EL TEOREMA CHINO

LÓGICA Y MATEMÁTICA DISCRETA

María González García

Mediante las ecuaciones diofánticas se permite la resolución de una sola ecuación perteneciente a los números enteros. En el estudio de las ecuaciones diofánticas, nos enfrentamos al desafío de encontrar valores enteros que satisfagan las condiciones de la ecuación proporcionada. Sin embargo, hay problemas en los que se precisa la resolución de sistemas en congruencia, y para ello se aplica el Teorema Chino del Resto.

1ª. PARTE: TEÓRICA

1.1. Cálculos con congruencias:

En el campo de la teoría de números, los cálculos con congruencias tratan un papel fundamental. Estos cálculos permiten trabajar a través de las propiedades modulares de números enteros, centrándose en la relación de equivalencia que mantienen los números entre ellos cuando se dividen por un numero en específico, siendo este el módulo.

1.2. El teorema chino del resto:

El teorema chino del resto fue desarrollado durante el siglo III por el matemático Sun Tzu con la finalidad de resolver los antiguos problemas prácticos de la época relacionados con la astronomía, predecir eclipses solares y lunares, o las matemáticas, resolver problemas de división. En relación con ello, su nombre se debe a que este teorema fue usado para repartir un tesoro de manera equitativa entre varios herederos.

Este teorema permite encontrar una única solución para un sistema de ecuaciones lineales en congruencias. Se trata de un resultado matemático que establece que para unas ciertas ecuaciones lineales en congruencias con todos los módulos siendo primos entre sí, se puede encontrar una solución única mediante otra ecuación de primer grado cuyo modulo equivale al producto de los anteriores módulos.

1.2.1 Enunciado

$$\begin{cases} x \equiv b_1 (mod. m_1) \\ x \equiv b_2 (mod. m_2) \\ \dots \\ x \equiv b_n (mod. m_n) \end{cases}$$

Sean $b_n \in \mathrm{Z}\ y\ m_n \in \mathrm{N}/(m_i, m_j) = 1\ ;\ \forall\ i \neq j$ tiene única solución módulo $M = m_1 * m_2 * \dots * m_n$. A su vez, la solución viene dada a través de la siguiente ecuación: $x \equiv b_1 * c_1 * d_1 + b_2 * c_2 * d_2 + \dots + b_n * c_n * d_n\ (mod. M)$. Verificándose: $c_i = \frac{M}{m_i}\ ;\ c_i * d_i \equiv 1\ (mod. m_i)\ \forall\ 1 \leq i \leq n$.

1.2.2 Demostración

Primeramente, denominamos sistema lineal de congruencia al siguiente conjunto de ecuaciones:

$$\begin{cases} x \equiv a_1 (mod. m_1) \\ x \equiv a_2 (mod. m_2) \\ \dots \\ x \equiv a_n (mod. m_n) \end{cases}$$

Además, se dice que x es solución del sistema cuando satisface simultáneamente a todas las ecuaciones planteadas.

La demostración se divide en dos partes, verificar la existencia y unicidad para la solución.

Existencia

Consideremos: $M = m_1 * m_2 * \dots * m_n$ y $c_i = \frac{M}{m_i}$. Como todos los módulos son coprimos entre sí, entonces c_i y m_i también lo serán: $(m_i, c_i) = 1$. Mediante la identidad de Bézout (dado un par de enteros su MCD es igual a la combinación lineal más pequeña de ellos siendo igual al MCD: $ax + by = (a, b)$), llegamos a la conclusión de que existen un $d_i e_i$, tal que: $d_i * c_i + e_i * m_1 = 1$.

Trabajando mediante módulos dónde $i \neq j$:

$$d_i * c_i \equiv 1(mod.\ m_i)$$
$$d_i * c_i \equiv 0(mod.\ m_j)$$

Definimos que $x = \sum_{i=1}^{k} a_i * d_i * c_i$, siendo x la solución del sistema. A su vez, al estar trabajando en el módulo m_i concluimos que: $x \equiv a_i\ (mod.\ m_i)\ \forall\ i = 1,2 \dots, k$.

Unicidad

Primeramente, debemos definir dos números enteros distintos entre sí (*x, y*) tal que:

$$\begin{matrix} x \equiv a_i(mod.\ m_i) \\ y \equiv a_i(mod.\ m_i) \end{matrix} \forall\ i = 1,2 \dots, k$$

Se deduce que $x - y \equiv 0\ (mod.\ m_i)$, pero al ser todos los m_i coprimos entre sí podemos plantear la siguiente ecuación: $x - y \equiv 0\ (mod.\ M)$, es decir, despejando: $x \equiv y\ (mod.\ M)$. En conclusión, la solución es única en módulo N

2ª. PARTE: PRÁCTICA

A continuación, se realizará la resolución de un problema para el que se necesita aplicar este teorema.

