Estructuras Discretas INF-313

Sergio Hernández, Mónica Acevedo
shernandez@ucm.cl, macevedo@ucm.cl

Facultad de Ciencias de la Ingeniería
UNIVERSIDAD CATOLICA DEL MAULE

Cociente y Residuo

Teorema (Algoritmo de la División)

Sean a y b enteros con $b \neq 0$. Entonces existen únicos enteros c y r tales que

$$a = bc + r$$

y $0 \leq r <| b |$

Cociente y Residuo

Teorema (Algoritmo de la División)

Sean a y b enteros con $b \neq 0$. Entonces existen únicos enteros c y r tales que

$$a = bc + r$$

y $0 \leq r < \mid b \mid$

- ¿Cómo se escribiría los siguientes números de acuerdo al teorema señalado?

Cociente y Residuo

Teorema (Algoritmo de la División)

Sean a y b enteros con $b \neq 0$. Entonces existen únicos enteros c y r tales que

$$a = bc + r$$

y $0 \leq r < \mid b \mid$

- ¿Cómo se escribiría los siguientes números de acuerdo al teorema señalado?
- $a = 4461,\ b = 16$
- $a = -262,\ b = 3$
- $a = -433,\ b = -17$

Algoritmo Euclidiano

Definición

Sean a y b enteros y $d = mcd(a, b)$. Donde d se encuentra siempre al enumerar todos los divisores de a y luego todos los divisores de b y entonces se escoge al máximo común divisor.

Un algoritmo muy eficiente, es el algoritmo euclidiano, con una complejidad del $O(\log n)$, para encontrar $d = mcd(a, b)$ al aplicar el algoritmo de división a a y b a cada cociente y residuo hasta obtener el residuo diferente a cero. El último residuo diferente de cero es $d = mcd(a, b)$.

Entonces, se tiene un algoritmo para desenredar, que regresa por los pasos del algoritmo euclidiano para encontrar los enteros x y y tales que $d = xa + yb$.

- Sea $a = 540$ y $b = 168$. ¿Cuál sería el primer paso?

- Sea $a = 540$ y $b = 168$. ¿Cuál sería el primer paso?
- Sería escribir $540 = 168 \cdot 3 + 36$

- Sea $a = 540$ y $b = 168$. ¿Cuál sería el primer paso?
- Sería escribir $540 = 168 \cdot 3 + 36$
- Ahora sería divisor dividido en el resto, es decir $168 = 36 \cdot 4 + 24$.

- Sea $a = 540$ y $b = 168$. ¿Cuál sería el primer paso?
- Sería escribir $540 = 168 \cdot 3 + 36$
- Ahora sería divisor dividido en el resto, es decir $168 = 36 \cdot 4 + 24$.
- Luego $36 = 24 \cdot 1 + 12$

- Sea $a = 540$ y $b = 168$. ¿Cuál sería el primer paso?
- Sería escribir $540 = 168 \cdot 3 + 36$
- Ahora sería divisor dividido en el resto, es decir $168 = 36 \cdot 4 + 24$.
- Luego $36 = 24 \cdot 1 + 12$
- $24 = 12 \cdot 2 + 0$

- Sea $a = 540$ y $b = 168$. ¿Cuál sería el primer paso?
- Sería escribir $540 = 168 \cdot 3 + 36$
- Ahora sería divisor dividido en el resto, es decir $168 = 36 \cdot 4 + 24$.
- Luego $36 = 24 \cdot 1 + 12$
- $24 = 12 \cdot 2 + 0$
- Entonces $d = 12$

- Sea $a = 540$ y $b = 168$. ¿Cuál sería el primer paso?
- Sería escribir $540 = 168 \cdot 3 + 36$
- Ahora sería divisor dividido en el resto, es decir $168 = 36 \cdot 4 + 24$.
- Luego $36 = 24 \cdot 1 + 12$
- $24 = 12 \cdot 2 + 0$
- Entonces $d = 12$
- Ahora nos faltaría encontrar x e y tales que $d = 540 \cdot x + 168 \cdot y$

