Neiva, 15/06/2021

Señores

CENTRO DE INFORMACIÓN Y DOCUMENTACIÓN

UNIVERSIDAD SURCOLOMBIANA

Ciudad, Neiva

Los suscritos:

Stheffani Vaquiro Lasso, con C.C**. No.1.075.292.264** y **Jonathan Rangel Castaño**, con C.C. **No.1.075.275.066**

Autores del trabajo de grado titulado:

"Aplicación de la relación congruencia módulo $m \in \mathbb{Z}^+$ y los Teoremas de Euler, Fermat y Wilson en el juego del ajedrez."

presentado y aprobado en el año 2021 como requisito para optar al título de Licenciado en Matemáticas;

Autorizan al CENTRO DE INFORMACIÓN Y DOCUMENTACIÓN de la Universidad Surcolombiana para que, con fines académicos, muestre al país y el exterior la producción intelectual de la Universidad Surcolombiana, a través de la visibilidad de su contenido de la siguiente manera:

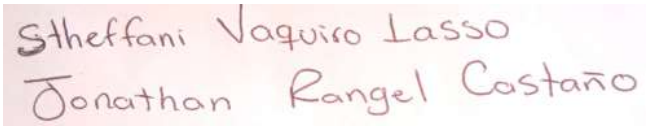
- Los usuarios puedan consultar el contenido de este trabajo de grado en los sitios web que administra la Universidad, en bases de datos, repositorio digital, catálogos y en otros sitios web, redes y sistemas de información nacionales e internacionales "open access" y en las redes de información con las cuales tenga convenio la Institución.

- Permita la consulta, la reproducción y préstamo a los usuarios interesados en el contenido de este trabajo, para todos los usos que tengan finalidad académica, ya sea en formato Cd-Rom o digital desde internet, intranet, etc., y en general para cualquier formato conocido o por conocer, dentro de los términos establecidos en la Ley 23 de 1982, Ley 44 de 1993, Decisión Andina 351 de 1993, Decreto 460 de 1995 y demás normas generales sobre la materia.

- Continúo conservando los correspondientes derechos sin modificación o restricción alguna; puesto que, de acuerdo con la legislación colombiana aplicable, el presente es un acuerdo jurídico que en ningún caso conlleva la enajenación del derecho de autor y sus conexos.

De conformidad con lo establecido en el artículo 30 de la Ley 23 de 1982 y el artículo 11 de la Decisión Andina 351 de 1993, “Los derechos morales sobre el trabajo son propiedad de los autores”, los cuales son irrenunciables, imprescriptibles, inembargables e inalienables.

AUTORES / ESTUDIANTES:



Firma: Stheffani Vaquiro Lasso

Jonathan Rangel Castaño

TÍTULO COMPLETO DEL TRABAJO: Aplicación de la relación congruencia módulo $m \in \mathbb{Z}^+$ y los Teoremas de Euler, Fermat y Wilson en el juego del ajedrez.

AUTOR O AUTORES:

Primero y Segundo Apellido	Primero y Segundo Nombre
Rangel Castaño	Jonathan
Vaquiro Lasso	Stheffani

DIRECTOR Y CODIRECTOR TESIS:

Primero y Segundo Apellido	Primero y Segundo Nombre
Castilla Peñate	Telvia Rosa
Silva Silva	Augusto

ASESOR (ES):

Primero y Segundo Apellido	Primero y Segundo Nombre
Castilla Peñate	Telvia Rosa

PARA OPTAR AL TÍTULO DE: Licenciado en Matemáticas

FACULTAD: Educación

PROGRAMA O POSGRADO: Licenciatura en Matemáticas

CIUDAD: Neiva **AÑO DE PRESENTACIÓN:** 2021 **NÚMERO DE PÁGINAS:** 59

TIPO DE ILUSTRACIONES (Marcar con una **X**)**:**

Diagramas___ Fotografías _Grabaciones en discos___ Ilustraciones en general X Grabados___ Láminas___ Litografías___ Mapas___ Música impresa___ Planos___ Retratos___ Sin ilustraciones___Tablas o Cuadros _

SOFTWARE requerido y/o especializado para la lectura del documento:

MATERIAL ANEXO:

PREMIO O DISTINCIÓN *(En caso de ser LAUREADAS o Meritoria)*:

PALABRAS CLAVES EN ESPAÑOL E INGLÉS:

Español	**Inglés**
1. Aprendizaje	Learning
2. Entornos Sociales	Social Settings
3. Conocimiento	Knowledge

RESUMEN DEL CONTENIDO: (Máximo 250 palabras)

La aplicación de la matemática en la resolución de problemas cotidianos se ha convertido en uno de los temas de mayor interés en todos los niveles de la educación.

La teoría de número es una de las ramas de la matemática que durante muchos años fue considerada como una ciencia pura. Pero ya en el siglo XX se inicia un movimiento que muestra otra cara de la teoría de números con el inicio de las aplicaciones.

Es por esto, que este trabajo tiene como objetivo aplicar la teoría de número al ajedrez. En este caso veremos algunas aplicaciones en divisibilidad, congruencia modular y teoremas de Euler, Wilson y Fermat.

Palabras Claves: Ajedrez, divisibilidad, congruencia modular, Teorema de Wilson, Teorema de Euler, Teorema de Fermat.

ABSTRACT: (Máximo 250 palabras)

The application of mathematics in solving everyday problems has become one of the topics of greatest interest at all levels of education.

Number theory is one of the branches of mathematics that for many years was considered a pure science. But already in the twentieth century a movement began that shows another side of number theory with the beginning of applications.

This is why this work aims to apply number theory to chess. In this case we will see some applications in divisibility, modular congruence and Euler, Wilson and Fermat theorems.

Keywords: Chess, divisibility, modular congruence, Wilson's theorem, Euler's theorem, Fermat's theorem

APROBACION DE LA TESIS

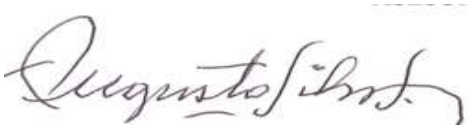
Nombre Presidente Jurado: Julio Cesar Vidal

Firma:

Nombre Jurado: Telvia Rosa Castilla Peñate

Firma: 

Nombre Jurado: Augusto Silva Silva

Firma: 

Universidad Surcolombiana

Facultad de Educación

Programa de Licenciatura en Matemáticas

Aplicación de la relación congruencia módulo $m \in \mathbb{Z}^+$ y los Teoremas de Euler, Fermat y Wilson en el juego del ajedrez

Jonathan Rangel Castaño
Stheffani Váquiro Lasso

Neiva, Huila
2021

Universidad Surcolombiana

Facultad de Educación

Programa de Licenciatura en Matemáticas

Aplicacioń de la congruencia módulo $m \in \mathbb{Z}^+$ y los Teoremas de Euler, Fermat, Wilson en el juego del ajedrez

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

Jonathan Rangel Castaño
2011199487
Stheffani Vaquiro Lasso
20131118504

Asesora:
Mg. Telvia Rosa Castilla Peñate

Neiva, Huila
2021

Nota de Aceptación

Jefe de Programa

Director

Segundo Lector

Neiva, Marzo 2021.

DEDICATORIA

A nuestro Padre Celestial, por brindarnos siempre su compañía y bendecirnos con salud para afrontar cada momento.

A nuestros padres, Franci Elena Castaño, Lunio Cesar Oliveros, Miriam lasso Rocha, Ramiro Vaquiro Moya, quienes son motivo de alegría y apoyo cada día.

A mi hija María Belén Vaquiro, quien es el motivo para dar siempre lo mejor de mí.

A nuestros hermanos y familiares, por su compañia en cada uno de los episodios de nuestras vidas.

AGRADECIMIENTOS

Damos gracias a Dios por bendecirnos con salud, vida y otorgarnos el privilegio de contar con el apoyo de nuestros padres en cada instante para finalizar este trabajo de grado con satisfacción. Igualmente a nuestra segunda casa, la Universidad Surcolombiana, que nos acogió en el proceso de formarnos como ciudadanos íntegros. Al programa de Licenciatura en Matemáticas por permitirnos conocer maestros de excelente cálidad humana e intelectual, que nos aportaron invaluables enseñanzas.

Agradecemos, de igual forma, a nuestra Asesora de trabajo de grado, la magíster Telvia Rosa Castilla Peñate por su interés y compromiso con el programa. A los docentes por su compromiso con la comunidad estudiantil y con la sociedad, por guiarnos para la construcción de un mejor porvenir contribuyendo a ser mejores personas cada día.

ÍNDICE GENERAL

RESUMEN

La aplicación de la matemática en la resolución de problemas cotidianos se ha convertido en uno de los temas de mayor interés en todos los niveles de la educación.

La teoría de número es una de las ramas de la matemática que durante muchos años fue considerada como una ciencia pura. Pero ya en el siglo XX se inicia un movimiento que muestra otra cara de la teoría de números con el inicio de las aplicaciones.

Es por esto, que este trabajo tiene como objetivo aplicar la teoría de número al ajedrez. En este caso veremos algunas aplicaciones en divisibilidad, congruencia modular y teoremas de Euler, Wilson y Fermat.

Palabras Claves: Ajedrez, divisibilidad, congruencia modular, Teorema de Wilson, Teorema de Euler, Teorema de Fermat.

INTRODUCCIÓN

"Steinitz aportó a la Teoría del Ajedrez una tabla de multiplicar, pero aún él estaba muy lejos de las Matemáticas superiores".

Garry Kasparov

La teoría de números es una rama de las matemáticas que estudia las propiedades aritméticas de los números enteros (Gauss, 1966).

(Puertas, 2012) afirma que la Teoría de Números nace con los problemas de divisibilidad de números naturales y además fue una de las disciplinas de estudio favoritas entre los matemáticos griegos de Alejandría (en Egipto) a partir del siglo III a. C., quienes tenían conciencia del concepto de ecuación diofántica en sus casos particulares. por lo que se considera que la Teoría de Números es una de las ramas más antiguas de las matemáticas.

El desarrollo moderno de la Teoría de Números se da con Euler, Fermat, Lagrange y Gauss. A Gauss se le considera como el creador de lo que actualmente se conoce bajo tal nombre, ya que antes la Teoría de Números no pasaba de ser una colección de resultados aislados (Ortiz, 2015). La teoría de números fue considerada por mucho tiempo como el paradigma de la matemática pura y muy alejada de las aplicaciones de la cotidianidad y los problemas reales. Pero en los años setenta del siglo XX el desarrollo de la Criptografía marca el inicio de la Teoría de Números como Ciencia Aplicada. (Gutierrez, 2018)

La aplicación de la Teoría de Números a la Criptografía y la teoría de la codificación se fundamentan en las propiedades de los números naturales y estas aplicaciones se extendieron a otras áreas como la acústica, biología y química entre otras. Con el siguiente trabajo queremos presentar una aplicación de la congruencia modular y los teoremas de Euler, Wilson y Fermat al ajedrez.

Para el desarrollo del presente trabajo se proponen cuatro capítulos:

En el primer capítulo se realiza la presentación, formulación del problema y los objetivos que tendremos en cuenta para la realización de nuestro trabajo.

En el segundo capítulo se presentan algunos conceptos básicos de divisibilidad y la demostración de algunos teoremas.

En el tercer capítulo se evidencian el tema de congruencia módulo m y se evidencian algunos resultados como el teorema de Euler, Fermat y Wilson.

En el capítulo cuarto mostraremos las aplicaciones del ajedrez en divisibilidad, congruencia módulo m, teorema de Euler, Fermat y Wilson. En este capítulo empezamos haciendo un recorrido por el juego del ajedrez, luego se establecen las formulas que relacionan a cada pieza del ajedrez con la congruencia modular, y de igual forma se establecen formulas para los teoremas de Euler, Fermat y Wilson. Ya después se aplican estas formulas en la resolución de problemas.

CAPÍTULO 1

PRESENTACIÓN DEL PROBLEMA

1.1. Planteamiento del problema

La teoría de números fue considerada por mucho tiempo como una matemática pura, y en ese tiempo estaba muy lejos de pensarse en aplicarla a la cotidianidad o a problemas reales. Hoy en día es posible encontrar aplicaciones a la Criptografía, teoría de la información y áreas como la biología, la química, la física y la acústica, pero muy pocas las que se encuentran al ajedrez.

1.2. Formulación del Problema

Dado lo anterior, ¿cómo podemos aplicar la congruencia modular y los teoremas de Euler, Wilson y Fermat al ajedrez?

1.3. Objetivos

1.3.1. Objetivo General

Aplicar la relación de congruencia módulo $m \in \mathbb{Z}^+$ y los teoremas de Euler, Fermat y Wilson en el juego del Ajedrez.

1.3.2. Objetivos Específicos

• Estudiar la relación de congruencia módulo $m \in \mathbb{Z}^+$ con sus propiedades.
• Identificar la relación existente entre los teoremas de Fermat, Euler y Wilson y la teoría de números de la relación de congruencia módulo $m \in \mathbb{Z}^+$.
• Aplicar los teoremas de la divisibilidad, de la congruencia módulo $m \in \mathbb{Z}^+$ y los tres teoremas de Euler, Fermat y Wilson al juego del ajedrez.

CAPÍTULO 2

PRELIMINARES

2.1. Divisibilidad

2.1.1. Divisibilidad

En este capítulo introducimos algunos conceptos útiles para el logro de nuestros objetivos. Entre ellos, algoritmo de Euclides, máximo común divisor, criterios de divisibilidad.

