Universidad Autónoma de Chihuahua

Facultad de Ingeniería

Resumen Exposición: Clases Residuales y Clases de Equivalencia Módulo n

Unidad de Aprendizaje 3

Matemáticas Discretas II

Martín Eduardo Chacón Orduño - 351840
Alexis Quirarte Grado - 374223
José Fernando Martínez García-355597
Ingeniería en Ciencias de la Computación
Maestra: Hermila Ortega Mendoza
19/04/2024

Contenido

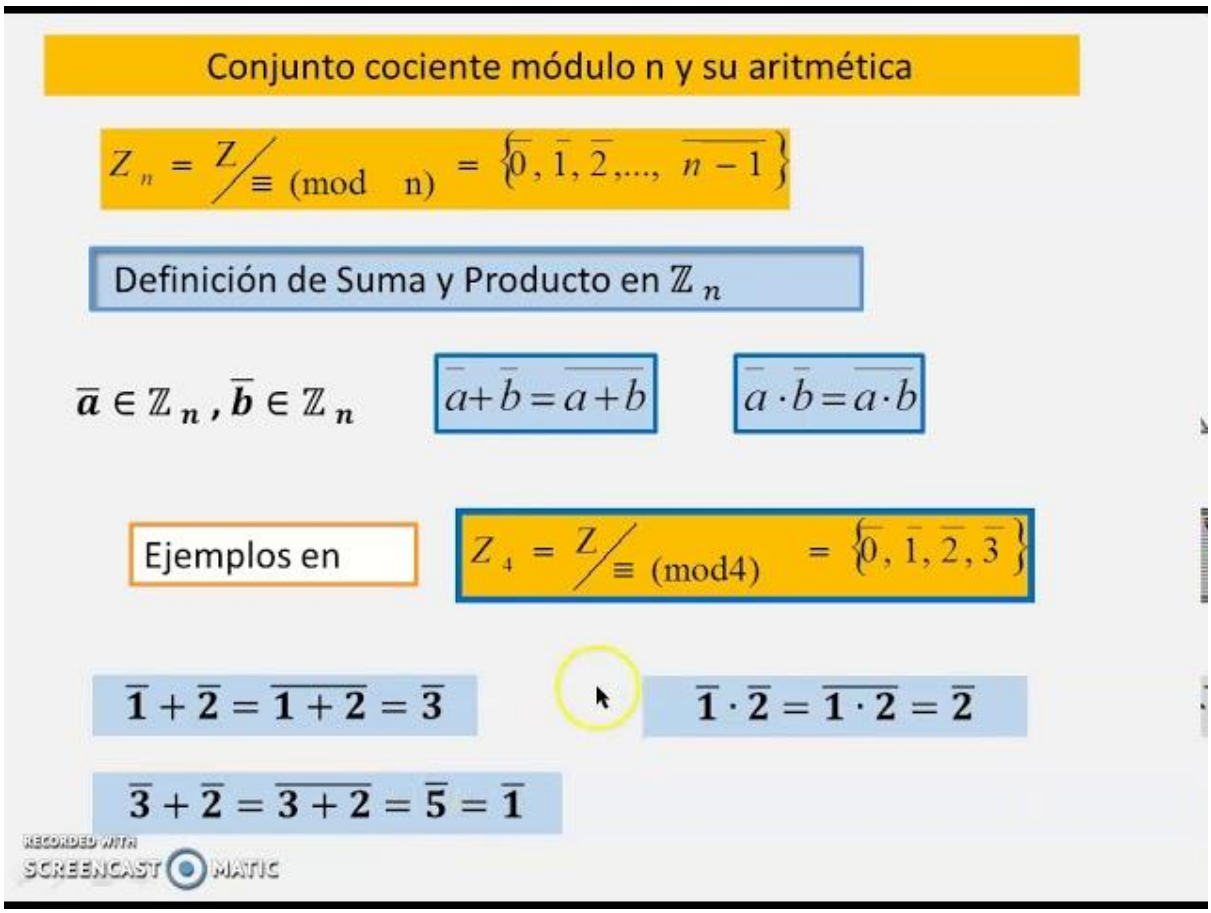
Clases residuales 2
Clases de equivalencia módulo n 3
Adición y Multiplicación en Clases de Equivalencia Módulo n 4
Anillo equivalencia módulo n 5
Aplicaciones en general 5
Criptografía 5
Ciencias de la Computación 6
Teoría de Números 6
Ingeniería 6
Matemáticas Computacionales 6
Juegos y Simulaciones 7
Aplicaciones en ciencias de la computación 7
Criptografía 7
Estructuras de Datos Hash 7
Algoritmos de Verificación de Redundancia 7
Teoría de Números y Algoritmos 7
Algoritmos de Graficación Computacional 8
Sistemas de Tiempo 8
Conclusión 8
Bibliografía 9

Clases residuales

En teoría de números, cuando trabajas con aritmética modular (como en aritmética de congruencia), las clases residuales se refieren a los restos obtenidos al dividir un número entero por otro. Por ejemplo, si estás trabajando en el módulo 7, las clases residuales serían los números 0, 1, 2, 3, 4, 5, y 6, ya que esos son los posibles restos al dividir cualquier número entero por 7.

