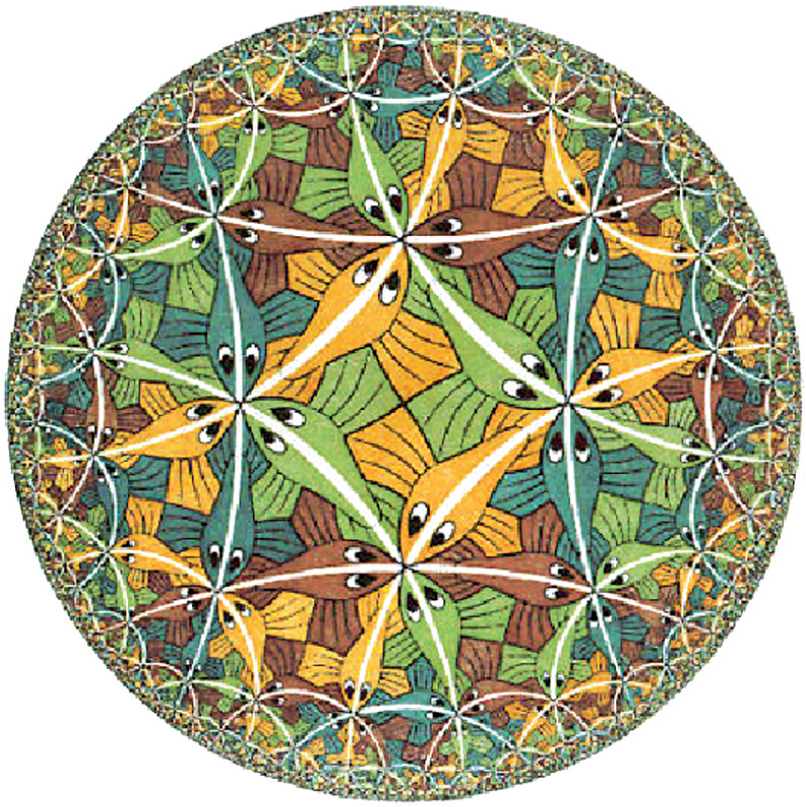
Desde la Aritmética Modular al Fascinante Mundo de los Números Perfectos

Proyecto de Pares Ordenados



Aprendiz:
Jesús Chávez Valencia
Instituto Politécnico Nacional
Ciudad de México - México

Mentor:
Dr. Pedro Fernando Fernández Espinosa
Universidad de Caldas
Manizales - Colombia

Junio de 2024

Índice general

1 Resumen

En el hermoso y diverso universo de las matemáticas vive la aritmética modular (congruencias módulo m) que es una fascinante, útil y entretenida parte de este universo que sirve entre muchas otras para comprender y analizar una amplia variedad de fenómenos numéricos y estructuras algebraicas. En el presente documento es una guía introductoria exploramos algunos elementos básicos de la aritmética modular, sus propiedades, su aparición en resultados clásicos de la matemática y alguna de sus aplicaciones en teoría de números y criptografía.

2 Introducción

La aritmética modular es un área clásica en cualquier curso elemental de teoría de números, ésta, fue introducida por Gauss en 1801 en su libro *Disquistiones Arithmeticae*, allí él introduce la noción de congruencia ($\equiv$), este concepto que ha sido ampliamente estudiado desde varios puntos de vista y que es relativamente elemental desde la intuición ha resultado ser supremamente poderoso en el desarrollo de la matemáticas (especialmente en álgebra abstracta, teoría de números y sus aplicaciones).

Por mencionar algunos ejemplos, las congruencias se destacan en resultados matemáticos clásicos como el teorema de Wilson, el pequeño teorema de Fermat,el teorema de Euler, los test de primalidad, entre otros. Sin embargo, las congruencias también aparecen en los contextos aplicados e incluso recreacionales por ejemplo en criptografía (Algoritmo RSA), la generación de códigos de barras, diseños modulares, el problema de las p- reinas, el calendario perpetuo, etc.

En este trabajo se presentará de manera auto contenida y ejemplificada un viaje que tendrá como primera parada algunas nociones básicas de las congruencias, sus propiedades y aplicaciones luego de ello haremos una pequeña parada en el estudio de los teoremas clásicos mencionados anteriormente. Con esto en mente emprenderemos nuestro viaje a la última parada que involucra al fascinante mundo de los números perfectos y los primos de Mersenne, allí describiremos algunas de sus propiedades conocidas, problemas abierto relacionados y avances en algunos de ellos.

Este documento es el resultado del interés del aprendiz en estudiar con detalle algunos conceptos que no se discutieron con suficiente detalle en el inicio de su carrera de matemáticas y esta distribuido de la siguiente manera: En la sección 3 se introducen las definiciones básicas relacionadas con las congruencias, algunas de sus propiedades y una aplicación en matemática recreativa. En la sección 4 se presentan las funciones multiplicativas y sus propiedades. En la sección 5 presentamos tres teoremas icónicos y clásicos como lo son los teoremas de Wilson, Euler y el pequeño teorema de Fermat. Luego, en la sección 6 presentaremos la definición de número perfecto y primo de Mersenne, algunas de sus propiedades y problemas abierto relacionados con este tipo de números.

3 Congruencias módulo m

En esta sección, se introducen las definiciones básicas y la notación que se usará a lo largo del documento basados principalmente en referencias clásicas tales como [1–6]. Para efectos de todo el documento asumiremos que $a, b, c \in \mathbb{Z}$ y $m \in \mathbb{Z}^+$.

Definición 1. *Sea $m \in \mathbb{Z}^+$. Entonces el entero a es **congruente** con el entero b **módulo** m si $m|(a-b)$. Denotado por $a \equiv b \ (mod\ m)$; con m el **módulo** de la **relación de congruencia**.*

Si a no es congruente con b módulo m, entonces a es **incongruente** con b módulo m, denotándolo por $a \not\equiv b \pmod{m}$.

Ejemplo 1. *Como $5|(23-3), 23 \equiv 3 \ (mod\ 5)$, de la misma manera, $6|(48-12)$, entonces $48 \equiv 12 \ (mod\ 6)$.*

A continuación mostramos algunas propiedades clásicas de la congruencia.

