Bol. Acad. C. Fís., Mat. y Nat. Vol. LXII No. 3-4
Diciembre, 2002: 37-45

SOBRE EL TEOREMA CHINO DEL RESTO

ON THE CHINESE REMAINDER THEOREM

Luis Báez-Duarte, Pedro Berrizbeitia e Ignacio L. Iribarren**

RESUMEN

El clásico Teorema Chino del Resto proporciona una condición suficiente, pero ciertamente no necesaria para la solución de un sistema de congruencias de primer grado. En este trabajo analizamos una condición necesaria y suficiente tal parece que poco conocida debida a Stieltjes (1890, p. 31-32) y la generalizamos al contexto de los anillos abstractos. Ofrecemos una caracterización de la clase de anillos a los cuales se cumple el teorema. Nuestra atención se dirigió a este tema por la necesidad de cálcular ciertas sumas que involucran la parte fraccionaria {x} de un número real en el contexto y que ocurren en el enfoque de Beurling a la hipótesis de Riemann (1955, p. 312-314).

ABSTRACT

The classical Chinese Remainder Theorem provides a sufficient but by no means necessary condition for the solvability of a system of first degree congruences. In this paper we survey an apparently little known necessary and sufficient condition due to Stieltjes (1890, p. 31-32) generalizing it to the context of abstract rings. We give a characterization of the class of rings to which the theorern applies. Our attention was drawn naturally to this subject from the necessity of calculating certain sums involving the fractional part {x} of a real nurnber in the context of Beurling's approach to the Riemann Hypothesis (1955, p. 312-314).

Palabras Clave: Teorema Chino del Resto, anillos abstractos, números reales.

Keywords: Chinese Remainder Theorem, abstract rings, real numbers.

INTRODUCCIÓN

El célebre Teorema Chino del Resto se refiere a la solución simultánea de un sistema de congruencias

$$x \equiv r_1 \pmod{a_1},\ x \equiv r_2 \pmod{a_2} \ldots\ x \equiv r_n \pmod{a_n} \qquad (1)$$

donde los módulos $a_1, a_2, \ldots, a_n$ son enteros positivos.

El teorema afirma que, si los $a_1, a_2, \ldots, a_n$ son primos relativos por pares, el sistema (1) admite solución. Aunque es fácil percatarse, sin embargo, que ésta es sólo una condición suficiente, ciertamente no necesaria.

La fuente más antigua de este problema se encuentra en la obra china Suan-chin (Aritmética) de Sun-Tsu[1] en el primer siglo de nuestra era. Unos oscuros versos recitan la regla para calcular un número que, dividido por 3,5,7, deje restos 2,3,2 respectivamente[2]. Problemas de la misma especie aparecen en las obras de Nicomachus (alrededor del año 100 D.C.) y en las del matemático indio Brahmagupta (siglo VII D.C.). El sacerdote chino Yih-hing († 717 D.C.) es el primero, de quien se tiene noticia, que aborda expresamente la generalización que nos concierne en este artículo: cuando los módulos pueden no ser primos relativos por pares. Durante la Edad Media, matemáticos árabes (Ibn al-Haitam), indios (Bhaskara), chinos (Ch'in Chiu-shao) y algún europeo, como el célebre Leonardo de Pisa (Fibonacci), atacaron el problema de "los

* Individuos de Número. Academia de Ciencias Físicas, Matemáticas y Naturales.

restos" (el concepto de congruencia comienza a emplearse en el siglo XVIII por Euler, Lagrange y Legendre, y el símbolo ≡ es de Gauss. Hasta bien entrado el siglo XVII, este problema, como casi todos, se trataba con casos numéricos concretos, como lo hizo Sun-Tsu, aunque con ánimo de proporcionar un método general. En Europa, durante los siglos XVI y XVII, el problema chino "de los restos" surgía con frecuencia, y fue estudiado por muchos, por ejemplo en cálculos de fechas con respecto al calendario juliano.

Puede decirse que Euler y Lagrange en el siglo XVIII fueron los primeros en dar un tratamiento general y simbólico al teorema chino del resto, aunque siempre sujeto a la exigencia de que los módulos fuesen primos relativos por pares. Así lo hace Gauss, expresándolo en términos de congruencias. No se puede descartar que Gauss conociera la versión no sujeta a módulos primos relativos, pero en las *Disquisitiones* sólo trata el caso general en una forma algo casuística, indicando como hallar una solución del sistema general de congruencias por reducciones sucesivas al caso particular de módulos co-primos, pero sin llegar a enunciar un criterio general que permita decidir a priori si el sistema tiene o no soluciones. Suponemos que el inmenso prestigio de Gauss puede haber influido para que, casi sin excepción, los textos más establecidos sobre teoría de números también se limitaran al teorema clásico.

