Universidad Nacional Autónoma de México

Facultad de Ingeniería

Estructuras Discretas

Grupo: 07

Profesor:

M.I Orlando Zaldívar Zamorategui

“Sistemas algebraicos. La aritmética de residuos en las computadoras. Aplicaciones en las computadoras.”

Equipo 5

Barrera Treviño José Gerardo

Espinosa Guzmán Magali Lizeth

Luna Valdin Uriel

Sampayo Aguilar Cinthia Gloricel

Vega Castillo Brandon

Índice

Objetivo **2**
Introducción **3**
Aritmética de Residuos **4**
Sistemas Numéricos 4
Aritmética de residuos 5
Congruencia y sus propiedades 5
Propiedades de congruencia: 7
Teorema de congruencia lineal 7
Operaciones básicas 9
Inverso modular 11
Teorema de los restos chinos 12
Aplicaciones en computación **13**
Criptografía 13
Algoritmo RSA 14
Algoritmo Hash 15
Ejercicios Resueltos **18**
Cuestionario **26**
Bibliografía **35**

Objetivo

El objetivo de este tutorial es presentar al usuario el concepto de aritmética de residuos y mostrar cómo esta rama de las matemáticas tiene aplicaciones importantes en el campo de la computación. En el mismo, el lector podrá aprender los elementos básicos del tema para poder trabajar con residuos y entender la congruencia modular.

Para lograr este objetivo explicaremos cómo los conceptos de aritmética de residuos se aplican en algoritmos eficientes para problemas como los sistemas criptográficos. Además, los ejemplos prácticos permitirán al usuario ver directamente cómo utilizar la aritmética de residuos. Mientras que el material audiovisual hará más dinámico el proceso de aprendizaje del usuario. Finalmente, implementaremos un cuestionario y un software especializado que está diseñado para evaluar los conocimientos adquiridos.

Al final del tutorial, el usuario tendrá una comprensión sólida de cómo la aritmética de residuos es esencial en el diseño y análisis de algoritmos computacionales.

Introducción

Uno de los aportes más importantes a las Matemáticas y, en específico a la Teoría de Números, es la formalización de la Aritmética Modular que Gauss realizó en su Investigaciones sobre aritmética en **Disquisitiones arithmeticae (1801)**. En esta obra, Gauss define la noción de congruencia entre dos enteros (módulo m); describe las propiedades de la dicha relación (congruencia) y la establece como el conjunto completo de residuos.

Gauss no sólo definió la congruencia modular, sino que también estableció reglas y propiedades que permiten simplificar cálculos y resolver problemas de una manera eficiente. Sus ideas han perdurado hasta hoy y son la base de muchos algoritmos y sistemas de seguridad que utilizamos a diario en la era digital.
A lo largo de este tutorial exploraremos cómo la aritmética de residuos nos permite:

- Reducir cualquier número entero a un conjunto finito de residuos.
- Realizar operaciones como suma, resta, multiplicación y división de manera eficiente en aritmética de residuos.
- Comprender la congruencia modular y su aplicación en áreas como la criptografía.

Aritmética de Residuos

Sistemas Numéricos

La información es uno de los recursos más valiosos que posee el ser humano, se puede administrar, modificar, comercializar y transmitir. Para ello, la manipulación de la información se lleva a cabo mediante representaciones que pueden ir desde símbolos hasta gráficos y otros tipos de diseño.

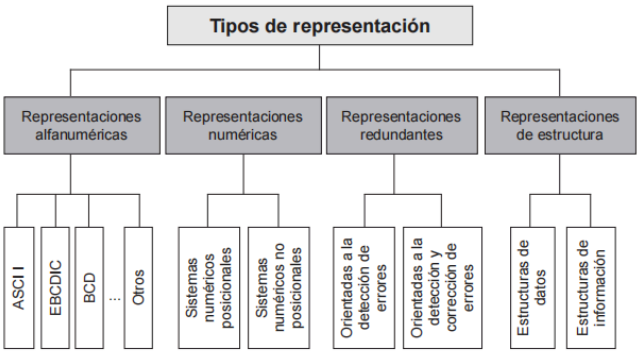
Las computadoras operan principalmente con dos tipos de elementos de información: instrucciones y datos; los cuales pueden adoptar diversas representaciones a nivel de máquina, determinando así las características de funcionamiento y la estructura del sistema.

Por lo tanto, el estudio de los sistemas de representación de información es esencial para comprender los procesos de tratamiento de datos. Con este propósito, se establecen tres criterios de clasificación:

1. Elemento primario a representar: cifra, letra, carácter especial, entre otros.
2. Forma de representación: punto fijo, punto flotante, empaquetado, etc.
3. Características de representación: tolerante a fallos, con prioridad, etc.

Estos criterios permiten identificar diversos tipos de representación:

Figura 1. Tipos de representación de los elementos de información que maneja el computador



Fuente: elaboración propia a partir de Joyanes (1990), Black (1997) y González (1987).

Cabe destacar que de las representaciones numéricas, la que más influye sobre la arquitectura de la máquina es la de las representaciones numéricas, pues constituye

el fundamento para la codificación de cantidades y proporciona elementos para organizar una aritmética computacional.

Investigaciones recientes han revelado que los sistemas numéricos posicionales no son suficientes para lograr un aumento significativo en la velocidad de procesamiento de la información, ni tampoco contribuyen a mejorar los niveles de desempeño y productividad. Además, los acarreos generados durante la ejecución de algunas de sus operaciones añaden complejidad al hardware y al sistema.

Por lo mismo, se han explorado alternativas de nuevos sistemas numéricos "no posicionales". Estos sistemas, como la aritmética modular o la aritmética de residuos, han surgido como opciones que no implican la generación de acarreos.

Aritmética de residuos

La aritmética residual, también conocida como aritmética modular o aritmética de congruencia, es un área de las matemáticas que se centra en el estudio de los **números enteros** en relación con un número fijo llamado **módulo**. Esta área tiene aplicaciones prácticas en campos como la criptografía, la informática, la teoría de números y la ingeniería.

La aritmética modular se enfoca en cómo se comportan los números enteros cuando los consideramos en grupos de tamaño fijo determinado por el módulo. Por ejemplo: si consideramos los números enteros módulo 5, estamos agrupando todos los enteros en cinco conjuntos diferentes, según su residuo al dividirlos por 5.

Esta área del conocimiento permite realizar todas las operaciones aritméticas (**suma, resta y multiplicación**), excepto la división, que son por principio procedimientos sin acarreos. Cada dígito en el resultado es una función sólo de dígitos correspondientes a los operandos.

Congruencia y sus propiedades

La aritmética residual se basa en el concepto de **congruencia**, que es fundamental para entender cómo funciona. Dos números enteros **a** y **b** se consideran congruentes módulo **m**, denotado como: **a≡b (mod m)**, si su diferencia **a−b** es un múltiplo de **m**. En otras palabras, **a** y **b** tienen el mismo residuo cuando se dividen por **m**.