Proposición 1. *$a \equiv b \ (mod\ m) \Leftrightarrow a = b + km$ para algún $k \in \mathbb{Z}$.*

Demostración. Suponemos que $a \equiv b \ (mod\ m)$. Entonces $m \mid (a-b)$, así $a-b = km$ para algún k; esto es, $a = b + km$. De manera similar, supongamos $a = b + km$ para algún k. Entonces $a - b = km$, lo que significa que $m \mid (a-b)$ y por lo tanto, $a \equiv b \ (mod\ m)$. □

Nota 1. *De la Definición 1 y de la Proposición 1, se sigue que para algún $a \in \mathbb{Z}$, $m \in \mathbb{Z}^+$, $a \equiv 0 \ (mod\ m) \Leftrightarrow m|a$. Lo que significa que $a \equiv 0 \ (mod\ m)$ y $m|a$ son definiciones equivalentes.*

El siguiente teorema indica que la relación de congruencia es una relación de equivalencia:

Teorema 1. *Sean $a, b, c \in \mathbb{Z}, m \in \mathbb{Z}^+$, se cumple:*

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

   Demostración. A continuación presentamos la demostración ítem por ítem

   Dado que $m \mid (a-a)$, se tiene que $a \equiv a \ (mod\ m)$.

2. Suponga que $a \equiv b \ (mod\ m)$. Entonces $m \mid (a-b)$; esto es, $m \mid -(b-a)$. Así $m \mid (b-a)$; esto es, $b \equiv a \ (mod\ m)$.

3. Suponga $a \equiv b \ (mod\ m)$ y $b \equiv c \ (mod\ m)$. Entonces $m \mid (a-b)$ y $m \mid (b-c)$, así por propiedades de transitividad $m \mid [(a-b)+(b-c)]$; que implica, $m \mid (a-c)$; en consecuencia, $a \equiv c \ (mod\ m)$.

□

Proposición 2. *$a \equiv b (mod\ m) \Leftrightarrow$ a y b tienen el mismo resto cuando son divididos por m.*

Corolario 1. *El entero r es el resto cuando a es dividido por $m \Leftrightarrow a \equiv r \ (mod\ m)$, con $0 \leq r < m$.*

Corolario 2. *Cada entero es congruente exactamente con al menos uno de los residuos* $0, 1, 2, ..., (m-1)$ *módulo m*

Las pruebas de la Proposición 2, Corolario 1 y 2 pueden ser consultadas en [1–6].

3.1. Clases de Equivalencia Módulo m

Usando los residuos al dividir por un número fijo m, el conjunto de números enteros $\mathbb{Z}$ puede dividirse en m clases disyuntas dos a dos, conocidas como **clases de congruencia módulo** m. Para ilustrar esto, sea $[r]$, el conjunto de números enteros que tienen a r como su residuo módulo m . Por ejemplo, si consideramos $m = 5$ las clases de congruencia módulo 5 son:

$$\begin{aligned}
[0] &= \{\ldots, -10, -5, 0, 5, 10, \ldots\} \\
[1] &= \{\ldots, -9, -4, 1, 6, 11, \ldots\} \\
[2] &= \{\ldots, -8, -3, 2, 7, 12, \ldots\} \\
[3] &= \{\ldots, -7, -2, 3, 8, 13, \ldots\} \\
[4] &= \{\ldots, -6, -1, 4, 9, 14, \ldots\}
\end{aligned}$$

Claramente, estas clases son no vacías, disyuntas dos a dos y su unión es el conjunto de los números enteros $\mathbb{Z}$. De acuerdo con esto, estas clases forman una partición en el conjunto de los enteros,como se muestra anteriormente. Los residuos $0, 1, 2, 3$ y 4 son representantes de las clases $[0], [1], [2], [3]$ y $[4]$.

Para finalizar esta sección presentamos algunas propiedades adicionales de las congruencias módulo m. Por ejemplo la siguiente ilustra que dos congruencias del mismo módulo pueden ser sumadas y multiplicadas.

Teorema 2. *Sea $a \equiv b \ (mod\ m)$ y $c \equiv d \ (mod\ m)$. Entonces:*

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

2. $ac \equiv bd \ (mod\ m)$.

Demostración. Dado que $a \equiv b \ (mod\ m)$ y $c \equiv d \ (mod\ m)$, tenemos que $a = b + \ell m$ y que $c = d + km$ para algunos enteros ℓ y m. Entonces

1.
$$\begin{aligned} a + c &= (b + \ell m) + (d + km) \\ &= (b + d) + (\ell + k)m \\ &\equiv b + d \ (mod\ m) \end{aligned}$$

2.
$$\begin{aligned} ac - bd &= (ac - bc) + (bc - bd) \\ &= c(a - b) + b(c - d) \\ &= c\ell m + bkm \\ &= (c\ell + bk)m \end{aligned}$$

Con lo cual $ac \equiv bd \ (mod\ m)$.

□

De manera similar y durante el periodo de estudio en pares ordenados se abordaron las siguientes propiedades de las congruencias. Algunas de sus demostraciones pueden ser consultadas en [1–6].

Teorema 3 (Propiedades)**.** *Sean $a, b, c, d, m \in \mathbb{Z}$ y sea $n \in \mathbb{N}$ entonces:*

1. *Si $a \equiv b \ (mod\ m)$ y $c \equiv d \ (mod\ m)$, entonces $a - c \equiv b - d \ (mod\ m)$*
2. *Si $a \equiv b \ (mod\ m)$ y sea $c \in \mathbb{Z}$, entonces*
   - $a + c \equiv b + c \ (mod\ m)$
   - $a - c \equiv b - c \ (mod\ m)$
   - $ac \equiv bc \ (mod\ m)$
   - $a^2 \equiv b^2 \ (mod\ m)$
3. *Si $a \equiv b \ (mod\ m)$, entonces $a^n \equiv b^n \ (mod\ m)$*
4. *Si $ac \equiv bc \ (mod\ m)$ y $(c, m) = 1$, entonces $a \equiv b \ (mod\ m)$.*
5. *Si $ac \equiv bc \ (mod\ m)$ y $(c, m) = d$, entonces $a \equiv b \ (mod\ m)$.*

