03 - Aritmética entera y modular

Aritmética Entera y Modular: Cuerpos Finitos

Este tema constituye uno de los pilares fundamentales del álgebra moderna, abarcando desde los conceptos básicos de divisibilidad hasta las estructuras algebraicas más complejas como los cuerpos finitos. La aritmética entera nos proporciona las herramientas para comprender cómo funcionan los números enteros y sus propiedades, mientras que la aritmética modular introduce un sistema de cálculo que resulta esencial en criptografía, teoría de códigos y muchas otras aplicaciones computacionales1.

Fundamentos de la Aritmética Entera

Conceptos Básicos y Divisibilidad

La aritmética entera se centra en el estudio de los números enteros y sus propiedades fundamentales. El concepto de divisibilidad constituye la base de toda esta teoría y debe entenderse desde sus fundamentos más elementales.

Definición de Divisibilidad: Decimos que un número entero **a** divide a otro número entero **b** (denotado como **a** ∣ **b**) si existe un número entero **k** tal que **b=a·k** En este caso, a se llama divisor de **b**, y **b** se llama múltiplo de **a**.

Por ejemplo, el número 3 divide a 12 porque existe un entero k=4 tal que 12=3·4. De manera similar, 7 divide a 21 porque 21=7·3. Sin embargo, 5 no divide a 13 porque no existe ningún entero que multiplicado por 5 dé como resultado 13.

Propiedades Fundamentales de la Divisibilidad: La relación de divisibilidad cumple varias propiedades importantes que forman la base de muchos teoremas posteriores. Si **a** ∣ **b** y **b** ∣ **c** entonces **a** ∣ **c** (propiedad transitiva).

Si **a** ∣ **b** y **a** ∣ **c**, entonces **a** ∣ **(b+c)** y **a** ∣ **(b−c)**. Además, si **a** ∣ **b** y **c** es cualquier entero, entonces **a** ∣ **(bc)**.

Algoritmo de la División: Este algoritmo establece que para cualquier par de números enteros **a** y **b** con **b>0**, existen únicos enteros **q** (cociente) y **r** (resto) tales que **a=bq+r** donde **0≤r<b**. Este resultado, aparentemente simple, tiene consecuencias profundas en toda la teoría de números.

Sistemas de Numeración y Bases

Los sistemas de numeración representan una herramienta fundamental para expresar números en diferentes bases, siendo esencial comprender cómo funcionan estos sistemas para avanzar en conceptos más complejos.

Base Decimal: El sistema decimal, que utilizamos cotidianamente, emplea la base 10. Esto significa que cada posición en un número representa una potencia de 10. Por ejemplo, el número 2537 se puede expresar como $2 \times 10^3 + 5 \times 10^2 + 3 \times 10^1 + 7 \times 10^0$.

Bases Generales: En un sistema de base b*b*, utilizamos los dígitos del 0 al **b−1,** y cada posición representa una potencia de **b.** El sistema binario (base 2) utiliza solo los dígitos 0 y 1, siendo fundamental en computación. El sistema hexadecimal (base 16) emplea los dígitos 0-9 y las letras A-F para representar los valores 10-15.

Conversión entre Bases: Para convertir un número de base 10 a base **b**, dividimos repetidamente por **b** y tomamos los restos en orden inverso. Por ejemplo, para **convertir 25 a base 2:**

25÷2=12 resto 1,

12÷2=6 resto 0,

6÷2=3 resto 0,

3÷2=1 resto 1,

1÷2=0 resto 1.

Leyendo los restos de abajo hacia arriba: $25_{10} = 11001_2$

Teoría de Números Primos

Los números primos constituyen los "átomos" de la aritmética, siendo elementos indivisibles que forman la base de todos los demás números enteros positivos.

Definición y Propiedades Básicas: Un número primo es un número natural mayor que 1 que tiene exactamente dos divisores positivos: 1 y él mismo. Los primeros números primos son 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, etc. El número 2 es el único número primo par, ya que todos los demás números pares son divisibles por 2.