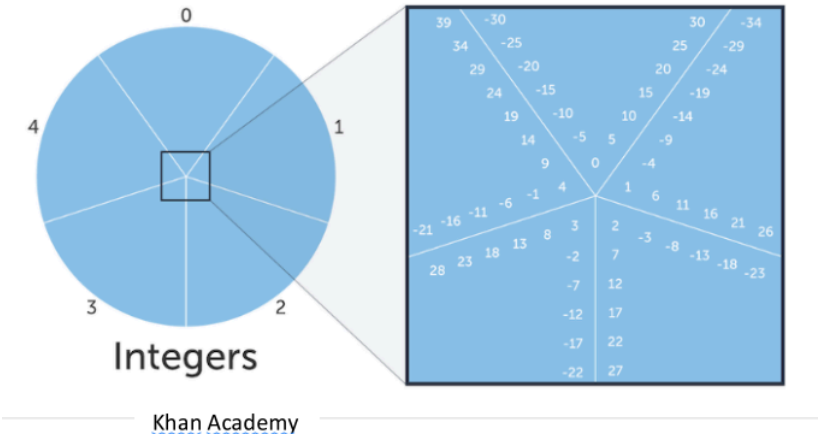
$$a \equiv b \pmod{m}$$

Por ejemplo, si tomamos los números enteros **7** y **17**, ambos son congruentes módulo **5**, ya que su diferencia es **17−7=10**, que es un múltiplo de **5**.

Asimismo, una de las ventajas de trabajar con este concepto es la posibilidad de manejar **clases de equivalencia de números enteros**. En lugar de operar con números individuales, operamos con clases de números que comparten el mismo residuo módulo m. Estas clases se conocen como **clases de congruencia** y están formadas por todos los números enteros que son congruentes entre sí módulo m.

Para comprender mejor el concepto de congruencia y las clases de congruencia con el siguiente ejemplo:

Si calculamos mod 5 para todos los enteros. Se supone que se etiquetan 5 rebanadas (0,1,2,3,4) y para cada número entero, al dividirlo por 5, se le clasifica de acuerdo a su residuo.



Así 27 iría en la rebanada etiquetada con el número 2 porque 27 mod 5 = 2 y para expresar los números que pertenecen a la misma rebanada que el 27, es decir de la misma clase de congruencia, se usa la expresión anterior:

$$a \equiv b \pmod{m}$$

Ejemplo:

26 ≡ 11 (mod 5)
26 es congruente a 11 módulo 5
26 mod 5 = 1
11 mod 5 = 1

26 y 11 tienen el mismo residuo, tienen la misma clase de congruencia

Propiedades de congruencia:

1. Reflexiva: $a \equiv b \pmod{p}$, para todo $a \in \mathbb{Z}$.
2. Simétrica: $a \equiv b \pmod{p} \implies b \equiv a \pmod{p}$.
3. Transitiva: $a \equiv b \pmod{p}$ y $b \equiv c \pmod{p} \implies a \equiv c \pmod{p}$.

Teorema de congruencia lineal

Sean **a** y **b** dos números enteros y **m** un entero positivo, entonces la congruencia se describe:

$$ax \equiv b \pmod{m}$$

En la que una solución para **x** si y sólo si b es divisible por el máximo común divisor de **a** y **m**. Existirán exactamente soluciones **d = mcd(a,m)** en el conjunto de residuos si y sólo si **b/d**

Una vez se encuentra x_0, las demás soluciones se encuentran de acuerdo a la siguiente expresión:

$$\{x_0 + km/d\}$$

donde x_0 es una solución particular y **0 ≤ k < d**

Ejemplo:

Encontrar todas las soluciones

$9x \equiv 12 \pmod{15}$

1) Encontrar el máximo común divisor de **a** y **m**
mcd (9,15) = 3 ; por lo tanto la expresión tiene 3 soluciones, **d = 3**.

2) Desglosar a **a** y **m**:

15 = 9*1 + **6** -> 9*1 es 9, 9+6 = 15
9 = 6*1 + **3** -> 6*1 es 6, 6+3 = 9

Una vez encontrado el residuo 3, que es el mcd de **a** y **m**.

3) Despejar residuos:

6 = 15 - 9*1
3 = 9 - 6*1

4) Se toma el despeje que contenga al mcd de **a** y **m,** y sustituye con los factores obtenidos.

3= 9 - 6*1 -> se sustituye a 6 con el despeje anterior y se simplifica:

3= 9 - (15 - 9*1)*1
3= 9 - (15 + 9*1)
3= 9 - 15 * 9
3= 9*2 - 15

5) Multiplicar a la expresión por un número que nos de **b**, en este caso 12.

4(3 = 9*2 - 15)
12 = **9*8** - 15*4

de acuerdo a la expresión original:

$9x \equiv 12 \pmod{15}$
$x_0 = 8$

6) A partir de x0 se pueden encontrar las otras dos soluciones utilizando:

$\{x_0 + km/d\}$

$0 \leq k < d$

k= {0,1,2}
$x_0 = 8$

Para $x_1 = 8 + 0(15/3)$
$x_1 = 8$

Comprobación:
$9x \equiv 12 \pmod{15}$
$9(8) \equiv 12 \pmod{15}$
$72 \equiv 12 \pmod{15}$
Son congruentes ya que al dividir 72 y 12 entre m, que es 15, sus residuos son 12.

Para $x_2 = 8 + 1(15/3)$
$x_2 = 13$

Comprobación:
$9x \equiv 12 \pmod{15}$
$9(13) \equiv 12 \pmod{15}$

117 ≡ 12 (mod 15)
Son congruentes, ya que al dividir 117 y 12 entre m, que es 15, sus residuos son 12.

Para $x_3 = 8 + 3(15/3)$
$x_3 = 18$

Comprobación:
9x ≡ 12 (mod 15)
9(18) ≡ 12 (mod 15)
162 ≡ 12 (mod 15)
Son congruentes, ya que al dividir 162 y 12 entre m, que es 15, sus residuos son 12.

Por lo tanto el conjunto solución es $\mathbf{x_i = \{8,13,18\}}$ para que la expresión **9x ≡ 12 (mod 15)** sea congruente.

Operaciones básicas

Suma: Para sumar dos números en aritmética residual, simplemente sumamos los números y tomamos el residuo cuando dividimos por m.

