El Teorema de los Restos Chinos

Juana Contreras S.[1]
Claudio del Pino O.[2]

Instituto de Matemática y Física
Universidad de Talca

Resumen

El *teorema de los restos chinos* es un resultado de la aritmética modular, que permite resolver sistemas de congruencias lineales. En este trabajo se presenta una reseña histórica del teorema, una demostración del teorema que proporciona un método para determinar soluciones de un sistema de congruencias lineales, problemas clásicos y algunas aplicaciones del teorema.

Introducción

El *Teorema de los Restos Chinos*, es llamado así, debido a que las versiones más antiguas sobre estos problemas de congruencias se encuentran en trabajos matemáticos chinos.

El problema más antiguo se encuentra en el texto *Sun Zi Suan Ching* (Manual de Matemática de *Sun Zi*) escrito aproximadamente en el siglo III por el matemático chino *Sun Zi*, y corresponde al problema 26.

El enunciado del problema de *Sun Zi* es el siguiente:

Tenemos un número de cosas, pero no sabemos exactamente la cantidad. Si las contamos de a tres, quedan dos sobrando. Si las *contamos de a cinco, quedan tres sobrando. Si las contamos de a siete, quedan dos sobrando. ¿Cuántas cosas pueden ser?*

A continuación se describe la solución dada por *Sun Zi* en su obra:

- Determinó que se podía resolver usando los números 70, 21 y 15, que eran múltiplos de $5 \cdot 7$, de $3 \cdot 7$ y de $3 \cdot 5$ respectivamente.
- Observó que la suma $2 \cdot 70 + 3 \cdot 21 + 2 \cdot 15$ igual a 233, es una solución del problema.

[1] e-mail: jcontres@pehuenche.utalca.cl
[2] e-mail: cdelpino@pehuenche.utalca.cl

- Luego, restó a 233 múltiplos de $3 \cdot 5 \cdot 7$ tantas veces como fuera posible, obteniendo el número 23, siendo este número el menor entero positivo que resuelve el problema.

Desafortunadamente, en el texto se encuentra solo el problema 26 que ilustra el Teorema. No se sabe si *Sun Zi* desarrolló un método general para resolver tales problemas.

Una versión más popular del problema de *Sun Zi,* conocida por el nombre *Han Xing Dian Bing*, que significa *Han Xing cuenta sus soldados*, es el siguiente:

¿Cuántos soldados puede tener el ejército de Han Xing si al formarlos en tres columnas quedan dos soldados, si se ordenan en 5 columnas quedan tres soldados, y al ordenarlos en 7 columnas, quedan dos soldados?

Un primer enunciado del Teorema, se encuentra en el libro escrito por el matemático chino *Qin Jiushao*[1] (1202-1261), publicado en el año 1247. En su libro, *Qin* ofrece un método práctico para resolver este tipo de problemas.

Leonhard Euler
1707-1783

Aproximadamente mil años después, el matemático italiano conocido como *Fibonacci* (1170-1250) trabajó el problema de *Sun Zi*, pero no descifró el método presentado.

Posteriormente, el matemático suizo *Leonhard Euler* (1707-1783) se interesó en el teorema y en el método chino y presentó una versión moderna y más generalizada del teorema.

Luego, el matemático alemán *Carl F. Gauss*[2] (1777-1885) descubrió un nuevo método para resolver sistemas de congruencias lineales alrededor del año 1801.

El método de *Qin Jiushao* fue difundido en Europa por el misionero inglés *Alexander Wylie* (1815-1887) en su tratado *Jottings on the science of Chinese arithmetic*, publicado en 1852.

Antes de enunciar el teorema y un método que permite resolver sistemas de congruencias lineales se presentará un problema sobre restos y soluciones usando herramientas elementales de números, y se establecerá algunos conceptos sobre congruencias y propiedades básicas.

Carl F. Gauss
1777-1885

[1] *Qin Jiushao,* matemático chino (1202-1261), es considerado uno de los más grandes matemáticos del siglo XIII

[2] *Carl Friedrich Gauss*, matemático alemán (*1777-1885*), introdujo, en 1801 el concepto de congruencia y la aritmética de las clases de restos en su obra *Disquisitiones Arithmeticae*.