El propósito de este artículo es analizar y, desde luego, probar la forma general del teorema chino del resto; vale decir, determinar las condiciones necesarias y suficientes para la existencia de soluciones de un sistema (1); a saber, que para cada par de índices (i,j), se tenga

$$r_i \equiv r_j \pmod{\text{mcd}(a_i, a_j)}. \qquad (2)$$

(mcd es *máximo común divisor*)

Cuando fuimos llevados a esta formulación de manera natural, en un primer momento nos sentimos perplejos de que no se conociese. Sin embargo, una indagación bibliográfica cuidadosa nos enseñó que el matemático holandés Thomas Stieltjes (1856-94) había demostrado este caso general en su publicación en 1890. No obstante y con mayor razón, es sorprendente que no se incluya en los textos y que sea tan poco conocido; sólo lo hemos encontrado en el libro de Uspensky y Heaslet (1932), y como puede verse aquí, la versión general admite una prueba sencilla y de carácter elemental.

Este artículo se ha redactado con la intención de hacerlo accesible a un amplio público, incluyendo estudiantes. Una primera parte estudia el problema en el ámbito de los números enteros y, en una segunda quizás destinada a una audiencia más restringida, analiza la cuestión en el contexto abstracto de anillos. Cada uno de estos tratamientos está autocontenido.

El uso del teorema chino del resto se presenta en todas las ramas de la matemática y en muy variadas circunstancias, las más veces con módulos que no son primos relativos, desde la prueba del teorema de incompletitud de Gödel hasta muy abstrusas regiones del análisis, ni qué decir en teoría de números.

Precisamente, un esfuerzo por mejorar estimaciones de normas en el enfoque de Beurling (1955) de la Hipótesis de Riemann fue lo que nos condujo al cálculo de sumas del tipo

$$S(a_1, a_2, \ldots, a_k) := \sum_{m=1}^{a_1 a_2 \ldots a_k} p\left(\frac{m}{a_1}\right) p\left(\frac{m}{a_2}\right) \cdots p\left(\frac{m}{a_k}\right)$$

donde los a_1, a_2..., a_k son enteros positivos y $p(x)$ es la parte fraccionaria del número real x. El intento de hallar fórmulas cerradas para estas sumas nos llevó de modo muy natural a redescubrir la forma general del teorema chino del resto, con un pequeño retraso de 100 años.

Pudiera ser interesante para nuestros lectores indicar el resultado de las sumas para $k = 1,2$, dejando como problema el hallar la formula para $k = 3$.

$$S(a_1) = \frac{1}{2}\left(1 - \frac{1}{a_1}\right),$$

$$S(a_1, a_2) = \frac{1}{4}\left(1 - \frac{1}{a_1}\right)\left(1 - \frac{1}{a_2}\right) + \frac{d^2 - 1}{12 a_1 a_2},$$

donde d = mcd(a_1, a_2)

EL TEOREMA CHINO DEL RESTO EN LOS ENTEROS

Consideremos el sistema de congruencias (1). Los "restos" r_1, r_2, ..., r_n son enteros cualesquiera y los módulos a_1, a_2.., a_n son enteros positivos.

Supongamos que un entero x es solución de (1) y que y es otra solución. En virtud de la transitividad de la congruencia, tenemos $x \equiv y$ (mod a_i) para $i = 1,2,..., n$; o sea que x - y es múltiplo común de los a_1, a_2.., a_n, lo cual implica que el *mínimo común múltiplo* m = mcm(a_1, a_2,..., a_n) divide x - y, vale decir, $x \equiv y$ (mod m).

Recíprocamente, si existe una solución x de (1) e $y \equiv x$ (mod m) (donde, como antes, m = mcm(a_1, a_2,..., a_n)), entonces m divide y - x, por tanto a_1 divide y - x, para $i = 1,2,..., n$, es decir, y ≡ x (mod a_i) y, por la transitividad de la congruencia, concluimos que y es también solución del sistema.