Teorema Fundamental de la Aritmética: Este teorema establece que todo número entero mayor que 1 puede expresarse de manera única como producto de números primos (considerando el orden de los factores). Por ejemplo, $60 = 2^2 * 3 * 5$. Esta factorización única es fundamental para muchos algoritmos y demostraciones en matemáticas.

Criba de Eratóstenes: Este algoritmo clásico permite encontrar todos los números primos menores que un número dado **n**. Se comienza listando todos los números del 2 al **n**, luego se marcan los múltiplos de cada primo encontrado. Los números que quedan sin marcar son primos. Este método ilustra la distribución de los primos y su densidad decreciente.

Máximo Común Divisor y Mínimo Común Múltiplo: El máximo común divisor (MCD) de dos números es el mayor número que divide a ambos. Se puede calcular usando el algoritmo de Euclides: para encontrar **MCD(a,b)**, dividimos **a** por **b** y aplicamos el algoritmo recursivamente con **b** y el resto. El mínimo común múltiplo (MCM) se relaciona con el MCD mediante la fórmula $\text{MCM}(a,b) = \frac{a \times b}{\text{MCD}(a,b)}$.

Aritmética Modular y Estructuras Algebraicas

Introducción a la Aritmética Modular

La aritmética modular representa un cambio de paradigma en la forma de entender las operaciones matemáticas, introduciendo el concepto de "aritmética del reloj" que resulta fundamental en muchas aplicaciones modernas.

Congruencias Modulares: Decimos que dos números enteros **a** y **b** son congruentes módulo **n** (denotado **a≡b(modn)**) si **n** divide a **a−b.** Intuitivamente, esto significa que **a** y **b** tienen el mismo resto al dividirse por **n**. Por ejemplo, **17≡2(mod5)** porque ambos números dan resto 2 al dividirse por 5.

Propiedades de las Congruencias: Las congruencias preservan las operaciones básicas. Si **a≡b(modn)** y **c≡d(modn)**, entonces **a+c≡b+d(modn)** y **ac≡bd(modn**). Esta propiedad permite realizar cálculos complejos trabajando solo con los restos, simplificando enormemente los cálculos.

Clases de Equivalencia: El conjunto de todos los números congruentes a **a** módulo **n** forma una clase de equivalencia, denotada a_n .Por ejemplo, para **n=5**, la clase $[1]_5$contiene todos los números de la forma **5k+2: {..., -8, -3, 2, 7, 12, 17, ...}**. El conjunto $\mathbb{Z}_n = \{_n, _n, \ldots, [n-1]_n\}$ forma el conjunto de todas las clases de equivalencia módulo **n.**

Estructuras Algebraicas: Anillos

Los anillos representan estructuras algebraicas que generalizan las propiedades familiares de los números enteros, proporcionando un marco teórico para entender sistemas más complejos.

Definición de Anillo: Un anillo es un conjunto **R** equipado con dos operaciones (suma y multiplicación) que satisfacen ciertas propiedades. La suma debe ser

asociativa, conmutativa, tener elemento neutro (0) y cada elemento debe tener inverso aditivo. La multiplicación debe ser asociativa y distributiva respecto a la suma.

Ejemplos de Anillos: Los números enteros **Z** forman un anillo con las operaciones usuales. Los conjuntos Z_n con las operaciones módulo **n** también forman anillos. Las matrices cuadradas de tamaño fijo con suma y multiplicación matricial forman otro ejemplo importante de anillo.

Elementos Inversibles: En un anillo, un elemento **a** es inversible (o unidad) si existe un elemento **b** tal que **ab=ba=1**. En Z_n,un elemento $[a]_n$ es inversible si y solo si **MCD(a,n)=1**. Esto conecta la teoría de anillos con conceptos básicos de teoría de números.

Cuerpos Finitos

Los cuerpos finitos representan estructuras algebraicas donde cada elemento no nulo tiene inverso multiplicativo, generalizando las propiedades de los números racionales a conjuntos finitos.

Definición de Cuerpo: Un cuerpo es un anillo donde todo elemento no nulo es inversible. Esto significa que podemos dividir por cualquier elemento no nulo. Los números racionales **Q**, reales **R** y complejos **C** son ejemplos de cuerpos infinitos.