- Sea $a = 540$ y $b = 168$. ¿Cuál sería el primer paso?
- Sería escribir $540 = 168 \cdot 3 + 36$
- Ahora sería divisor dividido en el resto, es decir $168 = 36 \cdot 4 + 24$.
- Luego $36 = 24 \cdot 1 + 12$
- $24 = 12 \cdot 2 + 0$
- Entonces $d = 12$
- Ahora nos faltaría encontrar x e y tales que $d = 540 \cdot x + 168 \cdot y$
- Para ello debemos ver cada resto en las expresiones, entonces $36 = 540 - 168 \cdot 3$, $24 = 168 - 36 \cdot 4$ y $12 = 36 - 24$

- Sea $a = 540$ y $b = 168$. ¿Cuál sería el primer paso?
- Sería escribir $540 = 168 \cdot 3 + 36$
- Ahora sería divisor dividido en el resto, es decir $168 = 36 \cdot 4 + 24$.
- Luego $36 = 24 \cdot 1 + 12$
- $24 = 12 \cdot 2 + 0$
- Entonces $d = 12$
- Ahora nos faltaría encontrar x e y tales que $d = 540 \cdot x + 168 \cdot y$
- Para ello debemos ver cada resto en las expresiones, entonces $36 = 540 - 168 \cdot 3$, $24 = 168 - 36 \cdot 4$ y $12 = 36 - 24$
- $12 = 36 - 1 \cdot 24$

- Sea $a = 540$ y $b = 168$. ¿Cuál sería el primer paso?
- Sería escribir $540 = 168 \cdot 3 + 36$
- Ahora sería divisor dividido en el resto, es decir $168 = 36 \cdot 4 + 24$.
- Luego $36 = 24 \cdot 1 + 12$
- $24 = 12 \cdot 2 + 0$
- Entonces $d = 12$
- Ahora nos faltaría encontrar x e y tales que $d = 540 \cdot x + 168 \cdot y$
- Para ello debemos ver cada resto en las expresiones, entonces $36 = 540 - 168 \cdot 3$, $24 = 168 - 36 \cdot 4$ y $12 = 36 - 24$
- $12 = 36 - 1 \cdot 24$
- $12 = 36 - 1 \cdot (168 - 36 \cdot 4)$

- Sea $a = 540$ y $b = 168$. ¿Cuál sería el primer paso?
- Sería escribir $540 = 168 \cdot 3 + 36$
- Ahora sería divisor dividido en el resto, es decir $168 = 36 \cdot 4 + 24$.
- Luego $36 = 24 \cdot 1 + 12$
- $24 = 12 \cdot 2 + 0$
- Entonces $d = 12$
- Ahora nos faltaría encontrar x e y tales que $d = 540 \cdot x + 168 \cdot y$
- Para ello debemos ver cada resto en las expresiones, entonces $36 = 540 - 168 \cdot 3$, $24 = 168 - 36 \cdot 4$ y $12 = 36 - 24$
- $12 = 36 - 1 \cdot 24$
- $12 = 36 - 1 \cdot (168 - 36 \cdot 4)$
- $12 = 36 - 1 \cdot 168 + 36 \cdot 4$

- Sea $a = 540$ y $b = 168$. ¿Cuál sería el primer paso?
- Sería escribir $540 = 168 \cdot 3 + 36$
- Ahora sería divisor dividido en el resto, es decir $168 = 36 \cdot 4 + 24$.
- Luego $36 = 24 \cdot 1 + 12$
- $24 = 12 \cdot 2 + 0$
- Entonces $d = 12$
- Ahora nos faltaría encontrar x e y tales que $d = 540 \cdot x + 168 \cdot y$
- Para ello debemos ver cada resto en las expresiones, entonces $36 = 540 - 168 \cdot 3$, $24 = 168 - 36 \cdot 4$ y $12 = 36 - 24$
- $12 = 36 - 1 \cdot 24$
- $12 = 36 - 1 \cdot (168 - 36 \cdot 4)$
- $12 = 36 - 1 \cdot 168 + 36 \cdot 4$
- $12 = 36 \cdot 5 - 1 \cdot 168$

