MATEMÁTICA DISCRETA
Teoría de Números

Prof. Sergio Salinas

Facultad de Ingeniería
Universidad Nacional de Cuyo

Agosto 2024

Contenido

Aritmética Modular

CONCEPTOS BÁSICOS DE ARITMÉTICA MODULAR

Aritmética Modular

- La aritmética modular es una rama de la matemática que se centra en el estudio de los números bajo un sistema de residuos, se enfoca en los restos que resultan al dividir números enteros.
- Suponer un reloj de 12 horas, si son las 10 en punto y pasan 5 horas, el reloj no marcará las 15, sino la 3.
- Esto se debe a que después de llegar a las 12, el reloj "regresa" al 1.
- La aritmética modular funciona de manera similar: en lugar de seguir sumando sin fin, el sistema "se reinicia" cuando se alcanza un cierto número, llamado módulo.
- El módulo es el número en el que se reinicia el conteo. Por ejemplo, en el reloj de 12 horas, el módulo es 12.

Aritmética Modular

Áreas de aplicación:

- Criptosistemas de clave pública (ej. RSA).
- Criptografía de curvas elípticas.
- Algoritmos de hashing.
- Generación de números pseudoaleatorios.
- Códigos de Corrección de Errores.
- Consistencia de datos en sistemas distribuidos.
- Algoritmos de enrutamiento en redes.
- Teoría de juegos.
- Control de movimiento en sistemas robóticos.

OPERADOR MÓDULO n

Operador módulo n

El término módulo n, se denota como $a \mod n$, es una operación que calcula el residuo r cuando un número entero a es dividido por otro **entero positivo** n, de forma que se cumple que $a = qn + r$. Donde q es el cociente de la división de a entre n y $0 \leq r < n$

Ejemplos:

- $a = 17, n = 5$ entonces $17 \mod 5 = 2$ ya que $17 = 3 \cdot 5 + 2$, donde $0 \leq 2 < 5$.
- $a = 5, n = 17$ entonces $5 \mod 17 = 5$ ya que $5 = 0 \cdot 17 + 5$, donde $0 \leq 5 < 17$.
- $a = -8, n = 4$ entonces $-8 \mod 4 = 0$ ya que $-8 = -2 \cdot 4 + 0$, donde $0 \leq 0 < 4$.
- $a = -8, n = 5$ entonces $-8 \mod 5 = 2$ ya que $-8 = -2 \cdot 5 + 2$, donde $0 \leq 2 < 5$.
- $a = 5, n = 12$ entonces $5 \mod 12 = 5$ ya que $5 = 0 \cdot 12 + 5$, donde $0 \leq 5 < 12$.
- $a = -5, n = 12$ entonces $-5 \mod 12 = 5$ ya que $-5 = -1 \cdot 12 + 7$, donde $0 \leq 7 < 12$.

Operador módulo n

Observar lo que pasa cuando incrementamos números de uno en uno y luego los dividimos entre 3.

a	b	q	r	$a = bq + r$
0	3	0	0	$0 = 3 \cdot 0 + 0$
1	3	0	1	$1 = 3 \cdot 0 + 1$
2	3	0	2	$2 = 3 \cdot 0 + 2$
3	3	1	0	$3 = 3 \cdot 1 + 0$
4	3	1	1	$4 = 3 \cdot 1 + 1$
5	3	1	2	$5 = 3 \cdot 1 + 2$
6	3	2	0	$6 = 3 \cdot 2 + 0$
7	3	2	1	$7 = 3 \cdot 2 + 1$
8	3	2	2	$8 = 3 \cdot 2 + 2$

Podemos visualizar el operador módulo al usar círculos (ej. reloj). Escribimos 0 en la parte superior de un círculo y continuamos en sentido de las manecillas del reloj escribiendo enteros $1, 2, \cdots$ hasta uno menos que el módulo.

Aritmética con el operador módulo n

1. **Suma modular:** la suma de dos números a y b módulo n se define como $(a + b)$ mód n.

2. **Resta modular:** la resta de dos números a y b módulo n se define como $(a - b)$ mód n.

3. **Multiplicación modular:** la multiplicación de dos números a y b módulo n se define como $(a \cdot b)$ mód n.