Problema de un juego de naipes

Un juego especial de naipes se compone de n cartas. Si se distribuye equitativamente entre 7 jugadores queda una carta. Si se distribuye entre 11 jugadores quedan 10 cartas.
¿Cuáles son los posibles valores de n?. ¿Cuál es la mínima cantidad de cartas que tiene el juego de naipes?

Solución
Se trata de encontrar números naturales n que cumplan simultáneamente las condiciones: al dividir n por 7 queda resto 1, y al dividir n por 11 queda resto 10, obteniendo las siguientes ecuaciones:

$$n = 7s + 1$$
$$n = 11k + 10$$

donde s y k son números enteros no negativos.

Solución 1.
Una manera de resolver el problema es completando una tabla con dos filas, con números que dejan resto 1 al dividirlos por 7, y resto 10 al dividirlos por 11.

Números que dejan																		
resto 1 al dividirlo por 7	1	8	15	22	29	36	43	50	57	64	71	78	85	92	99	106	113	**120**
resto 10 al dividirlo por 11	10	21	32	43	54	65	76	87	98	109	**120**	131	142	153	164	175	186	197

Luego, el juego puede tener 43 naipes, o 120 naipes, etc.

Solución 2.
Algunas soluciones del problema se pueden determinar completando las siguientes tablas, con el propósito de encontrar valores de s y k tales que $7s + 1 = 11k + 10$:

s	$7s+1$
0	1
1	8
2	15
3	22
4	29
5	36
6	43
7	50
8	57
9	64
10	71
11	78

*

	k	$11k+10$
	0	10
	1	21
	2	32
*	3	43
	4	54
	5	65
	6	76
	7	87
	8	98
	9	109
**	10	120
	11	131

12	85
13	92
14	99
15	106
16	113
17	120
…	…

**

12	142
13	153
14	164
15	175
16	186
17	197
…	…

De la tabla se observa que para $s=6$ y $k=3$, se obtiene un valor común para n:

$$7\cdot 6+1=43 \quad \text{y} \quad 11\cdot 3+10=43$$

Luego, una solución del problema es $n=43$. Otra solución se obtiene para $s=17$ y $k=10$, $n=120$. De la tabla se observa que la mínima cantidad de naipes que puede tener el juego es 43.

Solución 3.

Otra forma de abordar el problema es, determinar números enteros s y k tales que $7s=11k+9$, equivalente a determinar los pares ordenados de números enteros (k,s) que satisfacen la ecuación. Gráficamente:

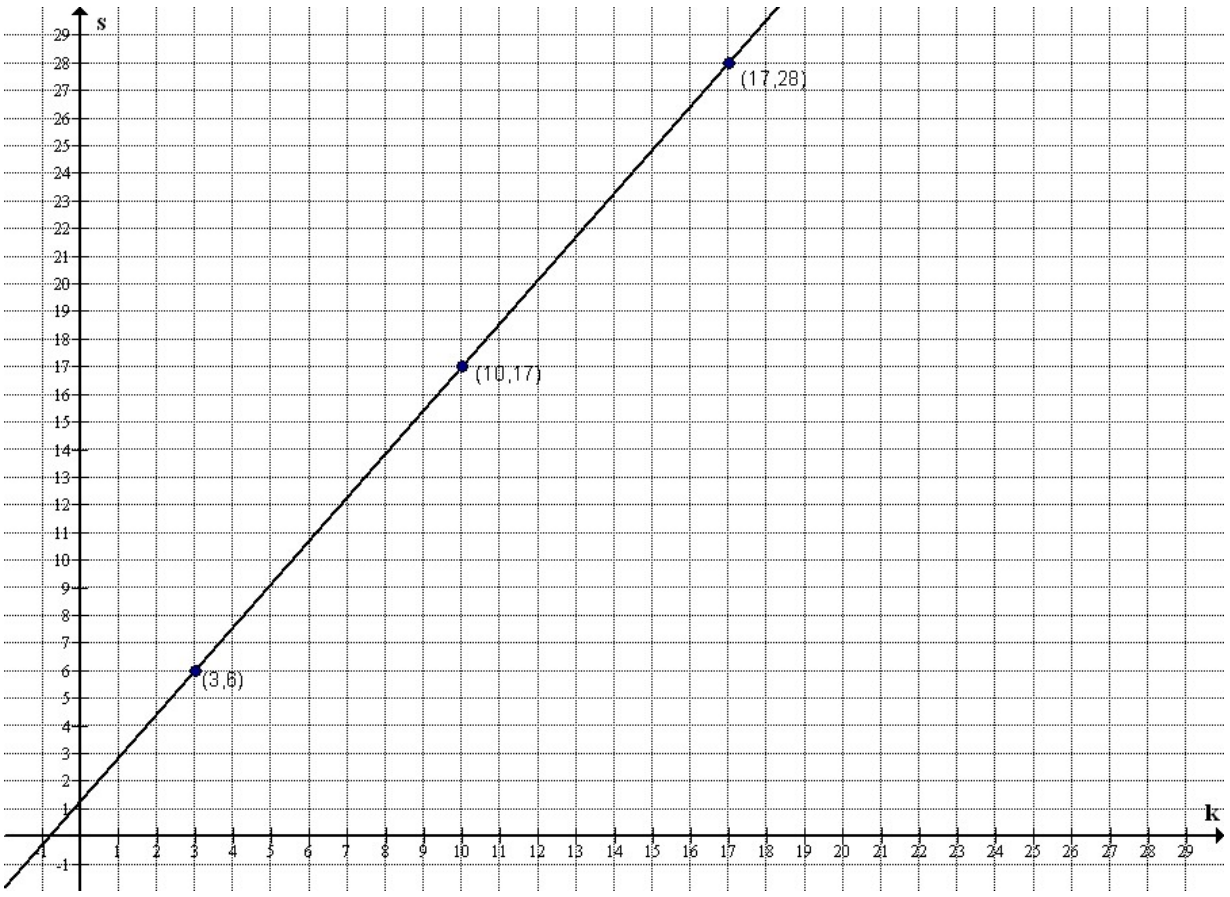

Gráfico de la ecuación $7s-11k=9$

Congruencias

Una de las grandes contribuciones de *Gauss* en matemática es el libro *Disquisitiones arithmeticae*, publicado en 1801. En esta obra introduce por primera vez el concepto de *conguencia* y la notación que se usa actualmente.

Definición. Sean a y b números enteros y sea n un número natural. Se dice que a es *congruente* con b módulo n, si y sólo si, n es un divisor de $a-b$.

De manera equivalente, a es *congruente* con b módulo n si y solo si $a-b$ es múltiplo de n.

Notación. La notación que se usa actualmente, introducida por *Gauss*, es: $a \equiv b(\text{mod } n)$. Luego:

$$a \equiv b(\text{mod } n) \text{ si y solo si } n \text{ es un divisor de } a-b$$

Por ejemplo:

- $49 \equiv 27(\text{mod } 11)$, ya que 11 es un divisor de $49-27=22$
- $17 \equiv 2(\text{mod } 5)$, ya que 5 es un divisor de $17-2=15$, o, $17-2$ es múltiplo de 5.

Una propiedad esencial

Si r es el resto de la división de a por n, entonces $a \equiv r(\text{mod } n)$. Es decir, todo número entero a es congruente con el resto de dividir a por n.

Por ejemplo:

- $11 = 5 \cdot 2 + 1 \Rightarrow 11 \equiv 1 \,(\text{mod } 5)$
- $124 = 4 \cdot 31 + 0 \Rightarrow 124 \equiv 0(\text{mod } 4)$
- $30 = 7 \cdot 4 + 2 \Rightarrow 30 \equiv 2(\text{mod } 7)$
- $-14 = 7 \cdot (-2) + 0 \Rightarrow -14 \equiv 0(\text{mod } 7)$

En particular:

$a \equiv 0(\text{mod } n)$ significa que a múltiplo de n, o que el resto de dividir a por n es 0.

Algunas propiedades de las congruencias

Sea n un número natural, y sean a y b números enteros.