- $12 = 5 \cdot (540 - 168 \cdot 3) - 1 \cdot 168$

- $12 = 5 \cdot (540 - 168 \cdot 3) - 1 \cdot 168$
- $12 = 5 \cdot 540 - 15 \cdot 168 - 1 \cdot 168$

- $12 = 5 \cdot (540 - 168 \cdot 3) - 1 \cdot 168$
- $12 = 5 \cdot 540 - 15 \cdot 168 - 1 \cdot 168$
- $12 = 5 \cdot 540 - 16 \cdot 168$

- $12 = 5 \cdot (540 - 168 \cdot 3) - 1 \cdot 168$
- $12 = 5 \cdot 540 - 15 \cdot 168 - 1 \cdot 168$
- $12 = 5 \cdot 540 - 16 \cdot 168$
- Entonces $x = 5$, $y = -16$

Enteros primos relativos

Definición

Dos enteros a y b son primos relativos o coprimos si $mcd(a, b) = 1$. En consecuencia, si a y b son primos relativos, entonces existen enteros x y y tales que $ax + by = 1$. A la inversa, si $ax + by = 1$, entonces a y b son primos relativos.

- Sea m un entero positivo. Se dice que a **es congruente con** b **módulo** m, lo que se escribe $a \equiv b$ (módulo m) o simplemente $a \equiv b \pmod{m}$

- Sea m un entero positivo. Se dice que a **es congruente con** b **módulo** m, lo que se escribe $a \equiv b$ (módulo m) o simplemente $a \equiv b \pmod{m}$
- si m divide a la diferencia $a - b$. El entero m se denomina módulo.

- Sea m un entero positivo. Se dice que a **es congruente con** b **módulo** m, lo que se escribe $a \equiv b$ (módulo m) o simplemente $a \equiv b \pmod{m}$
- si m divide a la diferencia $a - b$. El entero m se denomina módulo.

Teorema

Sea m un entero positivo. Entonces:

1. Para cualquier entero a se tiene $a \equiv a \pmod{m}$

- Sea m un entero positivo. Se dice que a **es congruente con** b **módulo** m, lo que se escribe $a \equiv b$ (módulo m) o simplemente $a \equiv b \pmod{m}$
- si m divide a la diferencia $a - b$. El entero m se denomina módulo.

Teorema

Sea m un entero positivo. Entonces:

1. Para cualquier entero a se tiene $a \equiv a \pmod{m}$
2. Si $a \equiv b \pmod{m}$ entonces $b \equiv a \pmod{m}$

- Sea m un entero positivo. Se dice que a **es congruente con** b **módulo** m, lo que se escribe $a \equiv b$ (módulo m) o simplemente $a \equiv b \pmod{m}$
- si m divide a la diferencia $a - b$. El entero m se denomina módulo.

Teorema

Sea m un entero positivo. Entonces:

1. Para cualquier entero a se tiene $a \equiv a \pmod{m}$
2. Si $a \equiv b \pmod{m}$ entonces $b \equiv a \pmod{m}$
3. $a \equiv b \pmod{m}$ y $b \equiv c \pmod{m}$ entonces $a \equiv c \pmod{m}$

Observación

Suponga que m es positivo y que a es cualquier entero. Por el algoritmo de la división, existen enteros q y r con $0 = r \leq m$ tal que $a = mq + r$. Por tanto,
$mq = a - r$ o $m(a - r)$ o $a \equiv r \pmod{m}$

Observación

Suponga que m es positivo y que a es cualquier entero. Por el algoritmo de la división, existen enteros q y r con $0 = r \leq m$ tal que $a = mq + r$.
Por tanto,
$mq = a - r$ o $m(a - r)$ o $a \equiv r \pmod{m}$
En consecuencia

1. Cualquier entero a es congruente con módulo m con un entero único en el conjunto $[0, 1, 2, \cdots, m - 1]$
   La unicidad proviene del hecho de que m no puede dividir a la diferencia de dos enteros así.