3.2. Algunas aplicaciones de las congruencias

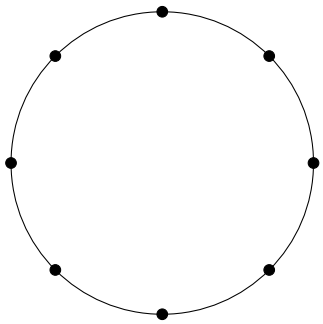
En este viaje que hemos emprendido finalizaremos nuestra primera parada mencionando que las congruencias tiene un gran número de aplicaciones entre las que se destacan los criterios de divisibilidad, acertijos recreativos, diseños modulares entre otros (para más detalle se puede consultar [6]). Sin embargo por gusto personal del aprendiz se presenta en este documento únicamente la aplicación que tiene que ver con matemática recreativa: los diseños modulares. Para más detalle de esta aplicación puede consultar [2, 6].

3.3. Diseños modulares

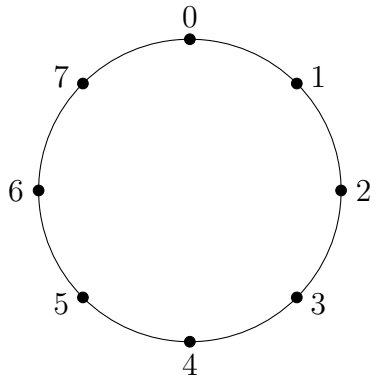
Uno de los usos de la aritmética modular es la creación de bellos y variados diseños geométricos como por ejemplo las conocidas como estrellas de $m - puntas$.

Estrellas de m-puntas y la imposibilidad de construir la Estrella de David.

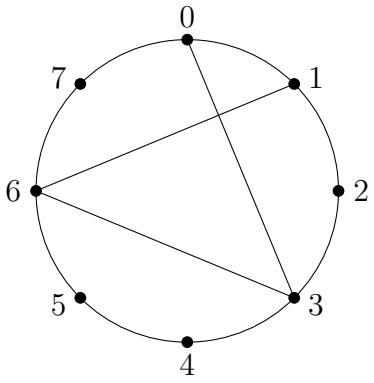
Para la construcción de una estrella de $m - puntas$, a partir de una circunferencia, debemos de colocar m marcas equidistantes a lo largo de esta, las cuales etiquetaremos con los residuos desde 0 hasta $(m-1)$ módulo m. Ahora escogeremos un residuo i módulo m, donde $(i, m) = 1$. Unimos cada punto x con el punto $x + i \ mod \ m$. Ahora coloreamos la región dentro del circulo con un color de preferencia. Obteniendo así una estrella de $m-$puntas. Por ejemplo si $m = 8$ e $i = 3$ entonces



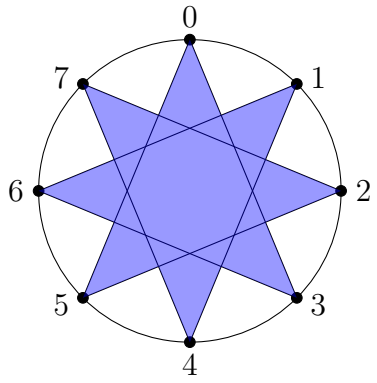
Paso 1 : Marcar Puntos



Paso 2: Enumerar los puntos marcados



Paso 3: Conectar puntos $x + i \ mod \ m$

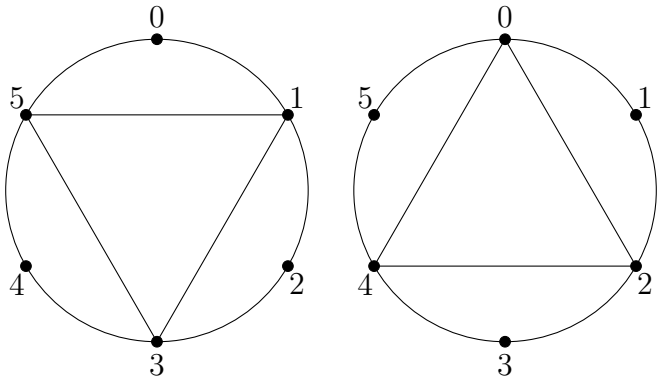


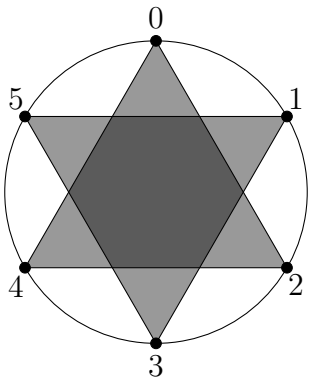
Estrella de 8 puntas

Dada esta manera de construir estrellas de $m-$puntas, surgen algunas preguntas de manera natural. Por ejemplo :

- ¿De cuantas manera puede una estrella de $m-$puntas ser dibujada sin despegar el lápiz de la hoja?
- Dado m un número natural. ¿Siempre puedo construir al menos una estrella de m puntas con las características descritas anteriormente?

La respuesta a la segunda pregunta es que no. Por ejemplo para $m = 6$ se debería obtener la estrella de 6 puntas (la Estrella de David). Supongamos que los puntos equidistantes sobre la circunferencia son etiquetados como: $\{0, 1, 2, 3, 4, 5\}$, de los cuales solo podemos tomar $i = 1$ o $i = 5$ ya que es la única manera en que $(m, i) = 1$. Sin embargo, en cualquiera de los dos casos obtendríamos un polígono regular y no una estrella como es deseado. También podríamos intentar por ejemplo tomar $i = 2$ si esto sucede conectaríamos el punto etiquetado con el número 0 con el número 2, este con el número 4 y finalizaríamos nuevamente conectándolo con el numero 0; obteniendo un triangulo en donde los puntos etiquetados con los números: $1, 3, 5$ no fueron conectados.





Para poder formar la Estrella de 6 puntas se deben de sobreponen dos triángulos, de allí que no pueda ser construida de una sola pieza. Durante las actividades de pares ordenados consultamos sobre Chryzodes [7].