Ejemplo:

Calcular 7 + 6 (mod 5):

- Suma los números: Comienza sumando los dos números que deseas operar. En este caso, sumamos 7 y 6 para obtener 13.
- Toma el residuo: Después de sumar los números, necesitas tomar el residuo cuando divides el resultado entre el módulo, que en este caso es 5. Entonces, divide 13 entre 5.
- Calcula el residuo: La división de 13 entre 5 te dará un cociente de 2 y un residuo de 3.
- Resultado final: **El resultado final de 7 + 6 (mod 5) es 3.**

$$7 + 6 \ (mod\ 5) =$$
$$13 \ (mod\ 5) =$$
$$13 \div 5 = 2 + 3$$

Con 3 como residuo.

Resta: Similar a la suma, para restar dos números en aritmética residual, restamos uno del otro y tomamos el residuo.

Ejemplo:

Calcular 8 − 2 (mod 5):

- Resta los números: Comienza restando el segundo número del primero. En este caso, restamos 2 de 8 para obtener 6.
- Verifica si es divisible por el módulo: Después de restar los números, verifica si el resultado es divisible por el módulo, que en este caso es 5.
- Comprueba la divisibilidad: Al restar 2 de 8, obtenemos 6, que es divisible entre 5.
- Resultado final: El resultado final de 8 - 3 (mod 5) es 1.

$$8 \ - \ 2 \ (mod \ 5) \ =$$
$$6 \ (mod \ 5) \ =$$
$$6 \ \div \ 5 \ = \ 1 \ + \ 1$$

Con 1 como residuo.

Multiplicación: Para multiplicar dos números en aritmética residual, multiplicamos los números y luego tomamos el residuo.

Ejemplo:

- Calcular 4×3(mod 5):
- Multiplica los números: Comienza multiplicando los dos números dados. En este caso, multiplica 4 por 3 para obtener 12.
- Verifica el residuo con el módulo: Después de obtener el resultado de la multiplicación, verifica el residuo cuando divides este número entre el módulo especificado, que es 5.
- Calcula el residuo: Al dividir 12 entre 5, obtenemos un cociente de 2 y un residuo de 2.
- Resultado final: Por lo tanto, el resultado final de 4 × 3 (mod 5) es 2.

$$4 \ * \ 3 \ (mod \ 5) \ =$$
$$12 \ (mod \ 5) \ =$$
$$12 \ \div \ 5 \ = \ 2 \ + \ 2$$

Con 2 como residuo.

Inverso modular

En aritmética modular no tenemos una operación de división. Sin embargo, sí tenemos inversos modulares.

El inverso modular de **a (mod m) es a^{-1}**

$$(a * a^{-1}) \equiv 1 \pmod{m}$$
o de otra forma
$$(a * a^{-1}) \bmod m = 1$$

Sólo los primos relativos de **m**, que no comparten factores primos con **m**, tienen inverso modular (mod m)

Procedimiento:

1) Calcula **a*b mod m** para los valores **b** entre 0 y m-1
2) El inverso modular de **a (mod m)** es el valor **b** que hace que se cumpla que **a*b (mod m) = 1**

Ejemplo:

Para a = 3, m = 7

1) Encontrar a b que esté entre 0 y m-1, en este caso b está entre 0 y 6

$$3 * 0 \equiv 0 \ (mod\ 7)$$
$$3 * 1 \equiv 3 \ (mod\ 7)$$
$$3 * 2 \equiv 6 \ (mod\ 7)$$
$$3 * 3 \equiv 9 \equiv 2 \ (mod\ 7)$$
$$3 * 4 \equiv 12 \equiv 5 \ (mod\ 7)$$
$$**3 * 5 \equiv 15 \equiv 1 \ (mod\ 7)**$$
$$3 * 6 \equiv 18 \equiv 4 \ (mod\ 7)$$

2) Una vez encontrado el número que cumple con la condición **a*b (mod m) = 1** se puede decir que encontramos el **inverso modular** en este caso 5, ya que: **5*3 (mod 7) = 1**

Es importante tener en cuenta que hay la posibilidad de que **no** exista el inverso modular, ya que a y m tienen que ser primos relativos.

Ejemplo:

Para a= 2 y m = 4

1) Encontrar a b que esté entre 0 y m-1, en este caso b está entre 0 y 3

$$2 * 0 \equiv 0\ (mod\ 4)$$
$$2 * 1 \equiv 2\ (mod\ 4)$$
$$2 * 2 \equiv 0\ (mod\ 4)$$
$$2 * 3 \equiv 6\ (mod\ 4)$$

2) En este caso no se encuentra el inverso modular, ya que 2 y 4 no son primos relativos, comparten el factor 2.

Teorema de los restos chinos

El teorema de los restos chinos es un resultado de la aritmética modular, que permite resolver sistemas de congruencias lineales.

El Teorema de los Restos Chinos, es llamado así, debido a que las versiones más antiguas sobre estos problemas de congruencias se encuentran en trabajos matemáticos chinos.

El problema más antiguo se encuentra en el texto Sun Zi Suan Ching (Manual de Matemática de Sun Zi) escrito aproximadamente en el siglo III por el matemático chino Sun Zi, y corresponde al problema 26.

El enunciado del problema de Sun Zi es el siguiente:

Tenemos un número de cosas, pero no sabemos exactamente la cantidad. Si las contamos de a tres, quedan dos sobrando. Si las contamos de a cinco, quedan tres sobrando. Si las contamos de a siete, quedan dos sobrando. ¿Cuántas cosas pueden ser?

A continuación se describe la solución dada por Sun Zi en su obra:

- Determinó que se podía resolver usando los números 70, 21 y 15, que eran múltiplos de 5*7, de 3*7 y de 3*5 respectivamente.
- Observó que la suma 2*70 + 3*21 + 2*15 igual a 233, es una solución del problema.
- Luego, restó a 233 múltiplos de 3*5*7 tantas veces como fuera posible, obteniendo el número 23, siendo este número el menor entero positivo que resuelve el problema.

Teorema

Sean k números naturales m_1, m_2, ..., m_k primos relativos dos a dos, y sean k números enteros r_1, r_2, ..., r_k. El sistema de congruencias:

$x \equiv r_1 \pmod{m_1}$
$x \equiv r_2 \pmod{m_2}$
…
$x \equiv r_k \pmod{m_k}$

Admite solución única módulo $M = m_1 m_2 ... m_k$. Es decir, existe un único número entero s entre 0 y M-1 que resuelve simultáneamente a todas las congruencias del sistema.

Demostración

Sea $M_i = M \div m_i$ para i = 1, 2, …, k.
a) Para cada i = 1, 2, …, k:

- M_i y m_i son primos relativos entre sí.
- Luego, existe u_i tal que $u_i M_i \equiv 1 \pmod{m_i}$
- Y se cumple: $u_1 M_1 r_1 + u_2 M_2 r_2 + ... + u_k M_k r_k \equiv r_i \pmod{m_i}$

b) Por lo tanto:$X = u_1 M_1 r_1 + u_2 M_2 r_2 + ... + u_k M_k r_k$ es una solución del sistema de congruencias.