4. **Exponenciación modular:** dados un número a, un exponente b, y un módulo n, la exponenciación modular se define como: (a^b) mód n.

5. **Inverso modular:** el inverso modular de a bajo el módulo n es un número x tal que: $(a \cdot x)$ mód $n = 1$. Esto significa resolver $ax = qn + 1$ equivalente a $ax - qn = 1$.

6. **División modular:** dados los números a,b y un módulo n, la división modular se define como $\frac{a}{b}$ mód n equivalente a $a \cdot b^{-1}$ mód n, donde b^{-1} es el inverso de b.

Aritmética con el operador módulo n

Ejemplos de operaciones básicas:

- $(7 + 5) \mod 4 = 0$
- $(7 - 5) \mod 4 = 2$
- $(7 \cdot 5) \mod 4 = 3$

Aritmética con el operador módulo n

Ejemplo del cálculo del inverso modular: $\frac{4}{3} \mod 11 = 1$.

- Calcular el inverso de 3 esto es $3 \cdot x \mod 11 = 1$
- Calcular el $d = mcd(3, 11) = 1$ por lo tanto el inverso existe.
- Aplicar el algoritmo de euclides:
  - $11 = 3 \cdot 3 + 2$
  - $3 = 1 \cdot 2 + 1$
  - $1 = 3 - 1 \cdot 2 = 3 - 1 \cdot [11 - 3 \cdot 3] = 3 - 1 \cdot 11 + 3 \cdot 3$
  - $1 = 11 \cdot (-1) + 3 \cdot (4)$
- El inverso de 3 es 4 expresado como $3^{-1} = 4$.
- Verificar el resultado: $3 \cdot 4 \mod 11 = 1$ ya que $12 = 1 \cdot 11 + 1$.
- Calcular $4 \cdot 3^{-1} \mod 11 = 4 \cdot 4 \mod 11 = 16 \mod 11 = 5$

CONCEPTOS BÁSICOS DE CONGRUENCIAS

Congruencia módulo n

Dos números enteros a y b son congruentes módulo n donde n **es un entero positivo**, si a y b tienen el mismo resto cuando se dividen por n. Esto se denota como:

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

y se define formalmente como:

$$a \equiv b \pmod{n} \text{ si y solo si } n|(a-b).$$

En otras palabras, $a - b$ es múltiplo de n, es decir, existe **un entero** k tal que:

$$a - b = kn.$$

También, se cumple que

$$a \mod n = b \mod n.$$

Congruencia Módulo n

Recordatorio

$$a \equiv b \pmod{n} \text{ si y solo si } n|(a-b)$$

$$a - b = kn \text{ donde } k \in \mathbb{Z}$$

Ejemplos

- $15 \equiv 1 \pmod{7}$ ya que $7|(15-1)$, es decir $15 - 1 = k \cdot 7$ donde $k = 2$.
- $29 \equiv 5 \pmod{12}$ ya que $12|(29-5)$, es decir $29 - 5 = k \cdot 12$ donde $k = 2$.
- $-8 \equiv 2 \pmod{5}$ ya que $5|(-8-2)$, es decir $-8 - 2 = k \cdot 5$ donde $k = -2$.
- $-14 \equiv -8 \pmod{6}$ ya que $6| -14 - (-8)$, es decir $-14 + 8 = k \cdot 6$ donde $k = -1$.
- $7 \equiv 19 \pmod{12}$ ya que $12|7 - 19$, es decir $7 - 19 = k \cdot 12$ donde $k = -1$.

Aritmética con congruencias

1. Sean las congruencias $a \equiv b \pmod{n}$ y $c \equiv d \pmod{n}$ entonces se define la **suma** de ambas congruencias como $(a + c) \equiv (b + d) \pmod{n}$.

2. Sean las congruencias $a \equiv b \pmod{n}$ y $c \equiv d \pmod{n}$ entonces se define la **diferencia** de ambas congruencias como $(a - c) \equiv (b - d) \pmod{n}$.

3. Sean las congruencias $a \equiv b \pmod{n}$ y $c \equiv d \pmod{n}$ entonces se define el **producto** de ambas congruencias como $(a \cdot c) \equiv (b \cdot d) \pmod{n}$.

