Tema 2

Aritmética modular

2.1 Relaciones de equivalencia

Definición 2.1 *Una relación que verifique las propiedades reflexiva, simétrica y transitiva se denomina* ***relación de equivalencia****. Dos elementos relacionados se dicen equivalentes.*

Ejemplo 2.2 *Son ejemplos de relaciones de equivalencia:*

- *Relación de paralelismo entre rectas del plano.*
- *La relación de equipotencia entre conjuntos definida por:*

  A *y* B *equipotentes* $\Leftrightarrow$ *existe una aplicación biyectiva* $f\colon A \to B$.
- *En un conjunto de personas la relación haber nacido el mismo año.*

Las relaciones de equivalencia sirven para clasificar los elementos de un conjunto.

Definición 2.3 *Sea R una relación de equivalencia sobre un conjunto y sea* $a \in A$*. El conjunto de todos los elementos relacionados con A se denomina* ***clase de equivalencia*** *de a y se denota por* $[a]$ ó $\bar{a}$:

$$\bar{a} = [a] = \{x \in A \mid x \,\mathrm{R}\, a\}$$

Teorema 2.4 *Sea R una relación de equivalencia sobre un conjunto y sean* a *y* $b \in A$*. Se verifica:*

1. $\bar{a} = \bar{b} \Leftrightarrow a\, R\, b$
2. $\bar{a} \neq \bar{b} \Leftrightarrow \bar{a} \cap \bar{b} = \varnothing$

El teorema anterior nos dice que dada una relación de equivalencia en un conjunto A, las clases de equivalencia pertenecientes a A a o son iguales o son disjuntas. Como consecuencia se tiene:

- Todos los elementos de una misma clase son equivalentes entre sí.
- Una clase queda determinada por uno cualquiera de sus elementos, es su

2.2 Congruencias en $\mathbb{Z}$ módulo *n*

Definición 2.6 (Congruencia módulo *n*) *En el anillo de los números enteros ($\mathbb{Z}$, +, .), dado un número entero positivo n, se define la siguiente relación:*

$$a \equiv b \ (mod\ n) \Leftrightarrow a - b \text{ es múltiplo de } n,$$

Esta relación es de equivalencia.

Teorema 2.7 *La relación de congruencia se puede reescribir como:*

$a \equiv b$ $(mod\ n) \Leftrightarrow$ *el resto de la división euclídea de a y de b por n es el mismo.*

Demostración.

Supongamos primero que $a \equiv b$ $(mod\ n)$.

$a \equiv b$ $(mod\ n) \Rightarrow$ Existe $k \in \mathbb{Z}$ tal que $a - b = kn$. Al realizar la división euclídea de b por n se tiene: $b = pn + r$ con $0 \leq r < n$. Sustituyendo b en la expresión anterior se tiene que $a = (k + p)n + r$, con $0 \leq r < n$. Se ha obtenido que el resto de la división euclídea de a por n es también r.

Recíprocamente, supongamos el resto de la división euclídea de a y de b por n es el mismo. Esto es, $a = qn + r$ y $b = pn + r$ con $0 \leq r < n$

Restando se obtiene $a - b = (q - p)n$, por tanto $a - b$ múltiplo de n. Lo que significa $a \equiv b$ $(mod\ n)$. ■

Por tanto, se tienen n clases de equivalencia en el conjunto cociente que suele escribirse en la forma $\mathbb{Z}/n\mathbb{Z}$ o $\mathbb{Z}_n$, cada una de ellas correspondiente a uno de los posibles restos, es decir, 0, 1, …, $n - 1$. El conjunto {0, 1,…, $n - 1$} constituyen un sistema de representante de la relación de congruencia módulo n.

$$\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}_n = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$$

2.3 Aritmética modular

Demostración.