Esta inocente anotación de la imposibilidad de construir la estrella de 6 puntas tiene una explicación matemática basada en las funciones multiplicativas que se exponen en la siguiente sección, ver [2].

4 Funciones multiplicativas

Como segunda para da en este viaje, en esta sección estudiamos ciertas funciones que son de gran a ayuda en el estudio de diversos conjuntos de números, así como de sus propiedades. Estas funciones se conocen como funciones multiplicativas. Las funciones multiplicativas permiten abordar una amplia gama de problemas, como la factorización de enteros, la distribución de números primos, la congruencia de números enteros, entre otros. Además, estas funciones son esenciales en la formulación y prueba de numerosas conjeturas y teoremas importantes en teoría de números.

Definición 2 (Función Multiplicativa)**.** *Una función f es llamada multiplicativa si $f(mn) = f(m)f(n)$, para cuales quiera m y n primos relativos.*

Ejemplo 2. *Las siguientes son funciones multiplicativas*

1. *La función constante $f(m) = 1$ es multiplicativa, ya que $f(mn) = 1 = 1 \cdot 1 = f(m)f(n)$.*
2. *Dada la función $g(n) = n^k$, con k numero entero fijo, tenemos que $g(mn) = (mn)^k = m^k n^k = g(m)g(n)$*

Ahora bien, notemos que, para ambos ejemplos de funciones multiplicativas no hicimos mención que $(m, n) = 1$, sin embargo estas funciones tienen la propiedad deseada.

El siguiente teorema que se denomina el **Teorema fundamental de funciones multiplicativas**, nos permite calcular el valor de una función multiplicativa cualesquiera, sabiendo los valores de potencias primas en n.

Teorema 4 (Teorema fundamental de las funciones multiplicativas)**.** *Sea f una función multiplicativa, y n entero positivo, cuya descomposición en sus factores primos esta dada de la forma $n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$. Entonces $f(n) = f(p_1^{e_1}) f(p_2^{e_2}) \cdots f(p_k^{e_k})$.*

Por inducción matemática. Si $k = 1$, tenemos que $n = p_1^{e_1}$, entonces $f(n) = f\left(p_1^{e_1}\right)$, con lo que el teorema se cumple.

Asumamos que el teorema es cierto para cualquier entero con descomposición en factores primos que contiene k primo distintos, esto es:

$$f(n) = f\left(p_1^{e_1}\right) f\left(p_2^{e_2}\right) \cdots f\left(p_k^{e_k}\right)$$

Sea n un entero arbitrario con $k+1$ primos distintos en su descomposición en factores primos, es decir, $n = p_1^{e_1} p_2^{e_2} \cdots p_{k+1}^{e_{k+1}}$. Dado que $\left(p_1^{e_1} \cdots p_k^{e_k}, p_{k+1}^{e_{k+1}}\right) = 1$ y f es multiplicativa,

$$f\left(p_1^{e_1} \cdots p_k^{e_k} p_{k+1}^{e_{k+1}}\right) = f\left(p_1^{e_1} \cdots p_{k^k}^{e}\right) f\left(p_{k+1}^{e_{k+1}}\right) = f\left(p_1^{e_1}\right) \cdots f\left(p_k^{e_k}\right) f\left(p_{k+1}^{e_{k+1}}\right),$$

por hipótesis de inducción. Por lo tanto el resultado se cumple para cualquier entero n. □

Este teorema es crucial para el posterior estudio de las funciones multiplicativas, ya que nos permiten analizarlas (encontrar fórmulas para ellas) y dotarlas de múltiples propiedades.

A continuación presentamos algunas de las funciones multiplicativas más importantes: φ, τ, σ.

4.1. La función φ

Definición 3. *Sea n un entero positivo. Denotamos a la función $\varphi(n)$ como todos los enteros positivos a menores o iguales que n, tales que $(n, a) = 1$. Es decir:*

$$\varphi(m) = |\{a \in \mathbb{Z}^+ | a \leq m \wedge (a, m) = 1\}|$$

Ejemplo 3. *Para poder ejemplificar la función φ, mostraremos el cálculo de φ para algunos números, esto es:*

1. $\varphi(1) = 1 = |\{1\}|$
2. $\varphi(2) = 1 = |\{2\}|$
3. $\varphi(3) = 2 = |\{2, 3\}|$
4. $\varphi(4) = 2 = |\{3, 4\}|$
5. $\varphi(5) = 4 = |\{2, 3, 4, 5\}|$

Nota 2. *Esta función, como muchas otras posee diversas propiedades que son útiles en la teoría de números:*

1. *Sea p un entero positivo, p es un número primo $\Leftrightarrow$ $\varphi(p) = p - 1$.*
2. *Sea p numero primo, las potencias p^α cumple:*
   $\varphi(p^\alpha) = (p-1)p^{\alpha-1} = p^\alpha(1 - \frac{1}{p})$
3. *La Función de Euler es función multiplicativa, es decir*
   $\varphi(nm) = \varphi(n)\varphi(m)$ *para todo n y m tales que $(n, m) = 1$.*
4. *Sea n un entero positivo. Entonces*

$$\sum_{d|n} \varphi(d) = n$$

5. *De 2) y de 3) se deducimos que dado* $m = \prod_i p_i^{e^i}$*, entonces* $\varphi(m) = \prod_i (p_i - 1)p_i^{e_i - 1}$ $(\forall e_i > 0)$*, o visto de otro modo, sin la restricción en los exponentes:* $\varphi(m) = m\prod_i (1 - \frac{1}{p_i})$.

Para ver más propiedades de la función φ el lector puede consultar [6].