4. Es posible definir la **división** $\frac{a}{c} \equiv \frac{b}{d} \pmod{n}$ como $a \cdot c^{-1} \equiv b \cdot d^{-1} \pmod{n}$ siempre que existan los inversos c^{-1} y d^{-1}.

Inverso modular

El **inverso modular** de un número entero a con respecto a un módulo n es otro número entero b tal que el producto de a y b es congruente a 1 módulo n. En otras palabras, b es el inverso modular de a si:

$$a \cdot b \equiv 1 \pmod{n}$$

Condición para la existencia del inverso modular

Un número a tiene un inverso modular módulo n si y solo si a y n son coprimos, es decir, $mcd(a, n) = 1$.

Ejemplo del cálculo del inverso modular 3 módulo 11:

1. Calcular el $mcd(3, 11)$ mediante el algoritmo de Euclides.
   - $11 = 3 \cdot 3 + 2$
   - $3 = 1 \cdot 2 + 1$
   - $2 = 2 \cdot 1 + 0$
2. Calcular la combinación lineal tal que $mcd(a, b) = au + bv$.
   - $1 = 1 \cdot 3 - 1 \cdot 2 = 1 \cdot 3 - 1[11 - 3 \cdot 3]$
   - $= 1 \cdot 3 - 1 \cdot 11 + 3 \cdot 3 = 4 \cdot 3 - 1 \cdot 11$
3. El inverso modular de 3 módulo 11 es "4".
4. Verificación: $a \cdot b \equiv 1 \pmod{n}$ donde $(3 \cdot 4) \equiv 1 \pmod{11}$, entonces $11|(12 - 1)$.

CONGRUENCIAS COMO RELACIÓN DE EQUIVALENCIA

Congruencias como una relación de equivalencia

Dos enteros a y b relacionados bajo la congruencia módulo n, se expresa la relación como $a \equiv_n b$ si y solo si $n \mid (a - b)$.

Propiedades de las Congruencias:

1. **Reflexiva:** para cualquier entero a y módulo n entonces $a \equiv_n a$.

2. **Simétrica:** para cualesquiera enteros a, b y módulo n entonces si $a \equiv_n b$ entonces $b \equiv_n a$.

3. **Transitiva:** si $a \equiv_n b$ y $b \equiv_n c$ entonces $a \equiv_n c$

Como la relación de congruencia modulo n cumple con las propiedades reflexiva, simétrica y transitiva, es posible concluir que la congruencia es una **relación de equivalencia**.

Clase de Congruencia

Para un número entero a y un entero positivo n, la clase de congruencia de a módulo n, denotada por $[a]_n$, es el conjunto de todos los enteros que son congruentes a módulo n. Formalmente, se define como:

$$[a]_n = \{b \in \mathbb{Z} | b \equiv a \pmod{n}\}$$

Esto significa que $[a]_n$ es el conjunto de todos los enteros b tales que la diferencia $b - a$ es divisible por n. En otras palabras, b y a tienen el mismo residuo cuando se dividen por n. Recordar que $b - a = kn$ entonces $b = kn + a$.

Clase de Congruencia

Ejemplos:

- Para $a = 0$ y $n = 3$ tenemos $[0]_3 = \{\ldots, -9, -6, -3, 0, 3, 6, \ldots\}$
  - $b = kn + a = -2 \cdot 3 + 0 = -6$
  - $b = kn + a = -1 \cdot 3 + 0 = -3$
  - $b = kn + a = 0 \cdot 3 + 0 = 0$
  - $b = kn + a = 1 \cdot 3 + 0 = 3$
- Para $a = 1$ y $n = 3$ tenemos $[1]_3 = \{\ldots, -8, -5, -2, 1, 4, 7, \ldots\}$
  - $b = kn + a = -2 \cdot 3 + 1 = -5$
  - $b = kn + a = -1 \cdot 3 + 1 = -2$
  - $b = kn + a = 0 \cdot 3 + 1 = 1$
  - $b = kn + a = 1 \cdot 3 + 1 = 4$
- Para $a = 2$ y $n = 3$ tenemos $[2]_3 = \{\ldots, -7, -4, -1, 2, 5, 8, \ldots\}$
  - $b = kn + a = -2 \cdot 3 + 2 = -4$
  - $b = kn + a = -1 \cdot 3 + 2 = -1$
  - $b = kn + a = 0 \cdot 3 + 2 = 2$
  - $b = kn + a = 1 \cdot 3 + 2 = 5$

