod n$.

Base de inducción. Para $r = 1$, $\alpha_0^m \equiv \alpha_1 \mod n$, lo cual es cierto, pues $(\alpha_0, \alpha_1) \in F(\Gamma(n, m))$.

Hipótesis de inducción. Si $(\alpha_0, \alpha_1, \ldots, \alpha_{r-1})$ es una trayectoria dirigida de longitud $r - 1$, entonces $(\alpha_0^{m^{r-1}}) \equiv \alpha_{r-1} \mod n$.

Paso inductivo. Si $T = (\alpha_0, \alpha_1, \ldots, \alpha_r)$ es una trayectoria dirigida de longitud r, entonces $(\alpha_0^{m^r}) \equiv \alpha_r \mod n$.

Consideremos $T' = (\alpha_0, \alpha_1, \ldots, \alpha_{t-1})$ una subtrayectoria dirigida de T, entonces por hipótesis de inducción $(\alpha_0^{m^{r-1}}) \equiv \alpha_{r-1} \mod n$. Además, como $(\alpha_{r-1}, \alpha_r \in F(\Gamma(n, m))$, tenemos que $\alpha_{r-1}^m \equiv \alpha_r \mod n$, entonces $(\alpha_0^{m^{r-1}})^m \equiv \alpha_r \mod n$, es decir, $\alpha_0^{m^r} \equiv \alpha_r \mod n$. □

Corolario 4.2.5. *Sea $\Gamma(n,m)$ una digráfica de congruencias de potencias m de orden n. Si $C=(\alpha_0,\alpha_1,\ldots,\alpha_r,\alpha_0)$ es un ciclo dirigido de $\Gamma(n,m)$, entonces $\alpha_0^{m^{r+1}}\equiv\alpha_0 \mod n$.*

Demostración: Como C es un ciclo dirigido de $\Gamma(n,m)$, consideremos la trayectoria dirigida $T=(\alpha_0,\alpha_1,\ldots,\alpha_r)$. Por el lema anterior, tenemos que $\alpha_0^{m^r}\equiv\alpha_r \mod n$ y sabemos que $\alpha_r^m\equiv\alpha_0 \mod n$, entonces $(\alpha_0^{m^r})^m\equiv\alpha_0 \mod n$, es decir, $\alpha_0^{m^{r+1}}\equiv\alpha_0 \mod n$. □

Lema 4.2.6. *Sea $\Gamma(n,m)$ una digráfica de congruencias de potencias m de orden n y $\{l,n\}\subseteq\mathbb{N}$ tal que $1<l\leq n-1$. Si $s\leq máx\{r\in\mathbb{N}: l^{m^r}<n\}$, entonces existe una s-trayectoria dirigida cuyo vértice inicial es l.*

Demostración: Notemos que para cada $r\in\left\{t\in\mathbb{N}: l^{m^t}<n\right\}$, $(l^{m^r},l^{m^{r+1}})\in F(\Gamma(n,m))$, pues $(l^{m^r})^m\equiv l^{m^{r+1}} \mod n$. De modo que podemos formar un camino dirigido con vértice inicial l de la siguiente manera: $T=(l,l^m,l^{m^2},\ldots,l^{m^r})$. Además, como $l>1$, entonces para cada $\{t_1,t_2\}\subseteq\left\{t\in\mathbb{N}: l^{m^t}<n\right\}$, si $t_1\neq t_2$, entonces $l^{m^{t_1}}\neq l^{m^{t_2}}$, concluyendo que T es una trayectoria dirigida.

Dada la definición de s, podemos ver que $l^{m^s}\leq n$; de manera que si $r=s$, entonces T es una s-trayectoria dirigida con vértice inicial l. □

Lema 4.2.7. *Sea $\Gamma(n,m)$ una digráfica de congruencias de potencias m de orden n. Si $\{n,k,t\}\subseteq\mathbb{N}$ es tal que $k^{m^{t-1}}\leq n$, entonces $n\mid k^{m^t}-k$ si y sólo si $\Gamma(n,m)$ tiene un t-ciclo dirigido que contiene a k.*

Demostración: Demostraremos la condición suficiente.

Como $n\mid k^{m^t}-k$, entonces $k^{m^t}\equiv k \mod n$, de modo que $(k^{m^{t-1}},k)\in F(\Gamma(n,m))$.

Por otro lado, por el lema anterior tenemos que existe una trayectoria dirigida de longitud $t-1$ con vértice inicial k digamos T. De esta manera, podemos definir $\gamma=T\cup(k^{m^{t-1}},k)$ como un ciclo dirigido de longitud t que contiene al vértice k.