Definición 2.1.1. *Sean a, b enteros con $b \neq 0$, decimos que b divide a a si existe un entero c tal que $a = bc$. Si b divide a a, escribimos $b|a$.*

Teorema 2.1.1. *Sean $a, b, d, p, q \in \mathbb{Z}$ Entonces:*

a) Si $d \mid a$ y $d \mid b$ entonces $d \mid (ax \pm by)$ para cualquier $x, y \in \mathbb{Z}$

b) Si $d \mid (p + q)$ y $d \mid p$ entonces $d \mid q$

c) Si $a, b \in \mathbb{Z}^+$ y $b \mid a$ entonces $a \geqslant b$

d) Si $a \mid b$, entonces $a \mid mb$, con $m \in \mathbb{Z}$

e) Si a, b $\in \mathbb{Z}$, $a \mid b$ y $b \mid a$ entonces $|a| = |b|$

Demostración.

a) Sea $a = nd$ y $b = md$ siendo $n, m \in \mathbb{Z}$ entonces $ax + by = (nx + my)d$ entonces $d \mid (ax + by)$

b) Sea $p = kd$ y $p + q = k'd$, entonces $q = d(k' - k)$ entonces $d \mid q$

c) Como $a, b \in \mathbb{Z}^+$, y $a = kb$ entonces $k \geqslant 1$ por tanto $a = bk \geqslant b$

d) Sea $b = ka$, entonces $mb = mka = (mk)a$ entonces $a \mid mb$

e) El ítem c) sólo aplica si a y b son positivos si $a \mid b$ y $b \mid a$ entonces, $\mid a \mid\mid\mid b \mid$ y $\mid b \mid\mid\mid a \mid$, por el ítem c), $\mid a \mid \leqslant \mid b \mid$ y $\mid b \mid \leqslant \mid a \mid$ entonces $\mid a \mid = \mid b \mid$ (Mora, 2014, p.21.)

□

Teorema 2.1.2. *Si $n \mid a$ y $n \mid b$, entonces $n \mid (a \pm b)$*

Demostración. Por hipótesis tenemos que :

$$n \mid a \Rightarrow a = nq, \text{ para algún } q \in \mathbb{Z}$$
$$n \mid b \Rightarrow b = nq', \text{ para algún } q' \in \mathbb{Z}$$

Sumando (y restando) miembro a miembro estas igualdades, tenemos:

$$a \pm b = nq \pm nq', \text{ por lo tanto tenemos } a \pm b = n(q \pm q')$$

□

2.1.2. Algoritmo de la División

Definición 2.1.2. *(Principio del buen orden: PBO). Todo conjunto no vacío S de números naturales contiene un elemento mínimo.*
En particular, si $S \subset \mathbb{Z}$ y si S tiene al menos un elemento positivo, entonces S tiene un entero positivo mínimo.

Ejemplo 2.1.2.1. *Probar que si $a, b \in \mathbb{Z}$ con $b \geqslant 1$, entonces existe $q \in \mathbb{Z}$ tal que $qb \leqslant a < (q+1)b$*

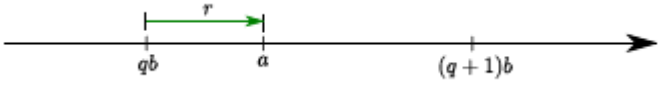
***Solución**: Sea $S = \{a - nb \text{ tal que } n \in \mathbb{Z} \wedge a - nb \geqslant 0\}$. Primero probamos que S no es vacío. En efecto, si $a \geqslant 0, a = a - 0 \cdot b \geqslant 0$, entonces $a \in S$. Si $a < 0, a - ab = a(1-b) \geqslant 0$ pues $b \geqslant 1$, entonces $a - ab \in S$. por PBO, S tiene un elemento mínimo $a - qb \geqslant 0$ y, por tanto $a - (q+1)b < 0$. Así, $qb < a < (q+1)b$.*

Teorema 2.1.3. *(Algoritmo de la división). Sean $a, b \in \mathbb{Z}$ con $b \neq 0$. Existen $q, r \in \mathbb{Z}$ únicos tales que $a = bq + r$ con $0 \leqslant r \leqslant \mid b \mid$*

Demostración. Primero vamos a demostrar el teorema para $a, b \in \mathbb{Z}$ con $b > 0$. Consideremos la progresión aritmética

$$..., -3b, -2b, -b, 0, b, 2b, 3b, ...$$

Por PBO (ver ejemplo 2.1.2.1) existe $q \in \mathbb{Z}$ tal que
$qb \leq a < (q+1)b$



Sea $r = a - qb$, entonces $a = bq + r$. De $qb \leq a$ obtenemos $0 \leqslant r$ y de $a < (q+1)b$ entonces $a - qb < b$ por tanto $a = bq + r$ con $0 \leqslant r < b$.

Unicidad: La prueba es por contradicción. Supongamos que existe $q_1, r_1 \in \mathbb{Z}$ tales que

$$a = bq_1 + r_1 \text{ con } 0 \leqslant r_1 < b \text{ y } a = bq + r \text{ con } 0 \leqslant r < b$$

Ahora supongamos que $r \neq r_1$ y que $r > r_1$. Como $a = bq_1 + r_1$ entonces,

$bq_1 + r_1 - (bq + r) = 0$ y $a = bq + r$ entonces $b(q_1 - q) = r - r_1$ luego $b|(r - r_1)$.

Como $b|(r - r_1)$, se tienen que $r - r_1 \geqslant b$, situación que es contradictoria pues $0 < r - r_1 < r < b$.

Por lo tanto $r = r_1$, de aquí: $b(q_1 - q) = r - r_1 = 0$ entonces $q_1 = q$.

Caso. Si $b < 0$**,** existen $q, r \in \mathbb{Z}$ únicos tales que $a = bq + r$ con $0 \leqslant r <\mid b \mid$ con lo que

$$a = b \cdot (-q) + r \text{ con } 0 \leqslant r <\mid b \mid.$$

Nota 1: Si $a, b \in \mathbb{Z}^+$, el algoritmo de la división corresponde a la división usual. si a o b es negativo, la división usual difiere del teorema de la división. □

2.1.3. Criterios de divisibilidad

Teorema 2.1.4. *Un entero positivo expresado en forma decimal es divisible por 2 si y solo termina en una cifra par (0,2,4,6,8), es decir si el número es par.*

Ejemplo 2.1.3.1. *El número 2758 es divisible por 2 (*$2 \mid 2758$*). Su último número termina en 8 y 8 es un número par.*

Teorema 2.1.5. *Un entero positivo expresado en forma decimal es divisible por 3 si y solo si la suma de sus dígitos es divisible por 3.*

Ejemplo 2.1.3.2. *El número 857 no es divisible por 3 (*$3 \nmid 857$*). Al sumar los dígitos que lo forman: 8 + 5 + 7 = 20 y 20 no es múltiplo de 3.*

Teorema 2.1.6. *Un entero positivo con más de un dígito expresado en forma decimal es divisible por 4, si y sólo si, al sumar el doble del penúltimos dígito y el último dígito da un número da como resultado un múltiplo de 4.*

Ejemplo 2.1.3.3. *El número 23824 es divisible por 4 (*$4 \mid 23824$*). Al sumar el doble penúltimos dígito y el último dígito se forman:* $2 \times 2 + 4 = 8$ *y 8 es múltiplo de 4.*

Teorema 2.1.7. *Un entero positivo expresado en forma decimal es divisible por 5 si y solo si sus dígitos terminan en 5 o en 0.*

Ejemplo 2.1.3.4. *El número 23670 es divisible por 5 (*$5 \mid 23670$*). Su último dígito termina en 0.*

Teorema 2.1.8. *Un entero positivo expresado en forma decimal es divisible por 6 si y solo si es divisible entre 2 y 3 a la vez, es decir, cuando es par y divisible por 3.*

Ejemplo 2.1.3.5. *El número 162 es divisible por 6 (*$6 \mid 162$*). Su último dígito termina en 2, que es una cifra par, y es divisible por 3 (*$3 \mid 162$*) porque 1+6+2=9, que es múltiplo de 3.*

Teorema 2.1.9. *Un entero positivo expresado en forma decimal es divisible por 9 si y sólo si la suma de sus dígitos es divisible por 9.*

Ejemplo 2.1.3.6. *el número 35.747.826 es divisible por 3 pues la suma de sus dígitos es*

$$3+5+7+4+7+8+2+6=42$$

y 42 es divisible por 3. Sin embargo como $9 \nmid 42$ *el número no es divisible por 9.*

2.1.4. El máximo común divisor

Definición 2.1.3. *Sean a y b enteros no ambos iguales a cero. El conjunto de todos los divisores comunes de a y b (un divisor común de a y b es un entero que divide a ambos números a y b) es un conjunto finito de números enteros cuyo máximo se denomina el Máximo Común Divisor de a y b. Lo notamos MCD(a, b) o simplemente (a, b).*

Puesto que, si $x|a$ entonces $x|(-a)$, es fácil observar que :

$$(a, b)=(a, -b)=(-a, b)= (-a, -b).$$ (Rubiano, p. 27)

Teorema 2.1.10. *Sean a y b enteros no ambos iguales a cero. El MCD (a, b) es el menor entero positivo que pueda escribirse en la forma $ax + by$ con x, y enteros.*

Demostración. supongamos que $d = (a, b)$ y sea

$$\mathbb{S} = \{z \in \mathbb{Z}^+ | z = ax + by \text{ con } x, y \in \mathbb{Z}\}$$

$\mathbb{S} \neq \emptyset$ puesto que $z = a^2 + b^2 \in \mathbb{S}$, luego por PBO, $\mathbb{S}$ posee un mínimo, llamémoslo g que podemos escribir en la forma $g = ax_0 + by_0$. Probaremos que $g = d = (a, b)$. En efecto g es divisor común de a y b, pues si dividimos a entre g tenemos:

$$a = qg + r \text{ con } 0 \leqslant r < g$$

luego,

$$\begin{aligned} r &= a - qg \\ &= a - q(ax_0 + by_0) \\ &= a(1 - qx_0) + b(-qy_0) \\ &= ax' + by'. \end{aligned}$$

Ahora, si $r \neq 0$ entonces $r \in \mathbb{S}$ lo cual contradice el mínimo de g, en consecuencia $r = 0$ y así $g|a$. Análogamente se verifica que $g|b$.

Como $d = (a, b)$ y g es un divisor común entonces $g \leqslant d$.

De otra parte $g = ax_0 + by_0$ y $d|a$ y $d|b$ luego $d|g$ y como ambos números son positivos $d \leqslant g$ y entonces $d = g$. □

Teorema 2.1.11. *Sean a y b enteros no ambos cero. Entonces $d = (a, b)$ si y sólo si d satisface las siguientes propiedades:*

1. $d > 0$

2. $d|a$ *y* $d|b$

3. *Si* $f|a$ *y* $f|b$ *entonces* $f|d$

Demostración. Supongamos que $d = (a, b)$. Tenemos inmediatamente que $d > 0$ y que $d|a$ y $d|b$. Además $d = ax + by$ para algún par de enteros x, y y si $f|a$ y $f|b$ entonces por el teorema 1.1.1. inciso (a) $f|d$.

Recíprocamente supongamos ahora que d satisface $(1), (2)$ y (3) y supongamos que f es un divisor común de a y b ; entonces por $(3) f|d$ y en consecuencia $|f| \leqslant |d| = d$, luego d es el mayor de los divisores comunes de a y b. □

Teorema 2.1.12. *Si $a = bq + r$ entonces $(a, b) = (b, r)$*

Demostración. Supongamos que $d = (a, b)$ y $d' = (b, r)$. Como $d|a$ y $d|b$ entonces $d|r = a - bq$ en consecuencia $d|d'$. Análogamente $d'|a = bq + r$ y en consecuencia $d'|d$. Como d y d' son positivos entonces $d = d'$. □

Teorema 2.1.13. *Sean a y b enteros no ambos nulos. Entonces,*

$$(a, b) = 1 \text{ si y sólo si existen enteros } x, y \text{ tales que } 1 = ax + by$$

Demostración. Si $(a, b) = 1$ el Teorema 2.1.6. garantiza la existencia de tales x, y. Recíprocamente, si existen x, y tales que $1 = ax + by$ entonces $(a, b)|1$ y por lo tanto, $(a, b) = 1$. □

Teorema 2.1.14. *Si $a|bc$ y $(a, b) = 1$ entonces $a|c$*

Demostración. Como $a|bc$ existe k tal que $bc = ak$. Como $(a, b) = 1$ existen enteros x, y tales que $ax + by = 1$. Por lo tanto,

$$c = c(ax + by) = acx + bcy = acx + bcy = a(cx + ky)$$

es decir $a|c$. □

Corolario 2.1.4. *Si $d = (a, b)$,entonces $(\frac{a}{d}, \frac{b}{d}) = 1$*

Demostración. Pues d=(a,b) existen enteros x,y tales que d=ax+by, por lo tanto, al dividir por d tenemos:

$1 = \frac{d}{d} = \frac{a}{d}x + \frac{b}{d}y$ □

Teorema 2.1.15. *Si $(a, b) = 1$ y $(a, c) = 1$ entonces $(a, bc) = 1$*

Demostración. Puesto que $(a, b) = 1$ y $(a, c) = 1$ tenemos que

$$1 = ax + by \text{ y también } a = qr + cs$$

con x, y, r, s enteros y por lo tanto

$$\begin{aligned} 1 &= (ax + by)(ar + cs) \\ &= a(xar + xsc + byr) + bc(ys) \end{aligned}$$

y en consecuencia $(a, bc) = 1$ □

2.1.5. Algoritmo de Euclides

Aun cuando hemos presentado criterios para decidir si un entero positivo es o no el máximo común divisor de dos enteros, no hemos presentado aún un procedimiento eficiente que nos permita encontrar el MCD de dos enteros dados a y b. Solucionamos ahora esta dificultad al presentar el denominado Algoritmo de Euclides. Euclides (365–300 AC) en su libro Elementos, dio este método para el cálculo del MCD.

Definición 2.1.5. *(Algoritmo de Euclides) Sean a y b números naturales, $b \neq 0$. Aplicando el teorema de la división se obtiene una sucesión finita a, $r_0 = b$,$r_1, r_2, r_3, ...r_n$. definida por*

$$\begin{aligned}
a &= r_0 q_1 + r_1 && 0 \leqslant r_1 < r_0 \\
r_0 &= r_1 q_1 + r_2 && 0 \leqslant r_2 < r_1 \\
r_1 &= r_2 q_2 + r_3 && 0 \leqslant r_3 < r_2 \\
&\cdot \\
&\cdot \\
&\cdot \\
r_{n-2} &= r_{n-1} q_n + r_n && 0 \leqslant r_n < r_{n-1} \\
r_{n-1} &= r_n q_{n+1} + 0 && 0 \leqslant r_{n+1} = 0
\end{aligned}$$

(Correctitud del algoritmo) Aplicando el teorema de la división obtenemos una sucesión decreciente de residuos $0 \leqslant ... < r_k < r_{k-1} < ... < r_1 < r_0 = b$. La sucesión es finita pues entre 0 y $r_0 \neq 0$ solo puede haber un número finito de enteros.

