ARITMÉTICA MODULAR

Gregorio Hernández

UPM

Matemática Discreta I

(MI)

CONGRUENCIAS EN **Z**

Dados $m \in \mathbf{N}$, $a,b \in \mathbf{Z}$ decimos que **a** y **b** son **congruentes módulo m** si $m \mid (a - b)$. Se indica por $a \equiv b \pmod{m}$

Propiedades

1. $a \equiv b \pmod{m} \Leftrightarrow$ los restos de las divisiones de **a** y **b** entre **m** coinciden
2. La congruencia módulo m es una relación de **equivalencia** para todo m

i) Prop. REFLEXIVA $a \equiv a \pmod{m}$
ii) Prop. SIMÉTRICA Si $a \equiv b \pmod{m}$ entonces $b \equiv a \pmod{m}$
iii) Prop. TRANSITIVA
Si $a \equiv b \pmod{m}$ y $b \equiv c \pmod{m}$ entonces $a \equiv c \pmod{m}$

GAUSS "Disquisitiones arithmeticae", 1798

CONGRUENCIAS EN **Z** **(Ejemplo módulo 6)**

Dados $a,b \in \mathbf{Z}$ decimos que **a** y **b** son **congruentes módulo 6** si $6 \mid (a - b)$. Se indica por $a \equiv b \pmod 6$

Clase del 2

$[2]_6 = \{ \ldots, -16, -10, -4, 2, 8, 14, 20, \ldots\} = [14]_6 = [602]_6 = \ldots$

$[0]_6 = \{ \ldots, -18, -12, -6, 0, 6, 12, 18, \ldots\} = [18]_6 = [594]_6 = \ldots$

$[1]_6 = \{ \ldots, -17, -11, -5, 1, 7, 13, 19, \ldots\} = [13]_6 = [301]_6 = \ldots$

$[3]_6 = \{ \ldots, -9, -3, 3, 9, 15, \ldots\} = \{a \in \mathbf{Z} / \ a = 6k + 3, \text{ con } k \in \mathbf{Z}\}$

$[4]_6 = \{ \ldots, -8, -2, 4, 10, 16, \ldots\} = \{a \in \mathbf{Z} / \ a = 6k + 4, \text{ con } k \in \mathbf{Z}\}$

$[5]_6 = \{ \ldots, -7, -1, 5, 11, 17, \ldots\} = \{a \in \mathbf{Z} / \ a = 6k + 5, \text{ con } k \in \mathbf{Z}\}$

RELACIONES DE EQUIVALENCIA

Una relación R en un conjunto A es una **relación de equivalencia** si es reflexiva, simétrica y transitiva.