Demostraremos la condición necesaria.

Sea $C=(\alpha_0,\alpha_1,\ldots,\alpha_{t-1},\alpha_0)$ un t-ciclo dirigido de $\Gamma(n,m)$ tal que, sin pérdida de generalidad, $\alpha_0=k$, por el Corolario 4.2.5 tenemos que $n\mid\alpha_0^{m^t}-\alpha_0$. □

Debido a que sólo pudo ser posible enunciar el Lema 4.1.4 para los exponentes impares y puesto que su análogo para $\Gamma(n)$ fue utilizado para demostrar algunos resultados posteriores, en este caso la generalización de los mismos sólo fue posible hacerla para tales exponentes.

Lema 4.2.8. *Sea $\Gamma(n,m)$ una digráfica de congruencias de potencias m de orden n, $\{\alpha_1,\alpha_2,\ldots,\alpha_k\}\subseteq\{0,\ldots,n-1\}$ y m impar. Definimos:*

$$D_1=\Gamma(n,m)\langle\{\alpha_1,\alpha_2,\ldots,\alpha_k\}\rangle \quad y \quad D_2=\Gamma(n,m)\langle\{n-\alpha_1,n-\alpha_2,\ldots,n-\alpha_k\}\rangle$$

entonces la función $\varphi:V(D_1)\to V(D_2)$ con regla de correspondencia $\varphi(\alpha_i)=n-\alpha_i$ es un isomorfismo.

Demostración: Notemos que por la definición de φ, ésta es biyectiva, por lo que resta demostrar que preserva adyacencias. Sea (α_r,α_s) alguna flecha de D_1, con $r,s\subseteq\{1,\ldots,k\}$.

Sabemos por el inciso (i) del Lema 4.1.4 que $(n-\alpha_r, n-\alpha_s) \in F(\Gamma(n,m))$, además, $\{n-\alpha_r, n-\alpha_s\} \subseteq V(D_2)$, de manera que $(n-\alpha_r, n-\alpha_s) \in F(D_2)$, es decir, $(\varphi(\alpha_r), \varphi(\alpha_s)) \in F(D_2)$.

Análogamente, sea $(n-\alpha_r, n-\alpha_s)$ alguna flecha de D_2, con $r, s \subseteq \{1, \ldots, k\}$, por el inciso (i) del Lema 4.1.4, $(\alpha_r, \alpha_s) \in F(\Gamma(n,m))$ y como $\{\alpha_r, \alpha_s\} \subseteq V(D_1)$, entonces $(\alpha_r, \alpha_s) \in F(D_1)$.

Dado lo anterior podemos concluir que $D_1 \cong D_2$. □

Corolario 4.2.9. *Sea $\Gamma(n,m)$ una digráfica de congruencias de potencias m de orden n, $k \in V(\Gamma(n,m))$ y m impar. Si H es la componente conexa tal que $k \in V(H)$ y H' es la componente conexa tal que $n-k \in V(H')$, entonces $H \cong H'$.*

Demostración: Sea H la componente conexa tal que $k \in V(H)$. Supongamos que $V(H) = \{\alpha_1, \ldots, \alpha_r\}$. Por el lema anterior sabemos que $D = \Gamma(n,m)\langle\{n-\alpha_1, n-\alpha_2, \ldots, n-\alpha_r\}\rangle$ es isomorfa a H y D contiene al vértice $n-k$. Demostraremos que D es una componente conexa.

Dado que H es conexa, entonces D es conexa. Sólo falta demostrar que D es conexa maximal. Procediendo por contradicción, supongamos que D' es conexa y D es una subdigráfica propia de D'. Si $V(D') = \{\beta_1, \ldots, \beta_t\}$, entonces $H_0 = \Gamma(n,m)\langle\{n-\beta_1, n-\beta_2, \ldots, n-\beta_t\}\rangle$ es isomorfa a D', por lo que H_0 es una subdigráfica conexa y H es una subdigráfica propia de H_0, lo cual no es posible, pues H es una componente conexa. Por lo tanto, $D = H'$ y en particular $H \cong H'$. □

Corolario 4.2.10. *Sea $\Gamma(n,m)$ una digráfica de congruencias de potencias m de orden n, $k \in \left\{\left\lceil \frac{n}{2} \right\rceil, \ldots, n\right\}$ y m impar. Si H es la componente conexa de $\Gamma(n,m)$ tal que $k \in V(H)$ y H' es la componente conexa de $\Gamma(n,m)$ tal que $n-k \in V(H')$, entonces $H \cong H'$.*