1. $a \equiv a(\text{mod } n)$
   Si $a \equiv b(\text{mod } n)$ entonces $b \equiv a(\text{mod } n)$
   Si $a \equiv b(\text{mod } n)$ y $b \equiv c(\text{mod } n)$ entonces $a \equiv c(\text{mod } n)$

   Por ejemplo: $23 \equiv 13(\text{mod } 5)$ y $13 \equiv 3(\text{mod } 5)$, luego $23 \equiv 3(\text{mod } 5)$

2. Si $a \equiv b(\text{mod } n)$ y c es un número entero, entonces $a+c \equiv b+c(\text{mod } n)$
   Si $a \equiv b(\text{mod } n)$ y c es un número entero, entonces $a-c \equiv b-c(\text{mod } n)$

Si $a \equiv b(\text{mod } n)$ y c es un número entero, entonces $a \cdot c \equiv b \cdot c(\text{mod } n)$

Por ejemplo: $2a \equiv 5(\text{mod } 7) \Rightarrow 4 \cdot 2a \equiv 4 \cdot 5(\text{mod } 7) \Rightarrow a \equiv 6(\text{mod } 7)$ ya que $8 \equiv 1(\text{mod } 7)$ y $20 \equiv 6(\text{mod } 7)$.

3. Si $a \cdot b \equiv c(\text{mod } n)$ y $a \equiv s(\text{mod } n)$, entonces $s \cdot b \equiv c(\text{mod } n)$

   Por ejemplo: $29 \cdot 8 \equiv 1(\text{mod } 11)$ y $29 \equiv 7(\text{mod } 11)$, luego $7 \cdot 8 \equiv 1(\text{mod } 11)$

4. Si $a \equiv b(\text{mod } n)$ y $n = m_1 \cdot m_2$, entonces $a \equiv b(\text{mod } m_1)$ y $a \equiv b(\text{mod } m_2)$.

5. Sean m y s números enteros primos relativos.

   Si $a \equiv b(\text{mod } m)$ y $a \equiv b(\text{mod } s)$ entonces $a \equiv b(\text{mod } m \cdot s)$

   En particular:

   Si $a \equiv b(\text{mod } p)$ y $a \equiv b(\text{mod } q)$, siendo p y q primos distintos, entonces $a \equiv b(\text{mod } pq)$

Propiedad importante.
Si a y n son primos relativos, entonces existe un número entero u, tal que $u \cdot a \equiv 1(\text{mod } n)$.

Por ejemplo:
- 4 y 7 son primos relativos y, $2 \cdot 4 \equiv 1(\text{mod } 7)$
- 21 y 31 son primos relativos y, $3 \cdot 21 \equiv 1(\text{mod } 31)$

Congruencias lineales

Definición. Una congruencia lineal en x es de la forma $a \cdot x \equiv c(\text{mod } n)$, donde a y c son número enteros.

Teorema. La congruencia $a \cdot x \equiv c(\text{mod } n)$ tiene solución, si y sólo si máximo común divisor entre a y n es un divisor de c.

Nota. En particular, si a y n son primos relativos entonces:
- La congruencia lineal $a \cdot x \equiv c(\text{mod } n)$ tiene solución única módulo n.
- Y, si u_0 es una solución de la congruencia tal que $a \cdot x \equiv c(\text{mod } n)$ entonces $x = u_0 + n\,t$, para todo número entero t, es la solución general de la congruencia.

Ejemplo. Resolver la congruencia $18 \cdot x \equiv 5(\text{mod } 7)$.

Solución.

$$18 \cdot x \equiv 5(\text{mod } 7)$$

a) Como $18 \equiv 4(\text{mod}\,7)$:

$$4 \cdot x \equiv 5(\text{mod } 7)$$

b) Como $2 \cdot 4 \equiv 8 \equiv 1(\text{mod}\,7)$, multiplicar por 2 la congruencia queda:

$$x \equiv 10(\text{mod } 7)$$

Como $10 \equiv 3(\text{mod}\,7)$, luego:

$$x \equiv 3(\text{mod } 7)$$

c) Por lo tanto:

$x = 3 + 7t$, para cualquier número entero t.

A continuación se presentará el teorema de los restos chinos y su demostración, para el caso de un sistema formado por **dos** congruencias lineales.

Teorema de los restos chinos (caso particular)
Si m y n son dos números naturales primos relativos entre sí, entonces el sistema de congruencias lineales:

$$\begin{array}{|l} x \equiv a(\text{mod}\,m) \\ x \equiv b(\text{mod}\,n) \end{array}$$

tiene solución única módulo $M = m \cdot n$.

