Tuplas, Producto Cartesiano, Relaciones

- Una n-tupla ordenada es una secuencia de n elementos, escrita en la forma $(x_1,\ldots,x_n)$.
- Nótese que a diferencia de los conjuntos, donde $\{1,2\}=\{2,1\}$, en una n-tupla el orden sí importa.
- Por lo tanto, la única forma de que $(x_1,\ldots,x_n)= (y_1,\ldots,y_n)$ es que $x_1=y_1,\ldots,x_n=y_n$.
- El producto cartesiano de n conjuntos $A_1,\ldots,A_n$ es el conjunto formado por las n-tuplas de la forma $(x_1,\ldots,x_n)$, donde $x_i \in A_i$, $1 \le i \le n$:

$$A_1 \times A_2 \times \cdots \times A_n = \{(x_1,\ldots,x_n) : x_i \in A_i \forall 1 \le i \le n\}$$

Un caso de particular interés es el producto cartesiano de sólo dos conjuntos: $A \times B$.
Una "relación" es un subconjunto $R \subseteq A \times B$.
Nótese que:

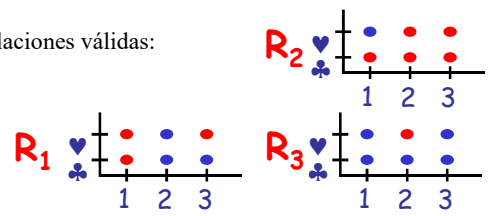
- no necesariamente A=B
- cualquier subconjunto $R \subseteq A \times B$ es válido

Con $A=\{1,2,3\}$,$B=\{\clubsuit,\heartsuit\}$, las siguientes son todas relaciones válidas:

$R_1=\{(1,\clubsuit),(1,\heartsuit),(3,\heartsuit)\}$

$R_2=A\times B \setminus \{(1,\heartsuit)\}$

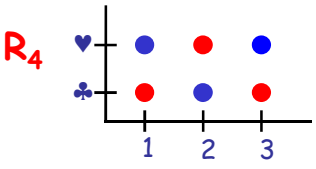
$R_3=\{(2,\heartsuit)\}$

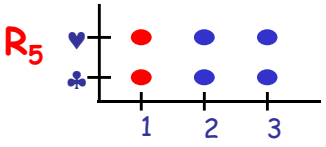


Relaciones: funciones

Un caso aún más particular son las funciones: son relaciones en que para cada $x \in A$, existe un único $y \in B$ tal que $(x,y) \in R$; así, se define una función de A en B.

Las tres relaciones en la transparencia anterior son *contraejemplos* : no son funciones. En cambio, R_4 (a la derecha) sí lo es.





¿Qué hay de R_5, a la izquierda? No es una función, porque estamos viéndolas como subconjuntos de $A\times B$. Pero en este caso si la "trasponemos", y la vemos como subconjunto de $B\times A$, entonces sí es una función... de B en A.

Relaciones: notación, propiedades

- Cuando una relación $R \subseteq A \times B$ es una función, y se tiene $(x , y) \in R$, solemos escribir $R(x)=y$. Por ejemplo, $R_4(1)=\clubsuit$.

- En el caso general (en que R es una relación cualquiera), cuando $(x , y) \in R$ se suele escribir $x \, R \, y$.

NOTA: En lo que sigue, consideraremos relaciones dentro de un mismo conjunto: A=B, y le llamaremos "S" (o sea, A=B=S). Anotamos $S^2 = S \times S$.

- Decimos que una relación $R \subseteq S^2$ es:
  - *Refleja:* si para todo $a \in S$, $(a , a) \in R$ [o sea, $a \, R \, a$].
  - *Transitiva:* si cada vez que $a \, R \, b$ y $b \, R \, c$, se tiene además $a \, R \, c$.
  - *Simétrica:* si $a \, R \, b \Leftrightarrow b \, R \, a$
  - *Antisimétrica:* si cada vez que $a \, R \, b$ y $b \, R \, a$, necesariamente $a = b$.
  - *Total:* para cualesquiera $a , b \in S$, se tiene que $a \, R \, b$ o bien $b \, R \, a$ (o ambas).