Demostración: Notemos que si $k \in \left\{\left\lceil \frac{n}{2} \right\rceil, \ldots, n\right\}$, entonces $n-k \in \left\{1, \ldots, \left\lfloor \frac{n}{2} \right\rfloor\right\}$ y por el corolario anterior tenemos que $H \cong H'$. □

Lema 4.2.11. *Sea $\Gamma(n,m)$ una digráfica de congruencias de potencias m de orden n. Cada componente conexa de $\Gamma(n,m)$ es un ciclo dirigido si y sólo si para cada k tal que $2 \leq k \leq \left\lfloor \frac{1}{2}n \right\rfloor$, existe $t \geq 1$ que satisface que $k^{m^t} \equiv k \mod n$.*

Demostración: Demostraremos la parte suficiente. Sean $\alpha_1 \in \left\{2, \ldots, \left\lfloor \frac{n}{2} \right\rfloor\right\}$ y H la componente conexa de $\Gamma(n,m)$ que contiene al vértice α_1. Por hipótesis, H es un ciclo dirigido, digamos $\gamma = (\alpha_1, \alpha_2, \ldots, \alpha_r, \alpha_1)$.

Como γ es un ciclo dirigido, entonces por el Corolario 4.2.5 tenemos que $n \mid \alpha_1^{m^r} - \alpha_1$, esto es, $\alpha_1^{m^r} \equiv \alpha_1 \mod n$.

Notemos que r es la longitud del ciclo dirigido y la mínima longitud que puede tener un ciclo dirigido es 1 pues tomamos a los lazos como ciclos dirigidos de longitud 1, por lo que $r \geq 1$, lo cual cumple con las condiciones del lema. Por lo tanto, para toda $k \in \left\{2, \ldots, \left\lfloor \frac{n}{2} \right\rfloor\right\}$, existe $t \geq 1$, que satisface que $k^{m^t} \equiv k \mod n$.

Ahora demostraremos la parte necesaria. Primero veremos que todo vértice en $\Gamma(n,m)$ está en un ciclo dirigido. Notemos que como $k^{m^t} \equiv k \mod n$, entonces $n \mid k^{m^t} - k$; además, $(k^{m^{t-1}}, k) \in F(\Gamma(n,m))$, entonces $\Gamma(n,m)$ tiene un camino dirigido cerrado, digamos $C = (k, k^m, k^{m^2}, \ldots, k^{m^{t-1}}, k)$. Sabemos que todo camino dirigido cerrado contiene al menos un ciclo dirigido, digamos γ; si $V(C) \neq V(\gamma)$, entonces existe

$x \in V(C) \cap V(\gamma)$ tal que $d^+(x) \geq 2$, lo cual es una contradicción, pues sabemos que para todo $v \in \Gamma(n,m)$, $d^+(v) = 1$, por lo que $V(C) = V(\gamma)$, de manera que C es un ciclo dirigido de longitud t que tiene al vértice k.

Por otro lado, como $(k^{m^{t-1}}, k) \in F(\Gamma(n,m))$ para cada $k \in \left\{2, \ldots, \left\lfloor \frac{n}{2} \right\rfloor\right\}$, entonces cada $k \in \left\{1, \ldots, \left\lfloor \frac{n}{2} \right\rfloor\right\}$ tiene un invecino.

Supongamos ahora que existe una componente conexa de $\Gamma(n,m)$, digamos H, tal que no es un ciclo dirigido y sea k un vértice de H. Por el Corolario 4.2.10 podemos suponer que $k \in \left\{2, \ldots, \left\lfloor \frac{n}{2} \right\rfloor\right\}$ y por lo visto anteriormente k está en un ciclo dirigido, digamos γ. Notemos que γ es un ciclo dirigido de H.

Como H no es un ciclo dirigido, entonces $V(H) \neq V(\gamma)$ o $F(H) \neq F(\gamma)$.

Supongamos primero que $V(H) \neq V(\gamma)$. Podemos ver que si $x \in V(\gamma)$ y $z \in V(H) \setminus V(\gamma)$, entonces $(x,z) \notin F(\Gamma(n,m))$, pues en $\Gamma(n,m)$ todos los vértices tienen exgrado 1. Además, como $V(H) \neq V(\gamma)$ y H es conexa, entonces existe $x_1 \in V(H) \setminus V(\gamma)$ y $k' \in V(\gamma)$ tales que x_1 y k' son adyacentes. Por lo mencionado anteriormente $(x_1, k') \in F(H)$.