Demostración

- Existencia de solución
  $x \equiv a(\text{mod}\,m) \quad \Rightarrow \quad x = a + mt$, para cualquier entero t.

  Sustituyendo $x = a + mt$ en la congruencia $x \equiv b(\text{mod}\,n)$ se obtiene:

  $$a + mt \equiv b(\text{mod}\,n)$$

  Luego:

  $$mt \equiv b - a(\text{mod}\,n)$$

  Como m y n son primos relativos, entonces existe un entero m' tal que $m'\,m \equiv 1(\text{mod}\,n)$

  Multiplicando por m' la ecuación obtenida en 2), se obtiene:

  $$t \equiv m'(b - a)\ (\text{mod}\,n)$$

  de donde:

  $$t = m'\,b - m'\,a + nk$$

  para cualquier número entero k.

  Sustituyendo $t = m'\,b - m'\,a + nk$ en la ecuación $x = a + mt$ se obtiene:

  $$x = a + m(m'\,b - m'\,a + nk)$$

Por lo tanto, la solución general del sistema de congruencias lineales es:

$$x = a + m\,m'\,b - m\,m'\,a + Mk \text{, donde } M = m \cdot n$$

- Existe una única solución X_0 del sistema de congruencias tal que $0 \le X_0 \le M - 1$
  En efecto, si X e Y son soluciones del sistema de congruencias lineales, tales que $0 \le X \le M - 1$ y $0 \le Y \le M - 1$, donde $M = m \cdot n$, entonces:

$$\left.\begin{array}{l} X \equiv a(\text{mod}\, m) \\ X \equiv b(\text{mod}\, n) \end{array}\right| \quad \text{y} \quad \left.\begin{array}{l} Y \equiv a(\text{mod}\, m) \\ Y \equiv b(\text{mod}\, n) \end{array}\right|$$

de donde:

$$X - Y \equiv 0(\text{mod}\, m) \quad \text{y} \quad X - Y \equiv 0(\text{mod}\, n)$$

Como m y n son primos relativos, entonces $X - Y \equiv 0(\text{mod}\, mn)$, o sea $X - Y \equiv 0(\text{mod}\, M)$

Y, como $0 \le X \le M - 1$ y $0 \le Y \le M - 1$, luego $X = Y$.

Ejemplo. *Solución del problema de un juego de naipes*, usando congruencias.

El problema consiste en resolver el sistema de congruencias

$$\left.\begin{array}{l} n \equiv 1(\text{mod } 7) \\ n \equiv 10(\text{mod } 11) \end{array}\right|$$

Solución

a) Primera congruencia: $n \equiv 1(\text{mod } 7) \Rightarrow n = 1 + 7s$

b) Sustituyendo en la segunda congruencia:
$$n \equiv 10(\text{mod } 11) \Rightarrow 1 + 7s \equiv 10(\text{mod } 11) \Rightarrow 7s \equiv 9(\text{mod } 11)$$

c) Como $8 \cdot 7 \equiv 1(\text{mod}\, 11)$, multiplicando la congruencia anterior por 8 se obtiene:
$$s \equiv 72 \equiv 6(\text{mod } 11)$$

d) Por lo tanto: $s = 6 + 11t$

e) Reemplazando $t = 6 + 11s$ en $n = 1 + 7s$, se obtiene: $n = 1 + 7(6 + 11t)$

Por lo tanto, la solución general del sistema de congruencias es: $n = 43 + 77t$, para cualquier número entero t, y la mínima cantidad de cartas que puede tener el juego es 43.

Ejercicio. Determinar número entero positivo que deja resto 2 al dividirlo por 3, y deja resto 3 al dividirlo por 7. Luego, encontrar el menor entero positivo con *tres dígitos* que cumple las condiciones del problema.

Nota. A continuación se presenta el teorema de los restos chinos para n congruencias. Una demostración del teorema se puede realizar usando inducción sobre k, efectuando sucesivas sustituciones, como en la demostración dada para el caso de sistemas de dos congruencias. La demostración que se presenta, dada por *Qin Jiushao*, proporciona un algoritmo para hallar la solución general del sistema de congruencias.