En síntesis, de existir alguna solución x del sistema (1), hay infinitas soluciones y éstas constituyen precisamente la "clase de residuos" $\overline{x}$ módulo m.

Supongamos nuevamente que el sistema (1) admite alguna solución x. Entonces a_i divide a r_i - x y a_j divide a x - r_j, para todo par de subíndices i,j, lo cual implica que r_i-x y x-r_j son divisibles por todo factor común de a_i y a_j, y en particular, divisibles por mcd(a_i,a_j); luego su suma r_i - r_j = (r_i-x) + (x-r_j) es divisible por mcd(a_i,a_j).

Hemos probado que una condición necesaria para la existencia de soluciones del sistema (1) es que $r_i \equiv r_j$ (mod mcd(a_i,a_j)), para todo par de subíndices i, j. Que esa condición es también suficiente para que el sistema admita solución es en esencia la generalización del clásico teorema chino del resto.

Teorema 1 (Teorema Chino del Resto Generalizado). *El sistema de congruencias (1): $x \equiv r_1$ (mod a_1), $x \equiv r_2$(mod a_2),....,$x \equiv r_n$ (mod a_n), tiene solución si, y sólo si, $r_i \equiv r_j$ (mod mcd(a_i,a_j)), para todo par de subíndices i,j. En tal caso, si x es solución, la clase $\overline{x}$ módulo m (donde m = mcm(a_1, a_2,..., a_n,)) es presisamente el conjunto de todas las soluciones.*

Demostración. La necesidad ('sólo si') ya fue probada arriba, así como la tipificación de las soluciones. Demostremos la suficiencia de la condición.

Procedemos por inducción en el número n de ecuaciones.

Consideremos el caso $n = 2$: $x \equiv r_1$ (mod a_1), $x \equiv r_2$ (mod a_2) y sea d = mcd(a_1, a_2). Sabemos que existen enteros b_1, b_2 tales que $d = a_1 b_1 + a_2 b_2$ y es hipótesis que r_1-r_2 = qd; luego, r_1-r_2 = $a_1 b_1 q + a_2 b_2 q$ y se infiere que $x_0 = r_1 - a_1 b_1 q = r_2 + a_2 b_2 q$ es solución del sistema.

Supongamos ahora que todo sistema de n ≥ 2 ecuaciones, que cumpla con la condición del enunciado, tiene solución y consideremos un sistema

$$x \equiv r_1 (\text{mod } a_1),...,x \equiv r_n \text{ (mod } a_n), \; x \equiv r_{n+1} \text{ (mod } a_{n+1}) \qquad \textbf{(3)}$$

que satisface la condición del enunciado sobre los $r_1,\ldots,r_n,r_{n+1}$.

En virtud de la hipótesis inductiva, el sistema

$$x\equiv r_1 (\text{mod } a_1),\ldots,x\equiv r_n \ (\text{mod } a_n)$$

admite una solución x_0. Sea $m = \text{mcm}(a_1,\ldots,a_n)$. Ya sabemos que todo entero y con $y = x_0$ (mod m) también es solución del mismo sistema. En consecuencia, toda solución de

$$x\equiv x_0 \ (\text{mod } m),\ x\equiv r_{n+1} \ (\text{mod } a_{n+1})$$

resuelve el sistema (3) y, como se trata de dos ecuaciones, es condición (necesaria y) suficiente para que admita solución el que

$$d = \text{mcd}(m,\ a_{n+1}) \qquad (4)$$

divida $x_0 - r_{n+1}$. Probemos que así es.

Expresemos $m = p_1^{h1}\ p_2^{h2}\ \ldots p_k^{hk}$ por sus factores primos p_j. Cada p_j^{hj}, es necesariamente factor de algún a_i. Además, como d divide a m, podemos expresar $d = p_1^{e1}p_2^{e2}\ldots p_k^{ek}$, donde los exponentes satisfacen $0 \le e_j \le k_j$

Por definición de d, su factor p_1^{e1} divide algún a_1 (y también a a_{n+1}); luego (para tal i), $x_0 \equiv r_i$ (mod p_1^{e1}), es decir que p_1^{e1} divide a x_0-r_i. Por otro lado, como r_i-r_{n+1} es divisible por mcd(a_i, a_{n+1}) (hipótesis del teorema) y p_1^{e1} es divisor común de a_i y a_{n+1}, se tiene que p_1^{e1} divide a r_i-r_{n+1}. En consecuencia, p_1^{e1} divide a $(x_0 - r_i) + (r_i - r_{n+1}) = x_0 - r_{n+1}$.