Relaciones: orden

Una *relación de orden parcial* cumple con ser refleja, transitiva y antisimétrica.

- Ejemplo: Sea A un conjunto finito, S=P(A) [el conjunto potencia de A], y R definida por $R = \{ (B,C): B,C \subseteq A \text{ y } B \subseteq C \}$ (es decir: es la relación de inclusión entre subconjuntos de A).

NOTA: esto es lo que se llama un orden "no estricto". En los órdenes *estrictos*, como "<" y "$\subset$", se prohíbe la igualdad, exigiendo que la relación sea antirrefleja: $(a , a) \notin R$ para ningún a.

Si además es total, entonces *es una relación de orden total*.

El ejemplo anterior es un caso de orden parcial que no es total.
Para ver por qué, consideremos $A=\{1,2\}$, $B=\{1\}$, $C=\{2\}$. Claramente, ni B está incluido en C, ni C está incluido en B.

Consideremos S=Z (los números enteros), y la relación $\leq$ habitual. Ese sí es un caso de relación de orden total.

Relaciones: equivalencia

Una *relación de equivalencia* cumple con ser refleja, transitiva y simétrica.

- Ejemplo: Sean **Z** los números enteros, y sea $m \in \mathbf{N}$, $m \neq 0$. Definiremos la relación R_m (ojo, depende del m) como $a \, R_m \, b \Leftrightarrow a \bmod m = b \bmod m$

[donde a mod m es el resto de dividir a por m]

Relaciones: equivalencia

Sea R una relación de equivalencia en S.

- Para cada elemento $a \in S$, definimos su *clase de equivalencia* $[a]=\{ b \in S: aRb \}$.
- El conjunto de las clases de equivalencia forma una partición de S. En efecto:
  - Todo elemento pertenece a alguna clase de equivalencia (la suya!).
  - La intersección entre dos clases de equivalencia distintas es vacía: si $c \in [a] \cap [b] \Rightarrow c \in [a]$ y $c \in [b] \Rightarrow$ cRa y cRb $\Rightarrow$ aRc y cRb (por simetría) $\Rightarrow$ aRb (por transitividad) $\Rightarrow [a]=[b]$.

Relaciones: equivalencia

•Ejemplo: consideremos ($\mathbf{Z}$,R_3), con la relación de "igualdad módulo 3" definida antes. Entonces

[0] = { ..., -6, -3, 0, 3, 6, 9,... }
[1] = { ..., -5, -2, 1, 4, 7, ... }
[2] = { ..., -4, -1, 2, 5, 8, 10, ... }

Al conjunto de clases de equivalencia (conjunto "cociente") lo anotamos S/R. En este caso,

$\mathbf{Z}/R_3$ = { [0], [1], [2] }

Naturalmente, en un mismo conjunto puede definirse más de una relación de equivalencia, y cada una dará una partición distinta.

Relaciones: equivalencia

•Ejemplo: Sea S una baraja de naipes [inglés],

S={ 1♠, 2♠, ..., K♠, 1♥, 2♥, ..., K♥,
1♣, 2♣,..., K♣, 1♦, 2♦, ..., K♦}

y consideremos las relaciones

R_p : si dos naipes son de la misma pinta
R_n : si dos naipes son del mismo número
R_c : si dos naipes son del mismo color
R_2 : si el número de dos naipes tiene la misma paridad.

Relaciones: equivalencia

Nota:

La relación entre relaciones de equivalencia y particiones es recíproca: dada una partición de un conjunto, siempre podemos definir una relación de equivalencia (según si los elementos quedan juntos o no) cuyas clases de equivalencias correspondan a esa partición.

congruencias

- Concepto de congruencia:
  - Sean dos números enteros **a** y **b**: se dice que **a** es congruente con **b** en el módulo o cuerpo **n** (Z_n) si y sólo si existe algún entero **k** que divide de forma exacta la diferencia (a - b) .
  - Esto podemos expresarlo así:

$$a - b = k * n$$

$$a \equiv_n b$$

$$a \equiv b \bmod n$$

CONGRUENCIA MODULO n

Sea n ∈ N. Definimos en Z^2 la relación "congruencia módulo n", como sigue:

$\forall a,b \in Z$: $a \equiv b \pmod n \Leftrightarrow n \mid a - b$

Ejemplos:

$73 \equiv 88 \pmod 3$ porque $73 - 88 = -15 \wedge 3 \mid -15$

$120 \equiv -45 \pmod 5$ pues $120 - (-45) = 165 \wedge 5 \mid 165$

Operaciones de congruencia en Z_n

¿Es 18 congruente con 3 módulo 5?

¿$18 \equiv 3 \bmod 5$?

Sí, porque: $18-3 = 15 = k*5$ con $k = 3$

Esta operación en Z_n se expresará así:

$18 \bmod 5 = 3$

El valor 3 será el **resto** o residuo.

Propiedades de la congruencia en Z_n

- Propiedad Reflexiva:

  $a \equiv a \bmod n \quad \forall\, a \in Z$

- Propiedad Simétrica:

  $a \equiv b \bmod n \Rightarrow b \equiv a \bmod n \quad \forall\, a,b \in Z$

- Propiedad Transitiva:

  Si $a \equiv b \bmod n$ y $b \equiv c \bmod n$

  $\Rightarrow a \equiv c \bmod n \quad \forall\, a,b,c \in Z$

Propiedades de las operaciones en Z_n

- **Propiedad Asociativa:**

  $a + (b + c) \bmod n \equiv (a + b) + c \bmod n$

- **Propiedad Conmutativa:**

  $a + b \bmod n \equiv b + a \bmod n$

  $a * b \bmod n \equiv b * a \bmod n$

- **Propiedad Distributiva:**

  $a * (b+c) \bmod n \equiv ((a * b) + (a * c)) \bmod n$

- **Existencia de Identidad:**

  $a + 0 \bmod n = 0 + a \bmod n = a \bmod n = a$

  $a * 1 \bmod n = 1 * a \bmod n = a \bmod n = a$

- **Existencia de Inversos:**

  $a + (-a) \bmod n = 0$

  $a * (a^{-1}) \bmod n = 1$ (si $a \neq 0$)

- **Reducibilidad:**

  $(a + b) \bmod n = [(a \bmod n) + (b \bmod n)] \bmod n$

  $(a * b) \bmod n = [(a \bmod n) * (b \bmod n)] \bmod n$

Conjunto completo de restos CCR

Para cualquier entero positivo n, el conjunto completo de restos será CCR = {0, 1, 2, ... n-1}, es decir:

$\forall a \in Z \quad \exists ! r_i \in CCR / a \equiv r_i \bmod n$

- CCR (11) = {0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10}
- CCR (6) = {0, 1, 2, 3, 4, 5} = {12, 7, 20, 9, 16, 35}
- El segundo conjunto es equivalente: 12 → 0, 7 → 1...
- Normalmente se trabajará en la zona canónica: 0 – n-1

Un ejemplo de homomorfismo

88 * 93 mod 13

8.184 mod 13

Resultado: 7

Se desbordaría la memoria de nuestro sistema ☹

Ahora ya no se desborda la memoria ☺

☜ Ejemplo: una calculadora capaz de trabajar sólo con tres dígitos ...

Solución por homomorfismo:

88 * 93 mod 13

[(88) mod 13 * (93) mod 13] mod 13

10 * 2 mod 13

20 mod 13 Resultado: 7

se llega a lo mismo, pero...

... y hemos usado siempre números de 3 dígitos. En este caso la operación máxima sería 12*12 = 144, es decir tres dígitos.

