# Teoría de Números 6

# Temas

1. **Ecuaciones de Congruencia**
2. **Sistema Residual Completo**
3. **Inverso multiplicativo módulo** $n$
4. **Teorema Chino del Resto**

# Ecuaciones de congruencias

> La ecuación $ax \equiv b\ mod(m)$ se llama de congruencia lineal, siendo $a, b, m$ números enteros conocidos con $m > 0$ y $x \in Z$ incógnita.

## Existencia de soluciones

Nótese que $ax \equiv b\ mod(m) \iff$ existen enteros $x, y$ tales que $ax - b = my$. Luego, se trata de solucionar la ecuación diofántica lineal anterior, de la cual conocemos que tiene infinitas soluciones $\iff mcd(a, m) \div b$.

## Soluciones congruentes

Es fácil ver que si $x_0$ es solución de la ecuación anterior $\implies$ todo número $n \equiv x_0\ mod(m)$ también será solución, por lo que existen infinitas soluciones con ese resto $x_0$, pero, existirán soluciones incongruentes? o sea, que no tengan el mismo resto

## Soluciones incongruentes

> La cantidad de soluciones incongruentes de una ecuación lineal de congruencia $ax \equiv b\ mod(m)$ es el $mcd(a, m)$

Sea $d = mcd(a, m)$. Ya vimos que $ax \equiv b\ mod(m)$ tiene solución $\iff d \div b$.
Entonces las soluciones de la ecuación diofántica correspondiente $ax + my = b$ (y por

tanto de la congruencia lineal) son de la forma:

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

$$y = y_0 - \frac{a}{d}t$$

Siendo $x_0, y_0$, una solución particular. Sean ahora $x_1, x_2$ dos soluciones de la congruencia $ax \equiv b\ mod(m)$. Entonces se tiene que:

$$x_1 = x_0 + \frac{m}{d}t_1$$

$$x_2 = x_0 + \frac{m}{d}t_2$$

Asumamos que ambas soluciones $x_1, x_2$ son congruentes módulo $m$, de esta forma hallaremos de cuántas formas posibles estas pueden ser congruentes, lo que nos dará la cantidad de soluciones incongruentes en la ecuación.

$$x_1 \equiv x_2\ mod(m)$$

$$x_0 + \frac{m}{d}t_1 \equiv x_0 + \frac{m}{d}t_2\ mod(m)$$

De donde:

$$\frac{m}{d}(t_1 - t_2) \equiv 0\ mod(m)$$

Como $\frac{m}{d} \div m$ al dividir la ecuación resulta:

$$t_1 - t_2 \equiv 0\ mod(d)$$
$$t_1 \equiv t_2\ mod(d)$$

Por tanto, si $t_1, t_2$ recorren un sistema completo de restos módulo $d$, se obtiene un sistema de soluciones incongruentes módulo $d$ y por tanto módulo $m$.

# Sistema Residual Completo (SRC)

Sea el conjunto $A$ un Sistema Residual Completo (SRC) módulo $p$ si se cumple que $A = \{0, 1, \dots, p-1\}$

## Propiedades

1. Si multiplicamos el SRC $P$ módulo $p$ por un número $a$ tal que $mcd(a,p) = 1 \implies$ el $P'$ resultante seguirá siendo un SRC módulo $p$

Supongamos que no se cumple $\implies$ sean $p_i, p_j$ dos elementos de $P$, luego, los elementos $ap_i, ap_j$ tendrán el mismo resto al ser divididos por $p \implies ap_i \equiv ap_j \ mod(p)$ y como $mcd(a,p) = 1 \implies$ al dividir entre $a$ resulta en $p_i \equiv p_j \ mod(p)$ lo cual es falso.

# Inverso multiplicativo

Sea $a, n \in Z_+^*$ y $mcd(a,n) = 1$, se llama inverso de $a$ módulo $n$ a la solución de $ax \equiv 1 mod(n)$

> Halla la solución de $4x \equiv 1 \ \ mod(13)$

Como $mcd(4, 13) = 1$ entonces existe $\overline{4}$ que representa el inverso multiplicativo de 4 módulo 13, el cual es 10.

# Teorema Chino del Resto

Sea $k$ un entero positivo y supongamos que $m_1, m_2, \dots, m_k$ son $k$ números naturales primos relativos dos a dos. Sean $b_1, b_2, \dots, b_k$ enteros cualesquiera. Entonces el sistema:

$$\begin{aligned} x &\equiv b_1 \ mod(m_1) \\ x &\equiv b_2 \ mod(m_2) \\ &\cdots \\ x &\equiv b_k \ mod(m_k) \end{aligned}$$

Tiene solución única módulo $M = m_1 m_2 \cdots m_k$

## Demostración existencia

Construiremos primero una solución: Sea:

$$M_k = \frac{M}{m_k} = m_1 m_2 \cdots m_{k-1} m_{k+1} \cdots m_n$$

Se sabe que $mcd(M_k, m_k) = 1$, pues $mcd(m_i, m_k) = 1 \forall\ i = k$. Entonces existe el inverso módulo $m_k$ de $M_k$. Sea este igual a $y_k$, o sea $M_k y_k \equiv 1\ mod(m_k)$.

Sea ahora $x = a_1 M_1 y_1 + a_2 M_2 y_2 + \cdots + a_n M_n y_n$. Para cada $m_k$ fijo se tiene que $m_k$ divide a $M_i$ para todo $i = k$, por lo que es:

$$M_i \equiv 0\ mod(m_k) \quad \forall i = k$$

Entonces se tiene:

$$x \equiv a_k M_k y_k\ mod(m_k)$$

Pero $M_k y_k \equiv 1\ mod(m_k)$ por lo que $x \equiv a_k\ mod(m_k) \implies x$ es una solución del sistema.