- Veamos primero que la suma está bien definida: Si $a \equiv b\ (mod\ n)$ y $c \equiv d (mod\ n)$, entonces $a + c \equiv b + d\ (mod\ n)$

$a \equiv b\ (mod\ n) \Rightarrow$ Existe $r \in \mathbb{Z}$ tal que $a - b = rn$

$c \equiv d\ (mod\ n) \Rightarrow$ Existe $s \in \mathbb{Z}$ tal que $c - d = sn$

Sumando se tiene $(a + c) - (b + d) = (r + s)\ n$, esto es, $a + c \equiv b + d\ (mod\ n)$

- Veamos que el producto está bien definido: Si $a \equiv b\ (mod\ n)$ y $c \equiv d (mod\ n)$, entonces $a\ .\ c \equiv b\ .d\ (mod\ n)$

$a \equiv b\ (mod\ n) \Rightarrow$ Existe $r \in \mathbb{Z}$ tal que $a - b = rn \Rightarrow$ Existe $r \in \mathbb{Z}$ tal que $(a - b).\ c = rnc$

$c \equiv d\ (mod\ n) \Rightarrow$ Existe $s \in \mathbb{Z}$ tal que $c - d = sn \Rightarrow$ Existe $s \in \mathbb{Z}$ tal que $b.(c - d) = bsn$

Sumando se tiene $a.c$ - $bd = (rc$ - $bs)\ n$, esto es, $a.c \equiv b.d\ (mod\ n)$.

- Se deja como ejercicio comprobar las propiedades. $\bar{0}$ es el elemento neutro respecto de la suma, el elemento opuesto de $\bar{a}$ es la clase $\overline{n-a}$ y que el elemento neutro respecto al producto es la clase $\bar{1}$. ■

Observación 2.9 Restos potenciales

El hecho de que el producto sea una operación bien definida en $\mathbb{Z}_n$ permite calcular los retos potenciales módulo n de las potencias sucesivas de un número dado N.

Si llamamos a estos restos potenciales $r_1, \ldots, r_k$ módulo n, esto es,

$$N \equiv r_1 (mod\ n),\ \ldots.,\ N^k \equiv r_k (mod\ n),$$

Se verifica que $N^{k+1} \equiv N\ N^k \equiv r_1.\ r_k (mod\ n)$,

Ejemplo 2.10 Los restos potenciales de 6 módulo 11 son:

$6 \equiv 6\ (mod\ 11)$, $6^2 \equiv 36\ (mod\ 11) \equiv 3\ (mod\ 11)$, $6^3 \equiv 6*3\ (mod\ 11) \equiv 7\ (mod\ 11)$,

$6^4 \equiv 6*7\ (mod\ 11) \equiv 9\ (mod\ 11)$, $6^5 \equiv 6*9\ (mod\ 11) \equiv 10\ (mod\ 11)$,

$6^6 \equiv 6*10\ (mod\ 11) \equiv 5\ (mod\ 11)$, $6^7 \equiv 6*5\ (mod\ 11) \equiv 8\ (mod\ 11)$,

Ejemplo 2.11 Una aplicación de las congruencias es la obtención de criterios de divisibilidad. Así, por ejemplo, se puede saber si un entero x es divisible por 3 sin realizar la división.

Sea $x = x_n\, x_{n-1} \ldots x_2\, x_1\, x_0$ un número natural escrito en base diez, es decir,

$$x = x_n \,.\, 10^n + x_{n-1}.10^{n-1} + \ldots + x_2.10^2 + x_1.10 + x_0, \text{ y } 0 \leq x_i \leq 9, \forall i \in \{0,\ldots, n\}$$

Como $10 \equiv 1$ $(mod\ 3)$, se tendrá que $x_i.10^i \equiv x_i$ $(mod\ 3)$, por tanto,

$x \equiv \sum_{i=1}^{n} x_i \ (mod\ 3).$

En consecuencia, *x es divisible por 3 si, y sólo si, $\sum_{i=1}^{n} x_i\, 0 (mod\ 3)$, es decir, la suma de sus cifras es múltiplo de 3.*

2.4 Ecuaciones y sistemas de congruencias

2.4.1 Ecuaciones de congruencias

En este apartado se trata de resolver congruencias del tipo $a\, x \equiv b$ $(mod\ n)$

Proposición 2.12 *La congruencia $ax \equiv b$ $(mod\ n)$ tiene solución si, y sólo si, $d = mcd(a,n)$ divide a b. Además, si existe solución, esta es única módulo n/d.*

Demostración. Basta observar que la congruencia anterior tiene solución si, y sólo si, la ecuación diofántica $ax + ny = b$ tiene solución. Sabemos que tiene solución si, y sólo si, $d = mcd(a, n)$ divide a b.