RESTOS POTENCIALES

Son los diferentes residuos positivos que se obtienen de analizar las potencias consecutivas de un número entero positivo mayor que la unidad con respecto a cierto módulo (divisor)

Esquema

$$a^n = r_n \pmod{b}$$

Donde:

n : 0; 1; 2;…
b : módulo
a $\in \mathbb{Z}^+ > 1$

Restos potenciales de las potencias de 3, con respecto al módulo 5

$3^n \equiv r^n \pmod 5$

$3^0 \equiv 1 \pmod 5$	$3^4 \equiv 1 \pmod 5$	$3^8 \equiv 1 \pmod 5$
$3^1 \equiv 3 \pmod 5$	$3^5 \equiv 3 \pmod 5$	$3^9 \equiv 3 \pmod 5$
$3^2 \equiv 4 \pmod 5$	$3^6 \equiv 4 \pmod 5$	$3^{10} \equiv 4 \pmod 5$
$3^3 \equiv 2 \pmod 5$	$3^7 \equiv 2 \pmod 5$	$3^{11} \equiv 2 \pmod 5$

los residuos 1; 3; 4 y 2 se repiten periódicamente.

GAUSSIANO(G)
Se llama así a la menor cantidad de restos diferentes posibles que forman el período.
Del ejemplo anterior: Gaussiano = g = 4

se puede observar:

$3^0 \equiv 1 \pmod 5$	$3^4 \equiv 1 \pmod 5$	$3^8 \equiv 1 \pmod 5$	$3^{4k} \equiv 1 \pmod 5$
$3^1 \equiv 3 \pmod 5$	$3^5 \equiv 3 \pmod 5$	$3^9 \equiv 3 \pmod 5$	$3^{4k+1} \equiv 3 \pmod 5$
$3^2 \equiv 4 \pmod 5$	$3^6 \equiv 4 \pmod 5$	$3^{10} \equiv 4 \pmod 5$	$3^{4k+2} \equiv 4 \pmod 5$
$3^3 \equiv 2 \pmod 5$	$3^7 \equiv 2 \pmod 5$	$3^{11} \equiv 2 \pmod 5$	$3^{4k+3} \equiv 2 \pmod 5$

RESTOS POTENCIALES

DE UNA BASE *a* RESPECTO DEL MÓDULO *m*

Son los restos de las divisiones entre *m* de las sucesivas potencias de $a \in N$

con $a \geq 2$, $a^0 \equiv r_0 = 1 \pmod m$; $a^1 \equiv r_1 \pmod m$; $a^2 \equiv r_2 \pmod m$; …; $a^n \equiv r_n \pmod m$;

El número de restos diferentes es menor o igual que *m-1* , por lo que se llegarán a repetir de forma periódica.

Para su cálculo es útil la propiedad: $a^k \equiv r_k \pmod m \Rightarrow a^{k+1} = a^k * a \equiv r_k * a \pmod m$

CRITERIO GENERAL DE DIVISIBILIDAD

Un número natural N que escrito en el sistema de base *a* se puede poner en la forma

$c_n a^n + c_{n-1}a^{n-1} + \ldots + c_1 a + c_0$ será divisible por *m* si y solo si $c_n r_n + c_{n-1}r_{n-1} + \ldots + c_1 r_1 + c_0$ es múltiplo de *m,* siendo $r_1, r_2, \ldots, r_n$ los restos potenciales de la base *a* respecto del módulo *m*.

Los criterios de divisibilidad más conocidos corresponden al sistema decimal (caso a=10).

Podemos deducir el criterio de divisibilidad por 11 de un número N que en el sistema decimal es

$N = c_n * 10^n + c_{n-1} * 10^{n-1} + \ldots + c_1 * 10 + c_0$

Resto potenciales de base 10 respecto al módulo 11:
$10^0 \equiv 1 \pmod{11}$
$10^1 \equiv 10 \pmod{11} \Rightarrow 10^1 \equiv -1 \pmod{11}$
$10^2 \equiv -10 \pmod{11} \Rightarrow 10^2 \equiv 1 \pmod{11}$
$10^3 \equiv 10 \pmod{11} \Rightarrow 10^3 \equiv -1 \pmod{11}$ ...

N será divisible por 11 si y sólo si $c_0 - c_1 + c_2 - c_3 + \ldots + (-1)^n c_n$ es múltiplo de 11.