Dado $a \in A$, se llama **clase de a** al conjunto $[a]=\{b \in A \,/\, bRa\}$

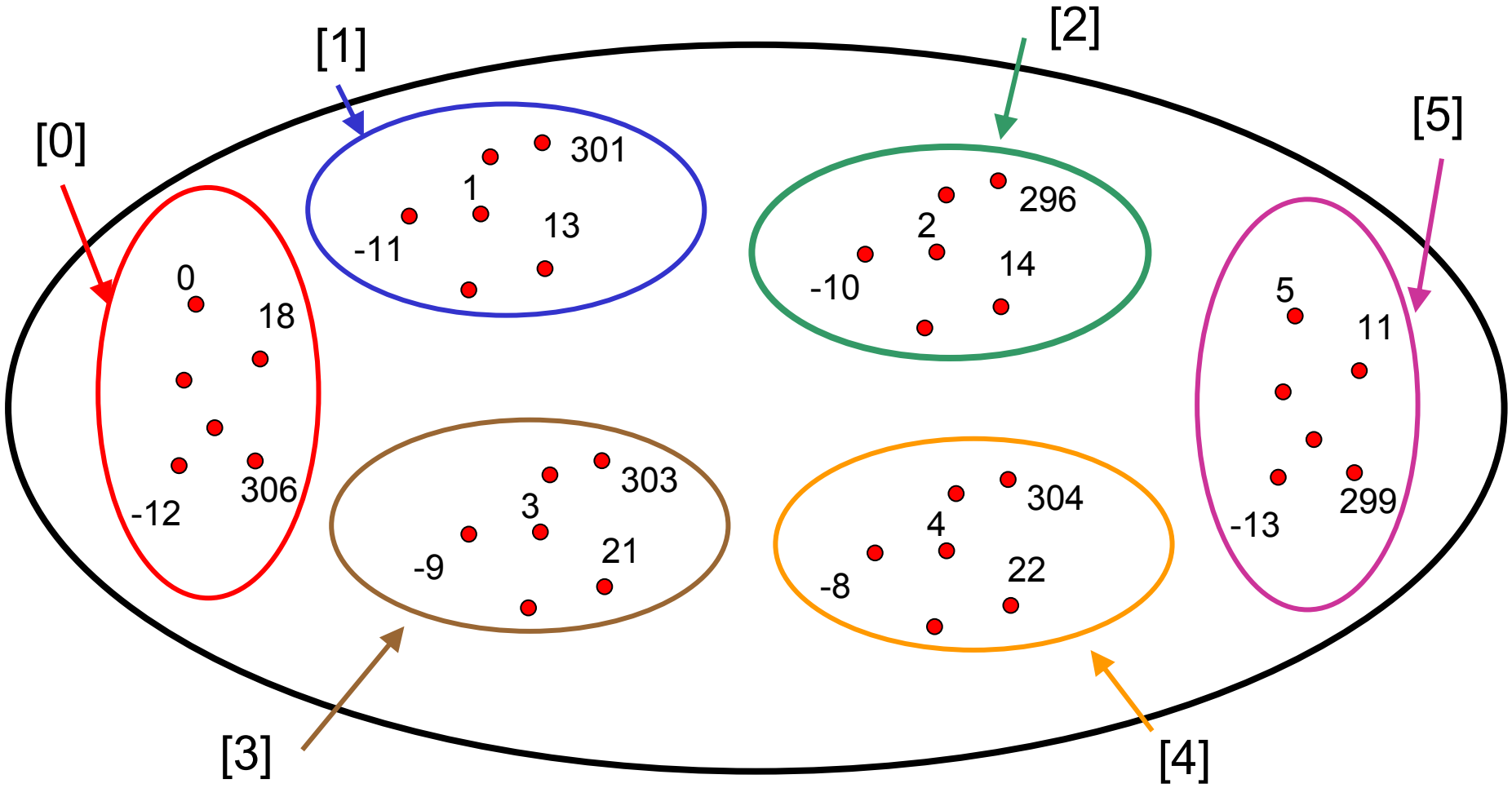
Cualquier elemento de [a] es un representante de la clase.

Conjunto cociente de A respecto de R es el conjunto formado por las clases de equivalencia,

$$A/R = \{[a] \,/\, a \in A\}$$

CONGRUENCIAS EN **Z** **(Ejemplo módulo 6)**

Dados $a,b \in \mathbf{Z}$ decimos que **a** y **b** son **congruentes módulo 6** si $6 \mid (a - b)$. Se indica por $a \equiv b \pmod 6$



Propiedades

3. Al conjunto cociente de **Z** respecto de la relación de **congruencia** módulo **m** se le designa por $\mathbf{Z_m}$

4. La clase de $x \in \mathbf{Z}$ módulo **m** se designa por $[x]_m$, x_m ó $\bar{x}$
5. $\mathbf{Z_m}=\{[0]_m, [1]_m ,..., [m-1]_m\}$, donde $[k]_m=\{ a \in \mathbf{Z} \mid a \equiv k \pmod m \}$