En forma idéntica se establece que x_0-r_{n+1} es múltiplo de cada p_j^{ej} para $j = 2,\ldots..,\ k$. Se infiere que x_0-r_{n+1} es divisible por el producto d de todos los p_j^{ej} (ya que éstos son primos por pares). □

Escolio 1. Quienes están familiarizados con las operaciones *booleanas* del mcd y el mcm habrán advertido, en la demostración anterior, que (4) puede expresarse

$d = \text{mcd}(m,\ a_{n+1}) = \text{mcm}(\text{mcd}(a_1,\ a_{n+1}),\ldots.,\ \text{mcd}(a_1,\ a_{n+1}))$,

y, para cada $i = 1,\ldots,\ n$, se tiene $x_0 \equiv r_i$ (mod mcd(a_i, a_{n+1})) (pues mcd(a_i, a_{n+1}) divide a_i) y también $r_i \equiv r_{n+1}$ (mod mcd(a_i, a_{n+1})) (hipótesis del teorema), de donde $x_0 \equiv r_{n+1}$ (mod mcd(a_i, a_{n+1})); es decir, $x_0 - r_{n+1}$ es múltiplo de todos los mcd(a_i, a_{n+1}), lo cual implica que d, el mcm de éstos, divide $x_0 - r_{n+1}$, y esto concluye la prueba.

Si los a_i son primos relativos dos a dos, vale decir, mcd(a_i,a_j)=1, para todo par $i \neq j$, la condición $r_i \equiv r_j$ (mod mcd(a_i,a_j)) se cumple trivialmente, *cualesquiera* sean los enteros r_i, r_j (y ahora $m = a_1a_2\ \ldots\ a_n$). Este caso particular de nuestro teorema 1 es, desde luego, el harto conocido Teorema Chino del Resto en su forma clásica:

Teorema 2. (Teorema Chino del Resto Clásico). *Dados los enteros positivos y primos por pares* $a_1a_2,\ldots,\ a_n$, *el sistema de congruencias* $x\equiv r_1 (\text{mod } a_1)$, $x \equiv r_2$ (mod a_2), ... $x \equiv r_n$ (mod a_n) *tiene solución, cualesquiera sean los enteros* $r_1,\ r_2,\ldots,\ r_n$. *Si* x *es una solución, la clase* $\overline{x}$ módulo $a_1a_2\ \ldots\ a_n$ *es precisarnente el conjunto de todas las soluciones.*

EL TEOREMA CHINO DEL RESTO EN ANILLOS

Todo anillo consierado en adelante se supondrá abeliano con 1.

Sea I un ideal en un anillo A. Recordemos que, para $a,\ b \in$ A,

$$a \equiv b \ (\text{mod } I) \ \Leftrightarrow a - b \in I$$

define una relación de equivalencia sobre A (congruencia módulo I) que es compatible con la suma y producto en A; vale decir, si $a \equiv b$ (mod I) y $a' \equiv b'$ (mod I), entonces $a + a' \equiv b + b'$ (mod I) y $aa' \equiv bb'$ (mod I).

Sabemos que en el anillo Z de los enteros todo ideal I es principal; es decir, I es el conjunto de todos los múltiplos de un cierto entero $d \geq 0$, de modo que $a \equiv b \pmod{I}$ equivale a que a - b es múltiplo de d, lo cual suele escribirse $a \equiv b \pmod{d}$ y es la familiar *congruencia módulo d*.

En un contexto de anillos en general, el Teorema Chino del Resto se refiere a la posibilidad de resolver un sistema simultáneo de congruencias

$$x \equiv r_1 \pmod{I_1}, x \equiv r_2 \pmod{I_2}, \ldots, x \equiv r_n \pmod{I_n} \quad \textbf{(5)}$$

donde $r_1, r_2, \ldots, r_n \in A$ e $I_1, I_2, \ldots, I_n$ son ideales en A.

Si x e y son soluciones, se infiere por transitividad que $x \equiv y \pmod{I_i}$ (o sea $x - y \in I_i$) para $i = 1,2,\ldots,n$, de donde $x - y \in \bigcap I_i$, es decir $x \equiv y \pmod{\bigcap I_i}$. Recíprocamente, si existe una solución x e $y \equiv x \pmod{\bigcap I_i}$, entonces $y - x \in \bigcap I_i$, o sea $y \equiv x \pmod{I_i}$, para $i = 1,2,\ldots,n$, y por transitividad y es solución de (5).