CLASES MODULO n

Consideremos la siguiente relación en Z:

$$(a,b) \in R \Leftrightarrow r(a,n) = r(b,n)$$

Por algoritmo de división, existen h, k ∈ Z/ a = k*n + r(a,n) y b = h*n + r(b,n) .

Luego a – b = k*n + r(a,n) - h*n - r(b,n) =

= (k – h)*n + [r(a,n) - r(b,n)] = (k – h)*n

pues si (a,b) ∈ R, r(a,n) = r(b,n). Luego: a ≡ b(mod n)

CLASES MODULO n

Recíprocamente, si a, b $\in$Z son tales que

$a \equiv b \pmod n$, $\exists k \in Z / a - b = k*n$. Luego;

$a = k*n + b$. Por algoritmo de división, $\exists h \in Z / b = h*n + r(b,n)$, con $0 \leq r(b,n) < n$.

Luego $a = k*n + h*n + r(b,n) = (k - h)*n + r(b,n)$

Por unicidad del cociente y el resto en la división entera, debe ser $r(a,n) = r(b,n)$.

ECUACIONES DE CONGRUENCIAS

Dados n natural, a y b enteros, queremos determinar si es posible hallar $x \in Z / ax \equiv b \pmod n$

Es decir, que buscamos $x \in Z / ax - b = k*n$, para algún número entero k. De esta manera, planteamos la ecuación diofántica $ax - kn = b$.

Una ecuación diofántica es una ecuación lineal de dos variables (x y k, en este caso), cuya solución debe ser un par de números enteros.

Inverso Aritmética Modular

- Si *a* y *m* son números enteros y primos relativos, y $m > 1$, entonces un inverso de *a mod m* existe. Además, el inverso es único módulo *m*.
- En la solución de la ecuación: $ax \equiv b \ (mod\ m)$, donde $a,m > 0$, sería decir $aa^{-1} \equiv 1 \ (mod\ m)$, ya que la multiplicación de un número y su inverso es 1.
  - Z_m
  - $[r]_m = \{c \in Z \mid r \equiv c \ (mod\ m)\} = \{r + k \bullet m \mid k \in Z\}$.
  - $r < m$

25

Inverso Aritmética Modular

- Ejemplo: Encontrar el inverso de 3 *mod* 7
  - 3 y 7 son primos relativos, sí hay inverso
  - $mcd(3,7) = 1$, por lo que $3x + 7y = 1$
  - Por el algoritmo de Euclides extendido: $x = -2$ y $y = 1$
  - $7 + -2 = 5$
  - $Z_7 \rightarrow [0]_7, [1]_7, [2]_7, [3]_7, [4]_7, [5]_7, [6]_7$.
  - $aa^{-1} \equiv 1 \ (mod\ m) \rightarrow 3*5 \equiv 1 \ (mod\ 7) \rightarrow 15 \equiv 1 \ (mod\ 7)$

26

Ecuaciones Lineales Modulares

- Se desea encontrar soluciones a la ecuación: $ax \equiv b \pmod{n}$, donde $a > 0$ y $n > 0$.
- Sea $\langle a \rangle$ el subgrupo de Z_n generado por a.
  - Ya que $\langle a \rangle = \{a^{(x)} : x > 0\} = \{ax \bmod n : x > 0\}$, la ecuación anterior se soluciona si y sólo si $b \in \langle a \rangle$.
  - El teorema de Lagrange dice que $|\langle a \rangle|$ puede ser un divisor de n.
- **Teorema.** Para cualesquiera enteros positivos a y n, si $d = mcd(a,n)$, entonces $\langle a \rangle = \langle d \rangle = \{0, d, 2d, \ldots, ((n/d) - 1)d\}$, en Z_n, y así $|\langle a \rangle| = n/d$.