Por tanto algún residuo debe ser cero (sino, se podría aplicar el teorema de la división indefinidamente y tendríamos una sucesión infinita de enteros entre 0 y b, lo cual es imposible). Si b/a , entonces r_1=0 y r_0 sería el mínimo residuo positivo. En general, debe haber un residuo mínimo $r_n > 0$ y $r_n + 1 = 0$.

$$\begin{aligned}
mcd(a,b) &= mcd(a - r_0 q, r_0) \\
&= mcd(r_1, r_0) \\
&= mcd(r_1, r_0 - r_1 q_2) \\
&= mcd(r_1, r_2) \\
&= mcd(r_1 - r_2 q_2, r_2) \\
&= mcd(r_3, r_2) \\
&= mcd(r_{(n-1)}, r_n) \\
&= mcd(r_n, 0) = r_n(Mora, 2014, p,37)
\end{aligned}$$

Ejemplo 2.1.6. *Encontrar* $(687, -234)$ *y expresarlo como combinación lineal de* 687 *y* -234. *Aplicando el Algoritmo de Euclides tenemos,*

$$687 = (234)(2) + 219$$

$$234 = (219)(1) + 15$$

$$219 = (15)(1) + 6$$

$$15 = (9)(1) + 6$$

$$9 = (6)(1) + (3)$$

$$6 = (3)(2) + 0.$$

Por lo tanto $(687, -284) = (687, 234) = 3$.
Además, empezando con la penúltima ecuación obtenemos

$$3 = 9 - 6$$

$$6 = 15 - 9$$

$$9 = 219 - (15)(14)$$

$$15 = 234 - 219$$

$$219 = 687 - (2)(234),$$

y reemplazando los residuos sucesivamente tenemos,

$$3 = 9 - 6$$

$$= 9 - [15 - 9] = (2)(9) - 15$$

$$= 2\,[219 - (14)(15)] - 15 = (2)(219) - (29)(15)$$

$$(2)(219) - 29\,[234 - 219] = (31)(219) - (29)(234)$$

$$31\,[687 - (2)(234)] - (29)(234)$$

$$(31)(687) - (91)(234),$$

luego

$$(687, -234) = 3 = (31)(687) + (91)(-234).$$

CAPÍTULO 3

LA RELACIÓN DE CONGRUENCIA MÓDULO $M \in \mathbb{Z}^+$

3.1. Congruencia

En este capítulo mostraremos algunos resultados de la relación de congruencia módulo $m \in \mathbb{Z}^+$ que serán de utilidad para el logro de los objetivos propuestos.

Definición 3.1.1. *Sea $m \in \mathbb{Z}^+$, Decimos que a es congruente con b módulo m y escribimos $a \equiv b \ (mod\ m)$, si $m \mid (a-b)$.*

Ejemplo 3.1.2. *Pruebe que las siguientes congruencias modulares son ciertas.*

a) $12 \equiv 2(mod\ 5)$

b) $20 \equiv -6(mod\ 2)$

c) $14 \equiv -1(mod\ 5)$

Solución

a) $12 \equiv 2(mod\ 5)$, pues $5 \mid (12-2)$, esto es, $5 \mid 10$

b) $20 \equiv -6(mod\ 2) \leftrightarrow 2 \mid 20+6 \leftrightarrow 2 \mid 26$

c) $14 \equiv -1(mod\ 5) \leftrightarrow 5 \mid 14+1 \leftrightarrow 5 \mid 15$

Si a no es congruente con b módulo m escribimos

$$a \not\equiv b(mod\ m)$$

Ejemplo 3.1.3. $16 \not\equiv -1(mod\ 15)$

Solución

$16 \not\equiv -1(mod\ 15)$, *pues* $15 \nmid 17$

Teorema 3.1.1. *Dos enteros a y b son congruentes módulo m si y sólo si dejan el mismo residuo al dividirlos por m.*

Demostración. Supongamos que $a \equiv b(mod\ m)$ y sea r el residuo de dividir b por m. Entonces, existe un entero k tal que $a - b = km$ y además $b = qm + r$ con $0 \leqslant r < m$. En consecuencia

$$a = b + km = (qm + r) + km$$

$$= (q + k)m + r$$

Como $(q + k) \in \mathbb{Z}$ y $r < m$, entonces r es el residuo de dividir a entre m.
Recíprocamente, supongamos que a y b tienen el mismo residuo al dividirlos por m. Tenemos entonces

$$a = q_1 m + r$$

$$b = q_2 m + r;$$

con $0 \leqslant r < m$. En consecuencia, restando término a tenemos

$$a - b = (q_1 - q_2)m,$$

es decir;

$$a \equiv b(mod\ m)$$

□

3.1.1. Relación de Equivalencia

Teorema 3.1.2. *La congruencia módulo m es una relación de equivalencia sobre $\mathbb{Z}$*

Demostración.

1 Reflexiva: Para cualquier entero a, $m \mid (a - a) = 0$ es decir, $a \equiv a(mod\ m)$

2 Simétrica : Si $a \equiv b(mod\ m)$entonces $m \mid (a - b)$, y por lo tanto $m \mid -(a - b) = b - a$, luego $b \equiv a(mod\ m)$

3 Transitiva: Si $a \equiv b(mod\ m)$ y $b \equiv c(mod\ m)$ entonces $m \mid (a - b)$ y $m \mid (b - c)$, por lo tanto $m \mid \{(a - b) + (b - c)\} = a - c$, es decir $a \equiv c(mod\ m)$ □

Teorema 3.1.3. *Si $a \equiv b(mod\ m)$ y $c \equiv d(mod\ m)$ entonces*

1) Para todo par de enteros r y s, $ar + cs \equiv br + ds(mod\ m)$

2) $a + c \equiv b + d(mod\ m)$

3) $a - c \equiv b - d(mod\ m)$

4) $ac \equiv bd(mod\ m)$

5) Para todo entero positivo k, $a^k \equiv b^k(mod\ m)$

6) Para todo entero r, $a + r \equiv b + r(mod\ m)$

7) Para todo r, $ar \equiv br(mod\ m)$

Demostración.

1) La hipótesis dice que $m \mid (a - b)$ y $m \mid (c - d)$ luego, por el Teorema 1.1.1 tenemos que $n \mid \{r(a - b) + s(c - d)\} = (ar + cs) - (br + ds)$ por lo tanto $ar + cs \equiv br + ds(modm)$

2) Por el teorema 2.1.1. $m \mid (a-b)$ y $m \mid (c-d)$ por tanto $m \mid (a+c)-(b+d)$ entonces $a+c \equiv b+d(mod\, m)$

3) Por el teorema 2.1.1. $a-c \equiv b-d(mod\, m)$ tomando que $r=1$ y $s=-1$ por lo tanto $ar \equiv br(mod\, m)$, entonces $a \equiv b(mod\, m)$ y $sc \equiv sd(mod\, m)$ donde $-c \equiv -d(mod\, m)$. En consecuencia $m \mid a-c-b+d$, entonces $a-c \equiv b-d(mod\, m)$

4) Sea $a \equiv b(mod\, m)$ y $c \equiv d(modm)$ para $m \mid c(a-b)+b(c-d)$ tal que $m \mid ac-bc+bc-bd$, entonces $ac \equiv bd(mod\, m)$

5) Por inducción sobre k tenemos que para $k=1$ la afirmación es obvia. Además si suponemos que $a^k \equiv b^k(mod\, m)$, puesto que $a \equiv b(mod\, m)$ obtenemos aplicando 4) que $a^{k+1} \equiv b^{k+1}(modm)$. Por el principio de inducción matemática el resultado es cierto para todo entero positivo k.

6) Sea $r=s=1$ con inciso 2) de las congruencias $r \equiv r(mod\, m)$ y $a \equiv b(mod\, m)$, entonces por 2) tenemos $a+r \equiv b+r(mod\, m)$

7) Sea $s=0$ por inciso 1), tenemos que $ar+0c \equiv br+0d(mod\, m)$ entonces $ar \equiv br(mod\, m)$ □

Corolario 3.1.4. *Si $ac \equiv bc(mod\, m)$ y $(c,m)=1$ entonces $a \equiv b(mod\, m)$*

Teorema 3.1.4. *Si $ac \equiv bc(mod\, m)$ y $d=(c,m)$ entonces $a \equiv b(mod\frac{m}{d})$*

Demostración. Por hipótesis $m \mid (ac-bc)$ es decir, $c(a-b)=km$ con k entero. De otra parte como $d=(c,m)$ tenemos por el colorario (si $d=(a,b)$, entonces (Corolario 2.1.4. $(\frac{a}{d},\frac{b}{d})=1$) que $c=dC$ y $m=dM$ donde $(C,M)=1$. Por lo tanto tenemos $dC(a-b)=kdM$ y entonces $C(a-b)=km$. Luego $M \mid C(a-b)$ y como $(C,M)=1$ entonces $M \mid (a-b)$. En otros términos $a \equiv b(mod\, M)$ o sea $a \equiv b(mod\frac{m}{d})$. □

Corolario 3.1.5. *Si $a \equiv b(mod\, m)$ y $p(x)$ es un polinomio con coeficientes enteros, entonces $p(a) \equiv p(b)(mod\, m)$.*

Ejemplo 3.1.6. *Hallemos el residuo obtenido al dividir 7^{135} por 8. Observemos que*

$$7^2 \equiv 1(mod\, 8)$$
$$(7^2)^{67} \equiv 1(mod\, 8)$$
$$(7^2)^{67} \cdot 7 \equiv 7(mod\, 8)$$

Como $(7^2)^{67} \cdot 7 = 7^{135}$, entonces $7^{135} \equiv 7(mod\, 8)$ luego por el teorema 2.1.3. tenemos

$$7^{135} = (7^2)^{67} \cdot 7 = 1 \cdot 7 \equiv 7(mod\, 8)$$

aplicando el teorema 2.1.1 (inciso 5) el residuo de dividir 7^{135} por 8 es el mismo de dividir 7 por 8, es decir 7.

3.1.2. Congruencia Lineales

Teorema 3.1.5. *La congruencia lineal $ax \equiv b(mod\, m)$ tiene solución si y solo si $d|b$, donde $d=(a,m)$. Si la congruencia tiene solución, entonces tiene exactamente d soluciones incongruentes.*

Dividimos la demostración en 5 partes

1) Si $d|b$, hay una solución

2) Si hay solución, $d|b$

3) Si x_0 es una solución entonces $x_0 + k\frac{n}{d}$ es solución para todo entero k

4) Todas las soluciones se encuentran entre las soluciones mencionadas en 3

5) Las soluciones incongruentes son precisamente

$$x_0, x_0 + \frac{a}{d}, x_0 + \frac{2n}{d}, ..., x_0 + \frac{(d-1)m}{d}$$

Demostración.

1) Supongamos que $d|b$, luego $b = cd$ Para algún c. Como $d = (a, m)$, por el teorema 1.1.6. podemos expresar d en la forma $d = ar+sm$.Multiplicando por c obtenemos $b = cd = car+csm$ por tanto $acr \equiv b(mod\, m)$ y cr es una solución de la congruencia lineal

$$ax \equiv b(mod\, m)$$

2) Supongamos que x_0 es una solución de la congruencia lineal, luego $ax_0 \equiv b(mod\, m)$ y por lo tanto existe un entero k tal que $ax_0 - b = km$. Como $d|a$ y $d|m$, se sigue que $d|b$ como habíamos mencionado.

3) Supongamos que x_0 es una solución de la congruencia dada. Para todo entero k tenemos

$$a\left(x_0 + k\frac{m}{d}\right) = ax_0 + km\left(\frac{a}{d}\right) \equiv ax_0 \equiv b(mod\, m)$$

puesto que $d|a$

4) Supongamos que x_1 es otra solución de las congruencia dada.
Tenemos

$$ax_1 \equiv b \equiv ax_0(mod\, m)$$

y por el teorema 3.1.4.

$$x_1 \equiv x_0(mod\frac{m}{d})$$

luego existe un entero k tal que

$$x_1 = x_0 + k\frac{m}{d}$$

5) Claramente la soluciones

$$x_0, x_0 + \frac{m}{d}, x_0 + \frac{2m}{d}, ..., x_0 + \frac{(d-1)m}{d}$$

Son incongruentes módulo m, puesto que dos cualesquiera de ellas no puede diferir por un múltiplo de m. Además cada solución de la forma $x_0 + \frac{km}{d}$ es congruente módulo m con alguna

de estas d soluciones, ya que por el algoritmo de la división podemos expresar a k en la forma $k = qd + r$ con $0 \leq r < d$, y en consecuencia

$$\begin{aligned} x_0 + k\frac{m}{d} &= x_0 + (qd + r)\frac{m}{d} \\ &= x_0 + qm + r\frac{m}{d} \\ &= x_0 + r\frac{m}{d}(mod\ m).(Rubiano, p, 122) \end{aligned}$$

□

Teorema 3.1.6. *Consideremos la congruencia lineal $ax \equiv b(modm)$ si y_0 es una solución de la congruencia $my \equiv -b(moda)$, entonces el número $x_0 = \dfrac{my_0 + b}{a}$ es una solución de la congruencia original.*

Demostración. Como y_0 es una solución de la congruencia $my \equiv -b(mod\ a)$, entonces x_o es un entero y además

$$\begin{aligned} ax_0 &= a\frac{my_0 + b}{a} \\ &= my_0 + b \\ &\equiv b(mod\ m) \end{aligned}$$

luego x_0 es una solución de $ax \equiv b(mod\ m)$ □

3.1.3. Congruencia Euler, Fermat, Wilson

Definición 3.1.7. *Para cada entero positivo m, definimos $\Phi(m)$ como el número de enteros positivos menores o iguales que m y primos relativos con m.*

Definición 3.1.8. *Un subconjunto R del conjunto de los enteros se llama un sistema reducido de residuos módulo m si satisface las condiciones siguientes*

1) R tiene $\Phi(m)$ elementos.

