Desde la Aritmética Modular al Fascinante Mundo de los Números Perfectos

Jesús Chávez Valencia

Pares Ordenados

June 8, 2024

¿Porqué entré al programa?

Una de las mas grandes motivaciones para entrar al programa fue el hecho que Pares Ordenados ofrece la posibilidad a estudiantes hispanohablantes de matemáticas de conectarlos con estudiantes de doctorado o doctores y desarrollar así un proyecto en conjunto de lectura dirigida.

Pares Ordenados
(mentores, aprendices)

Programa Virtual de Lectura Dirigida

Mi mentor, la base y guía en mi aprendizaje

Como parte de nuestros temas de interés en conjunto, mi mentor el Dr.Pedro Fernando implemento variadas técnicas de aprendizaje con las cuales comencé el estudio de nuestro tema y pude aclarar dudas que de haber abordado este estudio por mi cuenta no me hubiera percatado o analizado mas allá.

Aritmética modular, Funciones Multiplicativas y Aplicaciones

Siendo uno de los objetivos de este proyecto guiado, partimos en aprender y desglosar los temas relacionados a las Congruencias Modulo m. Comenzando dando una breve introducción a las definiciones de construcción de las congruencias modulo m.

Definición

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

Ejemplo

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

Definición

La clase residual de un número a módulo m es el conjunto de todos los números enteros que son congruentes con a módulo m. Esta clase se denota como $[a]_m$ y se define como:

$$[a]_m = \{x \in \mathbb{Z} | x \equiv a\ mod\ m\}$$

Clases residuales *mod* 5

Como ejemplo de esto tenemos las clases residuales modulo 5:

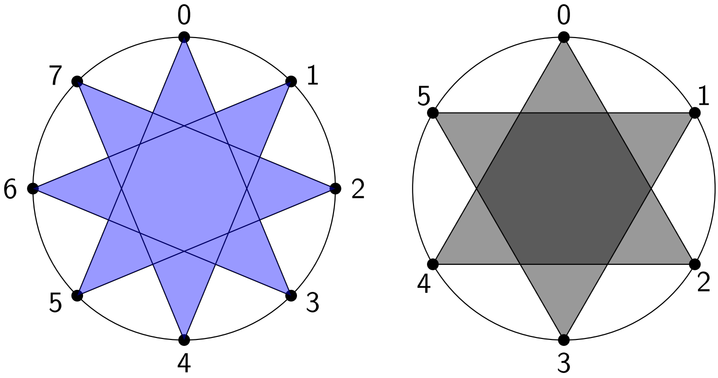
$$
\begin{aligned}
[0]_5 &= \{\ldots, -10, -5, 0, 5, 10, \ldots\} \\
[1]_5 &= \{\ldots, -9, -4, 1, 6, 11, \ldots\} \\
[2]_5 &= \{\ldots, -8, -3, 2, 7, 12, \ldots\} \\
[3]_5 &= \{\ldots, -7, -2, 3, 8, 13, \ldots\} \\
[4]_5 &= \{\ldots, -6, -1, 4, 9, 14, \ldots\}
\end{aligned}
$$

Usos en la vida diaria

Nosotros aun sin la necesidad de ser estudiantes de matemáticas o afines, hemos tenido presentes las congruencias modulo m en nuestro día a día. Estando estas presentes en conceptos muy básicos como lo es la medición del tiempo. Tales como relojes y calendarios.

Aplicaciones, Estrellas de m-puntas

Uno de los usos de la aritmética modular es la creación de bellos y variados diseños, siendo uno de estos la creación de estrellas de $m - puntas$.



Propiedades básicas

Por mencionar brevemente las propiedades de las congruencias *mod m*, podríamos decir:

Propiedades

1. $a \equiv a \pmod{m}$. (**Es reflexiva**)
2. Si $a \equiv b \pmod{m} \Rightarrow b \equiv a \pmod{m}$. (**Es simétrica**)
3. Si $a \equiv b \pmod{m}$ y $b \equiv c \pmod{m}$, entonces $a \equiv c \pmod{m}$. (**Es transitiva**)
4. $a + c \equiv b + c \pmod{m}$
5. $a - c \equiv b - c \pmod{m}$
6. $ac \equiv bc \pmod{m}$
7. $a^2 \equiv b^2 \pmod{m}$

Funciones Multiplicativas

Definición

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

$$n = \prod_{i=1} p_1^{l_i}$$

$$f(n) = \prod_{i=1} f(p_1^{l_i})$$

Ejemplos de funciones multiplicativas

- **La función** φ Denotamos a la funcion $\varphi(n)$ como todos los enteros positivos a menores o iguales que n, tales que $(n, a) = 1$.

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

- **La función** τ Sea n un entero positivo. Entonces $\tau(n)$ denota el número de factores positivos de n.

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

- **Función** σ Sea n un entero positivo. Entonces $\sigma(n)$ denota la suma de los factores positivos de n.

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

Tres teoremas clásicos

Los tres teoremas clásicos se destacan por su elegancia, profundidad y amplia aplicabilidad: el Pequeño Teorema de Fermat, el Teorema de Euler y el Teorema de Wilson.
Estos teoremas no solo proporcionan una comprensión más profunda de las propiedades de los números primos y las congruencias, sino que también tienen aplicaciones prácticas en campos como la criptografía y la informática.

Tres teoremas clásicos

1. **Pequeño Teorema de Fermat** Sea p número primo y a cualquier entero tal que se cumple $p \not| \; a$. Entonces $a^{p-1} \equiv 1 \; (mod \;\; p)$.
2. **Teorema de Wilson** Si p es número primo, entonces $(p-1)! \equiv -1 \; (mod \;\; p)$.
3. **Teorema de Euler** Sea α cualquier entero con $(\alpha, m) = 1$. Entonces $\alpha^{\varphi(m)} \equiv 1 \; (mod \;\; m)$.

Números perfectos y Primos de Mersenne

Los números primos, especialmente los números primos perfectos y los primos de Mersenne, tienen propiedades únicas y están conectados con teoremas fundamentales. Euler demostró que todos los números perfectos pares pueden describirse usando primos de Mersenne, mostrando una relación directa entre ellos.

Números perfectos y Primos de Mersenne

Definición

Un número perfecto es un entero positivo que es igual a la suma de sus divisores positivos excluyéndose a sí mismo.

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

Números perfectos y primos de Mersenne

Aquellos números de la forma $2^m - 1$ fueron exhaustivamente estudiados por el matemático francés y monje franciscano Marin Mersenne,

Definición

Sean aquellos números primos que pueden escribirse de la forma $M_p = (2^p - 1)$, son nombrados **Primos de Mersenne**.

$2^P - 1$

Great
Internet
Mersenne
Prime
Search

Finding World Record Primes Since 1996

Conclusiones

Una vez que hemos analizado y estudiado todos estos conceptos, a lo largo de este proyecto, puedo declarar que este ha sido de gran ayuda en el estudio de un tema que si bien he abordado en la escuela, lo que he visto con ayuda de mi mentor, complemento y me ayudo a comprender temas que en un primer caso no comprendí por completo y que gracias a esto puedo desempañarme en una mayor medida y que me da la experiencia para poder seguir estudiando de una manera mas autónoma para proyectos futuros.