En criptografía, las clases residuales son fundamentales en la construcción de sistemas criptográficos basados en teoría de números, como RSA. En este contexto, las operaciones se realizan en clases residuales módulo un número entero grande, lo que proporciona seguridad criptográfica.

Las clases residuales también son importantes en otras áreas de las matemáticas, como el álgebra abstracta y la teoría de grupos, donde se utilizan para construir estructuras algebraicas como anillos y cuerpos.



Clases de equivalencia módulo n

Las clases de equivalencia módulo nn son conjuntos de números enteros que producen el mismo residuo cuando se dividen por nn. Formalmente, si aa es un entero y nn es un entero positivo mayor que cero, entonces la clase de equivalencia de aa módulo nn, denotada como $[a]n[a]n$, es el conjunto de todos los enteros bb tales que $a≡b(\mod n)a≡b(\mod n)$.

En otras palabras, dos números enteros aa y bb están en la misma clase de equivalencia módulo nn si su diferencia $a−ba−b$ es divisible por nn.

Por ejemplo, considera $n=5n=5$. Las clases de equivalencia módulo 55 son:

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

Cada una de estas clases de equivalencia representa un conjunto de números enteros que producen el mismo residuo cuando se dividen por 55. La teoría de congruencia y las clases de equivalencia módulo nn son fundamentales en muchos campos de las matemáticas, como la teoría de números, la criptografía y la informática teórica.

Adición y Multiplicación en Clases de Equivalencia Módulo n

En matemáticas, las operaciones de suma y multiplicación en las clases de equivalencia módulo n, se realizan entre los residuos o representantes de estas clases. Esto se hace bajo la aritmética modular, donde básicamente "reiniciamos" el conteo una vez que alcanzamos$n$, el módulo.

Para dos enteros a y b , definimos adición módulo n como (a+b) (mod n). Es decir, el resto de la división de a+b entre n. Similarmente la multiplicación módulo n se define como (ab)(mod n), el resto de la división de ab entre n.

$$\begin{aligned} 7+4 &\equiv 1 \pmod 5 & 7\cdot 3 &\equiv 1 \pmod 5 \\ 3+5 &\equiv 0 \pmod 8 & 3\cdot 5 &\equiv 7 \pmod 8 \\ 3+4 &\equiv 7 \pmod{12} & 3\cdot 4 &\equiv 0 \pmod{12}. \end{aligned}$$

Estos cálculos son útiles en varios campos como criptografía, teoría de números, y en sistemas donde el "desbordamiento" es manejado por módulo (por ejemplo, en ciertas operaciones de computadora).

Anillo equivalencia módulo n

Un anillo formado por las clases de equivalencia módulo n es una estructura algebraica definida en teoría de números y álgebra abstracta. Este anillo, denotado comúnmente como Zn o Z/nZ, está compuesto por los restos de las divisiones euclidianas de los enteros por n.

Para definir formalmente este anillo, consideremos el conjunto de números enteros Z y una relación de equivalencia ≡ definida sobre Z. Dos enteros a y b se consideran equivalentes módulo n si su diferencia es un múltiplo entero de n. Formalmente, $a \equiv b \pmod{n}$ si n divide a $a-b$.

Las clases de equivalencia módulo n son entonces conjuntos de enteros que son equivalentes entre sí bajo esta relación. Por ejemplo, en 4 Z4, las clases de equivalencia son [0],[1],[2],[3], donde [0] representa todos los enteros que son múltiplos de 4, [1] representa los enteros que dejan un residuo de 1 al dividir entre 4, y así sucesivamente. El conjunto de clases de equivalencia módulo n forma un anillo bajo las operaciones de suma y multiplicación módulo n. Es decir, la suma y multiplicación se realizan entre los representantes de las clases de equivalencia, y el resultado se reduce al módulo n. Este anillo es conmutativo y tiene elementos identidad para la suma y el producto.

Aplicaciones en general

Las clases de equivalencia y las operaciones aritméticas en módulo n tienen numerosos usos prácticos en diferentes campos.

Criptografía

La aritmética modular es una base fundamental en varios algoritmos de criptografía. Por ejemplo:

RSA: Este popular algoritmo de cifrado utiliza la multiplicación modular para encriptar y desencriptar mensajes. En RSA, la seguridad se basa en la dificultad de factorizar grandes números primos y en las propiedades de la aritmética modular.
Diffie-Hellman: Este protocolo permite a dos partes establecer una clave compartida de manera segura sobre un canal inseguro. Utiliza exponenciación modular para generar las claves.