2) Para cada $r \in R$ se tiene que (r,m)=1,

3) Los elementos de R son incongruentes módulo m.

Teorema 3.1.7. *Si $\{r_1, r_2, ..., r_{\Phi(m)}\}$ es un sistema reducido de residuos módulo m y si $(k_{r_i}, m) = 1$ entonces $\{k_{r_1}, k_{r_2,...,k_{r_{\Phi(m)}}}\}$ también es un sistema reducido de residuos módulo m.*

Demostración. La condición 1) de la definición de sistema reducido es evidente. Como $(r_i, m) = 1$ para cada i y $(k, m) = 1$, por el teorema 2.1.12. se tiene que $(k_{r_i,m}) = 1$ para cada i y se cumple la condición 2.

Finalmente, no puede tenerse que dos de los números kr_i sean congruentes módulo m, ya que si $kr_i \equiv kr_j(mod\ m)$ entonces $r_i \equiv r_j(mod\ m)$ por el corolario 3.1.4. lo que contradice la hipótesis de que $\{\ r_1, ...r_{\Phi(m)}\ \}$ es un sistema reducido de residuos módulo m, por lo tanto, también se cumple la condición 3 de la definición y se tiene el teorema. □

Teorema 3.1.8. ***(Teorema de Euler).*** *Si* $(a, n) = 1$ *entonces*

$$a^{\Phi(m)} \equiv 1 \ (mod\, m).$$

Demostración. Sea $\{r_1, r_2, ..., r_{\Phi(m)}\}$ un sistema reducido de residuos módulo m. Por el teorema anterior el conjunto $\{ar_1, ar_2, ..., ar_{\Phi(m)}\}$ es también un sistema reducido de residuos módulo m. Por lo tanto el producto de los enteros del primer conjunto es congruente al producto de los enteros del segundo conjunto. Luego

$$r_1 r_2 ... r_{\Phi(m)} \equiv a^{\phi(m)} r_1 r_2 ... r_{\phi(m)} (mod\, m)$$

Como cada r_i es primo relativo con m, por el Corolario 3.1.4. podemos cancelar cada uno de los r_i y obtenemos

$$1 \equiv a^{\Phi(m)} \ (mod\, m)$$

□

Corolario 3.1.9. ***(Teorema de Fermat).*** *Si* m *es un número primo y* $(a, m) = 1$*, entonces*

$$a^{m-1} \equiv 1 \ (mod\, m).$$

Demostración. Es consecuencia inmediata del Teorema de Euler, tomando a $\Phi(m) = m - 1$. □

Una forma equivalente del Teorema de Fermat es el enunciado siguiente.

Teorema 3.1.9. *Si* m *es un número primo, entonces*

$$a^m \equiv a (mod\, m).$$

para cualquier entero a

Demostración. Si $m \nmid a$ entonces $(a, m) = 1$ y por el corolario anterior

$$a^{m-1} \equiv 1 (mod\, m).$$

Por el teorema 2.1.3 tenemos que

$$a^m \equiv a (mod\, m).$$

Si $m|a$, tenemos que

$$a \equiv 0 (mod\, m) \quad y \quad a^m \equiv 0 (mod\, m),$$

y por transitividad

$$a^m \equiv a (mod\, m).$$

□

Teorema 3.1.10. *Si* $(a, m) = 1$*,la solución de la congruencia lineal*

$$ax \equiv b (mod\, m)$$

es

$$x \equiv a^{\Phi(m)-1} b (mod\, m)$$

Demostración. Por el Teorema de Euler tenemos

$$a^{\Phi(x)} \equiv 1 (mod\, m)$$

Por lo tanto

$$a^{\Phi(x)}b \equiv b(mod\, m)$$

Luego la congruencia lineal toma la forma

$$ax \equiv a^{\Phi(x)}b(mod\, m)$$

de donde

$$x \equiv a^{\Phi(x)-1}b(mod\, m)$$

ya que (a,m)=1

□

Teorema 3.1.11. *(Teorema de Lagrange).Si m es un número primo y $f(x) = a_0 + a_1x + ... + a_nx^n$ es un polinomio de grado $n \geqslant 1$ con coeficientes enteros y tal que $a_n \not\equiv 0(mod\, m)$, entonces la congruencia polinómica*

$$f(x) \equiv 0(mod\, m)$$

tiene a lo más n soluciones incongruentes módulo m.

Demostración. La demostracción es por inducción sobre el grado n de $f(x)$.

Cuando $n = 1$, la congruencia es lineal,

$$a_0 + a_1x \equiv 0(mod\, m),$$

Con $a_1 \not\equiv 0(mod\, m)$ y por el teorema 3.1.5. esta congruencia tiene exactamente una solución.

Supongamos que el teorema es cierto para los polinomios de grado $n - 1$.
Consideramos un polinomio $f(x)$ de grado n y escojamos una solución a de la congruencia $f(x) \equiv 0(mod\, m)$.Podemos escribir

$$f(x) = (x - a)g(x) + r$$

Con r constante y $g(x)$ un polinomio de grado $n - 1$ con coeficientes enteros y coeficiente principal a_n.

De la ecuación anterior tenemos $f(a) = r$ y como $f(a) \equiv 0(mod\, m)$, entonces $r \equiv 0(mod\, m)$ y para todo x tenemos que

$$f(x) \equiv (x - a)g(x)(mod\, m) \tag{3.1}$$

Por la hipótesis de inducción de congruencia $g(x) \equiv 0(mod\, m)$ tiene a lo más $n-1$ soluciones incongruentes.Supongamos que ellas son $c_1, c_2, ..., c_r$ con $r \leqslant n - 1$.Si c es un número tal que $f(c) \equiv 0(mod\, m)$, entonces de (3.1.2.)

$$(c - a)g(c) \equiv 0(mod\, m)$$

Así que

$$c \equiv a(mod\, m)$$

o

$$g(c) \equiv 0(mod\, m)$$

En el este último caso $c = c_i$ para algún i con $1 \leqslant i \leqslant r$ y la congruencia $f(x) \equiv 0(mod\, m)$ tiene a lo mas $r+1 \leqslant n$ soluciones. Luego el teorema es verdadero por el principio de inducción. □

Corolario 3.1.10. *Si $f(x) = a_0 + a_1x + ... + a_nx^n$ es un polinomio de grado n con coeficientes enteros, y si la congruencia*

$$f(x) \equiv 0(mod\, m),$$

con m primo, tiene más de n soluciones, entonces todos los coeficientes de $f(x)$ son divisibles por m.

Demostración. Supongamos que no todos los coeficientes son divisibles por m. Sea k el mayor indice tal que $m \nmid a_k$. Luego $k \leq n$ y la congruencia $f(x) \equiv 0(mod\, m)$ se reduce a

$$a_0 + a_1x + ... + a_kx^k \equiv 0(mod\, m).$$

Como esta última congruencia tiene más de k soluciones, se contradice el Teorema d lagrange. Por lo tanto todos los coeficientes de $f(x)$ deben de ser divisibles por m. □

Teorema 3.1.12. ***(Teorema de Wilson).*** *Para todo número primo m se tiene que*

$$(m-1)! + 1 \equiv 0(mod\, m).$$

Demostración. Consideremos el polinomio de grado $m-2$ definido por

$$f(x) = (x-1)(x-2)...(x-m+1) - (x^{m-1} - 1).$$

Por el teorema de Fermat, cada uno de los números $1, 2, ..., m-1$ es una solución de la congruencia $f(x) = 0(mod\, m)$. Por el Corolario anterior los coeficientes de $f(x)$ son divisibles por m, en particular el término constante

$$f(0) = (-1)^{m-1}(m-1)! + 1,$$

es divisible por m, o sea
$(-1)^{m-1}(m-1)! + 1 \equiv 0(mod\, m)$. Si m es impar $(-1)^{m-1} = 1$,y si $m = 2, (-1)^{m-1} = -1 \equiv 1(mod\, m)$. Luego en cualquier caso

$$(m-1)! + 1 \equiv 0(mod\, m)$$

□

CAPÍTULO 4

APLICACIONES DEL AJEDREZ A LA TEORÍA DE NÚMEROS

4.1. Reseña histórica del ajedrez

El ajedrez, tal como lo conocemos en la actualidad, tiene más de cinco siglos de existencia, ya que su modificación definitiva ocurrió en el transcurso del siglo XV, en los albores del Renacimiento europeo. Sin embargo, en esencia es mucho más antiguo pues, se cree, proviene del "chaturanga", juego que se practicaba en la India por el siglo V antes de nuestra era. De ahí llegó a Persia y a fines del primer milenio lo introdujeron a Europa los árabes en la España Medieval, sufriendo cambios constantes en las reglas y forma de movimiento de las piezas a través de los siglos hasta llegar a su forma actual.

La imagen del ajedrez ha estado simbolizada a través de sus grandes figuras, desde el legendario jugador norteamericano Paul Morphy (considerado primer campeón no oficial al vencer a Anderssen en 1858) o el austriaco Wilhelm Steinitz (primer campeón oficial al derrotar a Zukertort en 1886). Le siguieron otras grandes personalidades del juego-ciencia como el alemán Emmanuel Lasker (poseedor del reinado más duradero: desde 1894 hasta 1921), el prodigioso cubano José Raúl Capablanca (vencedor de Lasker) y el ruso Alexander Alekhine. La hegemonía soviética comenzó luego de finalizar la segunda guerra mundial con Mijail Botvinnik y se mantuvo con Vassily Smyslov, Mijail Tal, Tigran Petrosian y Boris Spassky y sólo se detuvo con la aparición del genial jugador norteamericano "Bobby" Fischer.(que destronó a Spassky en 1972 en un memorable encuentro). En 1975 Anatoly Karpov se proclamó campeón mundial al negarse Fischer a defender su trono, pero lo perdió en 1985 contra otro grande: Garry Kasparov". Kasparov fue campeón de 1985 al 2000, le sucedió Vladimir Kramnik del 2000 al 2007 fecha en que fue derrotado por Viswanathan Anand quien actualmente sigue siendo poseedor del campeonato mundial (Balderas, 2010, P.5.).

4.1.1. El tablero

El tablero de ajedrez es un cuadrado subdividido en 64 casillas (8×8) cuadradas, alternativamente de color claro y de color oscuro. Cada jugador se sitúa de cara al ajedrecista contrincante, colocando el tablero de manera tal que cada jugador tenga una casilla blanca en su esquina derecha.

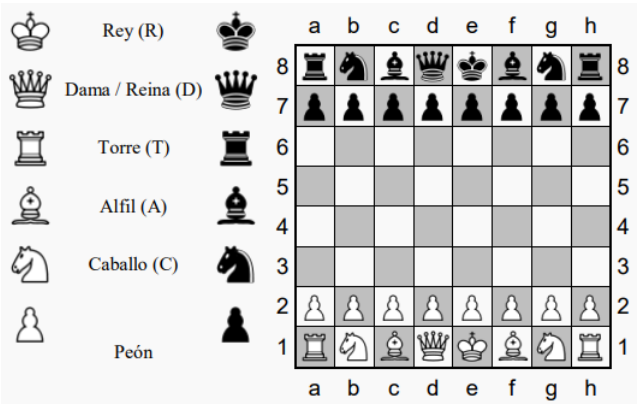
Los elementos básicos del tablero son:

• **Columna:** Es cada una de las ocho líneas de ocho casillas que se forman alineando éstas verticalmente respecto a los jugadores.
• **Fila:** Es cada una de las ocho líneas de ocho casillas que se forman alineando éstas horizontalmente respecto a los jugadores.
• **Diagonal:** Es cada una de las 16 líneas que se forman agrupando las casillas diagonalmente. Las dos diagonales mayores tienen ocho casillas.
• **Centro:** El centro del tablero son los cuatro escaques centrales. Por extensión, a veces se incluyen los 12 que rodean a esos cuatro.
• **Esquinas:** Cada una de las cuatro casillas ubicadas en las aristas del tablero.
• **Bordes:** Las dos columnas y dos filas situadas en las esquinas del tablero.
• **Casillas:** Los 64 cuadros que se originan de la intersección de filas y columnas donde cada casilla tiene su respectivo nombre de acuerdo a la letra y número encontrado entre la intersección de las filas y columnas.

	a	b	c	d	e	f	g	h	
8	a8	b8	c8	d8	e8	f8	g8	h8	8
7	a7	b7	c7	d7	e7	f7	g7	h7	7
6	a6	b6	c6	d6	e6	f6	g6	h6	6
5	a5	b5	c5	d5	e5	f5	g5	h5	5
4	a4	b4	c4	d4	e4	f4	g4	h4	4
3	a3	b3	c3	d3	e3	f3	g3	h3	3
2	a2	b2	c2	d2	e2	f2	g2	h2	2
1	a1	b1	c1	d1	e1	f1	g1	h1	1
	a	b	c	d	e	f	g	h	

"Balderas". (2010), figura 1.

En el tablero del ajedrez se ubican también las piezas para determinar su posición inicial.



"Balderas". (2010), figura 2.

Posición inicial de las piezas negras:

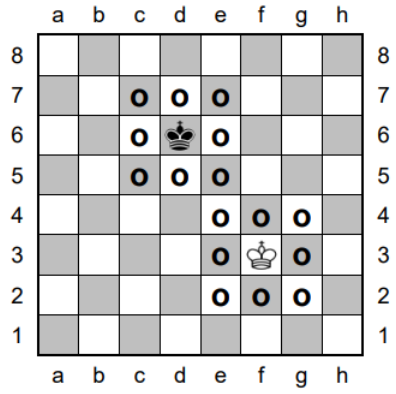
• Torre: posición $a8, h8$
• Caballo: posición $h8, g8$
• Arfil: posición $c8, f8$

• Reina: posición $d8$
• Rey: posición $e8$
• Peón: posición $a7, b7, c7, d7, e7, f7, g7, h7$.
Posición inicial de las piezas Blancas:
• Torre: posición $a1, h1$
• Caballo: posición $h1, g1$
• Arfil: posición $c1, f1$
• Reina: posición $d1$
• Rey: posición $e1$
• Peón: posición $a2, b2, c2, d2, e2, f2, g2, h2$.