Sea T una trayectoria dirigida de longitud máxima cuyo vértice final es k' y no tenga vértices en común con γ, salvo k', dicha trayectoria dirigida existe pues $(x_1, k') \in F(H)$. Sea w el vértice inicial de dicha trayectoria dirigida.

De esta manera, como cada vértice recibe una flecha, entonces en particular w recibe una flecha de algún vértice de H, pero por lo dicho anteriormente, tal vértice no puede ser un vértice de γ, entonces existe un vértice en T, digamos x_i tal que $(x_i, w) \in F(H)$, por lo que $d^+(x_i) \geq 2$, lo cual es una contradicción. Por lo tanto, no es posible que $V(H) \neq V(\gamma)$.

Ahora supongamos que $V(H) = V(\gamma)$. Como $H \neq \gamma$, entonces $F(H) \neq F(\gamma)$, esto es, para algún $\{u,v\} \subseteq V(\gamma)$, $(u,v) \in F(H) \setminus F(\gamma)$, pero como $u \in V(\gamma)$, entonces $d^+(u) \geq 2$, lo cual es una contradicción. Por lo tanto, la componente H es un ciclo dirigido. □

Como hemos podido ver en este capítulo, las propiedades que se trabajaron en el capitulo dos no son propias directamente de la digráfica $\Gamma(n)$ donde el exponente de la congruencia es 3, si no que se han podido generalizar para todos los enteros o en algunos casos para los enteros impares, lo cual nos da un amplio campo de estudio sobre las digráficas $\Gamma(n,m)$.

Conclusiones

A lo largo de esta tesis, trabajamos y desarrollamos diversos resultados presentados por J. Skowronek-Kazióow en [17], así como una generalización de los mismos en la digráfica propuesta por L. Somer y M. Křížek en [18].

En el Capítulo 2, se introdujo la definición de la digráfica de congruencias cúbicas de orden n, además de diversos ejemplos y notaciones relacionadas con ésta. Comenzamos a estudiar las propiedades básicas de la digráfica antes mencionada, por ejemplo hicimos notar que el exgrado de todos sus vértices siempre es igual a 1. Posteriormente mostramos que existen ciertos vértices que, independientemente del valor de n, siempre tendrán un lazo. Dichos vértices son $0, 1$ y $n-1$. Además, se demostraron condiciones sobre los invecinos del vértice 0 en términos de las potencias primas que dividen a n. Desarrollamos un lema respecto a la estructura de la digráfica, que fue de mucha ayuda en la demostración de diversos resultados: nos dimos cuenta que el conjunto de vértices tiene un comportamiento particular, pues si $(k,l) \in F(\Gamma(n))$, entonces $(n-k, n-l) \in F(\Gamma(n))$. La idea anterior muestra que basta conocer las vecindades de los vértices en $\{0, \ldots, \left\lfloor \frac{n}{2} \right\rfloor\}$ para comprender las vecindades de cualquier vértice de la digráfica $\Gamma(n)$. Como consecuencia, demostramos que, si k es un vértice en $\{0, \ldots, \left\lfloor \frac{n}{2} \right\rfloor\}$ y H es la componente conexa que contiene a k, entonces la componente conexa que contiene al vértice $n-k$ es isomorfa a H, lo cual nos da la idea de que, en algunos casos, podemos estudiar únicamente el comportamiento de la mitad de los vértices y conocer el comportamiento general de la digráfica.

Por otro lado, de acuerdo al Lema 2.1.4 y la Observación 2.1.5, notamos que si dos vértices son adyacentes en la digráfica $\Gamma(n)$, entonces ambos son primos relativos respecto a n o ambos no son primos relativos respecto a n. Esto nos llevó a demostrar que $\Gamma(n)$ es la unión ajena de la subdigráfica inducida por el conjunto de vértices que son primos relativos de n y la subdigráfica inducida por el conjunto de vértices que no son primos relativos de n.