En resumen, si (5) admite alguna solución x, entonces la clase lateral $\bar{x} = x + \bigcap I_i$ es precisamente el conjunto de todas las soluciones.

Supongamos una vez más que el sistema (5) admite una solución x. Entonces $r_i - x \in I_i$ y $x - r_j \in I_j$, por tanto $r_i - r_j = (r_i - x) + (x - r_j)$ está en $I_i + I_j$; es decir, $r_i \equiv r_j \pmod{I_i + I_j}$.

En síntesis, si (5) admite solución, entonces

$r_i \equiv r_j \pmod{I_i + I_j}$, para todo par de subíndices i, j. **(6)**

Nos referiremos a (6) corno la *condición de los restos.*

El recíproco, vale decir, la suficiencia de (6) para la existencia de soluciones del sistema (5), no puede afirmarse en un anillo cualquiera. El teorema 1 establece que este recíproco si es cierto en el anillo de los enteros (si I_i está generado por d_i e I_j por d_j, sabemos que $I_i + I_j$ está generado por $\text{mcd}(d_i, d_j)$). Nos proponemos identificar qué propiedades determinan que la condición de restos (6) sea suficiente para garantizar la solubilidad de (5) en un anillo general (abeliano con 1).

Supongamos que una familia de ideales $I_1, I_2, \ldots, I_n$ de un anillo A tiene la propiedad de que el sistema (5) tiene solución siempre que los $r_1, r_2, \ldots, r_n$ satisfagan la condición de restos (6). Tomemos cualquier subíndice k $(1 \leq k \leq n)$ y un

$$r \in \bigcap_{i \neq k} (I_k + I_i).$$

El sistema

$$x \equiv 0 \pmod{I_1}, \ldots, x \equiv r \pmod{I_k}, \ldots, x \equiv 0 \pmod{I_n}$$

satisface la condición de restos (puesto que $r - 0 = r \in I_k + I_i$ para todo $i \neq k$), de modo que, de acuerdo con nuestra hipótesis, admite una solución x_0. Pero entonces, $x_0 \in I_i$, para todo $i \neq k$, y $x_0 - r \in I_k$, o sea $r = u + x_0$, donde $u \in I_k$ y

$$x_0 \in \bigcap_{i \neq k} I_i.$$

es decir

$$r \in I_k + \bigcap_{i \neq k} I_i.$$

Hemos probado que

$$\bigcap_{i \neq k} (I_k + I_i) \subset I_k + \bigcap_{i \neq k} I_i,$$

pero la inclusión contraria es obviamente cierta, de modo que

$I_k + \bigcap_{i \neq k} I_i = \bigcap_{i \neq k} (I_k + I_i)$, cualquiera que sea k en $\{1, \ldots, n\}$.

Este resultado motiva la siguiente:

Definición 1. *Sea* F *una familia de ideales en un anillo* A. *Decimos que* F *es una familia admisible de ideales si, para todo conjunto finito* $I, J_1, \ldots, J_n$ *en* F, *se tiene*

$$I + \bigcap_{i=1}^{n} J_i = \bigcap_{i=1}^{n} (I+J_i).$$

Nótese que la inclusión

$$I + \bigcap_{i=1}^{n} J_i \subseteq \bigcap_{i=1}^{n} (I+J_i)$$

es evidente y siempre cierta entre ideales.

Una familia de sólo dos ideales es admisible trivialmente. También es obvio que toda subfamilia de una familia admisible es admisible.

Hemos demostrado arriba que, si $I_1, I_2, \ldots, I_n$ son ideales tales que *todo sistema* (5), donde los r_i satisfacen la condición (6), tiene solución, entonces la familia $I_1, I_2, \ldots, I_n$ es admisible.

El recíproco es también cierto y la situación se resume en el siguiente:

Teorema 3. (Teorema Chino del Resto en Anillos). *Sea* $I_1, I_2, \ldots, I_n$ *una familia de ideales en un anillo A. Si el sistema* (5):

$$x \equiv r_1 \pmod{I_1},\ x \equiv r_2 \pmod{I_2}, \ldots, x \equiv r_n \pmod{I_n}$$

tiene solución, entonces los r_i *satisfacen la condición de restos (6). El sistema tiene solución, para todo conjunto* $r_1, r_2, \ldots, r_n$ *que satisface la condición (6), si, y sólo si, los ideales* $I_1, I_2, \ldots, I_n$ *constituyen una familia admisible. En cualquier caso, si x es solución, el conjunto de todas las soluciones es precisamente la clase lateral* $x + \bigcap I_i$.