4.2. La función τ

Definición 4. *Sea* n *un entero positivo. Entonces* $\tau(n)$ *denota el número de factores positivos de* n*; esto es,*

$$\tau(n) = \sum_{d|n} 1$$

Ejemplo 4. *A continuación presentamos el cálculo de la función* τ *en algunos números*

- $\tau(21) = 4$*. Note que los divisores de* 21 *son* $1, 3, 7, 21$
- $\tau(125) = 4$*. Note que los divisores de* 125 *son* $1, 5, 25, 125$
- $\tau(5) = 2$*. Lo anterior ya que* 5 *es un número primo.*

Nota 3. *Algunas propiedades que se pueden verificar de la función* τ *son las siguientes*

1. τ *es una función multiplicativa.*
2. $\tau(n) = 2$ *si y solo si* n *es un número primo.*
3. *Si* p *es un número primo y* e *es cualquier entero positivo entonces* $\tau(p^e) = e + 1$
4. $\tau(n)$ *es impar si y solo si* n *es un número cuadrado.*
5. *Si* $\tau(n)$ *es primo, entonces* n *es de la forma* p *o* p^{2e}.

Para ver más propiedades de la función τ el lector puede consultar [6]. s

4.3. Función σ

Definición 5. *Sea* n *un entero positivo. Entonces* $\sigma(n)$ *denota la suma de los factores positivos de* n*; esto es,*

$$\sigma(n) = \sum_{d|n} d$$

Ejemplo 5. *A continuación presentamos el cálculo de la función* σ *en algunos números*

- $\sigma(21) = 32$*. Note que los divisores de* 21 *son* $1, 3, 7, 21$

- $\sigma(125) = 156$. *Note que los divisores de* 125 *son* $1, 5, 25, 125$
- $\sigma(5) = 6$. *Lo anterior ya que* 5 *es un número primo.*

Nota 4. *Algunas propiedades que se pueden verificar de la función* σ *son las siguientes*

1. σ *es una función multiplicativa.*
2. *Si* p *es un número primo y* e *es cualquier entero positivo entonces* $\sigma(p^e) = \frac{p^{e+1}-1}{p-1}$
3. *Si* p *es un número primo y* e *es cualquier entero positivo* $\sigma\left(p^e\right) - p^e = \frac{p^e-1}{p-1}$.
4. *Sea* n *el producto de números gemelos, donde* p *es el más pequeño de los dos entonces* $\sigma(n) = (p+1)(p+3)$ *y* $\sigma(p+2) = \sigma(p) + 2$
5. *Si* n *es una potencia de* 2, *entonces* $\sigma(n)$ *es impar.*

5 Tres Teoremas Clásicos

En la tercera parada de este fascinante viaje nos detendremos en tres resultados icónicos y fundamentales en el desarrollo y estudio de la teoría elemental de números: el Teorema de Wilson, el Pequeño Teorema de Fermat y el Teorema de Euler.

5.1. Teorema de Wilson

En 1770, el matemático inglés Edward Waring describió en sus *Meditationes Algebraicae* la siguiente conjetura de John Wilson, uno de sus antiguos alumnos: Si p es primo, entonces $p|((p-1)!+1)$. Es probable que Wilson haya conjeturado esto usando cierto reconocimiento de patrones. En cualquier caso, ni él ni Waring pudieron proporcionar una prueba de el resultado. Tres años después de que se anunciara la conjetura, Lagrange proporcionó la primera prueba. Lagrange también observó que lo contrario también es cierto.

Wilson, de hecho, no fue el primer matemático en descubrir el teorema, aunque lleva su nombre. Hay pruebas de que el destacado matemático alemán Gottfried Leibniz ya lo sabía desde 1682, aunque no lo publicó.

Para la demostración de este teorema fue necesario el estudio del siguiente Lema.

Lema 1. *Un entero positivo a es autoinvertible módulo p si y solo si $a \equiv \pm 1 \ (mod\ p)$.*

Demostración. Supongamos que a es auto invertible, entonces $a^2 \equiv 1 \ (mod\ p)$; esto es, $p \mid (a^2-1)$; así que $p \mid (a-1)(a+1)$. entonces, $p \mid a-1$ o $p \mid a+1$; así, o $a \equiv 1 \ (mod\ p)$ o bien $a \equiv -1 \ (mod\ p)$.

Recíprocamente, supongamos que $a \equiv 1 \ (mod\ p)$ o $a \equiv -1 \ (mod\ p)$. En este caso, $a^2 \equiv 1 \ (mod\ p)$, así que a es auto invertible módulo p. □

Teorema 5 (Teorema de Wilson)**.** *Si p es número primo, entonces $(p-1)! \equiv -1 \ (mod\ p)$.*

Demostración. Esta demostración se realizará por casos. Primero cuando $p = 2, (p-1)! = 1 \equiv -1 \ (mod\ 2)$; con lo cual el teorema se cumple.

Ahora, consideremos $p > 2$. Recordamos en este punto que la congruencia lineal $ax \equiv b \ (mod\ m)$ tiene única solución si y solo si $(a, m) = 1$ entonces los residuos menores de 1 a $p-1$ son invertibles módulo p. Pero, por el Lema anterior, dos de ellos, 1 y $p-1$, son sus propios inversos. Así, que nosotros podemos agrupar los $p-3$ residuos faltantes de 2 a $p-2$, en $\frac{p-3}{2}$

pares de inversos a y $b = a^{-1}$ tal que $ab \equiv 1\ (mod\ p)$ para todo par a y b. Esto es,

$$\begin{aligned} 2 \cdot 3 \cdots (p-2) &\equiv 1\ (mod\ p) \\ (p-1)! &= 1 \cdot [2 \cdot 3 \cdots (p-2)] \cdot (p-1) \\ &\equiv 1 \cdot 1 \cdot (p-1)\ (mod\ p) \\ &\equiv -1\ (mod\ p) \end{aligned}$$

□

En este punto es importante mencionar que hay otras pruebas alternativas del Teorema de Wilson, por ejemplo el autor estudió la prueba presentada en [6] usando la fórmula de Euler [1]. Además, resaltamos que el reciproco de este teorema también es cierto.

Teorema 6. *Si n es un entero positivo tal que $(n-1)! \equiv -1(\,\mathrm{mód}\,n)$, entonces n es un número primo.*

Demostración. Ver [6]. □

Los teoremas anteriores proporcionan una condición necesaria y suficiente para ver si un entero positivo es primo: Un entero positivo $n \geq 2$ es primo si y sólo si $(n-1)! \equiv -1(\mathrm{mód}n)$. Esta condición proporciona una prueba aparentemente sencilla de primalidad, ya que para comprobar si n es primo, todo lo que necesitamos es determinar si $(n-1)! \equiv -1(\mathrm{mód}n)$. Sin embargo, desafortunadamente, esta prueba no tiene importancia práctica, porque $(n-1)!$ se hace extremadamente grande a medida que n crece.
A continuación presentamos el segundo teorema icónico de este documento.