Dentro de este mismo capítulo, estudiamos el comportamiento de caminos dirigidos, ciclos dirigidos y componentes conexas. Desarrollamos un lema que nos muestra una manera de analizar los ciclos dirigidos de la digráfica en términos de la congruencia establecida en la definición de $\Gamma(n)$. Demostramos que el número de componentes conexas de la digráfica de congruencias cúbicas es igual al número de ciclos dirigidos de la misma, esto derivado del hecho de que cada componente conexa de $\Gamma(n)$ tiene exactamente un ciclo dirigido. Analizando la demostración del Lema 2.2.11, nos dimos cuenta que existen propiedades respecto a las congruencias que están determinadas por las trayectorias dirigidas, a saber, si a_0 es el vértice inicial de alguna trayectoria y a_r es el vértice final, entonces $a_0^{3^r} \equiv a_r \mod n$. Gracias a esto dedujimos diversos resultados,

por ejemplo, si a_0 es un vértice de un ciclo dirigido de longitud r, entonces $a_0^{3^{r+1}} \equiv a_0 \mod n$. También pudimos determinar, dado un vértice arbitrario a, el comportamiento de algunas trayectorias dirigidas cuyo vértice inicial es a. De igual manera, dado un vértice k, mostramos que la longitud del ciclo dirigido que contiene a dicho vértice es t si se satisface que $n \mid k^{3^t} - k$.

El Capítulo 3 está dedicado a contabilizar los lazos de las digráficas de congruencias cúbicas. A pesar de que el artículo demuestra un teorema que consiste en cuatro casos en el cual se calcula el número de lazos de $\Gamma(n)$, notamos que dicha demostración requería un análisis más detallado del mostrado por el artículo. Así, la demostración que desarrollamos se enfoca principalmente en el planteamiento de una función biyectiva entre el conjunto de vértices que tienen un lazo en la digráfica y un conjunto conveniente de s-ádas ordenadas, donde el valor de s depende de la descomposición canónica de n. Es importante mencionar que en las demostraciones ofrecidas se usó frecuentemente el Teorema Chino del Residuo. Además, dependiendo de los posibles valores de m tales que $2^m \mid n$, era necesario plantearse demostraciones particulares, es decir, había que considerar cada uno de los casos que menciona el teorema original por separado, dichos casos eran: $m = 0$, $m = 1$, $m = 2$ o $m \geq 3$. Esto nos llevó a la necesidad de plantear una función distinta para cada caso y, por lo tanto, un teorema que considerara cada caso en específico. No obstante al desarrollar la demostración de cada uno de los teoremas, notamos que los argumentos son prácticamente los mismos salvo los cambios que deben considerarse de un teorema a otro.

Por último, en el Capítulo 4, se plantea una generalización de la digráfica de congruencias cúbicas como se define en [18], en la que ahora el exponente de la congruencia que define la digráfica será cualquier entero m. Dicha digráfica es la digráfica de congruencias de potencia m de orden n, la cual denotamos por $\Gamma(n, m)$. Nos dimos cuenta que muchas de las propiedades desarrolladas a lo largo del Capítulo 2 no estaban directamente relacionadas con la paridad del exponente de la congruencia, por lo que fue posible generalizar varios de los resultados presentados en dicho capítulo. Como ejemplo de lo anterior, vimos que todos los vértices tienen exgrado igual a 1; los vértices $0, 1$ y $n - 1$ tienen un lazo independientemente del valor de n y m; también vimos propiedades de los invecinos del vértice 0 en términos de las potencias primas que dividen a n. Sin embargo, en algunos otros resultados había que considerar la paridad del exponente m. Por ejemplo, cuando $m = 3$ sabemos que dos vértices a y b son adyacentes si y sólo si $n - a$ y $n - b$ son adyacentes en $\Gamma(n)$, sin embargo, nos dimos cuenta, gracias al Binomio de Newton, que cuando m es par el enunciado no se satisface. A pesar de lo anterior, cuando m es impar, es posible replicar el comportamiento antes mencionado, es decir, a y b son adyacentes si y sólo si $n - a$ y $n - b$ son adyacentes en $\Gamma(n, m)$; como consecuencia, los resultados que hablan acerca de las componentes conexas isomorfas pudieron extenderse a la digráfica de congruencias de potencia m de orden n. También vimos que dos vértices son adyacente en $\Gamma(n, m)$ si y sólo si ambos son primos relativos con n, por lo que $\Gamma(n, m)$ es la unión ajena de la subdigráfica inducida por el conjunto de vértices que son primos relativos de n y la subdigráfica inducida por el conjunto de vértices que no son primos relativos de n. Por último, gracias a la definición de adyacencias en $\Gamma(n, m)$, todos los resultados respecto a caminos dirigidos, trayectorias dirigidas y ciclos dirigidos se extendieron de manera natural a estas digráficas.