Aplicaciones en computación

Criptografía

La criptografía es el estudio de los métodos para enviar mensajes secretos. Se trata de que un mensaje dominado como “texto simple” pase a un “texto cifrado”. El receptor del texto cifrado utiliza “descifrado” para convertir el texto cifrado a un texto simple.

Actualmente existen distintos algoritmos para la codificación de mensajes, como lo es el **cifrado César** que consiste en la sustitución de cada letra de un mensaje por otra letra que se encuentra un número fijo de posiciones más adelante en el alfabeto. El nombre de este método deriva del emperador romano Julio César, quien se dice lo utilizaba para comunicarse con sus generales.

El cifrado César consiste en desplazar cada letra del mensaje original un número fijo de posiciones en el alfabeto. Por ejemplo, si elegimos un desplazamiento de 3, la letra A se convierte en D, la letra B en E, y así sucesivamente. Este proceso se realiza para cada letra del mensaje, lo que resulta en un mensaje cifrado. El cifrado César es un ejemplo simple de criptografía de sustitución, donde cada letra del alfabeto se sustituye por otra letra.

Este algoritmo puede resultar no tan eficiente debido a que la decodificación es sencilla a comparación con la **RSA (Rivest-Shamir-Adleman)** que requiere de una metodología más compleja.

Algoritmo RSA

El sistema criptográfico RSA fue descubierto por Rivest, Shamir y Adleman en 1977 y es el primer algoritmo en utilizar una clave generada que se utiliza con más frecuencia para asegurar la transferencia de datos a través de redes inseguras, como Internet. La base del algoritmo RSA se basa en la aritmética modular.

Conceptos básicos:

Clave Pública y Privada: En RSA, cada usuario tiene una clave pública y una clave privada.
Clave Pública: Se utiliza para cifrar mensajes.
Clave Privada: Se utiliza para descifrar mensajes.

Pasos Algoritmo:

Generación de Claves:

- El usuario elige dos números primos grandes, p y q.
- Calcula $n = p*q$, que es el módulo.
- Calcula $\phi(n) = (p-1) * (q-1)$, que es la función ϕ de Euler de n
- Escoge un número e que sea coprimo con $\phi(n)$. Este será el exponente de cifrado y es su clave pública.
- Calcula d como el inverso multiplicativo de e módulo $\phi(n)$, es decir: $d \equiv e^{-1} \pmod{\phi(n)}$ Este será el exponente de descifrado y es su clave privada.

Cifrado:

Para cifrar un mensaje **M**, el usuario aplica la siguiente operación:

$$C \equiv M^e \pmod{n}$$

Donde **C** es el mensaje cifrado.

Descifrado:

Para descifrar el mensaje cifrado **C** , el usuario aplica la siguiente operación:

$$M \equiv C^d \pmod{n}$$

Donde **M** es el mensaje original.

Nota: En este algoritmo n debe tener al menos 340 dígitos

La aritmética modular se utiliza en el proceso de cifrado y descifrado para garantizar la seguridad de la comunicación. El módulo *n* es la base de las operaciones, y las claves pública y privada se utilizan para cifrar y descifrar los mensajes de forma segura.

Algoritmo Hash

Una Tabla Hash o un Mapa Hash es una estructura de datos que asocia llaves (keys) con valores (values) utilizando una Función Hash; asimismo permite almacenar y recuperar datos de manera eficiente.

Componentes:

- Tabla: Un arreglo donde se almacenen los datos.
- Claves (keys): Elementos únicos que se utilizan para identificar los valores asociados.
- Valores(values): Datos asociados a cada clave.
- Función Hash: Una función que toma una clave y devuelve un índice en el arreglo donde se almacenará el valor correspondiente.

Funcionamiento

Para el funcionamiento de este algoritmo es necesario contar con una Función Hash que distribuya las claves de forma uniforme a través del arreglo y minimice las colisiones, las cuales sólo ocurren cuando una clave diferente se asigna al mismo índice.

Una **Función Hash** transforma una clave en un índice en la tabla hash. Para que este índice sea válido dentro del tamaño de la tabla (que normalmente tiene una longitud m), se usa la aritmética de residuos, ya que la Función Hash a menudo incluye un paso que calcula el residuo de la división de la clave por el tamaño de la tabla.

Ejemplo:

Tenemos contactos que guardar en un arreglo de 10 índices.

Clave	marcos	lena
valor	7448992223	5512340

La Función Hash indica que se debe convertir cada letra a su valor ASCII para después sumar los valores y asignarlos a la Tabla Hash.

En el caso de marcos:

m	a	r	c	o	s
109	97	114	99	111	115

Posteriormente se suma: 109 + 97 +114 + 99 +111+ 115 = 645

Para asignarle un índice en la Tabla Hash se hace uso de la aritmética de residuos. Se toma al número de celdas disponibles como el módulo, en este caso 10.

$$645 \bmod 10 = 5$$

Por lo que el contacto de marcos será guardado en la posición 5 de la tabla Hash:

0	
1	
2	
3	
4	
5	7448992223
6	
7	5512340
8	
9	

Para el contacto de lena:

l	e	n	a
109	101	110	97

Se suman los números que componen el nombre: 109 +101+110+97 = 417

Se le asigna un índice en la Tabla Hash:

417 mod 10 = 7

Por lo tanto será guardado en la celda 7:

0	
1	
2	
3	
4	
5	7448992223
6	
7	5512340
8	
9	

Este procedimiento se repite en el caso de contar con más contactos para guardar en el arreglo. Cabe destacar que la Función Hash puede cambiar de acuerdo a las necesidades del algoritmo. Asimismo, existe la posibilidad de que dos claves pueden llegar a tener el mismo índice en la Tabla Hash, por lo cual hay estrategías específicas para el manejo de colisiones.

Hay varios métodos para manejar colisiones:

1) **Encadenamiento**: Cada índice de la tabla apunta a una lista enlazada de todos los elementos que se asignan a ese índice. Si ocurre una colisión, el nuevo elemento se añade a la lista enlazada correspondiente.

2) **Direccionamiento Abierto**: En lugar de utilizar listas enlazadas, este método encuentra otro índice en la tabla para almacenar el valor. Los métodos más comunes de direccionamiento abierto incluyen:

- Sondeo Lineal (Linear Probing): Se busca secuencialmente el siguiente índice disponible.
- Sondeo Cuadrático (Quadratic Probing): Se busca el siguiente índice usando un desplazamiento cuadrático.
- Hashing Doble (Double Hashing): Se aplica una segunda función hash para determinar el paso de búsqueda.

Las Tablas Hash son una útiles en el almacenamiento y la recuperación rápida de datos, siempre y cuando se utilice una Función Hash adecuada y se manejen correctamente las colisiones. Algunos de sus usos destacados están en la implementación de índices en bases de datos y almacenamiento de tablas de símbolos en compiladores.