Las soluciones de la ecuación diofántica $ax + ny = b$ son de la forma

$$\begin{aligned} x &= x_0 + \frac{n}{d}t \\ y &= y_0 - \frac{a}{d}t \end{aligned}$$

con t cualquier número entero y (x_0, y_0) una solución cualquiera de $ax + ny = b$.

Todas ellas son congruentes módulo $\frac{n}{d}$. Por tanto la solución es única módulo $\frac{n}{d}$. ■

Ejemplo 2.13 *Resuelve la siguiente congruencia:* $10x \equiv 15$ $(mód\ 25)$

$mcd(10,25) = 5$ y 5 no divide a 7, por tanto no tiene solución. ■

2.4.2 Sistemas de congruencias

Veamos qué ocurre si hay varias congruencias

Teorema 2.15 Teorema chino de los restos *Sean $m_1, \ldots, m_n$ números enteros positivos coprimos dos a dos, es decir, $mcd(m_i, m_j) = 1$ si $i \neq j$ y sean $b_1, \ldots, b_n$ enteros cualesquiera. Entonces, el sistema de congruencias*

$$x \equiv b_1 \ (mod\ m_1), \ldots, x \equiv b_n \ (mod\ m_n)$$

Posee una única solución entera entre 0 y $m_1 \ldots m_n$-1, es decir, una única solución entera módulo $m_1 \ldots m_n$.

Demostración. Sean $M = m_1 \ldots m_n$ y $M_k = \frac{M}{m_k} = m_1 \ldots m_{k-1} m_{k+1} \ldots m_n$ para $k = 1, \ldots, n$.

Puesto que los m_i son coprimos dos a dos, se tiene que $mcd(m_k, M_k) = 1$ y, por tanto, existen enteros t_k y s_k tales que

$$s_k M_k + t_k m_k = 1,\ k = 1,.., n$$

$s_k M_k$ es múltiplo de m_j si $j \neq k$ y congruente con 1 módulo m_k. En consecuencia $b_k s_k M_k$ es congruente con 0 módulo m_j si $j \neq k$ y congruente con b_k módulo m_k. Por tanto,

$$b_1 s_1 M_1 + \ldots + b_n s_n M_n \equiv b_k \ (mod\ m_k),\ \forall k \in 1\{,\ldots, n\}.$$

Consideremos $x = b_1 s_1 M_1 + \ldots + b_n s_n M_n$, es una solución al sistema dado.

Falta demostrar que es única módulo M:

Supongamos que existen dos soluciones, x e y. Restando se tiene que

$$x - y \equiv 0 \ (mod\ m_k),\ \forall k \in 1\{,\ldots, n\}.$$

es decir, $x - y$ es múltiplo de todos los m_k, luego es múltiplo del mínimo común múltiplo de m_1, $m_2, \ldots, .m_n$ que, al ser coprimos dos a dos es su producto, esto es, M. Por tanto, $x \equiv y$ ($mód\ M$).

■

Ejemplo 2.16 *Resolver el sistema de congruencias* $x \equiv 1\ (mod\ 2)$, $x \equiv 4\ (mod\ 7)$, $x \equiv 3\ (mod\ 11)$

$\{2, 7, 11\}$ son coprimos. Aplicando el teorema chino de los restos:

$M = 2*7*11 = 154$, $M_1 = 7*11 = 77$, $M_2 = 2*11 = 22$, $M_3 = 2*7 = 14$

$x = 25 + 154\,t$, con t cualquier número entero. ■

También lo podríamos hacer:

$x \equiv 1\ (mod\ 2) \Leftrightarrow x = 1 + 2.t$ para algún t entero

Sustituyendo en $x \equiv 4\ (mod\ 7)$: $1 + 2.t \equiv 4\ (mod\ 7) \Leftrightarrow\ 2.t \equiv 3\ (mod\ 7)$

Se tiene la ecuación diofántica: $2t + 7y = 3$, sus soluciones son $t = -9 + 7s$ para algún s entero.

Esto es, $x = 1 + 2.t = 1 + 2(-9 + 7s) = -17 + 14s$ para algún s entero.