6. La congruencia módulo m es compatible con la suma y el producto de **Z**,

   si $a \equiv b \pmod m$ y $c \equiv d \pmod m$ entonces se tiene que

   $a+c \equiv b+d \pmod m$ y $ac \equiv bd \pmod m$

$a \equiv b \pmod m \quad \Rightarrow \quad a - b = km$

$c \equiv d \pmod m \quad \Rightarrow \quad c - d = hm$

$(a + c) - (b + d) = (k - h)m \quad \Rightarrow \quad a+c \equiv b+d \pmod m$

Propiedades

3. Al conjunto cociente de **Z** respecto de la relación de **congruencia** módulo **m** se le designa por $\mathbf{Z_m}$

4. La clase de $x \in \mathbf{Z}$ módulo **m** se designa por $[x]_m$, x_m ó $\bar{x}$
5. $\mathbf{Z_m}=\{[0]_m, [1]_m, ..., [m-1]_m\}$, donde $[k]_m=\{ a \in \mathbf{Z} \mid a \equiv k \pmod m \}$

6. La congruencia módulo m es compatible con la suma y el producto de **Z**,

   si $a \equiv b \pmod m$ y $c \equiv d \pmod m$ entonces se tiene que

   $a+c \equiv b+d \pmod m$ y $ac \equiv bd \pmod m$

$$a \equiv b \pmod m \Rightarrow a - b = km \Rightarrow ac - bc = kcm$$

$$c \equiv d \pmod m \Rightarrow c - d = hm \Rightarrow bc - bd = bhm$$

$$(ac - bd) = (kc + bh)m \Rightarrow ac \equiv bd \pmod m$$

Propiedades

7. Simplificación

$6 \cdot 2 \equiv 4 \cdot 2 \pmod 4$ pero $6 \not\equiv 4 \pmod 4$

Si $ac \equiv bc \pmod m$ entonces $a \equiv b \left(\mod \left(\frac{m}{mcd(c,m)}\right)\right)$

Sea $d = mcd(c,m)$, así $c = c'd$, $m = m'd$ con $mcd(c',m') = 1$

$ac - bc = km \Rightarrow ac'd - bc'd = km'd \Rightarrow ac' - bc' = km'$

Luego, $m' \mid (a - b)c'$ y como $mcd(c',m') = 1$ resulta que

$m' \mid (a - b)$ es decir, $a \equiv b \left(\mod \left(\frac{m}{mcd(c,m)}\right)\right)$

Propiedades

8. Criterios de divisibilidad

Teorema

Si $P(x)$ es un polinomio con coeficientes en Z entonces

$a \equiv b \pmod m \quad \Rightarrow \quad P(a) \equiv P(b) \pmod m$

Si $n = a_k a_{k-1} \ldots a_1 a_0$ es la expresión decimal de n, entonces

$n = a_k 10^k + a_{n-1} 10^{k-1} + \ldots + a_1 10 + a_0 = P(10)$

para el polinomio $P(x) = a_k x^k + a_{n-1} x^{k-1} + \ldots + a_1 x + a_0$

Criterio de divisibilidad por 9

Como $10 \equiv 1 \pmod 9$ por el teorema se tiene que

$n = P(10) \equiv P(1) = a_k + a_{n-1} + \ldots + a_1 + a_0 \pmod 9$

Luego, n es múltiplo de 9 $\Leftrightarrow$ $n \equiv 0 \pmod 9$ $\Leftrightarrow$ $P(1) \equiv 0 \pmod 9$

Es decir, n es divisible por 9 si lo es la suma de sus cifras.

Propiedades

8. **Criterios de divisibilidad**

Criterio de divisibilidad por 11

Como $10 \equiv -1 \pmod{11}$ por el teorema se tiene que

$$n = P(10) \equiv P(-1) = a_0 - a_1 + a_2 + \ldots + (-1)^k a_k \pmod{11}$$

Es decir, n es divisible por 11 si lo es la suma alternada de sus cifras.