### Demostración unicidad

Sean $x_0, x_1$ soluciones, entonces $x_0 \equiv x_1 \equiv a_k\ mod(m_k) \forall k :\ 0 < k \leq n$, por lo que su mínimo común múltiplo lo divide (que como son primos relativos dos a dos el $mcm$ es el producto de todos ellos) y por tanto $M$ divide a $(x_0 - x_1)$, concluyendo así que $x_0 \equiv x_1$

## Ejercicios

### Problema 1

> Sean $a$ entero y $mcd(a, 10) = 1$. Prueba que existen infinitos múltiplos de $a$ que terminen en cualquier secuencia de dígitos dados.

### Solución 1

Sea la ecuación lineal de congruencia:

$$ax \equiv k\ mod(10^{k_d})$$

Donde $k$ es la secuencia de dígitos dados y $k_d$ su cantidad de dígitos. Dicha ecuación tiene solución ya que como $mcd(a, 10) = 1 \implies mcd(a, 10^{k_d}) = 1$ y $1 \div k$. Luego, existen infinitos valores $y$ tal que $y \equiv x\ mod(10^{k_d})$

## Solución 2

Estamos buscando un número $x$ tal que, si $d$ es la cantidad de dígitos de $d$ se cumpla que:

$$x \equiv d \ mod(10^d)$$
$$x \equiv 0 \ mod(a)$$

Lo cual, por el *Teorema Chino del Resto* está garantizado que tenga solución ya que, como $mcd(a, 10) = 1 \implies mcd(a, 10^d) = 1$, por lo cual, existen infinitas soluciones $y$ tal que $y \equiv x \ mod(a10^d)$

## Solución 3

Sea $k$ la secuencia de dígitos dados,$d$ la cantidad de dígitos que posee y $A = \{r_0, r_1, \dots, r_{a-1}\}$ un SRC módulo $a$, como $mcd(a, 10) = 1 \implies mcd(a, 10^d) = 1$ por lo que al multiplicar los elementos de $A$ por $10^d$ seguiremos teniendo $A$ como un SRC módulo $a$, luego, al sumarle a cada elemento la secuencia $k$ todos terminarán en $k$ y uno de ellos tendrá resto cero.

Para generar las infinitas soluciones basta con multiplicar el SRC por potencias de $10$ mayores que $10^d$

## Problema 2

> Resuelve:
>
> - $9x \equiv 21 \ mod(30)$
> - $19x \equiv 30 \ mod(40)$

## Solución

## Problema 3

> Resolver el siguiente sistema:
>
> $$x \equiv 3 \ mod(5)$$

$$x \equiv 2 \ mod(4)$$
$$x \equiv 1 \ mod(11)$$

## Solución

## Problema 4

Determine el mayor número impar mayor que 3 tal que 3 divide a $n$, 5 divide a $n+2$, 7 divide a $n+4$.

## Solución

## Problema 5

Resolver el siguiente sistema:

$$x \equiv 1 \ mod(2,3,4,5,6)$$
$$x \equiv 0 \ mod(7)$$

## Solución

## Problema 6

Sean $p$ y $q$ primos distintos. Prueba que exise un $k$ tal que $pn^q + qn^p + kn$ es divisible por $pq$ para todo $n \in \mathbb{N}$.

## Solución

Notemos que $pn^q + qn^p + kn = n(pn^{q-1} + qn^{p-1} + k)$. Analicemos los restos del segundo factor de la expresión con $p$ y $q$:

$$qn^{p-1} + k \equiv 0 \ mod(p)$$
$$pn^{q-1} + k \equiv 0 \ mod(q)$$

Analicemos el caso cuando $mcd(p,n) = mcd(q,n) = 1 \implies$ utilizando el *Pequeño Teorema de Fermat* se cumple que $n^{p-1} \equiv 1 \ mod(p)$ y $n^{q-1} \equiv 1 \ mod(p)$, luego, por el

*Teorema Chino del Resto* se cumple que el sistema:

$$k \equiv -q \ mod(p)$$
$$k \equiv -p \ mod(q)$$

Si $p \div n$ y $q \div n$ entonces es fácil ver que ambos dividen a $n(pn^{q-1} + qn^{p-1} + k)$

Si $p \div n$ pero $q$ no, luego $q \div n(pn^{q-1} + qn^{p-1} + k)$ y existe $k$ tal que $k \equiv -p \ mod(q)$. Análogamente se hace el análisis con $q$

## Problema 7

> Prueba que dado un $k$ entero es posible encontrar una secuencia de $k$ enteros consecutivos donde cada uno es divisible por un cubo mayor que 1.

## Solución

Sea el conjunto $A = \{a + 1, a + 2, \dots, a + k\}$ donde $a$ es el elemento que estamos buscando para el cual existe la secuencia de $k$ enteros consecutivos.

Sean $x_1, x_2, \dots, x_n$ los números tal que $a + i \equiv 0 \ mod(x_i)$ con $1 \leq i \leq k$. Tomando valores para los $x_i$ tal que sean coprimos dos a dos, por el *Teorema Chino del Resto* se cumple que existe $a$ tal que:

$$a \equiv -1 \ mod(x_1)$$
$$a \equiv -2 \ mod(x_2)$$
$$\dots$$
$$a \equiv -k \ mod(x_k)$$