Sustituyendo en $x \equiv 3\ (mod\ 11)$: $-17 + 14s \equiv 3\ (mod\ 11) \Leftrightarrow 14s \equiv 20\ (mod\ 11) \Leftrightarrow 14s \equiv 9\ (mod\ 11)$

Se tiene la ecuación diofántica: $14s+11z = 9$, sus soluciones son $s = 36+11k$ para algún k entero.

Esto es, $x = -17 + 14s = -17 + 14(36+11k) = 487 + 154k$ para algún k entero.

$x = 487 + 154k = 25 + 154*3 + 154k = 25 + 154r$ para algún r entero. ■

Ejercicio 2.17 Manteniendo la notación de la demostración del Teorema Chino de los restos, probar que $E_jE_k \equiv 0\ (mod\ M)$ si $j \neq k$, siendo $E_k = s_k M_k$. Probar que, para todo entero a, si $a \equiv a_k\ (mod\ m_k)$, se tiene

$$a\ \equiv \sum_{k=1}^{m} E_k\, a_k (mod\ M).$$

Ahora, llamemos a los coeficientes a_k coordenadas de a. Probar que si b tiene coordenadas b_k, entonces $a_k \pm b_k$ y a_kb_k son las coordenadas de $a \pm b$ y de ab, respectivamente.

Teorema 2.18 *El Teorema Chino de los Restos establece una biyección entre* $\mathbb{Z}_M$ *y* $\mathbb{Z}_{m_1} x \dots x\, \mathbb{Z}_{m_n}$. *Por otro lado, consideremos la aplicación dada por:*

$$\psi\colon \mathbb{Z}_M \longrightarrow \mathbb{Z}_{m_1} x \dots x\, \mathbb{Z}_{m_n},\ \ \psi(a) = \ (a_1, \dots, a_n),$$

Donde los a_k *son las coordenadas de a como se han definido en el Ejercicio. El teorema Chino de los Restos nos dice como construir* ψ^{-1}.

Por otro lado, recordando que se puede dotar a $\mathbb{Z}_{m_1} x \dots x\, \mathbb{Z}_{m_n}$ *de estructura de anillo definiendo suma y producto componente a componente. Lo que nos dice el ejercicio es que* $\psi(a + b) = \psi(a) + \psi(b)$ *y* $\psi(a\ .\ b) = \psi(a)\ .\ \psi(b)$, *es decir, que* ψ *es un homomorfismo de anillos y, al ser biyectivo, es un isomorfismo de anillos.*

En el Teorema Chino de los Restos, se supone que los módulos son siempre coprimos dos a dos. Veamos qué ocurre si los módulos no son necesariamente coprimos dos a dos.

- Supongamos, en primer lugar, que existe solución del sistema de congruencias. Si x es una solución, $x \equiv b_i$ ($mod\ m_i$) y $x \equiv b_j$ ($mod\ m_j$). En consecuencia, $x - b_i$ y $x - b_j$ son múltiplos de m_i y m_j. Por tanto, son múltiplos de mcd (m_i, m_j), de donde se deduce que $b_i \equiv b_j$ ($mod\ mcd$ (m_i, m_j)).

- La unicidad módulo $mcm(m_1,\ldots, m_n)$ se demuestra de forma análoga al teorema Chino de los Restos.

- Falta demostrar que si se verifica la condición del Teorema, entonces tiene solución.

La demostración se basa en la reducción de un par de congruencias a una sola. Supongamos, pues, que debemos resolver

$$x \equiv b_1\ (mod\ m_1),$$
$$x \equiv b_2\ (mod\ m_2),$$

De la primera se obtiene $x = b_1 + tm_1$, para algún $t \in \mathbb{Z}$. Sustituyendo en la segunda, se tiene $b_1 + tm_1 \equiv b_2$ ($mod\ m_2$), en consecuencia, $tm_1 \equiv b_2 - b_1$ ($mod\ m_2$).