27

Ecuaciones Lineales Modulares

- **Corolario 1.** La ecuación $ax \equiv b \pmod{n}$ se resuelve para un x desconocido si y sólo si $mcd(a,n) \mid b$.
- **Corolario 2.** La ecuación $ax \equiv b \pmod{n}$ tiene distintas soluciones d módulo n, donde $d = mcd(a,n)$, o no tiene soluciones.
- **Teorema.** Sea $d = mcd(a,n)$, y suponer que $d = ax' + ny'$ para cualesquier números x' y y' (como computando el algoritmo extendido de Euclides). Si $a \mid b$, entonces la ecuación tiene el valor x_0 como una de sus soluciones , donde $x_0 = x'(b/d) \bmod n$.

$$ax_0 \equiv ax'(b/d) \pmod{n}$$
$$ax_0 \equiv d(b/d) \pmod{n}, (\text{porque } ax' \equiv d \pmod{n})$$
$$ax_0 \equiv b \pmod{n}$$

28

Ecuaciones Lineales Modulares

- **Teorema.** Suponga que la ecuación $ax \equiv b \pmod{n}$ se puede resolver (ya que $d \mid b$, donde $d = mcd(a,n)$) y que x_0 es una solución de la ecuación. Entonces, esta ecuación tiene exactamente d soluciones distintas, módulo n, que se obtienen por $x_i = x_0 + i(n/d)$ para $i = 0, 1, 2, \ldots, d - 1$.

$$ax_i \bmod n = a(x_0 + in/d) \bmod n$$
$$ax_i \bmod n = (ax_0 + ain/d) \bmod n$$
$$ax_i \bmod n = ax_0 \bmod n, (\text{porque } d \mid a)$$
$$ax_i \bmod n = b$$

29

Ecuaciones Lineales Modulares

- **Corolario 1.** Para cualquier $n > 1$, si $mcd(a,n) = 1$, entonces la ecuación $ax \equiv b \pmod{n}$ tiene una única solución, módulo n.
- **Corolario 2.** Para cualquier $n > 1$, si $mcd(a,n) = 1$, entonces la ecuación $ax \equiv 1 \pmod{n}$ tiene una única solución, módulo n. En otro caso, no tiene solución.
  - Este corolario permite usar la notación ($a^{-1} \pmod{n}$) para referirse a la multiplicación inversa de a, módulo n, cuando a y n son primos relativos. Si $mcd(a,n) = 1$, entonces una solución de la ecuación es un entero x calculado por el algoritmo extendido de Euclides, ya que la ecuación $mcd(a,n) = 1 = ax + ny$ implica $ax \equiv 1 \pmod{n}$.

30

Ecuaciones Lineales Modulares

```
MODULAR-LINEAR-EQUATION-SOLVER(a,b,n)
1 (d,x',y') <-- EXTENDED-EUCLID(a,n)
2 if d|b
3    then x0 <-- x'(b/d) mod n
4         for i <-- 0 to d-1
5             do print(x0 + i(n/d)) mod n
6    else print "No solutions"
```

31

Ecuaciones Lineales Modulares

- Ejemplo:
  - Sea la ecuación $14x \equiv 30 \pmod{100}$, donde $a = 14$, $b = 30$ y $n = 100$.

Línea $1 \Rightarrow (d, x, y) = (2, -7, 1)$

Línea $2 \Rightarrow d \mid b = 2 \mid 30 = 15 \Rightarrow$ Se ejecutan las líneas 3 - 5.

Línea $3 \Rightarrow x_0 = (-7 \bullet (30/2)) \bmod 100 = (-7 \bullet 15) \bmod 100 = 95$

Línea $4 \Rightarrow$ El ciclo de la líneas 4 - 5 imprme dos soluciones: 95 y 45.

$$x_1 = (95 + 0 \bullet (100/2)) \bmod 100 = 95$$

$$x_2 = (95 + 1 \bullet (100/2)) \bmod 100 = (95 + 50) \bmod 100 = 145 \bmod 100 = 45$$

32

Algoritmo de Euclides Extendido e Inverso Aritmético Modular

- Se puede usar el algoritmo de Euclides Extendido para encontrar el inverso aritmético modular y así encontrar la solución de la ecuación lineal modular.
  - Sea la ecuación $11x \equiv 6 \pmod{92}$.
  - El inverso de 11 (*mod* 92) = -25 + 92 = 67
    - $67*11 \equiv 1 \pmod{92}$
  - Se multiplica por 67 a ambos lados de la congruencia lineal:
    - $67*11x = 67*6 \pmod{92}$
    - $x = 402 \pmod{92} = 34$
  - $x = 34$ es el número entero positivo más pequeño que soluciona el sistema.
  - Las soluciones son todas las x tales que $x = 34 + 92k$, $k \in \mathbb{Z}$.