2.1. Enunciado

Una banda de 13 piratas asaltó un barco mercantil y se hizo con una gran cantidad de monedas de oro, todas idénticas entre sí. Cuando trataron de distribuirlas equitativamente entre ellos, les sobraron 8 monedas. Por lo tanto, decidieron no repartirlas. Imprevistamente, dos de ellos contrajeron sarampión y murieron. Al volver a intentar repartir las monedas, les sobraron 3, y por lo tanto volvieron a cancelar la distribución. Posteriormente, murieron otros 3 piratas ahogados. Los restantes volvieron a intentar distribuir las monedas, pero les sobraron 5. Cansados de tanto intentar distribuir sin poder ser equitativos, optaron por guardar las monedas hasta que se les ocurriese una solución.

Tiempo después, los piratas se arrepintieron de todas sus fechorías y decidieron hacer un acto caritativo a modo de redención. Se dirigieron a un pueblo muy pobre en el que había exactamente 1136 personas viviendo, y decidieron integrarse al pueblo para iniciar una nueva vida. Más aún, decidieron que repartirían equitativamente todas las monedas entre todos los habitantes del pueblo, incluyéndose a ellos. Pero, para su sorpresa, volvieron a sobrar monedas. ¿Cuántas monedas sobraron?

2.2. Resolución

Primero obtenemos las ecuaciones:

$$\begin{cases} x \equiv 8(mod. 13) \\ x \equiv 3(mod. 11) \\ x \equiv 5(mod. 8) \end{cases}$$

Sabemos que tiene solución ya que todos los pares de módulos son coprimos dos a dos.

$$N = 13 * 11 * 8 = 1144$$

$$c_1 = {}^{1144}/_{13} = 88\ ;\ c_2 = {}^{1144}/_{11} = 104\ ;\ c_3 = {}^{1144}/_{8} = 143$$

Con estos distintos valores de c, debemos encontrar d:

$$d_1 * 88 \equiv 1(mod.13)$$
$$d_2 * 104 \equiv 8(mod.11)$$
$$d_3 * 143 \equiv 1(mod.8)$$

Calculando los inversos correspondientes mediante el algoritmo de Euclides, se consigue lo siguiente:

$$d_1 \equiv 4(mod.13)$$
$$d_2 \equiv 9(mod.11)$$
$$d_3 \equiv 7(mod.8)$$

De la siguiente manera obtenemos la siguiente solución final al sistema de congruencias (por el Teorema Chino del Resto):

$$x = 8 * 88 * 4 + 3 * 104 * 9 + 5 * 143 * 7 = 10629 \equiv 333\ (mod.1144)$$

Concluimos finalmente que cuando se intentó distribuir las monedas entre la población del pueblo, sobraron 333 monedas.

3ª. CONCLUSION: APLICACIONES

Mediante la teoría y a través de la práctica, se ha explorado su aplicación y algunos ejemplos simples sobre como calcular sistemas lineales de ecuaciones en congruencia. Sin embargo, este teorema es sumamente importante en numerosos ámbitos, sobre todo en la informática.

En la rama de la criptografía, este teorema es usado para garantizar la seguridad de la información mediante la realización de operaciones aritméticas en grandes números. Además de ello, se implementa en la informática teórica, exactamente en la teoría de autómatas y lenguajes formales, rama encargada del estudio de la aplicación a la resolución de problemas mediante maquinas.

En cuanto al ámbito matemáticos, ya mencionado en la introducción del tema, esta teoría es fundamental para la teoría de números y el estudio de las propiedades de los números enteros.

En resumen, se trata de una herramienta matemática versátil e importante implementada en distintas áreas para facilitar la resolución de problemas complejos.

4ª. BIBLIOGRAFÍA

Rasis, J. P. (29 de Mayo de 2019). Teorema Chino del Resto, Pequeño Teorema de Fermat. *http://cms.dm.uba.ar/academico/materias/1ercuat2019/algebra_I/TCRyPTF.pdf*.

S., J. C., & O., C. d. (2007). El Teorema de los Restos Chinos . *Revista del Instituto de Matemática y Física*.

UCM. (s.f.). *TEOREMA CHINO DEL RESTO.* Obtenido de http://blogs.mat.ucm.es/cruizb/wp-content/uploads/sites/48/2019/07/Z-Congruencias-7.pdf.