5.2. El pequeño teorema de Fermat

El 18 de octubre de 1640, Fermat escribió una carta a Bernhard Frenicle de Bessy, funcionario de la Casa de la Moneda francesa y un talentoso estudiante de teoría de números. En su carta, Fermat comunicó el siguiente resultado: *Si p es primo y p no divide a a, entonces $p|a^{p-1} - 1$.* Fermat no proporcionó una prueba de este resultado pero adjuntó una nota prometiendo que enviaría una prueba, siempre que no fuera demasiado larga. Este resultado se conoce como pequeño teorema de Fermat o simplemente teorema de Fermat, para distinguirlo del último teorema de Fermat.

[1] La fórmula de Euler establece que si $n \geq 0$ y x cualquier número real. Entonces,

$$\sum_{i=0}^{n} (-1)^i \binom{n}{i} (x-i)^n = n!$$

Sobre la prueba de este teorema se sabe que los chinos conocían un caso especial del pequeño teorema de Fermat para $a = 2$ desde 500 a.C.. Sin embargo la primera demostración del pequeño teorema de Fermat la dio Euler en 1736, casi un siglo después del anuncio de Fermat. Leibniz había dado una prueba idéntica en un trabajo inédito unos 50 años antes del de Euler, pero una vez más Leibniz no recibir su parte del crédito.

Al igual que para la prueba del teorema de Wilson para la demostración de este Teorema requerimos un Lema auxiliar.

Lema 2. *Sea p un número primo y a cualquier entero tal que $p \nmid a$. Entonces los residuos de los enteros $a, 2a, 3a, \ldots, (p-1)a$ módulo p son una permutación de los enteros $1, 2, 3, \ldots, (p-1)$.*

Demostración. Ver [6] □

Teorema 7 (Teorema pequeño de Fermat)**.** *Sea p número primo y a cualquier entero tal que se cumple $p \nmid a$. Entonces $a^{p-1} \equiv 1 \ (mod\ p)$.*

Demostración. Por el Lema anterior los residuos de $a, 2a, 3a, \ldots, (p-1)a$ módulo p son los mismos que los enteros $1, 2, 3, \ldots, (p-1)$ en el mismo orden , así sus productos son congruentes módulo p; esto es , $a \cdot 2a \cdot 3a \cdots (p-1)a \equiv 1 \cdot 2 \cdot 3 \cdots (p-1) (\text{mód} p)$. En otras palabras, $(p-1)!a^{p-1} \equiv (p-1)!(\text{mód} p)$. Pero $((p-1)!, p) = 1$, así recordando que si $ac \equiv bc(\text{mód} m)$ y $(c, m) = 1$, entonces $a \equiv b(\text{mód} m)$, implicaría $a^{p-1} \equiv 1(\text{mód} p)$. □

5.3. Teorema de Euler

Finalmente en esta parada enunciaremos el Teorema de Euler que es un resultado muy importante en la teoría de números y es una generalización de pequeño teorema de Fermat.

Teorema 8 (Teorema de Euler)**.** *Sea α cualquier entero con $(\alpha, m) = 1$. Entonces*

$$\alpha^{\varphi(m)} \equiv 1 \ (mod\ m)$$

.

Demostración. La prueba del teorema de Euler se da de manera similar a la ya presentada del Teorema de Fermat 7. Para la cual consideramos el conjunto de residuos primos módulo m:

$$r_1, r_2, ..., r_{\varphi(m)}$$

Donde se ha de multiplicar cada uno de los r_k elementos por b, de donde $(b, m) = 1$. Producto que altera la secuencia de los residuos, mas no el valor total de producto.
Esto, por supuesto es consecuencia que, la secuencia de los residuos de primos es grupo multiplicativo. Entonces

$$b^{\varphi(m)} r_1 r_2 ... r_{\varphi(m)} \equiv r_1 r_2 ... r_{\varphi(m)} \ mod \ m$$

Y como los residuos son por definición coprimos con m, tenemos que:

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

De donde finalmente obtenemos:

$$m | \varphi(p^m - 1) \quad \forall m \in \mathbb{Z}$$

□

El teorema de Euler es útil para encontrar residuos de números que involucran exponentes grandes. Incluso si el divisor es compuesto, siempre que este sea primo relativo con respecto a la base del número. Por ejemplo note que si deseamos encontrar el residuo cuando 245^{1040} se divide por 18, consideramos que $245 \equiv 11(\text{mód}18), 245^{1040} \equiv 11^{1040}(\text{mód}18)$ y como $(11, 18) = 1$, usando el Teorema de Euler, $11^{\varphi(18)} \equiv 11^6 \equiv 1(\text{mód}18)$. Por lo tanto, $11^{1040} = (11^6)^{173} \cdot 11^2 \equiv 1^{173} \cdot 13 \equiv 13(\text{mód}18)$. Así el residuo es 13.

Para finalizar presentamos una generalización del teorema de Euler dada por Koshy en 1996.

Teorema 9. *Sean $m_1, m_2, \ldots, m_k$ enteros positivos y a cualquier entero tal que $(a, m_i) = 1$ para $1 \leq i \leq k$. Entonces*

$$a^{[\varphi(m_1), \varphi(m_2), \ldots, \varphi(m_k)]} \equiv 1 \, (\text{mód} \, [m_1, m_2, \ldots, m_k])$$

6 Números perfectos y los primos de Mersenne

En las últimas paradas de este maravilloso viaje nos detendremos en las estaciones de los números perfectos y los primos de Mersenne. Estos números han sido estudiados desde distintos puntos de vista y durante este programa consultamos algunos documentos relacionados con ellos como [3, 5, 8].