Clase de Congruencia

Ejemplos:

- Para $a = 3$ y $n = 3$ tenemos $[3]_3 = \{\dots, -6, -3, 0, 3, 6, \dots\}$
  - $b = kn + a = -3 \cdot 3 + 3 = -6$
  - $b = kn + a = -2 \cdot 3 + 3 = -3$
  - $b = kn + a = -1 \cdot 3 + 3 = 0$
  - $b = kn + a = 0 \cdot 3 + 3 = 3$
- Para $a = 4$ y $n = 3$ tenemos $[4]_3 = \{\dots, -5, -2, 1, 4, 7, \dots\}$
  - $b = kn + a = -3 \cdot 3 + 4 = -5$
  - $b = kn + a = -2 \cdot 3 + 4 = -2$
  - $b = kn + a = -1 \cdot 3 + 4 = 1$
  - $b = kn + a = 0 \cdot 3 + 4 = 4$
- Para $a = 5$ y $n = 3$ tenemos $[5]_3 = \{\dots, -4, -1, 2, 5, 8, \dots\}$
  - $b = kn + a = -3 \cdot 3 + 5 = -4$
  - $b = kn + a = -2 \cdot 3 + 5 = -1$
  - $b = kn + a = -1 \cdot 3 + 5 = 2$
  - $b = kn + a = 0 \cdot 3 + 5 = 5$

Clases de equivalencia

Ejemplo para $n = 5$

$$
\begin{aligned}
[0]_5 &= \{b \in \mathbb{Z} \mid b \equiv 0 \pmod{n}\} \\
&= \{b \in \mathbb{Z} \text{ es un múltiplo de 5 o } b = 5k \text{ para algún entero } k\} \\
&= \{\cdots, -10, -5, 0, 5, 10, \cdots\} \\
[1]_5 &= \{b \in \mathbb{Z} \mid b \equiv 1 \pmod{n}\} \\
&= \{\cdots, -9, -4, 1, 6, 11, \cdots\} \\
[2]_5 &= \{b \in \mathbb{Z} \mid b \equiv 2 \pmod{n}\} \\
&= \{\cdots, -8, -3, 2, 7, 12, \cdots\} \\
[3]_5 &= \{\cdots, -7, -2, 3, 8, 13, \cdots\} \\
[4]_5 &= \{\cdots, -6, -1, 4, 9, 14, \cdots\} \\
[5]_5 &= \{\cdots, -5, 0, 5, 10, 15, \cdots\} = [0]_5
\end{aligned}
$$

Conjunto de residuos módulo n

Para un entero positivo n, el conjunto de residuos módulo n, se escribe como $\mathbb{Z}/n\mathbb{Z}$ o $\mathbb{Z}_n$, es el conjunto de todos los residuos posibles cuando un entero se divide por n. Matemáticamente, este conjunto es: $\mathbb{Z}/n\mathbb{Z} = \{[a]_n a \in \mathbb{Z}\}$

Ejemplos:

- $\mathbb{Z}/3\mathbb{Z} = \{[0]_3, [1]_3, [2]_3\}$
- $\mathbb{Z}/4\mathbb{Z} = \{[0]_4, [1]_4, [2]_4, [3]_4\}$
- $\mathbb{Z}/5\mathbb{Z} = \{[0]_5, [1]_5, [2]_5, [3]_5, [4]_5\}$

ECUACIONES DE CONGRUENCIAS

Ecuaciones de Congruencia

1. Ecuaciones de Congruencia Lineal: $ax \equiv b \pmod{m}$
2. Ecuaciones de Congruencia Cuadrática: $ax^2 + bx + c \equiv 0 \pmod{m}$
3. Congruencias Cúbicas y de Grados Superiores: $ax^k + bx^{k-1} + \cdots + z \equiv 0 \pmod{m}$
4. Ecuaciones de Congruencia Simultáneas:

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \vdots \\ x \equiv a_k \pmod{m_k} \end{cases}$$

5. Congruencias No Lineales y con Parámetros: $f(x) \equiv 0 \pmod{m}$
6. Ecuaciones de Congruencia con Parámetros: $ax + by \equiv c \pmod{m}$

Ecuaciones de Congruencia Lineal

Definición

Una congruencia lineal es una congruencia del tipo $ax \equiv b (\text{mód}\, m)$ *donde* a, b, m *son enteros y* $m > 0$.