Por hipótesis, $d = mcd$ (m_1, m_2) divide a $b_2 - b_1$ y se verifica que $mcd\left(\frac{m_1}{d},\frac{m_2}{d}\right) = 1$ divide a $\frac{b_2-b_1}{d}$. En consecuencia, la congruencia

$$t\ \frac{m_1}{d} \equiv \frac{b_2 - b_1}{d}\ \left(mod\ \frac{m_2}{d}\right)$$

tiene solución única módulo m_2/d, la solución será $t \equiv a$ ($mod\ m_2/d$). Esto es,

$$t = a + t_1\ \frac{m_2}{d} \text{ para algún } t_1 \in \mathbb{Z}.$$

Sustituyendo esta expresión en $x = b_1 + tm_1$, se tiene

$$x = b_1 + am_1 + t_1\ \frac{m_1 m_2}{d} = b_1 + am_1 + t_1\ mcm(m_1, m_2)$$

En consecuencia, $x \equiv b_1 + am_1$ ($mod\ mcm$ (m_1, m_2)).

Repitiendo la construcción n -1 veces se obtiene la solución del sistema.

■

Ejemplo 2.20 *Resolver el sistema de congruencias* $x \equiv 5$ (mod 6), $x \equiv 3$ (mod 10), $x \equiv 13$ (mod 20)

- $mcd(6,10) = 2 \mid 5-3 = 2$, $mcd(6,20) = 2 \mid 13-5 = 8$, $mcd(10, 20) = 10 \mid 13-3 = 10$, por tanto existe solución única módulo $mcm(6,10,20) = 60$.
- Consideremos primero las ecuaciones $x \equiv 5$ (mod 6), $x \equiv 3$ (mod 10), $mcd(6,10) = 2$ que es divisor de 5-3 = 2. Existe solución común.

$t\ \frac{m_1}{d} \equiv \frac{b_2-b_1}{d}\ \left(mod\ \frac{m_2}{d}\right)$, $3t \equiv -1$(mod 5), $3t + 5y = -1$, una solución particular $t = -2$

La solución es $x \equiv b_1 + am_1$ $(mod\ mcm\ (m_1,\ m_2))$, $x \equiv 23 - 7*30$ $(mod\ mcm\ (30,20)) \equiv -187$ $(mod\ 60) \equiv -7(mod\ 60) \equiv 53(mod\ 60)$.

La solución es $x \equiv 53(mod\ 60)$. ■

2.5 Aplicaciones del cálculo de congruencias: Sistema criptográfico de clave pública RSA.

En esta sección se va a describir un sistema criptográfico que se conoce como RSA. La idea es transmitir mensajes por canales "inseguros" (esto es, accesibles a individuos distintos del emisor y del receptor) sin que puedan ser comprendidos más que por el emisor y el receptor. Esto exige un proceso de codificación del mensaje y su posterior decodificación. Los caracteres del mensaje se traducen a números, se envían números.

Codificación 2.21

- Se eligen dos números primos grandes p y q y se considera $n = p.q$
- Se elige un número e, con $1 < e < (p-1)(q-1)$ y $mcd(e,(p-1)(q-1))=1$
- Se transforma el número entero M, que representa el mensaje a enviar, en C con $C \equiv M^e(mod\ n)$

Descifrado 2.22

El siguiente teorema, que demostraremos más adelante, justifica el descifrado.

Pequeño teorema de Fermat: "Si p es primo y a es un entero no divisible por p, entonces $a^{p-1} \equiv 1(mod\ p)$"

El mensaje se puede recuperar cuando se conoce la clave de descifrado d.

d verifica $de \equiv 1(mod\ (p-1)(q-1))$ (Este número d existe)

Se sigue que $C^d \equiv (M^e)^d\ (mod\ n) = M^{ed} \equiv M^{1+k\,(p-1)(q-1)}\ (mod\ n) \equiv M(M^{\,(p-1)})^{k(q-1)}\ (mod\ n)$

Al ser $n = p.q$, se verifica

$C^d \equiv M(M^{\,(p-1)})^{k(q-1)}\ (mod\ p) \equiv M.1\ (mod\ p) \equiv M\,(mod\ p)$

$C^d \equiv M(M^{\,(q-1)})^{k(p-1)}\ (mod\ q) \equiv M.1\ (mod\ q) \equiv M\,(mod\ q)$

Al ser C^d solución del sistema de congruencias $x \equiv M\ (mod\ p)$, $x \equiv M\ (mod\ q)$. Por el teorema chino de los restos se sigue que la solución, M, es única módulo $mcm(p,\ q) =$