6.1. Números Perfectos

Para introducir el concepto de números perfectos haremos uso de la función sigma. El término números perfectos fue acuñado por los pitagóricos. Los griegos antiguos pensaban que estos números tenían poderes místicos y los consideraban números *buenos*. Estos números también fueron estudiados por los primeros hebreos; Rabino Josef ben Jehuda en el siglo XII recomendando su estudio en su libro La curación de las almas.

Históricamente, algunos eruditos bíblicos consideraban que el número 6 era un número perfecto, porque ellos creían que Dios creó el mundo en seis días y que la obra de Dios es perfecta. San Agustín, por otro lado, creía que la obra de Dios era perfecta porque el 6 es un número perfecto. Él escribió: Seis es un número perfecto en sí mismo, y no porque Dios haya creado todas las cosas en seis días; más bien ocurre lo contrario; Dios creó todas las cosas en seis días porque 6 es un número es perfecto. Y seguiría siendo perfecto incluso si el trabajo de los seis días no existiera.

Los pitagóricos consideraban el 6 como el símbolo del " matrimonio, la salud y la belleza" por la integridad de sus partes y por la unidad que existen entre ellas. ¿Qué tiene de místico el 6? Los pitagóricos observaron que 6 es igual a la suma de sus factores propios: $6 = 1 + 2 + 3$. Los siguientes dos números perfectos son 28 y 496:

$$28 = 1 + 2 + 4 + 7 + 14$$

$$496 = 1 + 2 + 4 + 8 + 16 + 31 + 62 + 124 + 248$$

Su descubrimiento se atribuyen al matemático griego Nicómaco quien observó que la Luna orbita la Tierra cada 28 días, el segundo número perfecto [8]. Ahora podemos formalizar la definición de número perfecto.

Definición 6 (Número perfecto)**.** *Un número perfecto es un entero positivo que es igual a la suma de sus divisores positivos excluyéndose a sí mismo.*

Alternativamente un número n es perfecto si $\sigma(n) - n = n$, que es $\sigma(n) = 2n$.

Los primeros 8 números perfectos son:

$$6 = 2(2^2 - 1)$$
$$28 = 2^2(2^3 - 1)$$
$$496 = 2^4(2^5 - 1)$$
$$8128 = 2^6(2^7 - 1)$$
$$33550336 = 2^{12}(2^{13} - 1)$$
$$8589869056 = 2^{16}(2^{17} - 1)$$
$$137438691328 = 2^{18}(2^{19} - 1)$$
$$2305843008139952128 = 2^{30}(2^{31} - 1)$$

Como parte de los estudios realizados, los matemáticos de la Edad Media asumieron diversas proposiciones basadas en los primeros cuatro números perfectos, conjeturando lo siguiente:

1. Los números perfectos terminan alternándose en 6 y 8.
2. Hay un número perfecto entre dos potencias consecutivas de 10, esto es, hay un número perfecto de n dígitos para cada entero positivo.

Desafortunadamente ambas conjeturas son falsas, ya que no existen números perfectos con cinco dígitos de longitud y como ya se vio en el apartado anterior los números perfectos no terminan de manera alternada entre 6 y 8. Sin embargo Euclides demostró el siguiente resultado:

Teorema 10 (Euclides)**.** *Si n es un entero ≥ 2 tal que $2^n - 1$ es número primo, entonces $N = 2^{n-1}(2^n - 1)$ es un número perfecto.*

Demostración. Sea $2^n - 1$ un número primo, $\sigma(2^n - 1) = 1 + (2^n - 1) = 2^n$. Dado que σ es función multiplicativa,

$$\begin{aligned}\sigma(N) &= \sigma(2^{n-1})\sigma(2^n - 1) = (2^n - 1)(2^n) \\ &= 2 \cdot 2^{n-1}(2^n - 1) = 2N\end{aligned}$$

De allí que N es un número perfecto. □

Unos 2.000 años después del descubrimiento de Euclides, Euler demostró que el reciproco de este teorema también es cierto: si $N = 2^{n-1}(2^n - 1)$ es un número par perfecto, entonces $2^n - 1$ es primo.

Teorema 11 (Euler)**.** *Si $N = 2^{n-1}(2^n - 1)$ es un número par perfecto, entonces $2^n - 1$ es primo*

Aunque estos teoremas proporcionan una fórmula notable para construir números pares perfectos, no se sabe si hay infinitos números pares perfectos; la respuesta ha eludido a los teóricos de números de todo el mundo, a pesar de sus incansables esfuerzos. Además de esto hay algunas preguntas que aún permanecen abiertas:

- Determinar si existen infinitos números perfectos. Hasta diciembre del año 2018 se conocen 51 números perfectos.
- Demostrar la imposibilidad de un número perfecto impar o encontrar uno. Sin embargo, existen algunos resultados parciales al respecto. Si existe un número perfecto impar debe ser mayor que 10^{300}, debe tener al menos 8 factores primos distintos (y al menos 11 si no es divisible por 3). Uno de esos factores debe ser mayor que 10^7, dos de ellos deben ser mayores que 10000 y tres factores deben ser mayores que 100.

6.2. Primos de Mersenne

Para finalizar este documento prestaremos especial atención a los aspectos históricos y problemas abiertos relacionados ocn los primos de Mersenne. Primero recordemos que los números de la forma $2^m - 1$ fueron exhaustivamente estudiados por el matemático francés y monje franciscano Marin Mersenne y por esta razón W.W. Rouse Ball los nombró como los **Números de Mersenne** y en particular los primos de la forma $M_p = (2^p - 1)$, se denominan **Primos de Mersenne**.

En 1644, Mersenne escribió en su *Cogiata Physica-Mathematica*, que M_p es primo para $p =$ 2, 3, 5, 7, 13, 17, 19, 31, 67, 127 y 257 y compuesto para los otros primos menores que 257, sin embargo esta afirmación contenía algunos errores (describirlos tomo tres siglos).

En 1814, Peter Barlow escribió en : *A New Mathematical and Philosophical Dictionary:*, Euler comprobó que $2^{31} - 1 = 2{,}147{,}483{,}647$ es un número primo; y este es el mayor que se conoce hasta el presente, y probablemente el más grande que jamás se descubra; porque, como son simplemente curiosidades que no son útiles, no es probable que alguien intente encontrar uno más allá. Resulta que Barlow subestimó la curiosidad humana y pudo no prever el poder de las computadoras.