Nota: *si la congruencia lineal* $ax \equiv b (\text{mód}\, m)$ *tiene una solución* x_0, *entonces existen infinitas soluciones* $x_0 + km$ *para cualquier entero* k.

Solución de una Congruencia Lineal

- En una congruencia lineal del tipo $ax \equiv b \pmod{m}$ se cumple que $m \mid ax - b$, esto es $ax - b = mk$.
- Ordenando los términos de la expresión anterior obtenemos la siguiente ecuación diofántica $ax + m(-k) = b$.
- La ecuación diofantina lineal $ax + m(-k) = b$ tiene una solución si y solo si $d \mid b$, donde $d = mcd(a, m)$.
- La **solución particular** para x_0 se calcula mediante la expresión: $x_0 = \frac{ub}{d}$
- La **solución general** x se calcula por medio de

$$x = x_0 + \frac{m}{d}t$$

Ecuaciones de Congruencia Lineal

Resolver la siguiente congruencia lineal: $27x \equiv 12(\text{mód}15)$ donde $a = 27, b = 12$ y $m = 15$.

1. Si $27x \equiv 12(\text{mód}15)$, entonces $15 \mid 27x - 12$ esto es $27x - 12 = 15k$ equivalente a la ecuación diofántica $27x + 15(-k) = 12$.

2. Calcular el $d = mcd(a, m) = mcd(27, 15) = 3$

3. Calcular la combinación lineal $d = au + mv$ la cual es $3 = 15 + (-1) \cdot 12 = 15 + (-1)[(1) \cdot 27 + (-1) \cdot 15] = 27 \cdot (-1) + 15 \cdot (2)$ donde $u = -1$ y $v = 2$.

4. Calcular la solución particular $x_0 = \frac{ub}{d}$ cuyo valor es $x_0 = \frac{-1 \cdot 12}{3} = -4$

5. Calcular la solución general $x = x_0 + \frac{m}{d}t$ es $x = -4 + \frac{15}{3}t$

6. Verificar el resultado, por ejemplo para $k = 4, x = -4 + 20 = 16$, entonces $27 \cdot (16) \equiv 12(\text{mód}15)$ esto es $432 \equiv 12(\text{mód}15)$. Es posible verificar que $15 \mid (432 - 12)$ ya que $432 - 12 = 28 \cdot 15 = 420$.

Algortimo de la división para números negativos

Algoritmo de la división convencional

Si $a, b \in \mathbb{Z}$, con $b > 0$, entonces existen valores únicos para $q, r \in \mathbb{Z}$ donde $a = qb + r$, $0 \leq r < b$.

Cómo aplicar el algoritmo de la división para casos dónde $b < 0$?

Algortimo de la división para números negativos

Ejemplo 1 (a<0,b<0,q>0): $a = -27$ y $b = -4$

1. Calcular $|-27| \div |-4| = 6.75$ dónde $q = 6$.
2. Ajustar los valores de q y r de forma que $0 \leq r < |b|$, es decir que $0 \leq r < |-4|$, entonces $-27 = (7) - 4 + 1$, esto es $a = -27, b = -4, q = 7, r = 1$

Ejemplo 2 (a<0,b>0,q<0): $a = -27$ y $b = 4$

1. Calcular $|-27| \div 4 = 6.75$ dónde $q = 6$.
2. Ajustar los valores de q y r de forma que $0 \leq r < |b|$, es decir que $0 \leq r < 4$, entonces $-27 = (-7) + 4 + 1$, esto es $a = -27, b = 4, q = -7, r = 1$

Ejemplo 3 (a>0,b<0,q<0): $a = 27$ y $b = -4$

1. Calcular $27 \div |-4| = 6.75$ dónde $q = 6$.
2. Ajustar los valores de q y r de forma que $0 \leq r < |b|$, es decir que $0 \leq r < 4$, entonces $27 = (-6) - 4 + 3$, esto es $a = 27, b = -4, q = -6, r = 3$

Fin