4.1.2. Piezas del Ajedrez

El rey

En un juego convencional de ajedrez, el blanco empieza el juego con el rey en la primera fila junto a la dama. El rey se mueve en dirección horizontal, vertical o diagonal, aunque sólo se puede desplazar una casilla en cada movimiento, a excepción de la jugada especial llamada enroque. El rey no puede moverse a una casilla que esté amenazada por una pieza enemiga, o una que esté ocupada por una pieza del mismo equipo. Cada equipo tiene un rey.

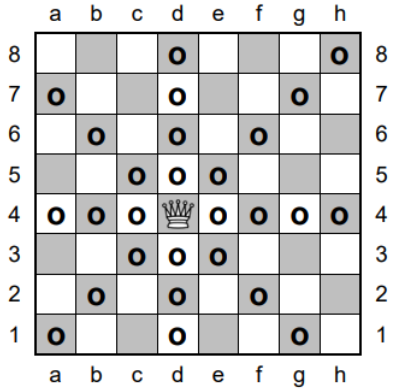


"Balderas". (2010), figura 3.

Además, los reyes nunca pueden ocupar casillas adyacentes, ya que estas son casillas amenazadas por el rey contrario. Los reyes se encuentran en oposición cuando se encuentran uno frente al otro en columnas, filas ó diagonales; gracias a la oposición podemos ganar espacio para poder pasar a un lugar deseado (Balderas,2010, P.9.).

La Reina

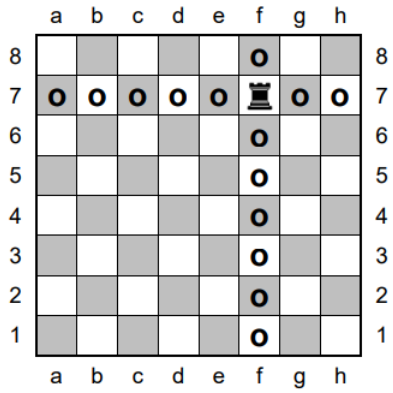
La Reina puede ser jugada sobre columnas, filas y diagonales, en una línea recta y en cualquier número de casillas vacantes sin pasar por encima de una pieza o de un peón, por lo tanto, o bien se detiene delante de éstos, o bien puede capturarlos si se trata de una pieza o peón del equipo contrario. Cada equipo tiene una reina.



"Balderas". (2010), figura 4.

La Torre

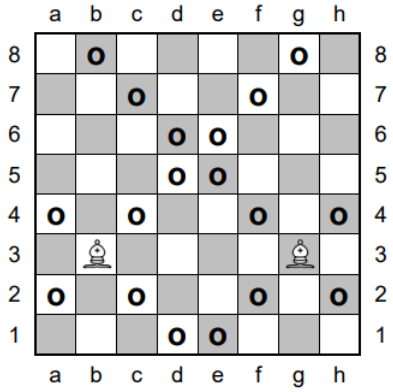
La torre se juega siempre en línea recta, recorriendo tanto columnas como filas; se puede desplazar una o más casillas sin pasar por encima de una pieza o de un peón, por lo tanto, o bien se detiene delante de éstos, o bien puede capturarlos si se trata de una pieza o peón del equipo contrario. Cada equipo tiene dos torres.



"Balderas". (2010), figura 5.

El alfil

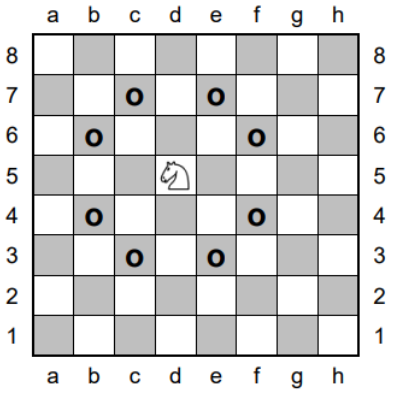
El Alfil se juega siempre en línea recta, recorriendo únicamente las diagonales; se puede desplazar una o más casillas sin pasar por encima de una pieza o de un peón, por lo tanto, o bien se detiene delante de éstos, o bien puede capturarlos si se trata de una pieza o peón del equipo contrario. Cada equipo tiene dos alfiles uno en casillas blancas y uno en negras. Cada equipo tiene dos alfiles.



"Balderas". (2010), figura 6.

El caballo

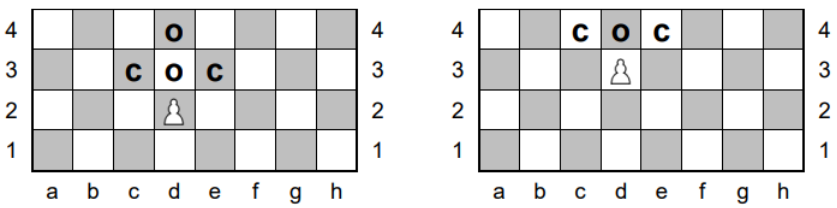
Al mover, el caballo siempre cambia de color su casilla; es decir, si parte de una casilla blanca, terminará en una negra y viceversa; siempre será al segundo cuadro concéntrico al que está posicionado. Cada equipo tiene dos caballos.



"Balderas". (2010), figura 7.

El peón

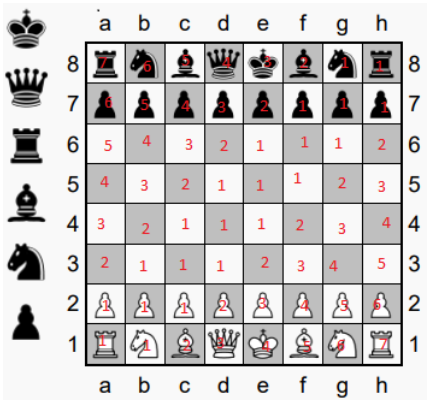
Cada bando tiene ocho peones y se colocan en la segunda línea los blancos y en la séptima los negros. Su movimiento es limitado, ya que se mueven una casilla hacia adelante, aunque en su posición inicial pueden mover también dos escaques. Un peón no puede retroceder, siempre va hacia adelante, cuando captura alguna pieza rival, lo hace en forma diagonal, una sola casilla. Es decir, sus movimientos de avance y de captura son diferentes.



"Balderas". (2010), figura 8.

4.2. Notación numérica

El ajedrez cuenta con una 64 casillas en el tablero, cada una de ellas tiene un valor númerico donde reflejamos la simetría, es decir, parte de una diagonal de valor númerico uno donde esta se halla a partir de la primera fila y columna, realizando la resta entre las casillas, allí cada casilla se convierte en el valor posicional de la pieza.



"Vaquiro y Rangel". (2021), figura 9.

De manera análoga el ajedrez es un juego para practicar la memoria y el razonamiento que serán la herramienta para el pensamiento lógico donde el valor numérico de las piezas en cada casilla teniendo en cuenta la Figura 9 y la posición inicial de la pieza será:

Valor númerico de las piezas negras:

- Torre $a8$: **7**
- Torre $h8$: **1**
- Caballo $b8$: **6**
- Caballo $g8$: **1**
- Alfil $c8$: **5**
- Alfil $f8$: **2**
- Reina $d8$: **4**
- Rey$e8$: **3**
- Peón $a7$: **6**
- Peón $b7$: **5**
- Peón $c7$: **4**
- Peón $d7$: **3**
- Peón $e7$: **2**
- Peón $f7$: **1**
- Peón $g7$: **1**
- Peón $h7$: **1**

Valor númerico de las piezas blancas:

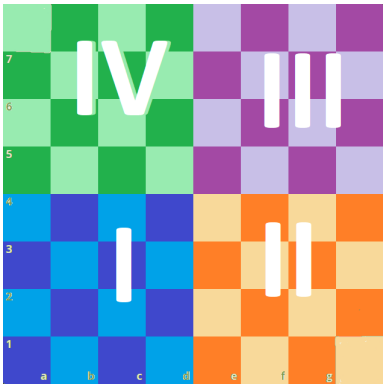
- Torre $a1$: **1**
- Torre $h1$: **7**
- Caballo $b1$:**1**
- Caballo $g1$: **6**

- Alfil $c1$: **2**
- Alfil $f1$: **5**
- Reina $d1$: **3**
- Rey $e1$: **4**
- Peón $a2$: **1**
- Peón $b2$: **1**
- Peón $c2$: **1**
- Peón $d2$: **2**
- Peón $e2$: **3**
- Peón$f2$: **4**
- Peón$g2$: **5**
- Peón $h2$: **6**

4.2.1. Definiciones y fórmulas en el ajedrez

Para las aplicaciones de resolución de problema en el ajedrez vamos a tener en cuenta la simetría del tablero, el valor numérico y las dimensiones de este.

Definición 4.2.1. Los ejes de coordenadas en el ajedrez son dos rectas perpendiculares que se cortan en un punto dividiendo el tablero en cuatro cuadrantes, formando cada uno la misma cantidad de casillas (16).



"Vaquiro y Rangel". (2021), figura 10.

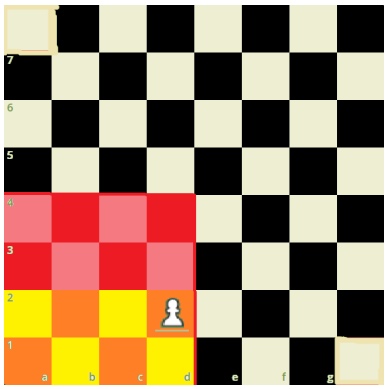
Definición 4.2.2. Llamaremos área mayor a la cantidad de filas por columnas de los cuadrantes en el tablero del ajedrez.

Definición 4.2.3. Llamaremos área menor a la base por la altura desde la posición de la pieza en el tablero del ajedrez.

Definición 4.2.4. Llamaremos la razón de una pieza en el tablero del ajedrez a la diferencia entre el área mayor menos el área menor.

Ejemplo 4.2.1.1. Hallar el área mayor, el área menor y la razón del peón en la posición d2

Solución:



"Vaquiro y Rangel". (2021), figura 11.

$$\text{Área mayor} = 4 \times 4 = 16$$
$$\text{Área menor} = 4 \times 2 = 8$$

Luego,

$$\text{Área mayor - área menor} = \text{razón}$$
$$16 - 8 = 8$$

Por tanto la razón del peón d2 es 8.

Teniendo en cuenta las definiciones anteriores se aplicarán las siguientes fórmulas para las piezas del ajedrez en el uso adecuado de situaciones problemas.

• **Fórmula del peón :** Tendremos en cuenta que,

$\boldsymbol{a}$= Cantidad de movimientos de la pieza
$\boldsymbol{b}$=Valor posicional de la pieza inicial
$\boldsymbol{q}$= Razón
$\boldsymbol{r}$= Posición de llegada

A partir de lo anterior, se aplica la fórmula del algoritmo de la división, la pieza estará en cualquier posición ubicada en el tablero teniendo en cuenta que sus movimientos sean correctos y partan de la posición incial adecuada:

$$a = bq + r \text{ donde } 0 \leq r \leq q \qquad (4.2.1.)$$
$$\text{Movimientos=(partida)(razón)+llegada}$$

• **Fórmula de la torre:** Teniendo en cuenta que,

$\boldsymbol{m}$= Valor posicional de la pieza inicial
$\boldsymbol{a}$= Movimientos de la pieza
$\boldsymbol{x = y}$= Areá menor
$\boldsymbol{b}$= Posición de llegada

A partir de lo anterior, se aplica la fórmula:

$$m \mid ax - by \qquad (4.2.2.)$$

La pieza estará en cualquier posición ubicada en el tablero teniendo en cuenta que sus movimientos sean correctos y partan de la posición incial adecuada.

• **Fórmula del caballo:** Teniendo en cuenta que,

$\boldsymbol{a}$= Movimiento de la pieza
$\boldsymbol{b}$= Valor númerico de la casilla de llegada
$\boldsymbol{m}$= Razón
$\boldsymbol{x}$= Valor númerico de la casilla inicial

A partir de lo anterior, se aplica la fórmula:

$$m|ax - b \qquad (4.2.3.)$$

La pieza estará en cualquier posición ubicada en el tablero teniendo en cuenta que sus movimientos sean correctos y partan de la posición incial adecuada.

• **Fórmula del Alfil:** Teniendo en cuenta que,

$\boldsymbol{a}$= Movimiento de la pieza
$\boldsymbol{b}$= Valor númerico de la casilla de llegada
$\boldsymbol{c}$=Movimiento horizontal por movimiento vertical de la diagonal que genera la pieza
$\boldsymbol{m}$= Valor númerico de la casilla inicial

A partir de lo anterior, se aplica la fórmula:

$$m|ac - bc \qquad (4.2.4.)$$

La pieza estará en cualquier posición ubicada en el tablero teniendo en cuenta que sus movimientos sean correctos y partan de la posición incial adecuada.

• **Fórmula del rey y la reina:** para estas dos piezas utilizaremos la fórmula del alfil, torre o peón de acuerdo a su movimiento.