Demostración. Ya hemos probado que, si existe solución, se cumple la condición de los restos, así como la tipificación de las soluciones en una clase lateral. También hemos visto que si el sistema (5) admite solución siempre que se cumpla la condición de restos (6), entonces los ideales constituyen una familia admisible.

Falta demostrar que, si los $I_1, I_2, \ldots, I_n$ son una familia admisible *y* los r_i satisfacen la condición de los restos (6), entonces el sistema (5) tiene solución.

Procedemos por inducción en *n*.

Para $n = 2$, tenemos el sistema $x \equiv r_1 \pmod{I_1}$, $x \equiv r_2 \pmod{I_2}$, donde $r_1 - r_2 \in I_1 + I_2$ (por (6)); luego, $r_1 - r_2 = u_1 + u_2$, para ciertos $u_1 \in I_1$, $u_2 \in I_2$, y se infiere que $x_0 = r_1 - u_1 = r_2 + u_2$ resuelve el sistema.

Supongamos nuestra tesis cierta para un $n \geq 2$ y probémosla para una familia admisible $I_1, \ldots, I_n, I_{n+1}$, *de* $n + 1$ ideales. Consideremos un sistema

$$x \equiv r_1 \pmod{I_1}, \ldots, x \equiv r_n \pmod{I_n}, x \equiv r_{n+1} \pmod{I_{n+1}} \qquad (7)$$

que cumple con la condición de restos. La hipótesis inductiva afirma que el sistema $x \equiv r_1 \pmod{I_1}, \ldots, x \equiv r_n \pmod{I_n}$ admite alguna solución x_0, y sabemos que x es también solución si, y sólo si,

$$x \equiv x_0 \left(\text{mod} \bigcap_{i=1}^{n} I_i\right)$$

En consecuencia, toda solución de

$$x \equiv x_0 \left(\text{mod} \bigcap_{i=1}^{n} I_i\right),\ x \equiv r_{n+1} \pmod{I_{n+1}}$$

resuelve nuestro sistema (7) y, por el caso $n = 2$, éste último es soluble si (y sólo si) cumple la condición de restos:

$$r_{n+1} - x_0 \in I_{n+1} + \bigcap_{i=1}^{n} I_i. \qquad (8)$$

En efecto, por definición de x_0 y por hipótesis del teorema, tenemos

$r_i - x_0 \in I_i$ y $r_{n+1} - r_i \in I_{n+1} + I_i$, ambos para cada $i = 1,..., n$; luego, $r_{n+1} - x_0 = (r_{n+1} - r_i) + (r_i - x_0) \in I_{n+1} + I_i$, para todo $i = 1,..., n$; de donde,

$$r_{n+1} - x_0 \in \bigcap_{i=1}^{n} (I_{n+1} + I_i)$$

lo cual demuestra (8), en virtud de que los ideales $I_1,...,I_n, I_{n+1}$ constituyen una familia admisible. □

Un caso de importancia es el de una familia $I_1,..., I_n$, de ideales propios ($\neq A$), con $I_i + I_j = A$, para todo par $i \neq j$. Se dice que estos ideales son *primos relativos por pares* o, más brevemente, *co-primos*. Ocurre que tal familia es siempre admisible. En efecto (por inducción en el número n de ideales), para $n = 2$ no hay nada que probar; tomemos $n = 3$ ideales I, J, K (véase la definición (1)). Basta con probar que $I + (J \cap K) = A$, ya que $(I + J) \cap (I + K) = A$. Tomemos un $x \in A$ cualquiera. Como $x \in I + J = A$ y $1 \in I + K = A$, se tiene $x = u, + v$ y $1 = u' + w$, donde $u,u' \in I$, $v \in J$, $w \in K$. Luego, $x = (u, + v)(u' + w) = (u,u' + uw + vu') + vw \in I + (J \cap K)$.