Criterio de divisibilidad por 7

Como $10 \equiv 3 \pmod{7}$ por el teorema se tiene que

$$n = P(10) \equiv P(3) = a_0 + 3a_1 + 3^2 a_2 + \ldots + 3^k a_k \pmod{7} =$$
$$= a_0 + 3a_1 + 2a_2 + 6a_3 + 4a_4 + 5a_5 + \ldots \pmod{7} =$$
$$= a_0 + 3a_1 + 2a_2 - a_3 - 3a_4 - 2a_5 + \ldots \pmod{7}$$

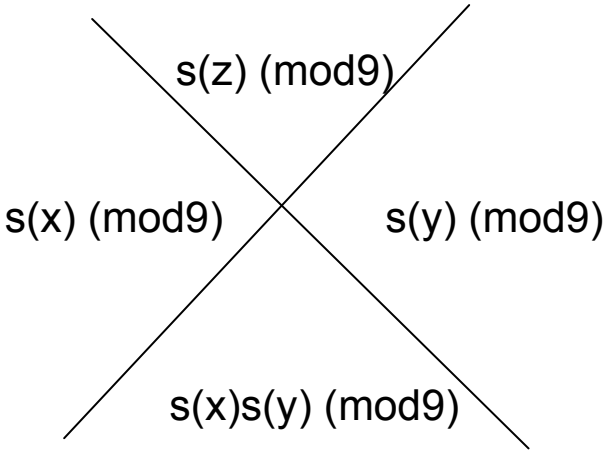
Es decir, n es divisible por 7 si lo es la suma indicada.

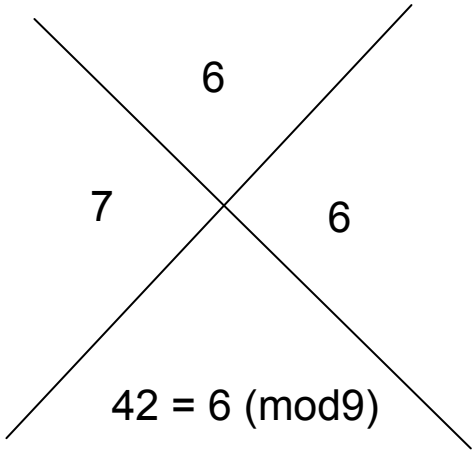
Propiedades

9. **Regla de los nueves** $x \equiv s(x) \pmod 9$

Si $xy = z$ entonces $s(x)s(y) \equiv s(z) \pmod 9$

$34108 \cdot 726 = 24762408$





~~$34108 \cdot 726 = 24762418$~~

~~$34108 \cdot 726 = 24762417$~~

Exponenciación con aritmética modular

Calcular $13^{46} \pmod{22}$

Operaremos siempre con números menores que 22

46 en base 2 es 101110_2 porque $46 = 32 + 8 + 4 + 2$

Por tanto $13^{46} = 13^{32} \cdot 13^{8} \cdot 13^{4} \cdot 13^{2}$

Calculemos: $13^2 = 169 = 15 \pmod{22}$

$13^4 = 15 \cdot 15 = 5 \pmod{22}$

$13^8 = 13^4 \cdot 13^4 = 5 \cdot 5 = 3 \pmod{22}$

$13^{16} = 13^8 \cdot 13^8 = 3 \cdot 3 = 9 \pmod{22}$

$13^{32} = 13^{16} \cdot 13^{16} = 9 \cdot 9 = 15 \pmod{22}$

Así $13^{46} = 15 \cdot 3 \cdot 5 \cdot 15 = 9 \pmod{22}$

Aritmética en Z_m $(Z_m, +, \cdot)$

$\bar{a} + \bar{c}$ = clase de a + c en Z_m

$\bar{a} \cdot \bar{c}$ = clase de $a \cdot c$ en Z_m

Las operaciones están bien definidas porque la congruencia es compatible con la suma y el producto

Simplificación

- Si ac = bc en Z_m entonces a = b en $Z_{m/mcd(m,c)}$

Adición y multiplicación en $\mathbb{Z}_5$:

$+$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$\times$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Adición y multiplicación en $\mathbb{Z}_6$:

$+$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

$\times$	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

Aritmética en Z_m $(Z_m, +, \cdot)$

$\overline{a} + \overline{c}$ = clase de a + c en Z_m

$\overline{a} \cdot \overline{c}$ = clase de $a \cdot c$ en Z_m

Divisores de cero

En Z_{12}, $\overline{3} \cdot \overline{4} = \overline{0}$, $\overline{2} \cdot \overline{6} = \overline{0}$

- Si m no es primo, en Z_m hay divisores de 0, es decir, existen a, b tales que $a \cdot b = 0$ en Z_m
- a es divisor de 0 $\Leftrightarrow$ mcd (a,m) $\neq 1$

Si mcd (a,m) = 1 y existe b tal que ab = 0 entonces ab = km luego a| ab =km y resulta a|k Así k = ak', luego ab = ak'm de donde b = k'm es decir, b = 0 en Z_m

Aritmética en Z_m $(Z_m, +, \cdot)$

$\overline{a} + \overline{c}$ = clase de a + c en Z_m

$\overline{a} \cdot \overline{c}$ = clase de $a \cdot c$ en Z_m

Divisores de cero

En Z_{12}, $\overline{3} \cdot \overline{4} = \overline{0}$, $\overline{2} \cdot \overline{6} = \overline{0}$

- Si m no es primo, en Z_m hay divisores de 0, es decir, existen a, b tales que $a \cdot b = 0$ en Z_m
- a es divisor de 0 $\Leftrightarrow$ mcd (a,m) $\neq 1$

Si mcd (a,m) = d $\neq 1$ entonces a = a'd, m = m'd, luego b=m' es tal que $a \cdot b = a'dm' = a'm = 0$ en Z_m

Aritmética en Z_m $(Z_m, +, \cdot)$

Elementos inversibles (divisores de 1 o unidades)

En Z_7, $\overline{2} \cdot \overline{4} = \overline{1}$, en Z_{15}, $\overline{2} \cdot \overline{8} = \overline{1}$, $\overline{4} \cdot \overline{4} = \overline{1}$

- Un elemento **a** $\in$ $\mathbf{Z_m}$ es **inversible** si existe **b** $\in$ $\mathbf{Z_m}$ tal que ab =1 en $\mathbf{Z_m}$. Es decir, $ab \equiv 1 \pmod m$
  Decimos que b es el inverso de a, $a^{-1} = b$

- x es inversible en $\mathbf{Z_m}$ $\Leftrightarrow$ mcd (x,m)= 1

x es inversible en $\mathbf{Z_m}$ $\Leftrightarrow$ existe b tal que $xb \equiv 1 \pmod m$
$\Leftrightarrow$ existen b y k tales que $xb - 1 = km$ $(xb - km = 1)$
$\Leftrightarrow$ mcd (x,m) = 1

Aritmética en Z_m

Elementos inversibles (divisores de 1 o unidades)

$\mathbf{U_m}$ conjunto de los elementos inversibles o unidades de $\mathbf{Z_m}$

Si a,b son inversibles entonces ab y a^{-1} son inversibles.
El inverso de ab es $a^{-1}b^{-1}$
El inverso de a^{-1} es a

$$\mathbf{U_n} = \{ x \in \mathbf{N} \mid 1 \leq x \leq n \text{ , } mcd\ (x,n)=1\}$$

El cardinal de este conjunto se designa $\Phi\mathbf{(n)}$ **Función de Euler**

$$\Phi\mathbf{(n)} = |\mathbf{U_n}|$$

Función de Euler

$\Phi(n) = |\{ x \in N \mid 1 \le x \le n , \text{mcd}(x,n) = 1\}|$

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

Contemos los elementos NO primos con p
Son $\{p, 2p, 3p, \ldots , p^{r-1}p\}$

- Si m=ab y m.c.d.(a,b)=1 entonces $\Phi(m) = \Phi(a)\,\Phi(b)$

Lema. El número de elementos primos con a en una progresión aritmética de a términos y razón b, con mcd(a,b)=1, es $\Phi(a)$

