Tema 3. Aritmética Modular

3.1. Congruencias enteras

→ Definición: Dados $m \in \mathbb{N}$, y $a, b \in \mathbb{Z}$, se dice que 'a es congruente con b' módulo m si y sólo si $m/(a-b)$. Se denota por $a \equiv b\ (mód\ m)$.

→ La relación de congruencia es una relación de equivalencia:
Reflexiva: $a \equiv a(mód\ m)$
Simétrica: Si $a \equiv b\ (mód\ m)$ entonces $b \equiv a\ (mód\ m)$
Transitiva: Si $a \equiv b\ (mód\ m)$ y $b \equiv c\ (mód\ m)$, entonces $a \equiv c\ (mód\ m)$

→ Teorema: Sea $m \in \mathbb{N}$. Se verifican las siguientes propiedades:

1) $a \equiv b\ (mód\ m)$ si y sólo si $a = m \cdot q + r,\ b = m \cdot q' + r$, con $0 \leq r < m$. Es decir, a y b tienen el mismo resto al dividirlos entre m.
2) Para todo $a \in \mathbb{Z}$, existe $r \in \{0, 1, 2, \dots, m-1\}$ tal que $a \equiv r(mód\ m)$.

→ Definición: Clase de congruencia módulo m es el conjunto

$$[r]_m = \{a \in \mathbb{Z} \,/\, a \equiv r(mód\ m)\} = \{a \in \mathbb{Z} \,/\, \exists\ q \in \mathbb{Z},\ con\ a = m \cdot q + r\} =$$

$$= \{\dots, r-2m, r-m, r, r+m, r+2m, \dots\}$$

→ Definición: Conjunto de mínimos restos no negativos módulo m es el conjunto de las clases de congruencias módulo m:

$$\mathbb{Z}_m = \{\,[0]_m,\ [1]_m, [2]_m, \dots,\ [m-1]_m\,\}$$

→ Proposición: La relación de congruencia es compatible con la suma y el producto en $\mathbb{Z}$. Es decir, si $a \equiv b\ (mód\ m)$ y $c \equiv d\ (mód\ m)$ entonces $a + c \equiv b + d\ (mód\ m)$ y $ac \equiv bd\ (mód\ m)$.

→ Definición: Se definen las siguientes operaciones en $\mathbb{Z}_m$:

Suma: $[a]_m + [b]_m = [a+b]_m$

Producto: $[a]_m \cdot [b]_m = [a \cdot b]_m$

→ Propiedades de la suma y el producto de clases. En general, NO se cumple la propiedad cancelativa del producto.

→ Proposición: Si $a \cdot c \equiv b \cdot c\ (mod\ m),\ c \not\equiv 0$, entonces $a \equiv b\ \left(mód\ \left(\frac{m}{mcd(m,c)}\right)\right)$

→ Consecuencia: En $\mathbb{Z}_m$ se verifica la propiedad cancelativa si m es primo.

Lema.- ac≡bc (mod mc) si y sólo si a≡b (mod m)

→ Definición: $[a]_m \in \mathbb{Z}_m$, con $[a]_m \neq [0]_m$, es un **divisor de cero** en $\mathbb{Z}_m$ si existe $[b]_m \in \mathbb{Z}_m$ tal que $[b]_m \neq [0]_m$ y $[a]_m \cdot [b]_m = [0]_m$.

→ Proposición: En $\mathbb{Z}_m$ hay divisores de cero si m **no** es primo, en cuyo caso, los divisores de cero son las clases $[a]_m$ tal que $mcd(a,m) \neq 1$.

→ Definición: $[a]_m \in \mathbb{Z}_m$ es inversible (**tiene inverso**) o es una **unidad** en $\mathbb{Z}_m$ si existe $[b]_m \in \mathbb{Z}_m$ tal que $[a]_m \cdot [b]_m = [1]_m$.

→ Proposición: $[a]_m$ tiene inverso en $\mathbb{Z}_m$ si y sólo si $mcd(a,m) = 1$; en cuyo caso, el inverso se calcula resolviendo la ecuación diofántica $ax + my = 1$, y el inverso de $[a]_m$, que notaremos $[a]_m^{-1}$, será la clase $[x]_m$ (se puede obtener una solución particular de la ecuación diofántica aplicando el Algoritmo de Euclides)

3.2. Criterios de Divisibilidad

Sea $x = (x_n, x_{n-1}, \dots x_1, x_0)$ la representación decimal del número entero $x = 10^n x_n + 10^{n-1} x_{n-1} + \cdots + 10x_1 + x_0 = \sum_{i=0}^{n} 10^i x_i$

→ Divisibilidad por 2 y por 5

→ Divisibilidad por 3 y por 9

→ Divisibilidad por 4

→ Divisibilidad por 11

→ Regla del 9

3.3. Unidades en $\mathbb{Z}_m$

→ Definición: U_m= Conjunto de unidades de $\mathbb{Z}_m$.

→ Propiedades de las unidades:

1) Si $[a]_m,\ [b]_m \in U_m$, entonces $[a]_m \cdot [b]_m \in U_m$. Además $[a \cdot b]_m^{-1} = [a]_m^{-1} \cdot [b]_m^{-1}$

2) Si $[a]_m \in U_m$, entonces $([a]_m^{-1})^{-1} = [a]_m$

3) Si $[a]_m \in U_m$, entonces $[a]_m U_m = [a]_m$

→ Proposición: Si p es primo, los únicos elementos que coinciden con su inverso en $\mathbb{Z}_p$ son $[1]_p$ y $[-1]_p$.

→ Teorema de Wilson: Si p es primo, entonces $(p-1)! \equiv (p-1)(mod\ p)$, y, por tanto, $(p-2)! \equiv 1(mod\ p)$.