Teorema de los Restos Chinos

Sean k números naturales $m_1, m_2, \cdots, m_k$ primos relativos dos a dos, y sean k números enteros $r_1, r_2, \cdots, r_k$. El sistema de congruencias:

$$\left.\begin{aligned} x &\equiv r_1 (\mathrm{mod}\, m_1) \\ x &\equiv r_2 (\mathrm{mod}\, m_2) \\ &\vdots \\ x &\equiv r_k (\mathrm{mod}\, m_k) \end{aligned}\right|$$

Admite solución única módulo $M = m_1 m_2 \cdots m_k$. Es decir, existe un único número entero s entre 0 y $M-1$ que resuelve simultáneamente a todas las congruencias del sistema.

Demostración

Sea $M_i = \dfrac{M}{m_i}$ para $i = 1, 2, ..., k$.

a) Para cada $i = 1, 2, ..., k$:
   - M_i y m_i son primos relativos entre sí.
   - Luego, existe u_i tal que $u_i M_i \equiv 1 (\mathrm{mod}\, m_i)$
   - Y se cumple:

$$u_1 M_1 r_1 + u_2 M_2 r_2 + \ldots + u_k M_k r_k \equiv r_i (\mathrm{mod}\, r_i)$$

b) Por lo tanto:

$$X = u_1 M_1 r_1 + u_2 M_2 r_2 + \ldots + u_k M_k r_k$$

es una solución del sistema de congruencias.

Nota. Si X e Y son dos soluciones tal que $0 \le X \le M-1$ y $0 \le Y \le M-1$ entonces $X - Y$ es múltiplo de m_i para cada $i = 1, 2, ..., k$. Como los enteros m_i son primos relativos dos a dos, luego, $X - Y$ es múltiplo de $M = m_1 m_2 \cdots m_k$, lo que implica que $X = Y$.

Por lo tanto, las soluciones del sistema de congruencias son de la forma:

$$x = u_1 M_1 r_1 + u_2 M_2 r_2 + \ldots + u_k M_k r_k + M t$$

para cualquier número entero t.

Solución *del problema de Sun Zi*, o *de los soldados de Han Xing*

Usando la notación de congruencias, el problema consiste en resolver el sistema:

$$\left.\begin{array}{l} x \equiv 2(\mathrm{mod}\,3) \\ x \equiv 3(\mathrm{mod}\,5) \\ \underline{x \equiv 2(\mathrm{mod}\,7)} \end{array}\right|$$

Solución 1: *Usando sustituciones sucesivas.*

a) Observar que 3, 5 y 7 son primos relativos entre sí.

b) Primera congruencia: $x \equiv 2(\mathrm{mod}\,3) \Rightarrow x = 2 + 3s$

c) Segunda congruencia: $x \equiv 3(\mathrm{mod}\,5) \Rightarrow 2 + 3s \equiv 3(\mathrm{mod}\,5) \Rightarrow 3s \equiv 1(\mathrm{mod}\,5)$

Multiplicando por 2: $s \equiv 2(\mathrm{mod}\,5) \Rightarrow s = 2 + 5k$

Reemplazando en $x = 2 + 3s$ se obtiene: $x = 2 + 3(2 + 5k)$.

Luego: $x = 8 + 15k$

d) Tercera congruencia: $x \equiv 2(\mathrm{mod}\,7) \Rightarrow 8 + 15k \equiv 2(\mathrm{mod}\,7) \Rightarrow 15k \equiv -6(\mathrm{mod}\,7)$

Como $15 \equiv 1(\mathrm{mod}\,7)$ y $-6 \equiv 1(\mathrm{mod}\,7)$ se obtiene: $k \equiv 1(\mathrm{mod}\,7)$

Luego: $k = 1 + 7t$

e) Sustituyendo en $x = 8 + 15k$, se obtiene $x = 8 + 15(1 + 7t)$.

Luego, la solución general del sistema es: $x = 23 + 105k$

Por lo tanto, el ejército de *Han Xing* puede tener como mínimo 23 soldados.

Nota. Otras soluciones del problema son: 128, 233, 338, 443, etc. Notar que dos soluciones cualquiera consecutivas, difieren en 105.

