Teorema Chino del Resto

Álgebra de enteros

Yago Pajariño

Febrero 2022

1 Introducción

Todos tuvimos en algún momento que contar cosas, normalmente nos alcanza con los dedos de las manos. Sin emgargo, existen ocasiones en las que el simple uso de las manos no basta para poder contar en grandes cantidades.

Imaginemos contar granos de arroz en un paquete, personas en un concierto, etc. Podríamos intentar numerar de uno en uno, posiblemente perdiendo la cuenta en unos pocos segundos/minutos.

Sin embargo imaginemos que, sin mucho esfuerzo, podemos organizar los elementos en grupos de cantidades fijas, digamos contamos cuantos grupos de 3 elementos, 5 elementos, 19 elementos, etc se pueden formar y, especialmente, cuantos de ellos quedan sueltos al final, ¿Podría ayudarnos a calcular el total?

En el siglo tres después de cristo aparece el siguiente enunciado en el escrito *Sunzi Suanjing* del matemático chino Sun-tzu:

"Hay ciertas cosas cuya cantidad es incierta. Si las contamos en grupos de tres, sobran dos; en grupos de cinco, tres; en grupos de siete, dos. ¿Cuántas cosas hay?"

Así surge el Teorema Chino del Resto, uso de restos para calcular totales.

2 Desarrollo

Primeramente demos notación a las cosas que sabemos, siguiendo el enunciado de Sun-Tzu. Definimos $n =$ "Cantidad total de una cosa". Lo primero que sabemos es que:

$$n \text{ es un número entero } \iff n \in \mathbb{Z}. \tag{1}$$

Sabemos que cualquier número entero, se puede escribir como divisor por cociente más resto. Digamos por ejemplo que $7 = 2.3 + 1$ Aquí decimos que 2 es el divisor, 3 es el cociente y 1 es el resto.

Como en este caso solo nos centramos en los restos, sin importar el cociente, podemos utilizar la notación de congruencias. Siguiendo el ejemplo, sabemos

que 7 es *congruente* a 1 *módulo* 2. Así tenemos una relación entre el dividendo, divisor y resto. Lo notamos $7 \equiv 1(2)$

Volviendo al enunciado de Sun-Tzu, podemos traducir el mismo usando congruencias como:

$$n \equiv 2(3)$$
$$n \equiv 3(5)$$
$$n \equiv 2(7)$$

Acá es donde el teorema nos ayuda. Está probado, no lo haremos aquí, que dadas las cogruencias de n en módulos comprimos dos a dos, existe una única solución módulo el producto de los módulos.

Resolvamos el problema del enunciado para terminar de entender que es lo que permite este teorema.

3 Solución

Tenemos tres ecuaciones de congruencia módulos 3, 5 y 7. Es claro que los tres son coprimos entre sí, más aún son primos. Además tenemos los restos de n para esos módulos así que, por ejemplo, la primer ecuación nos dice que n tiene que tener resto 2 al dividirlo por tres, es decir $n \in \{2, 5, 8, 11, 14, 17, 20, ...\}$, la segunda que tiene que tener resto 3 al dividirlo por 5, $n \in \{3, 8, 13, 18, 23, 28, 33, ...\}$ y resto 2 al dividirlo por 7, $n \in \{2, 9, 16, 23, 30, 37, 44, 51, ...\}$

Pero además sabemos por el teorema que la solución es unica congruente al producto de los móldulos. Así, n debe ser congruente a algún número módulo $3 * 5 * 7 = 105$

Así, si encontramos algún número menor a 105 que cumpla las tres ecuaciones en simultaneo, será el n que estamos buscando y será el único posible.

El primer método para resolver el sistema consiste en enumerar los candidatos que cumplen con cada una de las ecuaciones por separado y verificar cual es, el único, que aparece en los tres conjuntos.

Luego definamos:

- T_1 = números congruentes a 2 módulo 3 menores que 105.
- T_2 = números congruentes a 3 módulo 5 menores que 105.
- T_3 = números congruentes a 2 módulo 7 menores que 105.

Así,

$$T_1 = \{2, 5, 8, 11, 14, 17, 20, \mathbf{23}, 26, 29, 32, 35, 38, 41, 44, 47, 50, 53, 56, 59, 62, 65, 68, 71, 74, 77, 80, 83, 86, 89, 92, 95, 98, 101, 104\}$$

$$T_2 = \{3, 8, 13, 18, \mathbf{23}, 28, 33, 38, 43, 48, 53, 58, 63, 68, 73, 78, 83, 88, 93, 98, 103\}$$

$$T_3 = \{2, 9, 16, \mathbf{23}, 30, 37, 44, 51, 58, 65, 72, 79, 86, 93, 100\}$$

Se ve que el único número que está contenido en los tres conjuntos es el 23, así concluímos que $n = 23$ es la solución al enunciado de Sun-Tzu.

Sin embargo, el tener que desarrollar todos los conjuntos puede ser muy engorroso e ineficiente. Probemos otra forma de resolver el sistema.

Podemos primero encontrar un número que cumpla con las dos primeras ecuaciones, las de menor módulo, y luego buscar una solución conjunta con la tercera. Así, primero buscamos un número congruente a 2 módulo 3 y a 3 módulo 5. Además debe ser menor que $3 * 5 = 15$. Es simple ver que 8 cumple con ambas.

Ahora, podemos rearmar el sistema como:

$$n \equiv 8(15)$$
$$n \equiv 2(7)$$

Tenemos un sistema de dos ecuaciones, pero los módulos siguen siendo coprimos entre sí. Luego, buscamos un número congruente a 8 módulo 15 y a 2 módulo 7, menor que $15 * 7 = 105$.

Podemos ir probando con los numeros de la forma $15 * k + 8$ con $0 \leq k \leq 6$ y ver cual es el primero que cumple lo pedido.

$$k = 0 \Rightarrow 15.0 + 8 = 8$$
$$k = 1 \Rightarrow 15.1 + 8 = 23$$

Así, llegamos también a que $n = 23$ es solución al problema.

References

[1] Departamento de Matemática, Facultad de Ciencias Exactas y Naturales, Universidad de Buenos Aires http://web.dm.uba.ar/

[2] Teorema Chino del Resto https://en.wikipedia.org/wiki/Chinese_remainder_theorem

[3] Sunzi Suanjing https://en.wikipedia.org/wiki/Sunzi_Suanjing