Fórmula del peón: Teniendo en cuenta que,
$\boldsymbol{a}$= Cantidad de movimientos de la pieza.
$\boldsymbol{b}$=Punto de llegada.
$\boldsymbol{m}$=Valor númerico de la pieza.
Entonces, la fórmula de esta pieza en la congruencia es:

$$a \equiv b(mod\ \ m) \qquad (4.2.5.)$$

• **Fórmula de la torre:** teniendo en cuenta que,
$\boldsymbol{a}$ =Cantidad de movimientos de la pieza.
$\boldsymbol{b}$=Punto de llegada.
$\boldsymbol{m}$=Valor númerico de la pieza.
$\boldsymbol{r}$= Razón
Entonces, la fórmula de esta pieza en la congruencia es:

$$ar \equiv br(mod\ \ m) \qquad (4.2.6.)$$

• **Fórmula de la caballo:** Teniendo en cuenta que,
a= Cantidad de movimientos de la pieza.
b=Punto de llegada.
m=valor númerico de la pieza.
x= Razón
Entonces, la fórmula de esta pieza en la congruencia es:

$$ax \equiv b(mod\ \ m) \qquad (4.2.7.)$$

• **Fórmula del alfil:** Teniendo en cuenta que,
a= Cantidad de movimientos de la pieza.
b=Punto de llegada.
m=Valor númerico de la pieza.
c= Razón
Entonces, la fórmula de esta pieza en la congruencia es:

$$\text{Si } ac \equiv bc(mod\ m) \text{ y } (c, m) = 1 \text{ entonces } a \equiv b(mod\ m) \qquad (4.2.8.)$$

Fórmula del rey y la reina: para estas dos piezas utilizaremos la fórmula del alfil, torre o peón de acuerdo a su movimiento.

• Partiendo de la fórmula (4.2.7.) y utilizando el corolario 3.1.8. tenemos que,

$$\begin{gathered} ax \equiv b(mod\ m) \text{ ,y, } a^{m-1} \equiv 1(mod\ m) \\ a^{m-1}(ax \equiv b(mod\ m)) \text{,y, } b(a^{m-1} \equiv 1(mod\ m)) \\ m \mid a^{m-1}(ax - b) + b(a^{m-1} - 1) \\ m \mid a^{m+1-1}x - a^{m-1}b + a^{m-1}b - b \\ m \mid a^m x - b \\ a^m x \equiv b(mod\ m) \end{gathered}$$

De acuerdo a lo anterior la fórmula del teorema de Fermat es:

$$a^m x \equiv b(mod\ m) \qquad (4.2.9.)$$

Donde:
a= Cantidad de movimientos de la pieza.
b=Punto de llegada.
m=Valor númerico de la pieza.
x= Razón

• Partiendo de la fórmula (4.3.7.) y utilizando el teorema 3.1.8. tenemos que,

$$\begin{gathered} ax \equiv b(m) \text{ ,y, } a^{\Phi(m)} \equiv 1(mod\ m) \\ m \mid a^{\Phi(m)}(ax - b) + b(a^{\Phi(m)} - 1) \\ m \mid a^{\Phi(m)+1}x - a^{\Phi(m)}b + a^{\Phi(m)}b - b \\ m \mid a^{\Phi(m)+1}x - b \\ a^{\Phi(m)+1}x \equiv b(mod\ m) \end{gathered}$$

De acuerdo a lo anterior la fórmula del teorema de Euler es:

$$a^{\Phi(m)+1}x \equiv b(mod\ m) \qquad (4.2.10.)$$

donde:
a= Cantidad de movimientos de la pieza.
b=Punto de llegada.
m=Valor númerico de la pieza.
x= Razón

• Partiendo de la fórmula (4.2.5.) y utilizando el teorema 3.1.12. tenemos que,

$$\begin{gathered} a \equiv b(mod\ m) \text{ ,y, } (p-1)! \equiv -1(mod\ m) \\ (p-1)!(a \equiv b(mod\ m)) \text{ ,y, } b((p-1)! \equiv -1(mod\ m)) \\ m \mid (a-b)(p-1)! + ((p-1)! + 1)b \\ m \mid (p-1)!(a) - b(p-1)! + b(p-1)! + b \\ m \mid (p-1)!a + b \\ a(p-1)! \equiv -b(mod\ m) \end{gathered}$$

De acuerdo a lo anterior la fórmula del teorema de Wilson es:

$$a(p-1)! \equiv -b(mod\ m) \qquad (4.2.11.)$$

donde:
a= Cantidad de movimientos de la pieza.
b=Punto de llegada.
m=Valor númerico de la pieza.
k= Razón

4.3. Aplicaciones

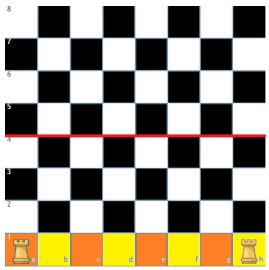
4.3.1. Aplicaciones en la Divisibilidad

Aplicación 1

¿ Cuál es la cantidad de movimientos que puede realizar la reina, el rey, la torre, el caballo, el alfil al desplazarse a la casilla $a1$ de las piezas blancas ?

Solución:

Torre: Utilizando la fórmula (4.2.2.) debemos hallar la cantidad de movimientos para llegar a la casilla $a1$ iniciando desde la posición $h1$, entonces:
a= ?
b=1
m= 7
k= 24 (razón)
x= 8

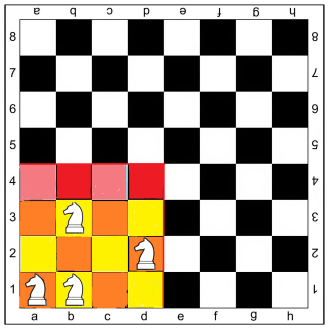


"Vaquiro y Rangel". (2021), figura 12.

Reemplazamos en la fórmula (4.2.2.),

$$7|\ a(8)\text{- }1(8)$$
$$7\ |\ a8\text{-}8$$
$$7(24)=a8\text{-}1(8)$$
$$176+8=a8$$
$$\frac{176}{8}=a$$
$$22=a$$

Por tanto la cantidad de movimientos de la Torre es 22.
Caballo: Inicia en la posición $b1$, para llegar a la posición $a1$ necesitara tres movimientos, entonces:
a =?
b =1
m =4
x =1

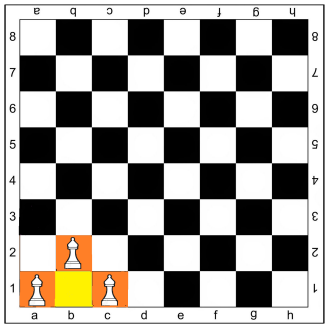


"Vaquiro y Rangel". (2021), figura 13.

Reemplazamos en la fórmula (4.2.3.),

$$4\ |\ \text{a}(1)\ \text{-}1$$

Por tanto la cantidad de movimientos del caballo es 5.
Alfil: La pieza esta ubicada en la posición $c1$, es decir; en la tercera posición, tiene dos movimientos para llegar a la primera casilla de la posición $a1$, entonces:
$m = 2$
a =?
$b = 6$
$c = 1$
$k = m \times c$



"Vaquiro y Rangel". (2021), figura 14.

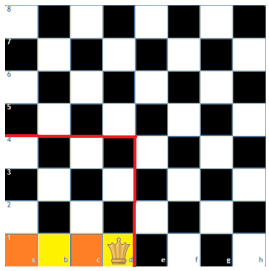
Reemplazamos en la fórmula (4.2.4.),
Iniciamos desde $(c1, b2)$

$$2|a(2) - 6(1)\ (1)$$
$$2(k) + 6 = a(1)$$
$$2(2) + 6 = a$$
$$4 + 6 = a$$
$$10 = a$$

por tanto la cantidad de movimientos del alfil es 10.

Reina: Partimos de la Reina (d1) para llegar a la casilla $(a1)$, en este caso no utilizaremos la fórmula (4.2.1.) y la fórmula (4.2.4.), por tanto aplicamos la fórmula (4.2.2.) siendo:

$m = 3$
$b = 1$
$x = 4$
$a =?$
$y = 4$
$k = 12$ (razón)

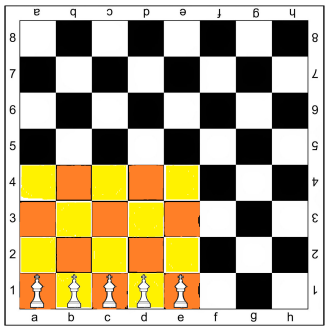


'Vaquiro y Rangel". (2021), figura 15.

$$3 \mid 4a - 1(4)$$
$$3(12) = 4a - 4$$
$$36 = 4a - 4$$
$$36 + 4 = 4a$$
$$40 = 4a$$
$$\tfrac{40}{4} = a$$
$$10 = a$$

Por lo tanto la cantidad de movimientos para la reina es 10.

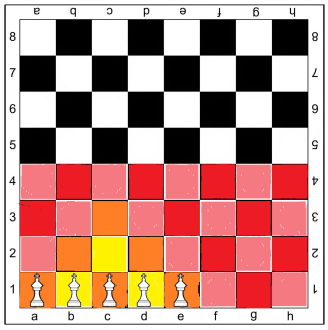
Rey: La pieza esta ubicada en la posición $e1$, es decir; en la quinta posición, tiene diferentes movimientos para llegar a la casilla de la posición $a1$, en este caso solo utilizaremos la fórmula (4.2.2.) y (4.2.4) para llegar a la casilla $a1$.
Desplazamiento de la reina con la fórmula (4.2.2.) siendo:
$m = 4$
$b = 1$
$x = y = 5$
$a =?$
$k = 15$ (razón)



"Vaquiro y Rangel". (2021), figura 16.

$$4 \mid 5a - 1(5)$$
$$4(15) = 5a - 5$$
$$60 = 5a - 5$$
$$60 + 5 = 5a$$
$$65 = 5a$$
$$\frac{65}{5} = a$$
$$13 = a \quad \textbf{(1)}$$

Por tanto la cantidad de movimientos para el rey con la fórmula (4.2.2.) es 13.
Desplazamiento de la reina con la fórmula (4.2.4.) siendo:
$m = 4$
$b = 15$
$c = 1$
$a =?$
$k = m \times c$



"Vaquiro y Rangel". (2021), figura 17.

$$4 \mid a(1) - 15(1)$$
$$4(4) + 15 = a(1)$$
$$16 + 15 = a(1)$$
$$31 = a \quad \textbf{(2)}$$

Por tanto la cantidad de movimientos para el rey con la fórmula (4.2.4.) es 31.
Luego, sumamos (1) y (2) para hallar el total de movimientos realizados por el rey.

$$13 + 31 = a$$
$$44 = a$$

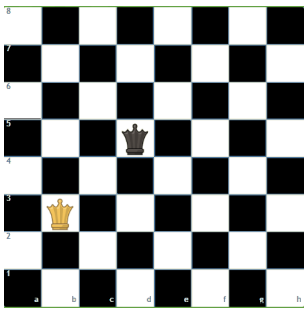
Por tanto la cantidad de movimientos para el rey es 44.

De acuerdo a lo anterior la cantidad de movimientos que realizados (torre, alfil, caballo, reina, rey) es 91 posibles movimientos.

Aplicación 2:

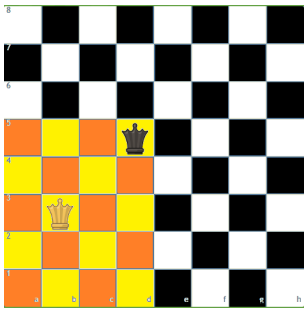
¿Cómo puede atacarse dos reinas $(b3, d5)$ en un tablero, utilizando un ataque en diagonal?

Solución: Las dos Reinas que se atacarán en forma diagonal se encuentran ubicadas en las casillas $b3$ y $d5$. Iniciaremos explicando con la reina $b3$ y luego procedemos $d5$.



"Vaquiro y Rangel". (2021), figura 18.

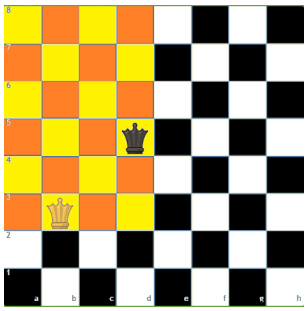
La reina $b3$ se desplaza teniendo en cuenta el movimiento del alfil por tanto:
$m = 1$
$b = 9$
$c = 1$
$a =?$
$k = 1$



"Vaquiro y Rangel". (2021), figura 19.

$$1|a(1) - 9(1)$$
$$9 + 1 = a(1)$$
$$10 = a$$

Por tanto la reina tiene 10 posibles movimientos para atacar la reina $d5$.
Ahora miremos los posibles movimientos que tendrá la reina $d5$ si fuese ella quien atacará a la reina $b3$ por tanto:
$m = 1$
$b = 1$
$c = 6$
$a =?$



"Vaquiro y Rangel". (2021), figura 20.

$$
\begin{gathered}
1|a(6)-1(6) \\
1(24)=6a-6 \\
24+6=6a \\
\frac{30}{6}=a \\
5=a
\end{gathered}
$$

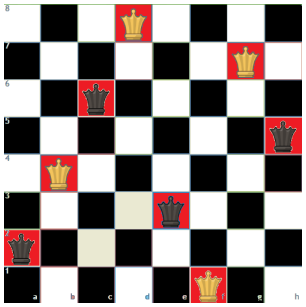
Por tanto la reina tiene 5 posibles movimientos para atacar la reina $b3$.

De acuerdo a lo anterior la reina $b3$ puede realizar 5 posibles movimientos y la reina $d5$ puede realizar 10 diagonales generando los posibles ataques de las piezas.

Aplicación 3:

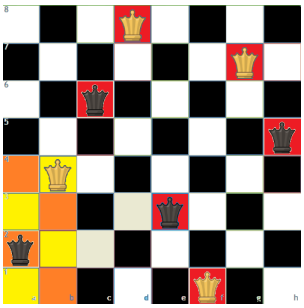
¿Cómo es posible colocar a ocho reinas en el tablero de tal forma que ninguna reina pueda ser atacada por otra?

Solución:
La posición de las 8 reinas deben estar en distintas filas como se muestra en la figura 21, debido a que estas piezas no se pueden atacar entre sí.



"Vaquiro y Rangel". (2021), figura 21.