33

Teorema Chino de los Restos

- El **Teorema Chino de los Restos** establece que cuando los módulos de un sistema de congruencias lineales están entre pares de primos relativos, hay una solución única del sistema de congruencia módulo el producto de los módulos.

34

Teorema Chino de los Restos

- Supongamos que m_1, m_2, …, m_k son enteros positivos coprimos dos a dos. Entonces, para enteros dados a_1,a_2, …, a_k, existe un entero x que resuelve el sistema de congruencias simultáneas

$$x \equiv a_1 (\mathrm{mod}\, m_1) \qquad M_k = m/m_k, k = 1,2,...,n$$
$$x \equiv a_2 (\mathrm{mod}\, m_2) \qquad M_k y_k \equiv 1 (\mathrm{mod}\, m_k)$$
$$... \qquad x = a_1 M_1 y_1 + a_2 M_2 y_2 + ... + a_n M_n y_n$$
$$x \equiv a_n (\mathrm{mod}\, m_n) \qquad x \equiv a_k M_k y_k \equiv a_k (\mathrm{mod}\, m_k), k = 1,2,...,n$$

- Todas las soluciones x de este sistema son congruentes módulo el producto $m = m_1 m_2 ... m_n$, donde $0 \le x \le m$ y otras soluciones son congruentes módulo m.

35

Teorema Chino de los Restos

- Se tiene el siguiente sistema:

$$x \equiv 2 (\mathrm{mod}\, 3)$$
$$x \equiv 3 (\mathrm{mod}\, 5)$$
$$x \equiv 2 (\mathrm{mod}\, 7)$$

$$m = 3*5*7 = 105, M_1 = 105/3 = 35, M_2 = 105/5 = 21, M_3 = 105/7 = 15$$
$$mcd(35,3) = 1, \text{inverso}\, 2$$
$$mcd(21,5) = 1, \text{inverso}\, 1$$
$$mcd(15,7) = 1, \text{inverso}\, 1$$
$$x \equiv a_1 M_1 y_1 + a_2 M_2 y_2 + a_3 M_3 y_3 = 2*35*2 + 3*21*1 + 2*15*1 = 233$$
$$x = 233 (\mathrm{mod}\, 105) = 23$$

- Solución x = 23, número entero positivo más pequeño que soluciona el sistema.
- Las soluciones son todas las x tales que $x = 23 + 105k$, $k \in \mathbb{Z}$.

36

Teorema Chino de los Restos

La ecuación en congruencias $ax \equiv b \pmod{m}$ *tiene solución si y sólo si* $d = \text{mcd}(a, m)$ *divide a b.*

Teorema (chino de los restos)

Sean $m_1, m_2, \ldots, m_n$ *enteros mayores que 1 , primos entre sí dos a dos, sean* $a_1, a_2, \ldots, a_n$ *enteros.*

El sistema de ecuaciones en congruencias $x \equiv a_1 \pmod{m_1}$ $x \equiv a_2 \pmod{m_2}$ $x \equiv a_n \pmod{m_n}$ *tiene solución.*

Además si x y x^j *son dos soluciones entonces* $x \equiv x^j \pmod{M}$, *donde* $M = m_1 m_2 \ldots m_n$.

Recíprocamente si x es una solución y $x^j \equiv x \pmod{M}$ *entonces* x^j *también es solución.*

Referencias

Sánchez-Rubio García, C., Ripollés Amela, M. (2000)
Manual de matemáticas para preparación olímpica
Castelló de la Plana: Universitat Jaume I
Guelfond, A. O., (1979) Resolución de ecuaciones en números enteros. Lecciones populares. Moscú: MIR
Ramírez Benavides k.D.
Matemática Discretas
Moreira A.
Informática Teórica