Solución 2. *Usando el algoritmo presentado en la demostración (método de Qin Jiushao).*

a) Sea $M = 3 \cdot 5 \cdot 7 = 105$

b) Luego: $\begin{cases} m_1 = 3 & m_2 = 5 & m_3 = 7 \\ r_1 = 2 & r_2 = 3 & r_3 = 2 \\ M_1 = 35 & M_2 = 21 & M_3 = 15 \end{cases}$

c) Resolver cada una de las congruencias:

$$\begin{array}{ccc} 35x \equiv 1(3) & 21x \equiv 1(5) & 15x \equiv 1(7) \\ \Downarrow & \Downarrow & \Downarrow \\ x \equiv 2(\mathrm{mod}\,3) & x \equiv 1(\mathrm{mod}\,5) & x \equiv 1(\mathrm{mod}\,7) \end{array}$$

Luego: $u_1 = 2,\ \ u_2 = 1,\ \ u_3 = 1$

d) Solución general del sistema de congruencias:

$$x \equiv M_1 u_1 a_1 + M_2 u_2 a_2 + M_3 u_3 a_3 (\mathrm{mod}\, M)$$

Sustituyendo se obtiene:

$$x \equiv 35 \cdot 2 \cdot 2 + 21 \cdot 1 \cdot 3 + 15 \cdot 1 \cdot 2 (\mathrm{mod}\ 105)$$

Luego:

$$x \equiv 233 (\mathrm{mod}\ 105)$$

e) Como $233 \equiv 23(\mathrm{mod}\ 105)$, el ejército de *Han Xng* puede tener como mínimo 23 soldados.

Un problema clásico

Una banda de 17 piratas se apodera de un botín compuesto por monedas de oro de igual valor. Deciden repartirse el botín en partes iguales y dar el resto al cocinero chino. Así, el cocinero recibiría tres monedas. Pero los piratas se pelean entre ellos y seis de ellos mueren en la riña. El cocinero recibiría entonces 4 monedas. Posteriormente ocurre un naufragio y solo 6 piratas, el cocinero y el tesoro se salvan. La nueva repartición dejaría 5 monedas de oro al cocinero. ¿Cuál es la fortuna mínima que esperaría el cocinero si decide liquidar al resto de los piratas?.

Solución.

Se trata de resolver el sistema de congruencias:

$$\left.\begin{array}{l} x \equiv 3(\mathrm{mod}\ 17) \\ x \equiv 4(\mathrm{mod}\, 11) \\ x \equiv 5(\mathrm{mod}\, 6) \end{array}\right|$$

Se resolverá el sistema usando propiedades de las congruencias.

$$\left.\begin{array}{l} x \equiv 3(\mathrm{mod}\ 17) \\ \\ \end{array}\right. \Rightarrow \left.\begin{array}{l} x = 3 + 17s \\ x \equiv 4(\mathrm{mod}\, 11) \end{array}\right\} \Rightarrow \quad 3 + 17s \equiv 4(\mathrm{mod}\, 11) \Rightarrow \quad s \equiv 2(\mathrm{mod}\, 11) \Rightarrow \quad s = 2 + 11k$$

$$\left.\begin{array}{l} x = 3 + 17s \\ s = 2 + 11k \end{array}\right\} \Rightarrow \quad x = 3 + 17(2 + 11k) \Rightarrow \quad x = 37 + 187k$$

$$\left.\begin{array}{l} x = 37 + 187k \\ x \equiv 5(\mathrm{mod}\, 6) \end{array}\right\} \Rightarrow \quad 37 + 187k \equiv 5(\mathrm{mod}\, 6) \Rightarrow \quad k \equiv 4(\mathrm{mod}\, 6) \Rightarrow \quad k = 4 + 6t$$

$$\left.\begin{array}{l} x = 37 + 187k \\ k = 4 + 6t \end{array}\right\} \Rightarrow \quad x = 37 + 187(4 + 6t) \Rightarrow \quad x = 785 + 1122t$$

Luego, la solución general del sistema es: $x = 785 + 1122t$

Por lo tanto, el tesoro tiene como mínimo 785 monedas de oro.