Ejercicios Resueltos

Ejercicio 1. Para cada uno de los siguientes valores de n y d, encuentre los enteros q y r tales que n = dq + r y $0 \leq r < d$.

Ejercicio de: Epp, S. S. (2012). Matemáticas Discretas Con Aplicaciones (4ta ed.). Cengage Learning.

a) n = 54, d = 4 b) n = -54, d = 4 c) n =54, d = 70

Solución:
Para la solución de este ejercicio se necesita revisar cada uno de los incisos que se proponen como solución:

a) n = 54, d = 4 b) n = -54, d = 4 c) n =54, d = 70

a) Si se requiere encontrar los enteros que cumplan con la expresión: n = dq + r con $0 \leq r < d$, sustituiremos los valores que nos da el inciso **a: n = 54 y d =4**.

$$n = dq + r$$

$$54 = 4q + r$$

Para encontrar **d** y **r** es necesario descomponer al 54 en el producto de dos factores, uno de los cuales es el 4. Por lo tanto:

$$54 = 4q + r$$

se debe tener en cuenta que r va de 0 a 4

$$54 = 4*13 + 2$$

Por lo tanto, para el inciso a se tiene:

$$54 = 4*13 + 2, \text{ con } q= 13 \text{ y } r= 2$$

b) Si se requiere encontrar los enteros que cumplan con la expresión: n = dq + r con 0 ≤ r < d, sustituiremos los valores que nos da el inciso **b: n = -54 y d = 4**.

$$n = dq + r$$

$$-54 = 4q + r$$

En este caso se tiene que tomar en cuenta que r está en el rango de 0 a 4, pero al ser n negativa la dinámica cambia.

$$-54 = 4*(-14) + r$$

Para conservar el signo negativo se requiere multiplicar por un número que nos de una cifra mayor a n

$$-54 = -56 + r$$

$$-54 = -56 + 2$$

Por lo tanto, para el inciso b se tiene:

$$-54 = 4*(-14) + 2, \text{ con } q= -14 \text{ y } r= 2$$

c) Si se requiere encontrar los enteros que cumplan con la expresión: n = dq + r con 0 ≤ r < d, sustituiremos los valores que nos da el inciso **c: n = 54 y d = 70**.

$$n = dq + r$$
$$54 = 70q + r$$
$$54 = 70*(0) + r$$
$$54 = 0 + r$$
$$54 = 0 + 54$$

Por lo tanto, para el inciso c se tiene:

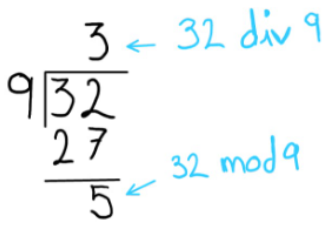
$$54 = 70*(0) + 54, \text{ con } q= 0 \text{ y } r= 54$$

Ejercicio 2. Cálculo de div y mod.

Ejercicio de: Epp, S. S. (2012). Matemáticas Discretas Con Aplicaciones (4ta ed.). Cengage Learning.

Calcule 32 ÷ 9 y 32 (mod 9) a mano y con calculadora para observar la diferencia entre estas operaciones.

Solución:
Cuando sea realice a mano la división se obtienen los siguientes resultados:



El enfoque de cada una de las operaciones es diferente, en el sentido en que con la división normal el resultado que nos interesa es el **cociente**, mientras que en el módulo se presta atención al **residuo**

Si utiliza una calculadora de cuatro funciones para dividir 32 entre 9, se obtiene una expresión como 3.555555556. Descartando la parte fraccionaria da 32 div 9 = 3 y así:

$$32 \bmod 9 =$$
$$32 - 9 * (32 \div 9) =$$
$$32 - 9* (3) =$$
$$32 - 27 = 5$$

Una calculadora con una función de parte entera integrada iPart permite introducir una sola expresión para cada cálculo:

$$32 / 9 = \text{iPart}(32/9)$$

$$\text{y } 32 \bmod 9 = 32 - 9 * \text{iPart}(32/9) = 5$$

Ejercicio 3. Determine 55*26 (mod 4)

Solución:

55*26 (mod 4)
1430÷4 = 357 + **2**
El módulo es = 2
Por lo tanto: 55*26 ≡ 2 (mod 4)

Ejercicio 4. Cálculo del día de la semana
Si se supone que hoy es martes y ni este año ni el próximo es un año bisiesto. ¿Qué día de la semana va a ser en año a partir de hoy?

Ejercicio de: Epp, S. S. (2012). Matemáticas Discretas Con Aplicaciones (4ta ed.). Cengage Learning.

Solución:
Hay 365 días en un año que no es un año bisiesto y cada semana tiene 7 días.
Ahora:

365/7 = 52 y
365 mod 7 = 1

Ya que 365 = 52 * 7 + 1. Así, 52 semanas, o 364 días, a partir de hoy será un martes y 365 días para que a partir de hoy será un día más tarde, es decir: **miércoles**.

En términos más generales, si DíaT es el día de la semana de hoy y DíaN hoy es el día de la semana en N días, entonces:

$$DíaN = (DíaT + N) \bmod 7$$

Ejercicio 5. Supongamos que *m* es un número entero. Si *m mod* 11 = 6, ¿qué es 4 *m mod* 11

Ejercicio de: Epp, S. S. (2012). Matemáticas Discretas Con Aplicaciones (4ta ed.). Cengage Learning.

Solución:
Debido a que *m mod* 11 = 6, se obtiene el residuo cuando *m* divido entre 11 es 6. Esto significa que hay algún entero *q*, tal que:

$$m = 11q + 6$$

¿Qué es 4 *m mod* 11

Así 4(m= 11q + 6) ->
4 m = 44q + 24 ->
44q + 22 + 2 = ->
11(4q + 2) + 2

Ya que 4q + 2 es un número entero en su totalidad (porque los productos y las sumas de los números enteros son números enteros) y ya que 2 < 11. El residuo que se obtiene cuando 4m se divide por 11 es 2. Por tanto:

4m mod 11 = 2

Ejercicio 6. Dada una cadena de caracteres, calcula su valor hash utilizando una función hash simple basada en la suma de los valores ASCII de sus caracteres.

Solución:
Suponiendo que la cadena es "hola" y el tamaño del array (arreglo) es 10.
Convertir cada carácter a su valor ASCII:

“h”	104
“o”	111
“l”	108
“a”	97

Sumar estos valores ASCII:

104 + 111 + 108 + 97 = 420

Aplicar la operación módulo para obtener el índice del array:

420 (mod 10) = 0

Por lo tanto, el índice hash para la cadena "hola" ocupará la celda 0.