Ciencias de la Computación

Hashing: Las funciones hash, que son críticas para estructuras de datos como tablas hash, utilizan aritmética modular para asignar datos grandes a un rango fijo de valores pequeños (los índices de la tabla).
Generación de números aleatorios: Algunos métodos para generar secuencias de números aleatorios utilizan operaciones modulares para mantener los números dentro de un rango específico.

Teoría de Números

Teoremas y pruebas: La aritmética modular se utiliza para demostrar numerosos resultados y teoremas en teoría de números, como el Pequeño Teorema de Fermat o el Teorema Chino del Resto.

Ingeniería

Sistemas de control y señales: En el procesamiento de señales digitales, la aritmética modular se puede usar para manejar el desbordamiento de números (wrap around) en operaciones de filtro y para modelar sistemas que tienen comportamiento cíclico.

Matemáticas Computacionales

Algoritmos de factorización: Métodos como la criba cuadrática o la criba de campos de números usan aritmética modular para encontrar factores de números grandes, lo cual es crucial para la criptografía.

Juegos y Simulaciones

Lógica de juego: La aritmética modular puede ser utilizada para determinar turnos, ciclos de eventos recurrentes o comportamientos que deben repetirse en un intervalo fijo en simulaciones y juegos.

Aplicaciones en ciencias de la computación

Criptografía

La aritmética modular es fundamental en varios algoritmos criptográficos, incluyendo RSA, que es uno de los métodos más comunes para el cifrado y firma digital de datos. La generación de claves, el cifrado y el descifrado en RSA involucran operaciones con números muy grandes bajo módulo \(n \), donde \(n \) es el producto de dos números primos grandes.

Estructuras de Datos Hash

Las funciones hash, que son críticas para muchas estructuras de datos como las tablas hash, utilizan aritmética modular para asignar datos de entrada de gran tamaño a un número fijo de índices (o "cubetas"). Por ejemplo, para asegurar que los índices resultantes se ajusten dentro de los límites del arreglo, se puede usar el módulo \(n \) del valor hash para obtener un índice dentro del rango deseado.

Algoritmos de Verificación de Redundancia

En la detección y corrección de errores en la transmisión de datos, como en el algoritmo de CRC (Cyclic Redundancy Check), se utilizan polinomios y cálculos en un campo finito, basados en aritmética modular para asegurar la integridad de los datos.

Teoría de Números y Algoritmos

Muchos algoritmos eficientes para test de primalidad, búsqueda de factores, y otros relacionados con la teoría de números, dependen de la aritmética modular. Por

ejemplo, la prueba de primalidad de Miller-Rabin utiliza operaciones de multiplicación y adición modular para determinar si un número es primo.

Algoritmos de Graficación Computacional

En la generación de patrones periódicos o en el diseño de efectos visuales que se repiten a intervalos regulares, se puede utilizar la aritmética modular para calcular posiciones y transformaciones que deben "envolverse alrededor" de ciertos límites, como en un entorno toroidal o en un mapa repetitivo.

Sistemas de Tiempo

Para operaciones que involucran el cálculo de tiempos, especialmente aquellos que se "envuelven alrededor" (como de 23 horas a 0 horas), la aritmética modular es una herramienta natural para manejar estos cálculos sin tener que escribir lógica condicional adicional.

Conclusión

En conclusión, las clases residuales y las clases de equivalencia módulo n, n son conceptos fundamentales en diversas ramas de las matemáticas y tienen aplicaciones importantes en teoría de números, criptografía, álgebra abstracta, informática teórica y otros campos relacionados. Estas clases proporcionan una manera de agrupar números enteros que comparten ciertas propiedades bajo operaciones de suma y multiplicación módulo n. En particular, el anillo formado por las clases de equivalencia módulo n, denotado como Zn o Z/nZ es una estructura algebraica bien definida que tiene propiedades importantes como conmutatividad y la existencia de elementos identidad para la suma y el producto. Estos conceptos son esenciales para el desarrollo de sistemas criptográficos, la comprensión de estructuras algebraicas y el análisis de problemas relacionados con operaciones modulares

Bibliografía

AATA Clases de equivalencia de enteros y simetrías. (s. f.). http://abstract.ups.edu/aata-es/section-mod-n-sym.html

Congruencia módulo (artículo). (s/f). Khan Academy. Recuperado el 4 de mayo de 2024, de https://es.khanacademy.org/computing/computer-science/cryptography/modarithmetic/a/congruence-modulo

Martínez, I., & Solís, R. (2019). Grafo n- residual Módulo m y su aplicación en la estructuración de Residuos n- ádicos. Revista de Matemática Teoría y Aplicaciones, 26(2), 299-318. https://doi.org/10.15517/rmta.v26i2.38320