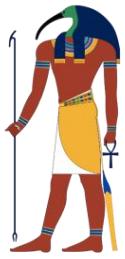

Píldora nº 12: ¿Qué son los inversos multiplicativos en un cuerpo?

Escena 1: Concepto de inverso multiplicativo

Se dice que un número a, elemento del cuerpo n, tiene inverso multiplicativo en dicho cuerpo, o simplemente inverso, si existe otro número x que haga cumplir la condición de que a * x mod n = 1, la identidad de la multiplicación.

Viendo la ecuación anterior y aunque matemáticamente no sea correcto, por simplicidad podríamos asociar el concepto del inverso a que a = 1/x y que x = 1/a en ese cuerpo n.

Escena 2: Condición necesaria para la existencia del inverso

Para que se cumpla relación a * x mod n = 1, es imprescindible que el máximo común divisor entre a y n sea la unidad, es decir mcd (a, n) = 1.

Si esto no se tiene en cuenta, podríamos llegar al sinsentido de cifrar algo y que el receptor sea incapaz de descifrarlo. Por ejemplo, tal sería el caso si en un sistema elemental de cifra en módulo 27 multiplicamos el código de cada letra por 3; la cifra se produce pero no será posible descifrar ya que no existe el inverso de 3 en ese módulo 27.

Escena 3: Visualización de los inversos

Sea el cuerpo n = 10 con elementos o restos {0, 1, 2, 3, 4, 5, 6, 7, 8, 9}. A excepción del 0 y del 1 donde no tiene sentido hablar de estos inversos, los únicos elementos en 10 que tendrán inversos son el 3, el 7 y el 9, pues el máximo común divisor de estos números y 10 es igual a 1.

Para comprobar que el 3 tiene inverso en 10, podríamos multiplicar todos los elementos de n por 3 reduciendo módulo 10 y ver qué sucede.

3*0 = 0 mod 10 = 0	3*1 = 3 mod 10 = 3	3*2 = 6 mod 10 = 6	3*3 = 9 mod 10 = 9
3*4 = 12 mod 10 = 2	3*5 = 15 mod 10 = 5	3*6 = 18 mod 10 = 8	3*7 = 21 mod 10 = **1**
3*8 = 24 mod 10 = 4	3*9 = 27 mod 10 = 7		

Realizando esta operación con los 10 elementos del cuerpo, observamos que se obtienen todos los restos y que solamente en el caso de x = 7 obtenemos el resultado 1 que estábamos esperando.

Por lo tanto, el inverso de 3 en el cuerpo 10 es 7, de la misma manera que el inverso de 7 en el cuerpo 10 es 3. Además, ese valor será único.

Escena 4: Cálculo de inversos

El ejercicio anterior es adecuado para explicar de una manera gráfica qué significa un inverso dentro de un cuerpo, pero en absoluto es un algoritmo eficiente para encontrarlo. Para realizar este cálculo se utilizará el Algoritmo Extendido de Euclides, pero esto será materia de una próxima píldora.

Madrid, octubre de 2014

Autor del guion: *Jorge Ramió Aguirre*
Dirección Proyecto Thoth: *Jorge Ramió Aguirre, Alfonso Muñoz Muñoz*