0	hola
1	
2	
3	
4	
5	
6	
7	
8	
9	

Ejercicio 7. Determine el inverso modular para 3 mod 5.
Para obtener el inverso modular se debe recordar que para a (mod c) se debe encontrar una b que al multiplicarse por a de como resultado 1.

Solución:

$$a*b \pmod{c} = 1$$

Calcular a*b (mod c) para una b con valores entre 0 y c-1

a = 3, c= 5, c-1= 4

3*0 ≡ 0 (mod 5)
3*1 ≡ 3 (mod 5)
3*2 ≡ 1 (mod 5) -> Este es el inverso modular
3*3 ≡ 9 ≡ 4 (mod 5)
3*4 ≡ 12 ≡ 2 (mod 5)

Ejercicio 8. Encuentra un número entero x que cumpla las siguientes tres congruencias:

$$x \equiv 3 \pmod{5}$$
$$x \equiv 4 \pmod{7}$$
$$x \equiv 5 \pmod{11}$$

Solución:

1) Encuentra el producto de los módulos:

$$M = 5 * 7 * 11 = 385$$

2) Calcula las "tasas de división" para cada congruencia:

$$a1 = M / 5 = 385 / 5 = 77$$
$$a2 = M / 7 = 385 / 7 = 55$$
$$a3 = M / 11 = 385 / 11 = 35$$

3) Encuentra las soluciones particulares:

$$3 * 77 \equiv 231 \equiv 1 \pmod{5}$$
$$4 * 55 \equiv 220 \equiv 1 \pmod{7}$$
$$5 * 35 \equiv 175 \equiv 2 \pmod{11}$$

4) Suma las soluciones particulares ponderadas para obtener la solución general:

$x \equiv (1 * 77 * 3) + (1 * 55 * 4) + (2 * 35 * 5) \equiv 231 + 220 + 350 \equiv 801 \pmod{385}$

5) Simplifica la solución a módulo 385 para obtener el resultado en el rango adecuado:

$$x \equiv 801 \,\%\, 385 \equiv 31$$

La solución es $x \equiv 31 \pmod{385}$.

El número entero x que satisface todas las congruencias es 31.

Ejercicio 9. Cifrado RSA

Bob quiere enviar el mensaje HOLA a Alicia. ¿Cuál es el texto cifrado para su mensaje? Bob enviará sus mensaje en cuatro bloques, para la H, para la O, para la L y para la A. Puesto que H es la octava letra en el alfabeto, se codifica como 8, O es la quinceava letra del alfabeto, se codifica como 15 y así sucesivamente.

Solución:

H es la octava letra del alfabeto, por lo tanto:

$$C = 8^{3} \bmod 55$$
$$= 512 \bmod 55$$
$$= 17$$

Ya que O es la quinceava letra del alfabeto, se codifica como 15. El texto cifrado correspondiente es:

$$C = 15^{3} \bmod 55$$
$$= 3375 \bmod 55$$
$$= 20$$

L es la doceava letra del alfabeto, se codifica como 12. El texto cifrado correspondiente es:

$$C = 12^{3} \bmod 55$$

$$= 1728 \bmod 55$$
$$= 23$$

A es la primera letra del alfabeto, se codifica como 01 o 1. El texto cifrado correspondiente es:

$$C = 1^3 \bmod 55$$
$$= 1 \bmod 55$$
$$= 1$$

Por lo tanto, Bob envía a Alicia el mensaje:

17 20 23 01

Ejercicio 10. del problema de Sun-Tzu, o de los soldados de Han Xing:

“Hay cosas cuyo número se desconoce. Si las contamos de tres en tres nos sobran 2; si las contamos de cinco en cinco nos sobran tres; y si las contamos de siete en siete nos sobran ¿Cuántas cosas hay?”

$$x \equiv 2 \pmod 3$$
$$x \equiv 3 \pmod 5$$
$$x \equiv 2 \pmod 7$$

Solución:

1) Observar que 3,5 y 7 son primos relativos entre sí

2) Primera congruencia $x \equiv 2 \pmod 3 \rightarrow x = 2 + 3s$

3) Segunda Congruencia: $x \equiv 3 \pmod 5 \rightarrow 2 + 3s \equiv 3 \pmod 5 \rightarrow 3s \equiv 1 \pmod 5$

Multiplicando por 2: $s \equiv 2 \pmod 5 \rightarrow s = 2 + 5k$
Reemplazando en $x = 2 + 3s$ se obtiene:
$x = 2 + 3(2 + 5k)$
Luego: $x = 8 + 15k$

4) Tercera congruencia $x \equiv 2 \pmod 7 \rightarrow 8 + 15k \equiv 2 \pmod 7 \rightarrow 15k \equiv -6 \pmod 7$

Como $15 \equiv 1 \pmod 7$ y $-6 \equiv 1 \pmod 7$ se obtiene:
$k \equiv 1 \pmod 7$
Luego: $k = 1 + 7t$

5) Sustituyendo en $x = 8 + 15k$, se obtiene: $x = 8 + 15(1 + 7t)$

Luego, la solución general del sistema es: x = 23 + 105k
Por lo tanto, el ejército de Han Xing
puede tener como mínimo 23 soldados.

Cuestionario

1. ¿Cuál de los siguientes no es un tipo de representación de la información mencionado?
a) Símbolos
b) Gráfos
c) Algoritmos
d) Diseño
Respuesta correcta: c) Algoritmos

2. ¿Qué tipo de elementos de información operan principalmente las computadoras?
a) Gráficos y datos
b) Instrucciones y gráficos
c) Instrucciones y datos
d) Datos y símbolos
Respuesta correcta: c) Instrucciones y datos

3. ¿Quién introdujo la aritmética modular?
a) Fibonacci
b) Jackson
c) Gauss
d) Arquímedes
Respuesta correcta: c) Gauss

4. ¿Cómo se llama la obra en la que Gauss introdujo una demostración de la aritmética modular?
a) Disquisitiones Arithmeticae
b) Acta Sanctorum in Sello
c) Philosophia Naturalis Principia Mathematica
d) Popol Vuh
Respuesta correcta: a) Disquisitiones Arithmeticae

5. ¿En qué año se publicó Disquisitiones Arithmeticae?
a) 1923
b) 1801
c) 1746
d) 1798

Respuesta correcta: b) 1801

6. ¿Con qué número se obtiene un residuo de 0 al dividir entre 17?
a) 69
b) 84
c) 1001
d) 357
Respuesta correcta: d) 357

7. ¿Cuál es el propósito del estudio de los sistemas de representación de información?
a) Mejorar la estética de los datos
b) Aumentar la velocidad de procesamiento
c) Comprender los procesos de tratamiento de datos
d) Reducir el tamaño de los archivos
Respuesta correcta: c) Comprender los procesos de tratamiento de datos