Observación

Suponga que m es positivo y que a es cualquier entero. Por el algoritmo de la división, existen enteros q y r con $0 = r \leq m$ tal que $a = mq + r$.
Por tanto,
$mq = a - r$ o $m(a - r)$ o $a \equiv r \pmod{m}$
En consecuencia

1. Cualquier entero a es congruente con módulo m con un entero único en el conjunto $[0, 1, 2, \cdots, m - 1]$
La unicidad proviene del hecho de que m no puede dividir a la diferencia de dos enteros así.
2. Dos enteros cualesquiera a y b son congruentes con módulo m si y sólo si tienen el mismo residuo cuando se dividen entre m.

- La notación $[x]_m$ o simplemente $[x]$ se usa para indicar la clase de residuos (módulo m) que contiene a un entero x, es decir, los enteros que son congruentes con x. En términos matemáticos $[x] = \{a \in Z \mid a \equiv x\}$ (módulo m)
  En consecuencia, las clases de residuos pueden denotarse por $[0], [1], [2], \cdots, [m-1]$ o con cualquier otra elección de enteros en un sistema de residuos completo.

Teorema

Suponga que $a \equiv c \pmod{m}$ y $b \equiv d \pmod{m}$. Entonces:

1. $a + b \equiv c + d \pmod{m}$.
2. $a \cdot b \equiv c \cdot d \pmod{m}$.

Teorema

Suponga que $a \equiv c \pmod{m}$ y $b \equiv d \pmod{m}$. Entonces:

1. $a + b \equiv c + d \pmod{m}$.
2. $a \cdot b \equiv c \cdot d \pmod{m}$.

Teorema

- Suponga que $ab \equiv ac \pmod{m}$ y $\text{mcd}(a, b)=1$ entonces $b \equiv c \pmod{m}$.

Teorema

Suponga que $a \equiv c \pmod{m}$ y $b \equiv d \pmod{m}$. Entonces:

1. $a + b \equiv c + d \pmod{m}$.
2. $a \cdot b \equiv c \cdot d \pmod{m}$.

Teorema

- Suponga que $ab \equiv ac \pmod{m}$ y $\text{mcd}(a, b)=1$ entonces $b \equiv c \pmod{m}$.
- Suponga que $ab \equiv ac \pmod{m}$ y $d = \text{mcd}(a, b)$ entonces $b \equiv c \pmod{\frac{m}{d}}$.

Teorema

Suponga que $a \equiv c \pmod{m}$ y $b \equiv d \pmod{m}$. Entonces:

1. $a + b \equiv c + d \pmod{m}$.
2. $a \cdot b \equiv c \cdot d \pmod{m}$.

Teorema

- Suponga que $ab \equiv ac \pmod{m}$ y mcd(a, b)=1 entonces $b \equiv c \pmod{m}$.
- Suponga que $ab \equiv ac \pmod{m}$ y d =mcd(a, b) entonces $b \equiv c \pmod{\frac{m}{d}}$.
- **OBSERVACION** suponga que p es primo. Entonces los enteros desde 1 hasta $p - 1$ son primos relativos con p. Por tanto, la ley de cancelación de costumbre se cumple cuando el módulo es un primo p. Es decir, $ab \equiv ac \pmod{p}$ y $a \neq 0 \pmod{p}$ entonces $b \equiv c \pmod{p}$

Teorema

- Si a y m son primos relativos, entonces $ax \equiv 1 \pmod{m}$ tiene una solución única; en otro caso, no tiene solución.