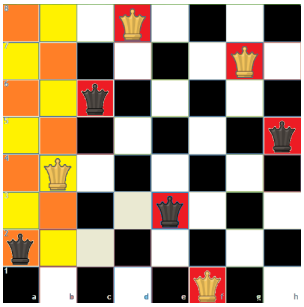
Iniciamos realizando el movimiento de la reina $a2$ con respecto a la reina $b4$:
$m=2$
$b=1$
$c=4$
$a=?$



"Vaquiro y Rangel". (2021), figura 22.

$$
\begin{gathered}
2|4a-4(1) \\
2(8)=4a-4 \\
16+4=4a \\
\frac{20}{4}=a \\
5=a
\end{gathered}
$$

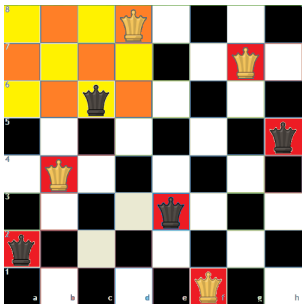
Por tanto los movimientos de la reina $a2$ son 5.
El movimiento de la reina $b4$ con respecto a la reina $a2$:
$m=1$
$b=2$
$c=7$
$a=?$



"Vaquiro y Rangel". (2021), figura 23.

$$
\begin{gathered}
1|7a-7(2) \\
1(14)=7a-14 \\
14+14=7a \\
\frac{28}{7}=a \\
4=a
\end{gathered}
$$

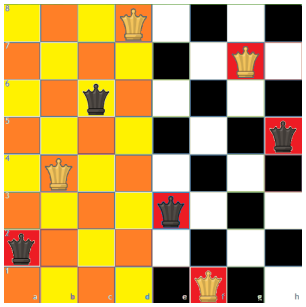
Por tanto los movimientos de la reina $b4$ son 4.
El movimiento de la reina $c6$ con respecto a la reina $d8$:
$m=3$
$b=4$
$c=3$
$a=?$



"Vaquiro y Rangel". (2021), figura 24.

$$3|3a-4(3)$$
$$3(12)=3a-12$$
$$36+12=3a$$
$$\frac{48}{3}=a$$
$$16=a$$

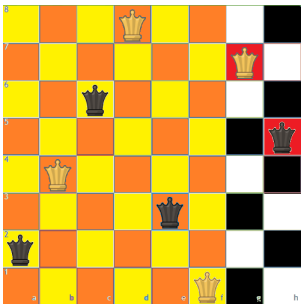
Por tanto los movimientos de la reina $c6$ son 16.
El movimiento de la reina $d8$ con respecto a la reina $c6$:
$m=4$
$b=3$
$c=8$
$a=?$



"Vaquiro y Rangel". (2021), figura 25.

$$4|8a-3(8)$$
$$4(32)=8a-24$$
$$128+24=8a$$
$$\frac{152}{8}=a$$
$$19=a$$

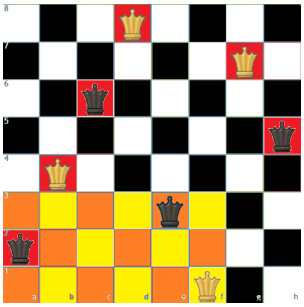
Por tanto los movimientos de la reina $d8$ es 19.
El movimiento de la reina $e3$ con respecto a la reina blanca $f1$:
$m=2$
$b=5$
$c=6$
$a=?$



"Vaquiro y Rangel". (2021), figura 26.

$$
\begin{gathered}
2|6a-6(5) \\
2(48)=6a-30 \\
96+30=6a \\
\frac{126}{6}=a \\
21=a
\end{gathered}
$$

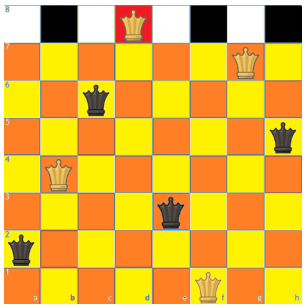
Por tanto los movimientos de la reina $e3$ es 21.
El movimiento de la reina $f1$ con respecto a la reina blanca $e3$:
$m=5$
$b=2$
$c=1$
$a=?$



"Vaquiro y Rangel". (2021), figura 27.

$$
\begin{gathered}
5|1a-1(2) \\
5(18)=1a-2 \\
90+2=1a \\
\frac{92}{1}=a \\
92=a
\end{gathered}
$$

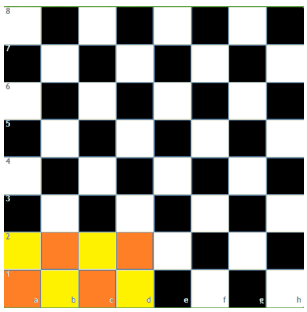
Por tanto los movimientos de la reina $f1$ son 92.
El movimiento de la reina $g7$ con respecto a la reina $h5$:
$m=1$
$b=3$
$c=7$
$a=?$



"Vaquiro y Rangel". (2021), figura 28.

$$1|7a-3(7)$$
$$1(56)=7a-21$$
$$56+21=7a$$
$$\frac{77}{7}=a$$
$$11=a$$

Por tanto los movimientos de la reina $g7$ son 11.
El movimiento de la reina $h5$ con respecto a la reina blanca $g7$:
$m=3$
$b=1$
$c=4$
$a=?$



"Vaquiro y Rangel". (2021), figura 29.

$$3|4a-4(1)$$
$$3(32)=4a-4$$
$$96+4=4a$$
$$\frac{100}{4}=a$$
$$25=a$$

Por tanto los movimientos de la reina $h5$ son 25.

De acuerdo a lo anterior, las ocho reinas no se atacan teniendo los posibles movimientos, porque ninguna de las piezas está en posición de amenaza y cada una de ellas también se encuentra en posición diferente en el tablero del ajedrez.

Aplicación 4:

¿ Se puede desarrollar una fórmula para colocar p reinas en un tablero de ajedrez $p \times p$ donde $p > 3$?.

Solución:
Para presentar una fórmula que resuelva el problema de p-reinas, coloquemos las reinas fila por fila. Se denota como $f(i)$ la ubicación (indice de la columna) de la i-ésima reina, donde $1 \leq i \leq p$; entonces $f(i)$puede ser definida recursivamente.

Definición 4.3.1. *(una definición recursiva de f).*
$f(0) = 0$
$f(i) \equiv f(i-1) + \frac{p+1}{2}(mod p), 1 \leq i \leq p-1$
$f(p) = p$

Usando iteraciones, se puede usar esta definición para encontrar la siguiente formula explicíta para $f(i)$.

Definición 4.3.2. *(una fórmula explícita para $f(i)$).*
$f(i) \equiv \frac{p+1}{2}(mod\, p)$, *si* $1 \leq i \leq p$

Teorema 4.3.1. *La función f es inyectiva.*

Demostración. Sean i y j los residuos mínimos módulo p tal que

$$f(i) = f(j)$$

entonces

$$(\frac{p+1}{2})i \equiv (\frac{p+1}{2})j(mod\, p)$$

Dado que $(\frac{(p+1)}{2}, p) = 1$, esto implica $i \equiv j(mod\, p)$. Pero i y j son los mínimos residuos módulo p, así $i = j$.
El teorema muestra que f asigna exactamente una reina a cada fila y a cada columna para $p = 7$.

i \ j	1	2	3	4	5	6	7
1	.	.	.	Q	.	.	.
2	Q	.	.	.	.	.	.
3	.	.	.	.	Q	.	.
4	.	Q	.	.	.	.	.
5	.	.	.	.	.	Q	.
6	.	.	Q	.	.	.	.
7	.	.	.	.	.	.	Q

"Moreno". (2015), figura 30.

□

A continuación se muestra que no hay dos reinas colocadas sobre el tablero de ajedrez $p \times p$ asignadas por f que pueda atarcarse una a la otra.

Teorema 4.3.2. *No hay dos reinas colocadas sobre el tablero de ajedrez $p \times p$ asignadas por f que puedan atacarse una a la otra.*

Demostración. Dado que todas las filas y todas la columnas contienen exactamente una reina, dos reinas no pueden atacarse una a la otra a lo largo de filas y columnas, así, que es suficiente mostrar que no pueden atarcase a lo largo de la diagonal sureste o noroeste.

Para cada diagonal noreste, la suma $i+j$ del índice de la fila i y el índice de la columna j es una constante, donde $2 \leq k \leq 2p$. Claramente solo buscamos las diagonales donde $3 \leq k \leq 2p-1$.

Supongamos que existen dos reinas en las posiciones (i_1, j_1) y (i_2, j_2). Entonces

$$f(i_1) \equiv (\frac{p+1}{2})i_1 (mod\, p)$$
$$f(i_2) \equiv (\frac{p+1}{2})i_2 (mod\, p)$$

Esto es,

$$j_1 \equiv (\frac{p+1}{2})i_1 (mod\, p) \quad \text{y} \quad j_2 \equiv (\frac{p+1}{2})i_2 (mod\, p) \qquad (3.3.1.)$$

donde $i_1 + j_1 = k = i_2 + j_2$. Entonces

$$i_1 + j_1 \equiv (\frac{p+3}{2})i_1 (mod\, p)$$

Esto Es,

$$k \equiv (\frac{p+3}{2})i_1 (mod\, p)$$

Similarmente,

$$k \equiv (\frac{p+3}{2})i_2 (mod\, p)$$

Estas dos congruencias implican que $\frac{(p+3)i_1}{2} \equiv \frac{(p+3)i_2}{2} (mod\, p)$, así $i_1 \equiv i_2 (mod\, p)$ puesto que $\frac{p(p+3)}{2} = 1$. Así, $i_1 = i_2$, como estos son residuos mínimos módulo p. Entonces, por congruencias de (3.3.1.), $j_1 = j_2$. Así, ninguna reina esta contenida en la diagonal noreste.

Para mostrar que ninguna reina esta contenida en la diagonal sureste, notar que para cada diagonal $i-j$ es una constante l, donde $1-p \leq l \leq p-1$. Claramente se puede asumir $l \neq 1-p$ y $l \neq p-1$.

Suponer una diagonal sureste que contenga dos reinas en las posiciones (i_1, j_1) y (i_2, j_2).

Entonces

$$f(i_1) \equiv (\frac{p+1}{2})i_1 (mod\, p)$$
$$f(i_2) \equiv (\frac{p+1}{2})i_2 (mod\, p)$$

Esto es,

$$j_1 \equiv (\frac{p+1}{2})i_1 (mod\, p) \quad \text{y} \quad j_2 \equiv (\frac{p+1}{2})i_2 (mod\, p) \qquad (3.3.2.)$$

donde $i_1 - j_1 = l = i_2 - j_2$. Entonces

$$i_1 - j_1 \equiv (\frac{p+1}{2})i_1(mod\ p)$$
$$l \equiv (\frac{1-p}{2})i_1(mod\ p)$$
$$l \equiv (\frac{p+1}{2})i_1(mod\ p)$$
$$l \equiv (\frac{p+1}{2})i_2(mod\ p)$$

Estas dos congruencias tienen $i_1 = i_2$, como $((p+1) \setminus 2, p) = 1$ y 1 y i_1 y i_2 son residuos mínims módulo p. Así, por congruencias (3.3.2.), $j_1 = j_2$, la diagonal sureste no contiene ninguna reina. Por lo tanto, no hay dos reinas sobre el tablero de ajedrez $p \times p$ que puedan atacarse una a a la otra. (Moreno, 2015, P.47.) □

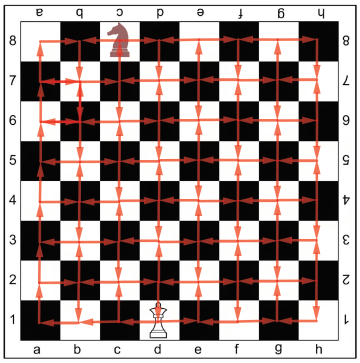
4.3.2. Aplicaciones en la Congruencia módulo m

Aplicación 5:

¿Cómo puede ser atacado un caballo, sí la Reina cuenta con una posición fija, teniendo en cuenta que el caballo se encuentra en la posición $b8$ y la Reina $d1$?

Solución:

Comenzamos primero contando los movimientos posibles que puede generar la Reina, para poder atacar al Caballo.
$a = 137$
$b = 5$
$m = 3$
Aplicamos la fórmula (4.2.9.) :



"Vaquiro y Rangel". (2021), figura 31.

$$137 \equiv 5(mod\ 3)$$
$$3| \ 137\text{- } 5$$
$$3| \ 132$$
$$44 = k$$

Por lo tanto existe 44 resultados para ser atacada.

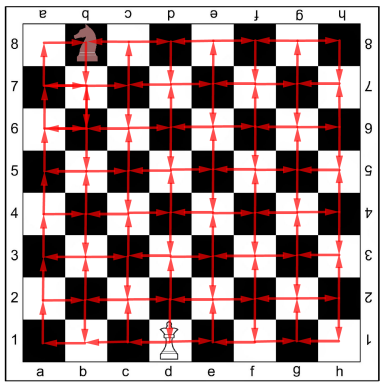
Aplicación 6:

¿ Cuántos movimientos puede realizar la Reina en la posición $d1$ para atacar el caballo que se encuentra en la posición $c8$?

Solución:

Comenzamos primero contando los movimientos posibles que puede generar la reina, para poder atacar al caballo:

$a = 140$
$b = 5$
$m = 3$
Aplicamos la fórmula de la reina :



"Vaquiro y Rangel". (2021), figura 32.

$$140 \equiv 5(mod\ 3)$$
$$3|\ 140\text{- }5$$
$$3|\ 135$$
$$45 = k$$

Por lo tanto existe 45 movimientos para ser atacada.

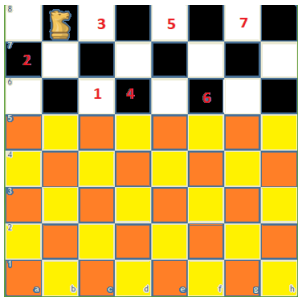
Aplicación 7:

¿Cuál es el cociente (k) de 7 saltos posibles del Caballo en la posición $b8$ para llegar a la casilla $g8$, solo utilizando la fila 8, 7 y 6 del tablero del ajedrez?

Solución:

Utilizaremos la fórmula (4.2.7.) para realizar la cantidad de movimientos sin utilizar la fila cuatro y cinco.