8. ¿Qué elemento es fundamental para la codificación de cantidades en la arquitectura de la máquina?
a) Representaciones gráficas
b) Representaciones numéricas
c) Representaciones de texto
d) Representaciones de audio
Respuesta correcta: b) Representaciones numéricas

9. ¿Qué tipo de sistemas numéricos se han explorado como alternativas a los sistemas posicionales?
a) Sistemas gráficos
b) Aritmética modular
c) Representaciones textuales
d) Sistemas binarios
Respuesta correcta: b) Aritmética modular

10. ¿Qué tipo de cifrado es RSA?
a) Cifrado simétrico
b) Cifrado asimétrico
c) Cifrado básico
d) Cifrado de flujo
Respuesta correcta: b) Cifrado asimétrico

11. ¿Sobre qué tema se está hablando en el tutorial?
a) La división
b) La aritmética residual
c) La variable compleja
d) La aritmética de los números naturales

Respuesta correcta: b) La aritmética residual

12. ¿Cuántos sistemas numéricos existen?
a) 1
b) 3
c) 2
d) 5
Respuesta correcta: b) 3

13. ¿Cuáles son los tipos de sistemas numéricos?
a) Posicional, semi-posicional y no posicionales
b) Dirigidos y no dirigidos
c) Negativos y positivos
d) Naturales, primos y compuestos
Respuesta correcta: a) Posicional, semi-posicional y no posicionales

14. ¿Para qué sirve la operación mod?
a) Para obtener un módulo de un vector
b) Para obtener el residuo de una división
c) Para obtener el valor de una constante de integración
d) Para obtener los valores de x
Respuesta correcta: b) Para obtener el residuo de una división

15. Con base en la información del tutorial, ¿cuál es el método más seguro de criptografía?
a) César
b) RSA
c) DSA
d) El Gamal
Respuesta correcta: b) RSA

16. En el mundo de la criptografía pasamos de texto simple a...
a) Texto compuesto
b) Texto descifrado
c) Texto cifrado
d) Texto normal
Respuesta correcta: c) Texto cifrado

17. ¿Cuál de las siguientes características de los sistemas numéricos posicionales los hacen complejos?
a) Mejoran significativamente la velocidad de procesamiento
b) Generan acarreos durante algunas operaciones
c) Son tolerantes a fallos
d) No añaden complejidad al hardware
Respuesta correcta: b) Generan acarreos durante algunas operaciones

18. ¿Qué se busca evitar con la exploración de sistemas numéricos no posicionales?
a) La generación de símbolos
b) La creación de gráficos
c) La generación de acarreos
d) La administración de datos
Respuesta correcta: c) La generación de acarreos

19. ¿Por qué el cifrado César NO se usa tanto?
a) Porque es muy difícil
b) Porque no hace nada
c) Porque era muy fácil descifrar un mensaje
d) Porque es muy fácil cifrar un mensaje
Respuesta correcta: c) Porque era muy fácil descifrar un mensaje

20. ¿Qué se ha revelado sobre los sistemas numéricos posicionales en investigaciones recientes?
a) Mejoran significativamente la productividad
b) No aumentan significativamente la velocidad de procesamiento
c) Simplifican la estructura del hardware
d) Aumentan la tolerancia a fallos
Respuesta correcta: b) No aumentan significativamente la velocidad de procesamiento

21. ¿Qué conocimiento se necesita para el cifrado RSA?
a) Modular
b) Bibliográfico
c) Imaginario
d) Superior
Respuesta correcta: a) Modular

22. ¿De dónde provienen las siglas RSA?
a) Son las siglas de una agencia
b) Son las siglas de los programas
c) Son las reglas del nombre de la presa
d) Son las siglas de los autores
Respuesta correcta: d) Son las siglas de los autores

23. ¿Cuándo se desarrolló el cifrado RSA?
a) 1994
b) 1984
c) 1960
d) 1977
Respuesta correcta: d) 1977

24. ¿Qué operaciones aritméticas no tienen acarreo en el sistema numérico residual?
a) Suma
b) Resta
c) Multiplicación
d) Todas las anteriores
Respuesta correcta: d) Todas las anteriores

25. ¿Cómo es la representación de la operación mod?
a) a mod b
b) a modulo b
c) a / b
d) a*b
Respuesta correcta: a) a mod b

26. ¿En qué libro se encuentra el indicio más antiguo del teorema chino?
a) Sin-Tzuk
b) Sun-tu
c) Sun-Tzu
d) Sugon-Tzu
Respuesta correcta: c) Sun-Tzu

27. ¿Actualmente para qué se usa la criptografía?
a) Enviar mensajes de texto
b) Enviar información privada a través de canales electrónicos
c) Rastrear mediante GPS
d) Solicitar información
Respuesta correcta: b) Enviar información privada a través de canales electrónicos

28. ¿Cómo se escribiría en formato modular, módulo de 63 entre la base 5 con residuo 3?
a) 3=63 mod 5
b) 63=3 mod 5
c) 63=5 mod 3
d) 5=63 mod 3
Respuesta correcta: a) 3=63 mod 5

29. ¿Quién expuso el problema en el que se basa el teorema chino de los restos en el siglo III d.C.?
a) Sun-Tzu
b) Fibonacci
c) Euclides
d) Pitágoras
Respuesta correcta: a) Sun-Tzu

30. ¿Cuál es el problema planteado por Sun-Tzu en el siglo III d.C. en relación con el teorema chino de los restos?
a) Contar de tres en tres
b) Contar de cinco en cinco
c) Contar de siete en siete
d) Todas las anteriores
Respuesta correcta: d) Todas las anteriores

31. ¿En qué consiste el teorema chino de los restos?
a) Resolver ecuaciones cuadráticas
b) Resolver congruencias lineales simultáneamente
c) Encontrar la raíz cuadrada de un número
d) Resolver ecuaciones exponenciales
Respuesta correcta: b) Resolver congruencias lineales simultáneamente

32. ¿Qué propiedad es fundamental en el teorema chino de los restos para que se puedan resolver simultáneamente las congruencias lineales?
a) Propiedad conmutativa
b) Propiedad de linealidad
c) Propiedad asociativa
d) Propiedad distributiva
Respuesta correcta: b) Propiedad de linealidad

33. ¿Qué concepto fundamental se utiliza en la aritmética residual?
a) Resolver ecuaciones de segundo grado
b) Suma
c) Congruencia
d) Inverso
Respuesta correcta: c) Congruencia