3.4. Función de Euler

→ Función de Euler. ϕ: $\mathbb{N} \to \mathbb{N}$, de forma que

$$\phi(n) = card\ \{1 \leq a \leq n\ /mcd(a,n) = 1\} = card\ U_n = card\ \{[a]_n\ /mcd(a,n) = 1\}$$

→ Propiedades de la función de Euler

Si p es primo entonces $\phi(p^r) = p^r - p^{r-1}$

Si $mcd(a,b) = 1$ entonces $\phi(a \cdot b) = \phi(a)\phi(b)$

→ Teorema de Euler: Si $[a]_m \in U_m$, entonces $[a]_m{}^{\phi(m)} = [1]_m$

Equivalentemente, Si $mcd(a,m) = 1$, entonces $a^{\phi(m)} \equiv 1\ (mod\ m)$

3.5. Ecuaciones en congruencias. Sistemas de ecuaciones

→ Ecuaciones en congruencias. $[a]_m \cdot [x]_m = [b]_m$ o equivalentemente $ax \equiv b\ (mod\ m)$

- Si $mcd(a,m) = 1$, entonces $[x]_m = [a]_m^{-1} \cdot [b]_m$ o $x \equiv a^{-1}b\ (mod\ m)$
- Si $mcd(a,m) \neq 1$, entonces la ecuación tiene solución si y sólo si $mcd(a,m) = d$ divide a b. En este caso, el número de soluciones no congruentes (distintas) en $\mathbb{Z}_m$ es d. Las soluciones se obtienen resolviendo la ecuación difántica $ax + my = b$ y serán de la forma $[x]_m = \left[x_0 + \frac{m}{d}t\right]_m$ con $t \in \{0,1,\dots,d-1\}$, y siendo x_0 sol. particular de la ecuación diofántica (se puede obtener aplicando el Algoritmo de Euclides).

→ Sistemas de congruencias. Teorema Chino del Resto.

Proposición. El sistema de congruencias $\begin{cases} x \equiv a_1 (mod\ m_1) \\ \vdots \\ x \equiv a_n (mod\ m_n) \end{cases}$ tiene solución única en $\mathbb{Z}_m$, con $m = mcm(\ m_1\ , m_2 \ldots, m_k)$ si y sólo si $\forall\ i \neq j\ \ mcd(m_i, m_j)$ divide a $(a_i - a_j)$.

Teorema Chino del Resto. En particular, si en el sistema de congruencias

$$\begin{cases} x \equiv a_1 (mod\ m_1) \\ \vdots \\ x \equiv a_n (mod\ m_n) \end{cases}$$

$mcd(m_i, m_j) = 1\ \ \forall\ i \neq j$, entonces el sistema tiene solución única en $\mathbb{Z}_m$, con $m = \prod_{i=1}^{n} m_i$. Además, una solución particular es $x_0 = \sum_{k=1}^{n} a_k \frac{m}{m_k} \left[\frac{m}{m_k}\right]_{m_k}^{-1}$ y la solución general $x = \{x_0 + mt\ ,\ t\ \in \mathbb{Z}\} = [x_0]_m$

Lema.- Si $mcd(p, q) = 1$, entonces

$$a \equiv b\ (mod\ p \cdot q) \iff \begin{cases} a \equiv b\ (mod\ p) \\ y \\ a \equiv b\ (mod\ q) \end{cases}$$

Dem.- $\Longrightarrow\ a \equiv b\ (mod\ p \cdot q)\ \dashrightarrow\ \exists\ k\ \in \mathbb{Z}$ tal que $p \cdot q \cdot k = a - b$. Por tanto, $p/(a-b)$ y $q/(a-b)$. Entonces $a \equiv b\ (mod\ p)$ y $a \equiv b\ (mod\ q)$.

$\Leftarrow$ $p/(a-b)$ y $q/(a-b)$. Entonces, $\exists\ k, h\ \in \mathbb{Z}$ tales que

$p \cdot k = a - b$ y $q \cdot h = a - b$. Por tanto $p \cdot k = q \cdot h$, $p/\ q \cdot h$, y como

$mcd(p, q) = 1$, se tiene que $p/\ h$. $\exists\ r\ \in \mathbb{Z}$ tal que $p \cdot r = h$, y sustituyendo

$q \cdot p \cdot r = a - b$, con lo que $q \cdot p\ /(a-b)$ y $a \equiv b\ (mod\ p \cdot q)$.

$\rightarrow$ Consecuencia: en general si $m = p_1^{r_1} \cdot\ p_2^{r_2} \cdot \ldots \cdot p_k^{r_k}$ con $p_1, p_2, \ldots, p_k$ primos distintos entre sí, entonces

$$a \equiv b\ \left(mod\ p_1^{r_1} \cdot\ p_2^{r_2} \cdot \ldots \cdot p_k^{r_k}\right) \iff \begin{cases} a \equiv b\ \left(mod\ p_1^{r_1}\right) \\ \vdots \\ a \equiv b\ \left(mod\ p_k^{r_k}\right) \end{cases}$$

Por tanto, el Lema nos permite transformar una ecuación en congruencias en un sistema de congruencias con módulos primos entre sí. Una vez hecha esta transformación con cada ecuación del sistema, tendremos un sistema con módulos potencias de números primos. En el caso de que haya varias ecuaciones con módulo que sean distintas potencias de un mismo número primo, eliminaremos las ecuaciones que tengan las potencias más pequeñas. Así, nos quedará un sistema con módulos potencias de números primos distintos,

es decir, un sistema con módulos primos entre sí (mcd de cada dos igual a 1), y podremos aplicar el Teorema Chino del Resto.