Pensamos que aún queda mucho por estudiar respecto a las digráficas de congruencias cúbicas, empezando por extender algunos resultados que se encuentran en [17], en términos de $\Gamma(n, m)$, además de desarrollar y estudiar a profundidad el comportamiento de las mismas.

De igual manera, respecto al conteo de lazos, nos gustaría encontrar una demostración más general en

la que se puedan sintetizar las demostraciones de los teoremas del Capítulo 3 en un solo enunciado como el propuesto en [17]. Por otro lado, creemos que se deben analizar y estudiar con mayor detenimiento las digráficas de congruencias de potencia m de orden n definidas en el Capítulo 4, puesto que a pesar de que muchas de las propiedades se pudieron generalizar del caso $m = 3$, muchas otras pudimos ver que dependen de la paridad de m, por lo que resulta interesante pensar en qué otras propiedades y resultados podríamos obtener pensando en esto. Uno de los resultados propuestos para desarrollar en un futuro sería encontrar algún teorema que nos ayude a contabilizar los lazos de estas digráficas, pues no resulta tan fácil desarrollar una demostración similar a la que tenemos para el caso $m = 3$. Además, teniendo como antecedente el artículo [18], podemos notar que existen muchos otros aspectos desde los cuales se pueden estudiar este tipo de digráficas.

Bibliografía

[1] S. Allesina, A. Bodini, C. Bondavalli, *Ecological subsystems via graph theory: the role of strongly connected components*, Oikos, Vol. 11(1), 2005, 164-176. (document)

[2] R. Alur, C. Courcoubetis, y T. Henzinger, *The observational power of clocks*, CONCUR, Vol. 836, 1994, 162-177. (document)

[3] J. Bang-Jensen y G. Gutin, *Digraphs theory, algorithms and applications*, Berlin, 2007.

[4] A. Berliner, N. Dean, J. Hook, A. Marr, A. Mbirika y C. McBee, *Coprime and prime labelings of graphs*, Jour. of Int. Seq., Vol. 19, 2016, 1-14. (document)

[5] S. Bryant, *Groups, graphs and Fermat's last theorem*, Amer. Math. Monthly, Vol. 74, 1967, 152-156. (document)

[6] G. Chartrand y P. Zhang, *A first course in graph theory*, Nueva York, 2012.

[7] L. Euler, *Solutio problematis ad geometriam situs pertinentis*, S. I. (document)

[8] C. Johnson, *Functions of number theory in music*, Math . Teachers, Vol. 94 (8), 2001, 700-707. (document)

[9] B. Kalita, *Graph and Goldbach conjecture*, I.J.P.A.M., Vol. 82 (4), 2013, 531-546. (document)

[10] N. Koblitz, A. Menezes y S. Vanstone, *The state of elliptic curve cryptography*, Kl. Ac. Pub., Vol. 19, 2000, 173-193. (document)

[11] T. Koshy, *Elementary number theory with applications*, Londres, 2007. 1.1.4

[12] M. Křížek y L. Somer, *On a connection of number theory with graph theory*, Czech. Math. J., Vol. 54 (129), 2004, 465-485. (document)

[13] R. Lane y S. Everett, *The origin of the Julian Period: An application of congruences and the Chinese Remainder Theorem*, Amer Jour. of Phys., Vol. 49, 1981, 658-661. (document)

[14] R. Pathak y B. Kalita, *Consecutive even number finding graph (CENFG) related to Golbach conjecture*, I.J.P.A.M., Vol. 89 (1), 2013, 55-70. (document)

[15] F. Riaz y K. M. Ali, *Applications of Graph Theory in Computer Science*, 2011 Third International Conference on Computational Intelligence, Communication Systems and Networks, Bali, 2011, 142-145. (document)

[16] H. Schultz, *Topological organic chemistry. 1. Graph theory and topological indices of alkanes*, J. Chem. Inf. Comput. Sci., Vol. 29 (3), 1989, 227-228. (document)

[17] J. Skowronek-Kaziów, *Properties of digraphs connected with some congruence relations*, Czech. Mat., Vol. 59 (134), 2009, 39-49. (document), 2, 2.1, 3, 4.2

[18] L. Somer y M. Křížek, *On semiregular digraphs of the congruence* $x^k \equiv y \mod n$, Com. Math. Univ. Carol., Vol. 48 (1), 2007, 41-58. (document), 4.2

[19] L. Szalay, *A discrete iteration in number theory*, BDTF Tud. Közl., Vol. 8, 1992, 71-91.

(document)