Observación. El teorema de los restos chinos es un caso especial de un resultado más general presentado por el monje budista *Yi Xing* alrededor del año 700. El teorema general establece que, el sistema de congruencias:

$$\left.\begin{array}{l} x \equiv r_1 (\mathrm{mod}\, m_1) \\ x \equiv r_2 (\mathrm{mod}\, m_2) \\ \vdots \\ x \equiv r_k (\mathrm{mod}\, m_k) \end{array}\right|$$

tiene solución si y sólo si, para cada i, j el máximo común divisor entre m_i y m_j es un divisor de $a_i - a_j$, para todo i, j tal que $1 \le i \le k$ y $1 \le j \le k$.

Un problema con historia

El siguiente problema se encuentra en trabajos del matemático indio *Bhaskara* (siglo VI), también aparece en trabajos del matemático egipcio *Al-Hasan* (siglo XI) y en la obra *Liberacci* de *Fibonacci*. El problema es el siguiente:

Una mujer fue al mercado y un caballo quebró los huevos que tenía en su canasto. El dueño del caballo ofreció pagarle por el daño causado. Le preguntó cuantos huevos había quebrado su caballo. La mujer dijo que no sabía, pero recordó que cuando los ordenó de dos en dos, quedaba uno. Igual cosa sucedió cuando los ordenó en grupos de 3, de 4, de 5, y de 6. Pero cuando los ordenó en grupos de 7, no quedó ninguno. ¿Cuál es la mínima cantidad de huevos que había en el canasto?.

Solución

Se debe determinar los números enteros x que cumplen simultáneamente:

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

Resolviendo el sistema de congruencias, se obtiene la solución general $x \equiv 301(\mathrm{mod}\, 420)$, es decir $x = 301 + 420t$ para cualquier número entero t.

Un problema de aplicación

Determinar todos los números enteros que son múltiplos de 13, cuyo dígito de las unidades es 4, y tales que, al dividirlos por 7 se obtiene resto 2. Luego, encontrar el menor entero positivo de cuatro cifras que resuelve el problema.

Comentarios

Actualmente el *teorema de los restos chinos* ha cobrado importancia por su aplicación en criptografía, específicamente en el sistema RSA[1]. En este contexto, se suele usar el teorema para recuperar claves. El teorema permite reconstruir un entero en un cierto rango, a partir de los restos módulo un par de factores del entero, relativamente primos. De esta forma se obtiene una representación del número, en números más *pequeños*.

Por ejemplo, el número $A = 973(\text{mod } 1813)$ se puede representar por el par de números 11 y 42, módulo 37 y 49 respectivamente, ya que $973 \equiv 11(\text{mod}\,37)$ y $973 \equiv 42(\text{mod}\,49)$. En efecto, la solución del sistema de congruencias $x \equiv 11(\text{mod}\,37)$, $x \equiv 42(\text{mod}\,49)$ es $x \equiv 973(\text{mod } 1813)$.

También se puede aplicar para resolver congruencias como por ejemplo $13x \equiv 36(\text{mod}\,792)$, descomponiendo 792 en factores primos relativos 8, 9 y 11, y luego resolver el sistema de congruencias $13x \equiv 36(\text{mod}\,8)$, $13x \equiv 36(\text{mod}\,9)$, $13x \equiv 36(\text{mod}\,11)$.

Bibliografía

[1] Bilgot, J. et all. *Aritmethique*. CRDP Auvergne. 1998.

[2] Hardy, G. H. y Wright, E. M., *An introduction to the theory of numbers*, Claredon Press - Oxford, 1985.

[3] Ore, O., *Number theory and its history*, Mc Graw-Hill, 1948.

[4] Ireland, K., Rosen, M. *A Classical Introduction to Modern Number Theory.* Springer-Verlag. 1990.

[5] Stewart, B. M., *Theory of Numbers*, The Macmillan Company, 1965.

[6] Tattersall, J., *Elementary Number Theory in Nine Chapters.* Cambridge Universite Press. 1999.

[7] Wiener, M., *Cryptanalysis of Short RSA Secret Exponents.* IEEE Transactions on Information Theory. Presented at Eurocrypt '89, Houthalen, Belgium. 1989.

[1] El *algoritmo RSA* es el algoritmo de clave pública más utilizado en la actualidad. Su nombre proviene de sus tres inventores: Ron ***R****ivest*, Adi ***S****hamir* y Leonard ***A****dleman*.