Supongamos que nuestra afirmación es cierta para toda familia de $n \geq 3$ ideales co-primos y consideremos la familia $I_1,..., I_n, I_{n+1}$ de $n + 1$ ideales co-primos. Tenemos

$$I_1 + \bigcap_{i=2}^{n+1} I_i = I_1 + \left(\bigcap_{i=2}^{n+1} I_i\right) \cap I_{n+1}$$

pero $I_1 + I_{n+1} = A$ y (hipótesis inductiva)

$$I_1 + \bigcap_{n=2}^{n} I_i = A;$$

luego, por el caso $n = 3$,

$$I_1 + \bigcap_{i=2}^{n+1} I_i = A = \bigcap_{i=2}^{n+1} (I_1 + I_i)$$

y la demostración sería idéntica tomando cualquier otro de los ideales en lugar de I_1.

En resumen, toda familia de ideales co-primos es admisible.

Por otra parte, con respecto a una familia de ideales co-primos $I_1,..., I_n$, todo conjunto de elementos $r_1,..., r_n$ en A satisface trivialmente la condición de los restos (6). Aplicando entonces el teorema general (3), ha quedado establecido (casi todo) el siguiente:

Teorema 4. (Teorema Chino del Resto Clásico en Anillos (a)). *Sea $I_1,..., I_n$ una familia de ideales propios de un anillo A. El sistema (5) tiene solución, para cualquier conjunto de elementos $r_1,..., r_n$ en A, si, y sólo si, los ideales $I_1,..., I_n$ son co-primos. Si x es solución, el conjunto de todas las soluciones es precisamente la clase lateral $x + \bigcap I_i$.*

Demostración. Sólo falta probar el recíproco; vale decir, si existe solución del sistema para cualquier conjunto de elementos $r_1,..., r_n$ en A, entonces los ideales $I_1,..., I_n$ son co-primos. En efecto, como el sistema

$$x \equiv 0 \pmod{I_1},...,x \equiv 1 \pmod{I_k},...,x \equiv 0 \pmod{I_n}$$

tiene solución, satisface la condición de los restos, por tanto $1 = 1 - 0 \in I_k + I_i$ lo cual implica $I_k + I_i = A$ y esto es cierto para todo par $k \neq i$.

El teorema precedente se puede expresar en esta otra forma elegante, perfectamente equivalente, cuyo examen se deja al lector.

Teorema 5. (Teorema Chino del Resto Clásico en Anillos (b)). *Sea $I_1,..., I_n$ una familia de ideales propios de un anillo A. Los anillos*

$$\frac{A}{\bigcap I_i} \quad \text{y} \quad \frac{A}{I_1} \times .... \times \frac{A}{I_n}$$

son isomorfos bajo $\psi(x + \bigcap I_i) = (x + I_1,..., x + I_n)$ si, y sólo si, los ideales $I_1,..., I_n$ son co-primos.

La función ψ es un homomorfismo inyectivo (monomorfismo) para cualquier familia de ideales de A. Es su sobreyectividad la que ocurre si, y sólo si, los ideales son co- primos.

Si no se exige esa condición a la familia de ideales, ψ puede no ser sobreyectiva, y la pregunta de cuándo un $(r_i + I_i,...,r_n + I_n)$ pertenece a su rango es precisamente la que responde el Teorema Chino del Resto General 3.

Anillos chinos. Pronto veremos que, en general, un anillo puede contener familias no-admisibles de ideales (véase la definición 1). Sin embargo, si la familia de todos los ideales del anillo es admisible, es obvio que cualquier familia de ideales en semejante anillo es admisible. Más abajo comprobaremos que existe un abundante repertorio de tales anillos, pero antes obtengamos una significativa caracterización de éstos.

Proposición. *La familia de todos los ideales de un anillo A es admi.sible si, y sólo si, la intersección de ideales en A es distributiva con respecto a la suma de los mismos.*

Demostración. Supongamos que la totalidad de los ideales es admisible y tomemos tres ideales I, J, K. Aplicando dos veces la definición 1,

$$I \cap J + I \cap K = (I \cap J + I) \cap (I \cap J + K)$$
$$= I \cap (K + I \cap J) =$$
$$= I \cap [(K + I) \cap (K + J)] = [I \cap (K + I)] \cap (K + J) = I \cap (J + K).$$

Recíprocamente, supongamos la intersección distributiva con respecto a la suma de ideales y probemos que toda familia de éstos es admisible. Basta con verificar la definición 3.1 de admisibilidad para tres ideales I, J, K. El caso de n procede por inducción evidente.

$$(I + J) \cap (I + K) = I + I \cap K + J \cap I + J \cap K = I + J \cap K \qquad \square$$

Definición 2. *Un anillo (abeliano con 1) se denomina anillo chino si la intersección de sus ideales es distributiva con respecto a la suma de los mismos.*

Como corolario obvio del Teorema Chino General (3), obtenemos:

Teorema 4. Sea $I_1,...,I_n$ *una familia cualquiera de ideales en un anillo chino A. El sistema* $x \equiv r_1 \pmod{I_1},...,x \equiv r_n \pmod{I_n}$ *tiene solución si, y sólo si, los elementos* $r_1,...,r_n$ *satisfacen la condición de los restos* (6).