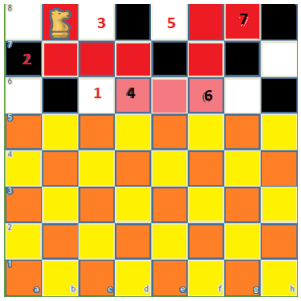
$a = 7$
$b = 1$
$m = 6$
$x = 30$ (Razón)
$k = ?$



"Vaquiro y Rangel". (2021), figura 33.

$$30(7) \equiv 1(mod6)$$
$$210 \equiv 1(mod6)$$
$$\frac{211-1}{6} = k$$
$$\frac{210}{6} = k$$
$$35 = k$$

Por tanto, el cociente (k) de los saltos posibles del Caballo es 35.



"Vaquiro y Rangel". (2021), figura 34.

Aplicación 8

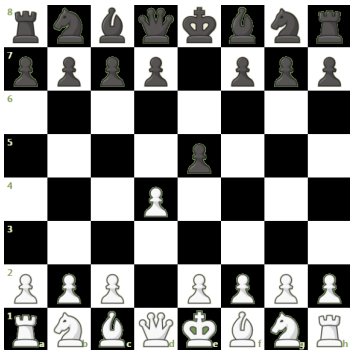
Acontinuación encontramos dos situaciones en el ajedrez utilizando solo dos peones :
a) Dos personas necesita mover dos peones (un peón Blanco y un peón Negro) ¿cómo puede utilizar la relación de congruencia módular ?
b) Una persona requiere que dos peones se ataquen ¿cómo puede utilizar la relación de congruencia módular?

Solución:

a) Para atacar el Peón Blanco al Peón Negro deberá realizar un sólo movimiento, que será en diagonal:
Jugada con el Peón blanco en la casilla $d4$
A partir de su fórmula (4.2.5.):

$a = 1$
$b = 1$
$m = 1$
Sustituimos en la fórmula:
$1 \equiv 1(mod\ 1)$ Ecuación 1

Jugada con el Peón negro en la casilla e5
A partir de su fórmula (4.2.5.)
$a = 1$
$b = 1$
$m = 1$
Sustituimos en la fórmula:
$1 \equiv 1(mod\ 1)$ Ecuación 2



"Vaquiro y Rangel". (2021), figura 35.

b)Del inciso anterior, utilizaremos la ecuación 2 para luego utilizar ecuación 3 y encontrar la mejor opción.

Existe dos opciones así:
1)Cuando los dos peones no se atacan
2)Cuando los dos peones se atacan
Lo que haremos es verificar cual de las dos opciones es la mejor.
por tanto sumamos los valores de a y b teniendo en cuenta la ecuación (1) y (2):

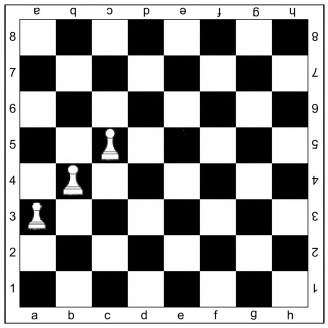
$$1 + 1 \equiv 1 + 1(mod\ 1)$$
$$2 \equiv 2(mod\ 1)$$

Obtenemos como resultado cero, es decir, deberá llegar a la pocisión 1. Como podemos observar nos sirve atacar al otro peón.

4.3.3. Aplicaciones de las congruencias de Wilson, Euler, Fermat

Aplicación 9:

A partir de los peones $a3, b4, c5$. ¿De cuántas maneras se pueden desplazar las piezas en el tablero, de tal manera que cumpla con la fórmula (4.2.11.)?



"Vaquiro y Rangel". (2021), figura 36.

Solución:

Vamos a verificar que cumpla para cada uno de los peones exigidos:

Desplazamiento del peón $a3$ teniendo en cuenta que,
$a =?$
$b = 7$
$m = 2$
$k = 13$ (razón)
luego,

$$\begin{gathered} a(2-1)! \equiv -7(mod\ 2) \\ a(1)! \equiv -7(mod\ 2) \\ a(1) \equiv -7(mod\ 2) \\ a = 2(k) - 7 \\ a = 2(13) - 7 \\ a = 26 - 7 \\ a = 19 \quad \textbf{(1)} \end{gathered}$$

Por lo tanto existen 19 movimientos para realizar.

Desplazamiento del peón $b4$ teniendo en cuenta que,
$a =?$
$b = 6$
$m = 2$
$k = 8$ (razón)
luego,

$$\begin{gathered} a(2-1)! \equiv -6(mod\ 2) \\ a(1)! \equiv -6(mod\ 2) \\ a(1) \equiv -6(mod\ 2) \\ a = 2(k) - 6 \\ a = 2(8) - 6 \\ a = 16 - 6 \\ a = 10 \quad \textbf{(2)} \end{gathered}$$

Por lo tanto existen 10 movimientos para realizar.

Desplazamiento del peón $c5$ teniendo en cuenta que,
$a =?$
$b = 5$
$m = 2$
$k = 17$ (razón)
luego,

$$\begin{gathered} a(2-1)! \equiv -5(mod\ 2) \\ a(1)! \equiv -5(mod\ 2) \\ a(1) \equiv -5(mod\ 2) \\ a = 2(k) - 5 \\ a = 2(17) - 5 \\ a = 34 - 5 \\ a = 29 \quad \textbf{(3)} \end{gathered}$$

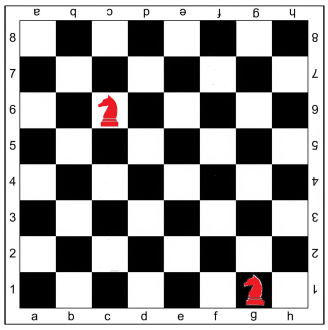
Por lo tanto existen 29 movimientos para realizar.
De acuerdo a lo anterior, sumamos el resultado de (1) , (2) y (3) para hallar el total de desplazamientos:

$$19 + 10 + 29 = a$$
$$58 = a$$

Por tanto el total de desplazamiento entre los peones $a3, b4, b5$ es 58.

Aplicación 10:

Utilizando dos Caballos $(g1, c6)$en posición fija de valor numérico primo. ¿Cual es el punto de llegada de los caballo, teniendo en cuenta la fórmula (4.2.10.)?



"Vaquiro y Rangel". (2021), figura 37.

Solución:

Vamos a verificar que cumpla para cada uno de los caballos exigidos:

Desplazamiento del caballo $c6$ teniendo en cuenta que,
$a = 2$
$b =?$
$m = 3$
$x = 14$
Iniciamos hallando el valor de $\Phi(m)$ para este caso:

$$\Phi(3) = 3^{1-1} \times (3 - 1)$$
$$\Phi(3) = 1(2)$$
$$\Phi(3) = 2$$

Luego,

$$2^{\Phi(3)+1}(14) \equiv b(mod\ 3)$$
$$2^{2+1}(14) \equiv b(mod\ 3)$$
$$2^3(14) \equiv b(mod\ 3)$$
$$8(14) \equiv b(mod\ 3)$$

ahora, hallamos el resto de 8 y 14 entonces,

$$8 \div 3 = 2 + \frac{2}{3}, \text{ su resto es } 2 \quad \textbf{(1)}$$

$$14 \div 3 = 4 + \frac{2}{3}, \text{ su resto es } 2 \quad \textbf{(2)}$$

luego multiplicamos el resto de (1) y (2)

$$2 \times 2 = 4$$

hallamos el resto de 4

$$4 \div 3 = 1 + \frac{1}{3}, \text{ su resto es } 1$$

por lo tanto ,

$$2^{\Phi(m)+1}(x) \equiv 1(mod\, m)$$

Es así como b= 1 , por tanto

$$8(14) \equiv 1(mod\, 3)$$
$$112 \equiv 1(mod\, 3)$$

Por lo tanto el punto de llegada del caballo $c6$ es 1.

Desplazamiento del caballo $g1$ teniendo en cuenta que,
$a = 2$
$b =?$
$m = 6$
$x = 26$
Iniciamos hallando el valor de $\Phi(m)$ para este caso:

$$\Phi(6) = 6^{1-1} \times (6-1)$$
$$\Phi(6) = 1(5)$$
$$\Phi(6) = 5$$

Luego,

$$2^{\Phi(6)+1}(26) \equiv b(mod\, 6)$$
$$2^{5+1}(26) \equiv b(mod\, 6)$$
$$2^{6}(26) \equiv b(mod\, 6)$$
$$64(26) \equiv b(mod\, 6)$$

ahora, hallamos el resto de 64 y 26 entonces,

$$64 \div 6 = 10 + \frac{4}{6}, \text{ su resto es } 4 \quad \textbf{(1)}$$

$$26 \div 6 = 4 + \frac{2}{6}, \text{ su resto es } 2 \quad \textbf{(2)}$$

luego multiplicamos el resto de (1) y (2)

$$4 \times 2 = 8$$

hallamos el resto de 8

$$8 \div 6 = 1 + \frac{2}{6}, \text{ su resto es } 2$$

por lo tanto ,

$$2^{\Phi(m)+1}(x) \equiv 2(mod\, m)$$

Es así como b= 2 , por tanto

$$64(26) \equiv 2(mod\, 6)$$
$$1664 \equiv 2(mod\, 6)$$

Por lo tanto el punto de llegada del caballo $g1$ es 2.

Aplicación 11:

¿Cuál es el valor de llegada de los Caballos $c6, e3$ en el tablero del ajedrez sin repetir las casillas y aplicando la fórmula (4.2.9.)?

Solución:

Vamos a verificar que cumpla para cada uno de los caballos exigidos:

Desplazamiento del caballo $c6$ teniendo en cuenta que,
$a =?$
$b =?$
$m = 3$
$x = 14$
Iniciamos hallando el valor de a:

$$a^{3-1} \equiv 1(3)$$
$$a^2 \equiv 1(3)$$
$$3 \mid a^2 - 1$$
$$3 \mid (a+1)(a-1)$$
$$a + 1 = 3(14)$$
$$a = 42 - 1$$
$$a = 41$$

luego,

$$41^3(14) \equiv b(mod\ 3)$$
$$68921(14) \equiv b(mod\ 3)$$

ahora, hallamos el resto de 68921 y 14 entonces,

$$68921 \div 3 = 22973 + \frac{2}{3}, \text{ su resto es } 2 \quad \textbf{(1)}$$
$$14 \div 3 = 4 + \frac{2}{3}, \text{ su resto es } 2 \quad \textbf{(2)}$$

luego multiplicamos el resto de (1) y (2)

$$2 \times 2 = 4$$

hallamos el resto de 4

$$4 \div 3 = 1 + \frac{1}{3}, \text{ su resto es } 1$$

por lo tanto ,

$$a^m(x) \equiv 1(mod\ m)$$

Es así como b= 1 , por tanto

$$68921(14) \equiv 1(mod\ 3)$$
$$964894 \equiv 1(mod\ 3)$$

Por lo tanto el punto de llegada del caballo $c6$ es 1.

Desplazamiento del caballo $e3$ teniendo en cuenta que,
$a =?$
$b =?$
$m = 2$
$x = 17$
iniciamos hallando el valor de a:

$$\begin{gathered} a^{2-1} \equiv 1(mod\ 2) \\ a^1 \equiv 1(mod\ 2) \\ 2 \mid a-1 \\ 2(17) = a-1 \\ 34-1 = a \\ 33 = a \end{gathered}$$

luego,

$$\begin{gathered} 33^2(17) \equiv b(mod\ 2) \\ 1089(17) \equiv b(mod\ 2) \end{gathered}$$

ahora, hallamos el resto de 1089 y 17 entonces,

$$1089 \div 2 = 544 + \frac{1}{2}, \text{ su resto es } 1 \quad \textbf{(1)}$$
$$17 \div 2 = 8 + \frac{1}{2}, \text{ su resto es } 1 \quad \textbf{(2)}$$

luego multiplicamos el resto de (1) y (2)

$$1 \times 1 = 1$$

Por tanto el resto es 1, luego

$$a^m(x) \equiv 1(mod\ m)$$

Es así como b= 1 , por tanto

$$\begin{gathered} 1089(17) \equiv 1(mod\ 2) \\ 18513 \equiv 1(mod\ 2) \end{gathered}$$

Por lo tanto el punto de llegada del caballo $e3$ es 1.

CONCLUSIONES

El presente trabajo permitió recopilar y mostrar diferentes maneras de comprender los Teoremas de Wilson, Euler y Fermat relacionados con la congruencia módulo $m \in \mathbb{Z}^+$ y el algoritmo de la división como elemento importante para la comprensión del tema.

Por otro parte, se logró establecer una relación de la congruencia modular, los teoremas de Euler, Fermat, Wilson y el juego del ajedrez para determinar los posibles movimientos que pueden realizar las diferentes piezas.

El poder de entrelazar los tres teoremas (Euler, Fermat, Wilson) con la congruencia modular, y los criterios de divisibilidad, se convitió en una herramienta importante para la construcción de posibles jugadas que permitan tener una partida victoriosa en el ajedrez.

De igual forma, la aplicación del juego del ajedrez a través de la resolución de problemas de congruencia modular y divisibilidad permitió el análisis y el razonamiento matemático para generar tácticas que ayuden a ganar la partida .

BIBLIOGRAFIA

[1] Mora, W. M. (2014).Introducción a la teoría de números. Costa Rica.

[2] Zarate, L. F. (2008). El ajedrez y las matemáticas en la escuela primaria (un curso taller para potencializar las habilidades cognitivas en el niño de cuarto grado). Universidad Pedagógica Nacional. México.

[3] Rubiano, O.J. (2004). Teoría de números para principiantes 2^a edición. Universidad Nacional de Colombia. Bogotá.

[4] Urriola, F.J.(2011). Los teoremas de Fermat, Wilson y Euler

[5] Gutierrez, F. J. (2004). Apuntes de Matemáticas Discreta (clases de restos modulo m).

[6] Gauss, C. F. (1966). Disquisitiones Arithmeticae. Traducida por Arthur A. Clarke New Haven and London, Yale University Press.

[7] Gutierrez, J. (2018). Historia de las matemáticas, Teoría de números de ciencia pura a ciencia aplicada. Pensamiento Matemático.

[8] Ortiz, W. M. (2015). Implementación de algunos algoritmos en teoría de números usando programación funcional. Quito - Ecuador.

[9] Puertas, M. J. (2012). La Teoría Elemental de números y su historia. Madrid. Aebius