- Si $n = p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k} \Longrightarrow \Phi(n) = n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_k}\right)$

Teorema de Euler

Si $\bar{a} \in U_m$ entonces $\bar{a}^{\Phi(m)} = \bar{1}$ en $\mathbf{Z_m}$,

es decir, si mcd(a,m) = 1 entonces $a^{\Phi(m)} \equiv 1 \pmod{m}$

Lema
Si $a \in U_m$ entonces $aU_m = U_m$

Si $z \in U_m$ entonces $z = a(a^{-1}z) \in aU_m$

Si $z \in aU_m$ entonces $z = ay$ con $y \in U_m$, luego $z \in U_m$

Teorema de Euler

Si $\bar{a} \in U_m$ entonces $\bar{a}^{\Phi(m)} = \bar{1}$ en $\mathbf{Z_m}$,

es decir, si mcd(a,m) = 1 entonces $a^{\Phi(m)} \equiv 1 \pmod m$

Dem. (teorema)

Sea u el producto $u = x_1 x_2 \cdot \ldots \cdot x_k$ de los elementos de U_m $(k=\Phi(m))$

Como $aU_m = U_m$ los elementos $ax_1, ax_2, \ldots, ax_k$ son una reordenación de los elementos $x_1, x_2, \ldots, x_k$

Por tanto, $u = x_1 x_2 \cdot \ldots \cdot x_k = ax_1\, ax_2 \cdot \ldots \cdot ax_k = a^{\Phi(m)} u$

Y así, como $u \in U_m$ resulta $a^{\Phi(m)} = 1$

Corolarios

1. Teorema de Fermat

Si p es primo y p no es divisor de a entonces $a^{p-1} \equiv 1 (\text{mod } p)$

2. Las últimas cifras de a y a^5 coinciden

Si p es primo entonces $a^p \equiv a \pmod p$

Si p es divisor de a entonces $a^p \equiv a \equiv 0 \pmod p$

Si p no divisor de a, por Fermat, $a^p \equiv a \pmod p$

Así para p=5, $a^5 - a$ es múltiplo de 5

Y también de 2 porque en $a^5 - a = a(a-1)(a+1)(a^2+1)$ siempre hay un factor par

Teorema de Fermat

Si p es primo y p no es divisor de a entonces $a^{p-1} \equiv 1 (\mathrm{mod}\ p)$

Observación:
El recíproco NO es cierto

$2^{340} \equiv 1 (\mathrm{mod}\ 341)$ pero 341 NO es primo, $341 = 31 \cdot 11$

341 es pseudoprimo en base 2

Números de Carmichael

Son los números compuestos n tales que $a^{n-1} \equiv 1 (\mathrm{mod}\ n)$ para todo a primo con n
Son los pseudoprimos en cualquier base

$b^{560} \equiv 1 (\mathrm{mod}\ 561)$ para todo b tal que $\mathrm{mcd}(b, 561) = 1$

$561 = 3 \cdot 11 \cdot 17$

ECUACIONES EN CONGRUENCIAS		ECUACIONES EN Z_m
$2x \equiv 5 \pmod 7$	Solución única	$2x = 5$ en Z_7
$2x \equiv 5 \pmod 6$	No hay solución	$2x = 5$ en Z_6
$2x \equiv 4 \pmod 6$	Más de una solución	$2x = 4$ en Z_6

La ecuación lineal $ax \equiv b \pmod m$ tiene solución en **x** si y sólo $ax - b$ es múltiplo de m, es decir, si la ecuación diofántica $ax + my = b$ tiene solución

La ecuación lineal $ax \equiv b \pmod m$ tiene solución en **x**
$\Leftrightarrow$ $mcd(a,m) \mid b$