Teorema

- Si a y m son primos relativos, entonces $ax \equiv 1 \pmod{m}$ tiene una solución única; en otro caso, no tiene solución.
- Suponga que a y m son primos relativo. Entonces $ax \equiv b \pmod{m}$ tiene solución única. Adem'as, si s es la única solución de $ax \equiv 1 \pmod{m}$, entonces la solución única de $ax \equiv b \pmod{m}$ es $x = bs$

Teorema

- Si a y m son primos relativos, entonces $ax \equiv 1 \pmod{m}$ tiene una solución única; en otro caso, no tiene solución.
- Suponga que a y m son primos relativo. Entonces $ax \equiv b \pmod{m}$ tiene solución única. Adem'as, si s es la única solución de $ax \equiv 1 \pmod{m}$, entonces la solución única de $ax \equiv b \pmod{m}$ es $x = bs$
- Considere la ecuación $ax \equiv b \pmod{m}$, donde d=mcd(a, m).
  1. Suponga que d no divide a b. Entonces $ax \equiv b \pmod{m}$ no tiene solución.
  2. Suponga que d divide a b. Entonces $ax \equiv b \pmod{m}$ tiene d soluciones, todas congruentes módulo M con la solución única de $Ax \equiv B \pmod{M}$ donde $A = \frac{a}{d}$, $B = \frac{b}{d}$, $M = \frac{m}{d}$

Teorema chino del Residuo

Considere el sistema
$x \equiv r_1 \pmod{m_1}$, $x \equiv r_2 \pmod{m_2}$, $\cdots$, $x \equiv r_k \pmod{m_k}$
donde los m_i son primos relativos por pares. Entonces el sistema tiene una solución única módulo $M = m_1 \cdot m_2 \cdots m_k$

Teorema chino del Residuo

Considere el sistema

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

donde los m_i son primos relativos por pares. Entonces el sistema tiene una solución única módulo $M = m_1 \cdot m_2 \cdots m_k$

Proposición Considere el sistema mencionado de relaciones de congruencia. Sean $M = m_1 \cdot m_2 \cdots m_k$ y

$M_1 = \dfrac{M}{m_1}, M_2 = \dfrac{M}{m_2}, \cdots, M_k = \dfrac{M}{m_k}$

(Entonces, cada par M_i y m_i son coprimos) Sean $s_1, s_2, \cdots, s_k$ las soluciones, respectivamente, de las ecuaciones de congruencia

$M_1 x \equiv 1 \pmod{m_1}, M_2 x \equiv 1 \pmod{m_2}, \cdots, M_k x \equiv 1 \pmod{m_k}$

Entonces la siguiente es una solución del sistema:

$x_0 = M_1 s_1 r_1 + M_2 s_2 r_2 + \cdots + M_k s_k r_k$

- Resuelve la siguiente ecuación de congruencia $4x^4 - 3x^3 + 2x^2 + 5x - 4 = 0 \pmod 6$

- Resuelve la siguiente ecuación de congruencia $4x^4 - 3x^3 + 2x^2 + 5x - 4 = 0 \pmod{6}$
- Resuelva la ecuación lineal de congruencia $3x \equiv 2 \pmod{8}$

- Resuelve la siguiente ecuación de congruencia $4x^4 - 3x^3 + 2x^2 + 5x - 4 = 0 \pmod{6}$
- Resuelva la ecuación lineal de congruencia $3x \equiv 2 \pmod{8}$
- Resuelva la ecuación lineal de congruencia $4x \equiv 6 \pmod{10}$

- Resuelve la siguiente ecuación de congruencia $4x^4 - 3x^3 + 2x^2 + 5x - 4 = 0 \pmod{6}$
- Resuelva la ecuación lineal de congruencia $3x \equiv 2 \pmod{8}$
- Resuelva la ecuación lineal de congruencia $4x \equiv 6 \pmod{10}$ item Resuelva la ecuación de congruencia $1092x \equiv 213 \pmod{2295}$