34. ¿Qué indica $a \equiv b \pmod{m}$?
a) a y b tienen el mismo valor
b) a es mayor que b
c) a y b tienen el mismo residuo cuando se dividen por m
d) a es menor que b
Respuesta correcta: c) a y b tienen el mismo residuo cuando se dividen por

m

35. ¿Qué resultado obtenemos si calculamos 27 mod 5?
a) 1
b) 2
c) 3
d) 4

Respuesta correcta: b) 2

36. ¿En qué consiste la contribución principal del teorema chino de los restos en la matemática?
a) Resolver problemas de geometría
b) Facilitar la manipulación de números grandes
c) Descubrir nuevos números primos
d) Demostrar teoremas sobre funciones trigonométricas
Respuesta correcta: b) Facilitar la manipulación de números grandes

37. ¿Qué números se necesitan para ejecutar la operación mod?
a) Que sean enteros
b) Que sean irracionales
c) Que sean imaginarios
d) Que sean negativos
Respuesta correcta: a) Que sean enteros

38. ¿En qué consiste el cifrado César en la criptografía?
a) Uso de claves asimétricas
b) Sustitución de letras por desplazamiento
c) Cifrado de bloque
d) Encriptación cuántica
Respuesta correcta: b) Sustitución de letras por desplazamiento

39. ¿Cuál es un ejemplo de información que se protege mediante criptografía?
a) Receta de cocina
b) Datos personales
c) Horario de trenes
d) La Matrix
Respuesta correcta: b) Datos personales

40. ¿Qué representan las clases de congruencia en la aritmética modular?
a) Números con el mismo residuo cuando se dividen por m
b) Números que son múltiplos de m
c) Números que son primos entre sí
d) Números que suman cero
Respuesta correcta: a) Números con el mismo residuo cuando se dividen por m

41. ¿Cómo se encuentra el valor de las demás soluciones una vez encontrado x0?
a) {x0 + km}
b) {x0 - km}
c) {x0 + km/d}
d) {x0 - km/d}
Respuesta correcta: c) {x0 + km/d}

42. ¿Qué hace difícil el sistema numérico residual?
a) Sumar números
b) Comparar números
c) Representar números negativos
d) Usar números fraccionarios
Respuesta correcta: b) Comparar números

43. ¿Cómo se define el residuo en aritmética residual?
a) Como el sobrante de dividir dos números
b) Como la diferencia de dos números
c) Como el producto de dos números
d) Como la suma de dos números
Respuesta correcta: a) Como el sobrante de dividir dos números

44. ¿Cuál es una característica del cifrado RSA?
a) Usa una sola clave para cifrar y descifrar
b) Usa una clave pública y otra privada
c) Basado en el cifrado César
d) No utiliza la aritmética modular
Respuesta correcta: b) Usa una clave pública y otra privada

45. ¿Qué no es un ejemplo de aplicación de criptografía?
a) Protección de datos personales
b) Enviar mensajes secretos
c) Enviar cosas no cifradas
d) Seguridad en transacciones bancarias
Respuesta correcta: c) Enviar cosas no cifradas

46. ¿Por qué no existe el inverso modular de 2 (mod 4)?
a) Porque 2 es mayor que 4
b) Porque 2 es menor que 4
c) Porque 2 y 4 no son primos relativos
d) Porque 2 y 4 son múltiplos
Respuesta correcta: c) Porque 2 y 4 no son primos relativos

47. ¿Cómo se denota la congruencia entre dos números enteros en la aritmética modular?
a) $a \equiv b \bmod m$
b) $a \cong b \bmod m$
c) $a \equiv b \pmod m$
d) $a \cong b \pmod m$
Respuesta correcta: c) $a \equiv b \pmod m$

48. ¿Qué teorema es crucial en la aritmética modular?
a) Teorema de Pitágoras

b) Teorema chino de los restos
c) Teorema de Fermat
d) Teorema de Euler
Respuesta correcta: b) Teorema chino de los restos

49. ¿Cómo se denota la congruencia entre dos números enteros en la aritmética modular?
a) a ≡ b modm
b) a ≅ b modm
c) a ≡ b (modm)
d) a ≅ b (modm)
Respuesta correcta: c) a ≡ b (modm)

50. ¿Cuál es una característica de los sistemas numéricos posicionales?
a) No usan el número 0
b) Usan una base fija
c) El valor de un símbolo depende de su posición
d) Representan cantidades negativas únicamente
Respuesta correcta: c) El valor de un símbolo depende de su posición

51. ¿Con qué otro nombre se le conoce a la Aritmética de Residuos?
a) Aritmética de sobras
b) Aritmética Modular o de Congruencia
c) Aritmética Algebraica
d) Aritmética Proposicional
Respuesta correcta: b) Aritmética Modular o de Congruencia

52. ¿Cómo se denota la congruencia entre dos números enteros en la aritmética modular?
a) a ≡ b modm
b) a ≅ b modm
c) a ≡ b (modm)
d) a ≅ b (modm)
Respuesta correcta: c) a ≡ b (modm)

53. ¿Qué números encontró Sun Zi que son múltiplos de 57, de 37 y de 3*5 respectivamente para resolver el problema?
a) 50, 21, 15
b) 70, 21, 15
c) 70, 27, 35
d) 35, 42, 15
Respuesta correcta: b) 70, 21, 15

Bibliografía

- Coronado, J. (2014). Sistemas numéricos residuales: fundamentos lógicos-matemáticos. Universidad de La Salle.
- Epp, S. S. (2012). Matemáticas Discretas Con Aplicaciones (4ta ed.). Cengage Learning.
- Espinosa Ramón. (2016). Matemáticas Discretas (2nda ed.). Alfaomega.
- García, C. (2002). Matemática discreta: Problemas y ejercicios resueltos. Prentice Hall.
- García Ríos, A. (1991). Procesamiento digital de señales de altas prestaciones utilizando el Sistema Numérico de Residuos [Tesis doctoral, Universidad de Granada]. Recuperado de enlace
- Gayoso, C. A. (2009). Generadores de números pseudoaleatorios en aritmética de residuos: teoría e implementación en FPGAs [Tesis doctoral, Universidad Nacional de Mar del Plata]. Recuperado de enlace
- Gayoso, C. A. Reducción del Número de Transistores en Operaciones Aritméticas en el Sistema Numérico de Residuos. Universidad Nacional de Mar del Plata. Recuperado de enlace
- Hubner Janampa Patilla. (2020). La aritmética modular como mecanismo de seguridad y vulnerabilidad en el sistema criptográfico RSA. Revista Cubana de Ciencias Informáticas. Recuperado de enlace
- Tremblay J. (2000). Matemáticas Discretas con Aplicación a las Ciencias de la Computación (1era ed.). Compañía Editorial Continental. Universidad de Saskatchewan, Saskatoon.
- Moreia Gómez Bello. (sin fecha). La aritmética modular y algunas de sus aplicaciones. Universidad Nacional de Colombia. Recuperado de enlace
- Taylor Fred (1984). Residue Arithmetic: A Tutorial with

Examples in Computer, vol. 17, no. 5, pp. 50-62, May 1984, doi: 10.1109/MC.1984.1659138.