La ecuación lineal $ax = b$ en Z_m tiene solución en **x**
$\Leftrightarrow$ $mcd(a,m) \mid b$

ECUACIONES EN CONGRUENCIAS

Resolver la ecuación $12x \equiv 9 \pmod{21}$

Tiene solución porque $\text{mcd}(12, 21) = 3 \mid 9$
Debemos resolver la ecuación diofántica $12x + 21y = 9$

Dividimos por mcd(12,21)=3, $4x + 7y = 3$

Una solución de $4x + 7y = 1$ es $x=2,\ y = -1$

Una solución de $4x + 7y = 3$ (y de la congruencia dada) es **x=6**

Y todas las soluciones (en x) de la ecuación diofántica $12x + 21y = 9$ son de la forma:

$$x = 6 + 7t$$

Las soluciones de la congruencia $12x \equiv 9 \pmod{21}$ son:

$6,\ 6+7=13,\ 6+2\cdot 7=20$

$\boxed{6,\ 13,\ 20}$

Nº de soluciones
3 = mcd(12,21)

ECUACIONES EN CONGRUENCIAS

Resolver la ecuación $5x \equiv 15 \pmod{20}$

Tiene solución porque $\text{mcd}(5, 20) = 5 \mid 15$
Una solución de la congruencia dada es **$x = 3$**

Y todas las soluciones (en x) de la ecuación diofántica $5x + 20y = 15$ son de la forma:

$$x = 3 + 4t$$

Las soluciones de la congruencia $5x \equiv 15 \pmod{20}$ son:

$3,\ 3+4,\ 3+4\cdot 2,\ 3+4\cdot 3,\ 3+4\cdot 4$

$3,\ 7,\ 11,\ 15,\ 19$

Nº de soluciones
$5 = \text{mcd}(5,20)$

ECUACIONES EN CONGRUENCIAS

Resolver la ecuación $ax \equiv b \pmod{m}$

Tiene solución si $\text{mcd}(a, m) = d \mid b$

Encontramos una solución $\mathbf{x_1}$ de la congruencia dada (o de la ecuación diofántica $ax + by = m$)

Las soluciones de la congruencia $ax \equiv b \pmod{m}$ son:

$$x = x_1 + \frac{m}{d}t, \qquad t = 0,1,2,\ldots,d-1$$

Nº de soluciones
d = mcd(a,m)

ECUACIONES EN CONGRUENCIAS

Resolver la ecuación $ax \equiv b \pmod m$ $\quad\quad$ $\mathrm{mcd}(a, m) = d \mid b$

$$x = x_1 + \frac{m}{d}t, \qquad t = 0,1, 2, \ldots, d-1$$

Comprobemos que cada uno de estos valores es solución
Como d=mcd(a,m) será a=a'd, m=m´d con mcd(a',m')=1

$$a(x_1 + \frac{km}{d}) \equiv ax + \frac{akm}{d} \equiv b + a'km \equiv b \pmod m$$

Veamos ahora que cualquier otra solución s es de esa forma
Si s y z son soluciones será $as \equiv b \pmod m$, $az \equiv b \pmod m$
luego $a(s-z) \equiv 0 \pmod m$.

$a(s-z) = km \Rightarrow a'd(s-z) = km'd \Rightarrow a'(s-z) = km'$

pero mcd(a',m')=1 luego m' | (s–z) $\Rightarrow s-z = tm' \Rightarrow s = z + \frac{m}{d}t$

SISTEMAS DE CONGRUENCIAS

Sun Zu (siglo I)

$$\begin{cases} x \equiv 2 \pmod 3 \\ x \equiv 3 \pmod 5 \\ x \equiv 5 \pmod 7 \end{cases}$$

Teorema chino del resto

Si m_1 , m_2 ,..., m_n son primos entre sí dos a dos, entonces el sistema de congruencias