En 1876, Lucas demostró que M_{67} es compuesto, aunque no proporcionó ninguna factorización; pero en octubre de 1903, el matemático estadounidense Frank Nelson Cole proporcionó una factorización:

$$2^{67} - 1 = 193707721 \times 761838257287$$

Se dice que Cole invirtió sus tardes de domingo durante 20 años para tratar de encontrar estos dos factores.

En 1883, I. M. Pervushin probó que $M_{61} = 2^{61} - 1$ es un primo que Mersenne no tuvo en cuenta. R. E. Powers descubrió que $2^{89} - 1$ y $2^{107} - 1$ son primos , en 1911 y 1914, respectivamente. En 1922, M. Kraitchik mostró que $M_{257} = 2^{257} - 1$ es compuesto.

Al igual que en el caso de los números perfectos relacionadas con los primos de Mersenne hay varias preguntas abiertas alguna de ellas son las siguientes:

- La pregunta de si hay infinitos números primos de Mersenne aún no tiene respuesta. Si los hay, entonces habría una infinidad de números pares perfectos y, por tanto, de números perfectos.
- Tampoco se sabe si cada M_p es libre de cuadrados.
- Si dos de las siguientes afirmaciones sobre un primo impar p es cierta, entonces la tercera también es cierta:
  1. $p = 2^k \pm 1$ o $p = 4^k \pm 3$
  2. M_p es primo
  3. $(2^p + 1)/3$ es primo

Dada la fascinación por estos números, la comunidad matemática no solo se ha valido de mentes brillantes para poder llegar más lejos en el estudio de estos números, sino que también se ha valido de las computadoras modernas que han proporcionado una poderosa herramienta en la búsqueda de números de Mersenne cada vez mas grandes.

Por ejemplo Bryant Tuckerman, junto con *International Business Machines (IBM)*, encontrarón que $2^{19937} - 1$ es primo. De la misma manera, para el año 1994, 33 primos de Mersenne habían sido descubiertos,él número 33 había sido descubierto en 1993 por David Sloqinski de Harwell Laboratory, este proceso tomó 7.2 horas en la súper computadora *Cray C90*. Varios números más han sido descubiertos usando computadoras para más detalles el lector puede consultar GIMPS, este el proyecto *Great Internet Mersenne Prime Search* **GIMPS**, fundado en 1996 por George Woltman, tiene como propósito que con la ayuda de cualquier persona con acceso a un ordenador e internet, se puedan encontrar primos de Mersenne cada vez mas grandes, tal como fue el caso de Jonathan Pace, ingeniero eléctrico que, como voluntario que usa el software gratuito descubrió el pasado 18 de diciembre del 2018 el primo de Mersenne más grande que ha descubierto la humanidad, siendo este $2^{77232917} - 1$, un número primo de 23249425 cifras.

Esto último puede demostrarnos que tal lejos puede llegar el apetito de conocimiento y cooperación entre la comunidad. Abriéndole las puertas a personas que quizás no están especializadas

con un grado en matemáticas, si no que cualquiera con acceso a internet y un ordenador puede ser participe de grandes descubrimientos que favorezcan al desarrollo de las matemáticas.

7 Nuevos Intereses del Aprendiz

Luego de iniciar y terminar este corto pero entretenido viaje por el mundo de la aritmética modular y sus aplicaciones en mi rol de aprendiz del programa pares ordenados logré enriquecer mi quehacer académico desde muchas perspectivas, no solo desde la mirada matemática sino desde los aspectos históricos, humanos entre otros.

Para el futuro cercano luego de mi aprendizaje en pares ordenados me quedaron algunos intereses futuros como:

- Criptografía - Sistema criptográfico RSA.
- Curvas Elípticas
- Criptografía Post-Cuántica.

8 Agradecimientos

Quisiera expresar mis más sinceros agradecimientos a todas las personas involucradas en la realización de este texto. En primer lugar, quiero agradecer a mi mentor, Pedro Fernando Fernández Espinosa, por su constante guía, apoyo, críticas constructivas y dedicación en la realización de este trabajo. Su experiencia y conocimiento fueron fundamentales para la elaboración de este texto.

También agradezco a Pares Ordenados por haber creado un ambiente de aprendizaje colaborativo y por darme la oportunidad de participar en este proyecto.

Por último, agradezco a los lectores por su interés y dedicación en la lectura de este texto. Espero sinceramente que sea de su agrado y que haya logrado transmitirles un poco de la curiosidad e interés que estos temas han despertado en mí.

9 Bibliografía

[1] Conway John H. and Guy Richard., *The book of numbers*, 2nd ed., Springer-Verlag New York, Inc., 1996.

[2] David. Burton, *Elementary Number Theory*, 1st ed., McGraw-Hill, 2007.

[3] Luis H. Gallardo and Olivier Rahavandrainy, *New Conguences for Odd Perfect Numbers*, 2nd ed., The Rocky Mountain Journal of Mathematics, 2006.

[4] Richard K. Guy, *Unsolved problems in number theory*, 3rd ed., Problem Books in Mathematics, Springer-Verlag, New York, 2004. MR2076335

[5] Sándor J. and Crstici B., *Handbook of Number Theory II*, 2nd ed., Kluwer Academic Publishers, 2004.

[6] Thomas. Koshy, *Elementary Number Theory with Applications*, 2nd ed., Academic Press - Elsevier, 2007.

[7] Moreia Gómez Bello, *La aritmética modular y algunas de sus aplicaciones*, Universidad Nacional de Colombia, 2011.

[8] Agustín Moreno Cañadas, *El Código de los Números Perfectos*, Memorias XV Encuentro de Geometría y III de Aritmética, 2005.

[9] Inc. Mersenne Research, *Great Internet Mersenne Prime Search* (1996), `https://www.mersenne.org/`. Accessed: 2024-06-07.

[10] Alec Forssman, *Descubierto el número primo más grande conocido* (2018), `https://www.nationalgeographic.com.es/ciencia/actualidad/descubierto-numero-primo-mas-grande-conocido_12236`. Accessed: 2024-06-07.