Píldora nº 24: ¿Por qué usamos el algoritmo de Euclides para calcular inversos?

Escena 1: Buscando el máximo común divisor

Sabemos que Euclides fue un importante matemático griego que vivió entre los años 330 y 275 antes de Cristo. El algoritmo que lleva su nombre permite encontrar el máximo común divisor entre dos números. Por ejemplo, entre los números 450 y 120 el máximo común divisor será 30 porque es el mayor número por el cual podemos dividir 450 y 120 y obtener como resultado un número entero.

A partir de este conocido algoritmo, que no ha lugar analizar en esta píldora, nace el algoritmo extendido de Euclides que nos permitirá encontrar el inverso multiplicativo de un número dentro de un cuerpo cuando estos dos números en cuestión son coprimos o primos relativos, es decir, no tienen factores en común. Tal sería el caso de los números 28 y 135 puesto que 28 es igual a 2^2x7 y 135 es igual a 3^3x5. En este caso diremos que el número 28 tendrá un inverso en 135 porque el máximo común divisor entre ellos es la unidad; esto es MCD (28, 135) = 1.

Escena 2: El algoritmo extendido de Euclides y los inversos

Si MCD (a, n) = 1, existirá el inverso de a en el cuerpo n. En nuestro ejemplo, el inverso del elemento 28 en el cuerpo 135 sí existe. Aplicando Euclides a estos dos números, tenemos:

135 = 4 x **28** + **23** (resto)	Ordenando por restos:	**23** = **135** – 4 x **28**
28 = 1 x **23** + **5** (resto)		**5** = **28** – 1 x **23**
23 = 4 x **5** + **3** (resto)		**3** = **23** – 4 x **5**
5 = 1 x **3** + **2** (resto)		**2** = **5** – 1 x **3**
3 = 1 x **2** + **1** (resto)		**1** = **3** – 1 x **2**
2 = 2 x **1** + 0 (resto)	Fin del algoritmo MCD (28, 135) = 1	

Reordenando por restos seremos capaces de encontrar el inverso que buscamos, inv (28, 135). Esto es, expresaremos mcd (28, 135) = 1 como la mínima combinación lineal de esos números.

Escena 3: Ordenando por restos, el principio del algoritmo extendido de Euclides

En el ejemplo anterior, reemplazando los restos de manera que todas las ecuaciones queden en función de los valores **28** y **135**, los de nuestro problema, tendremos:

a) 23 = **135** – 4 x **28**

b) 5 = 28 – 1 x 23 = **28** – 1 x (**135** – 4 x **28**) = 5 x **28** – **135**

c) 3 = 23 – 4 x 5 = (**135** – 4 x **28**) – 4 x (5 x **28** – **135**) = -24 x **28** + 5 x **135**

d) 2 = 5 – 1 x 3 = (5 x **28** – **135**) – 1 x (-24 x **28** + 5 x **135**) = 29 x **28** – 6 x **135**

e) 1 = 3 – 1 x 2 = (-24 x **28** + 5 x **135**) – 1 x (29 x **28** – 6 x **135**) = -53 x **28** + 11 x **135**

1 = -53 x **28** + 11 x **135**, lo que es cierto puesto que multiplicando: 1 = - 1.484 + 1.485

Como el módulo es 135 entonces 1 = (-53 x 28 + 11 x 135) mod 135 = -53 x 28 mod 135. Por tanto en módulo 135 se tiene que 1 = -53 x 28 mod 135. Pero como -53 mod 135 = 82, se tiene finalmente que 1 = 82 x 28 mod 135, que efectivamente cumple la característica de inverso porque 82 x 28 mod 135 = 2.296 mod 135 = (17 x 135 + 1) mod 135 = 1.

Por tanto, se concluye que el inverso de 28 en el cuerpo 135 es el valor 82. El hecho de que aparezcan los dígitos 2 y 8 intercambiados en los inversos es sólo una simpática casualidad.

¿Podríamos encontrar este inverso de una manera más sencilla y directa? Claro que sí, pero esto será materia de una siguiente píldora.

Madrid, enero de 2015

Autor del guion: *Jorge Ramió Aguirre*

Dirección Proyecto Thoth: *Jorge Ramió Aguirre, Alfonso Muñoz Muñoz*