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ \ldots\ldots\ldots\ldots \\ x \equiv a_n \pmod{m_n} \end{cases}$$

tiene solución única en $Z_{m_1 m_2 \ldots m_n}$

SISTEMAS DE CONGRUENCIAS

Teorema chino del resto

Si m_1 , m_2 ,..., m_n son primos entre sí dos a dos, entonces el sistema de congruencias

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ \ldots\ldots\ldots\ldots \\ x \equiv a_n \pmod{m_n} \end{cases}$$ tiene solución única en $\mathbb{Z}_{m_1 m_2 \ldots m_n}$

Dem.: Sean $m = m_1 \cdot \ldots \cdot m_n$ y $M_k = m_1 \cdot \ldots \cdot \overline{m}_k \cdot \ldots \cdot m_n$

$\mathrm{mcd}(m_k, M_k)=1$, luego existe b_k tal que $M_k b_k \equiv 1 \pmod{m_k}$

$M_k b_k \equiv 0 \pmod{m_j}$ $j \neq k$

$x = a_1 M_1 b_1 + a_2 M_2 b_2 + \ldots + a_n M_n b_n$ es solución

Si x, y son soluciones entonces $x \equiv a_j \pmod{m_j}$ $y \equiv a_j \pmod{m_j}$

luego $x - y$ múltiplo de m_j $\forall j$, es decir, $x - y$ es múltiplo de m

SISTEMAS DE CONGRUENCIAS

Teorema chino del resto (Enunciado general)

El sistema de congruencias

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ \cdots\cdots\cdots\cdots \\ x \equiv a_n \pmod{m_n} \end{cases}$$

tiene solución si para cada par i,j $\quad \mathrm{mcd}(m_i, m_j) \mid a_i - a_j$

En ese caso la solución es única módulo $\mathrm{mcm}(m_1 \cdot m_2 \cdot \ldots \cdot m_n)$

$$\begin{cases} 120\,x \equiv 180 \pmod{450} \\ 24\,x \equiv 76 \pmod{100} \end{cases}$$

No se puede aplicar el teorema

Simplificamos y resolvemos por sustitución

Si $ac \equiv bc \pmod{m}$ entonces $a \equiv b \left(\mathrm{mod}\left(\frac{m}{mcd(c,m)}\right)\right)$

$$\left.\begin{array}{l} 120x \equiv 180 \pmod{450} \\ 24x \equiv 76 \pmod{100} \end{array}\right\} \Rightarrow \left.\begin{array}{l} 2\cdot 60x \equiv 3\cdot 60 \pmod{450} \\ 6\cdot 4x \equiv 19\cdot 4 \pmod{100} \end{array}\right\} \Rightarrow \left.\begin{array}{l} 2x \equiv 3 \pmod{15} \\ 6x \equiv 19 \pmod{25} \end{array}\right\}$$

Resolvemos la primera ecuación (mult. por 8, inverso de 2 (mod 15))

$x \equiv 24 \pmod{15} \equiv 9 \pmod{15}$, es decir **x = 9 +15 k**

Sustituimos en la segunda ecuación

$6(9 + 15k) \equiv 19 \pmod{25} \Rightarrow 4 + 15k \equiv 19 \pmod{25} \Rightarrow 15k \equiv 15 \pmod{25}$

Es decir, $k \equiv 1 \pmod{5}$, luego $k = 1 + 5t$, sustituyendo en **x**

$x = 9 + 15(1+5t) = 24 + 75t$

$x \equiv 24 \pmod{75}$

Polinomios con coeficientes en Z_m

Algunas diferencias con Z

- grado(f(x)g(x)) ≤ grado(f(x)) + grado(g(x))
  En $Z_8[x]$ $(2x^3 + 5x)(4x + 3) = 6x^3 + 4x^2 + 7x$

- Un polinomio puede tener más raíces que su grado
  En $Z_6[x]$ $x^2 + 3x + 2$ tiene 4 raíces

Resolver las ecuaciones $x^2 + 3x + 4 = 0$ y $x^2 - x - 1 = 0$ en Z_{11}