Cuerpos Z_p : Cuando p es un número primo, Z_p forma un cuerpo. Esto ocurre porque cuando **p** es primo, **MCD(a,p)=1** para todo **a** con **1≤a≤p−1**, garantizando que todos los elementos no nulos tengan inverso. Por ejemplo, en Z_5, el inverso de 2 es 3 porque **2·3=6≡1(mod5)**.

Propiedades de los Cuerpos Finitos: Los cuerpos finitos tienen propiedades únicas. Para cualquier primo **p** y entero positivo **n,** existe un único cuerpo finito

(salvo isomorfismo) con p^n elementos, denotado ${f_p}^n$ o **GF(p^n)**. Cuando **n=1**, obtenemos Z_p.

Aplicaciones: Los cuerpos finitos son fundamentales en criptografía moderna, códigos correctores de errores, y teoría de la información. Por ejemplo, el protocolo de intercambio de claves Diffie-Hellman se basa en la dificultad de calcular logaritmos discretos en cuerpos finitos.

Resolución de Ecuaciones y Sistemas en Aritmética Modular

Ecuaciones de Congruencia Lineales

Las ecuaciones de congruencia representan una generalización natural de las ecuaciones lineales al contexto modular, requiriendo nuevas técnicas de resolución.

Ecuaciones de la Forma *ax≡b(mod n):* Para resolver esta ecuación, necesitamos encontrar el inverso multiplicativo de **a** módulo **n**, lo cual es posible si y solo si **MCD(a,n)=1**. Si existe el inverso a^{-1}, entonces **x≡a^{-1}b(mod n).**

Algoritmo Extendido de Euclides: Este algoritmo no solo calcula el MCD de dos números, sino que también encuentra coeficientes enteros **s** y **t** tales que **MCD(a,n)=sa+tn**. Si **MCD(a,n)=1**, entonces **s** es el inverso de **a** módulo **n**.

Casos con Soluciones Múltiples: Cuando **MCD(a,n)=d>1**, la ecuación **ax≡b(mod n)** tiene solución si y solo si **d** | **b**. En este caso, existen exactamente **d** soluciones módulo **n.**

Teorema Chino del Resto

Este teorema clásico proporciona una herramienta poderosa para resolver sistemas de congruencias simultáneas cuando los módulos son coprimos entre sí.

Enunciado del Teorema: Si $n_1, n_2, ..., n_k$ **s**on enteros positivos mutuamente coprimos, entonces el sistema de congruencias $x \equiv a_1 \pmod{n_1}$, $x \equiv a_2 \pmod{n_2}$, ..., $x \equiv a_k \pmod{n_k}$ tiene una solución única módulo $N = n_1 \cdot n_2 \cdot ... \cdot n_k$.

Construcción de la Solución: Para cada **i** definimos $N_i = N/n_i$ y encontramos M_i tal que $N_i M_i \equiv 1 \pmod{n_i}$. La solución está dada por x≡ $\sum_{i=1}^{k} a_i N_i M_i \pmod{N}$.

Ejemplo Práctico: Consideremos el sistema **x≡2(mod3), x≡3(mod5), x≡2(mod7).** Como 3, 5 y 7 son mutuamente coprimos, el teorema garantiza una solución única módulo 3·5·7=105. Aplicando el algoritmo, obtenemos **x≡23(mod 105)**.

Conclusión

La aritmética entera y modular constituye un campo fundamental que conecta conceptos elementales con estructuras algebraicas sofisticadas. Desde los principios básicos de divisibilidad hasta la construcción de cuerpos finitos, estos conceptos forman la base teórica de numerosas aplicaciones en matemáticas, informática y criptografía. La comprensión profunda de estos temas requiere dominar tanto los aspectos computacionales como los fundamentos teóricos, proporcionando las herramientas necesarias para abordar problemas más avanzados en álgebra abstracta y sus aplicaciones. El dominio de la aritmética modular y las estructuras algebraicas asociadas abre las puertas a campos especializados como la criptografía de clave pública, la teoría de códigos y el álgebra computacional, demostrando la relevancia continua de estos conceptos clásicos en las matemáticas modernas.

Apuntes Pedro Lopez Galán