Y ya sabemos que la clase lateral de una solución comprende exactamente la totalidad de las soluciones. Más aún, el mismo Teorema Chino General (3) nos dice que si todo sistema $x \equiv r_1 \pmod{I_1},..., x \equiv r_n \pmod{I_n}$ que satisfaga la condición de los restos tiene solución, entonces toda familia de ideales es admisible, lo cual quiere decir que el anillo es chino.

Se infiere de esto último, en virtud del Teorema Chino Generalizado (1), que el anillo de los enteros Z es chino. Puede demostrarse directamente, desde luego, tomando tres ideales I, J, K en Z y probando que

$$I \cap (J + K) = I \cap J + I \cap K.$$

En efecto, se trata de ideales generados por enteros positivos a, b, c repectivamente y no es otra cosa que la identidad $\text{mcm}(a,\text{mcd}(b,c)) = \text{mcd}(\text{mcm}(a,b),\text{mcm}(a,c))$.

Más general y de manera idéntica se demuestra que todo *dominio de ideal principal*[4] es chino. Tal es el caso, por ejemplo, de un anillo de polinomios en x sobre un cuerpo.

Con argumentos más elaborados se prueba que todo *dominio de Dedekind* es chino.

En otro extremo del espectro, recordemos que un *anillo booleano* es un anillo con 1 cuyos elementos son todos *idempotentes*, es decir $x^2 = x$. Se prueba con facilidad que estos anillos, que son forzosamente abelianos (y siempre $x + x = 0$) también son chinos. En efecto, tomemos tres ideales I, J, K y

demostremos que $I \cap (J + K) \subseteq I \cap J + I \cap K$ (la inclusión contraria es obvia): si $x \in I \cap (J + K)$, entonces $x = u = v + w$, donde $u \in I$, $v \in J$, $w \in K$; luego, $x = x^2 = u(v + w) = uv + uw \in I \cap J + I \cap K$.

De modo muy similar se demuestra que un *anillo regular de von Neumann* (abeliano) es chino. Estos anillo son aquellos en los cuales a todo elemento x corresponde algún y tal que $x = yx^2$ (se deja al lector).

Terminemos con un sencillo ejemplo de un anillo no chino, el cual nos fue comunicado por el Profesor Thomas Berry (Universidad Simón Bolívar). Sea $Q[x,y]$ el anillo de polinomios en x, y sobre los racionales, y consideremos los ideales principales $I = \langle x + y \rangle$, $J = \langle x \rangle$, $K = \langle y \rangle$. Ocurre que $I \cap (J + K) \neq I \cap J + I \cap K$ (compruebe el lector que $x + y \in I \cap (J + K)$, pero $x + y \notin I \cap J + I \cap K$).

NOTAS

[1] No confundirlo con Sun-Tzu, autor del Artc de la Guerra, quien vivió en el siglo IV A.C. y tenía otras preocupaciones.

[2] Dickson (1965), pág. 57 y siguientes.

[3] Gauss

[4] dominio de integridad cuyos ideales son todos principales.

LITERATURA CITADA

BEURLING, A.
1955. Closure Problem related to the Riemann Zeta-Function. *Proc. Acad. Sci.*, 41: 312-314.

DICKSON, L.E.
1992. *History of the Theory of Numbers*, Vol. II, Chelsea, N.Y. Capítulo II, p. 64.

GAUSS, C.F.
1965 *Disquisitiones Aritmeticae*, trans. A.A. Clarke, Yale University Press, Section II, 34, p. 15.

STICLTJES, T.J.
1890. *Annales Fac. Sc. Toulouse* , 4: 31-32.

USPENSKY, J. V. AND M. A. HEASLET
1939. *Elementary Number Theory*. Cao VII, 5, pag. 1985. McGraw-Hill, New York and London.