Desafío 85 Bis. Número Racional (Dospew)

Número Racional , en forma decimal (No sirve p.ej. √2 como posible K)

N/D = K, que expreso como E,d (E, parte entera y d, parte decimal)

Entonces si con la primera K efectúo la operación 1/ (su parte decimal) obtengo K1

Con este K1, si su parte decimal no es 0, itero 1/(su parte decimal) y obtengo K2 y así hasta que obtengo un Kn entero, o sea su parte decimal es 0. Entones :

- 1º con todos los números decimales que he probado llego a un entero bastante rápido
- 2º El producto de todos esos K, sin el original, da un denominador y el producto de todos los K, incluido el original, da un Numerador , que resultan ser la fracción irreductible de K.

Solución.

El procedimiento parece muy interesante. ¿Estamos ante el descubrimiento de un nuevo método para descomponer enteros?. Si es así, en unas semanas nos cargaremos todos los sistemas criptográficos conocidos y nos forraremos.

Veamos las pegas. Formalicemos un poco el procedimiento. Los datos de partida son N_1, D_1. Los demás N_i, D_i se calculan así:

$$N_i = \begin{cases} Dato\ de\ partida\ para\ i = 1 \\ \\ 1\ para\ i > 1 \end{cases} \qquad D_i = \begin{cases} Dato\ de\ partida\ para\ i = 1 \\ \\ \frac{1}{d_{i-1}}\ para\ i > 1 \end{cases}$$

Para cada i, incluido i=1, los demás datos calculados son:

$$K_i = \frac{N_i}{D_i} \qquad E_i = Parte\ entera\ \{K_i\} \qquad d_i = Parte\ decimal\ \{K_i\}$$

Y lo que se afirma, y se puede comprobar es que, definiendo n, A, B del siguiente modo:

$$n = primer\ i\ tal\ que\ d_i = 0 \qquad A = \prod_{i=1}^{n} K_n \qquad B = \prod_{i=2}^{n} K_n$$

Entonces A/B es la fracción irreducible de N_1/D_1

Esto aparentemente permite obtener fácilmente los factores comunes de dos enteros cualesquiera. Lo cual es un bombazo si el algoritmo es rápido. El problema es que estamos usando aritmética de números flotantes. Es decir, estamos operando con números con decimales. En un PC, esto ocasiona que se alcance muy rápido el límite de precisión, y comprobar si K_i es cero no es trivial. Tampoco lo es multiplicar todos los K_i para obtener A o B.

Para analizar esto, mataremos tres pájaros de un tiro:

- Evitaremos las operaciones con números decimales, con el objetivo de pensar en una implementación en un ordenador libre de errores de precisión.
- De paso, obtendremos la demostración.
- Y por último, veremos si proporciona un algoritmo suficientemente rápido para reventar los sistemas criptográficos y entrar en los ordenadores de la CIA.

Modificación del algoritmo.

Lo primero que haremos es modificar el algoritmo para no tener que trabajar con números decimales. Si repasamos las ecuaciones más arriba, el problema lo obtenemos en estos casos, donde estamos realizando una división donde el denominador es decimal:

$$D_i = \frac{1}{d_{i-1}} \qquad K_i = \frac{N_i}{D_i}$$

Pero podemos esquivar esas operaciones, ya que lo que importa al final es obtener la parte entera y decimal de cada K_i. Para eso, expresaremos K_i como fracción de enteros, lo que nos obliga a que los N_i dejen de ser 1. Pero además, operaremos con la parte decimal también como fracción, en la forma Pi/Di (notese que la parte decimal escrita como fracción tendrá el mismo denominador que el número original). Esto no tiene ninguna trascendencia sobre los resultados finales, pero nos permite eliminar los errores de precisión. Un PC puede operar con enteros sin errores. Si se sobrepasa el límite para enteros, se pueden usar cadenas de texto con su representación en base 10 y programar funciones que operen sobre estas cadenas.

El algoritmo quedaría así:

$$N_i = \begin{cases} Dato\ de\ partida\ para\ i = 1 \\ \\ D_{i-1}\ para\ i > 1 \end{cases} \qquad D_i = \begin{cases} Dato\ de\ partida\ para\ i = 1 \\ \\ P_{i-1}\ para\ i > 1 \end{cases}$$

Para cada i, incluido i=1, los demás datos calculados son:

$$K_i = \frac{N_i}{D_i} \qquad E_i = Parte\ entera\ \{K_i\} = Parte\ entera\ \left\{\frac{N_i}{D_i}\right\}$$

$$d_i = Parte\ decimal\ \{K_i\} = Parte\ decimal\ \left\{\frac{N_i}{D_i}\right\} = \frac{P_i}{D_i}$$

Veamos que ahora no necesitamos hacer operaciones con números decimales. Los Ki y los di no se usan (o no es imprescindible usarlos) en los cálculos de los demas. La única duda es como calcular Pi, el numerador de la parte decimal de un cociente entre enteros. Pero se puede buscar una fórmula alternativa:

$$P_i = N_i - E_i\, D_i$$

Así que reformulamos el algoritmo prescindiendo de números decimales. Todas las variables en las siguientes expresiones serían enteras, y se calculan con aritmética entera.

$$N_i = D_{i-1} \qquad D_i = P_{i-1} \qquad E_i = Parte\ entera\ \left\{\frac{N_i}{D_i}\right\} \qquad P_i = N_i - E_i\, D_i$$

$$n\ tal\ que\ P_n = 0 \qquad A = \prod_{i=1}^{n} \frac{N_i}{D_i} = \frac{\prod_{i=1}^{n} N_i}{\prod_{i=1}^{n} D_i} \qquad B = \prod_{i=2}^{n} \frac{N_i}{D_i} = \frac{\prod_{i=2}^{n} N_i}{\prod_{i=2}^{n} D_i} \qquad \frac{A}{B} = \frac{N_1}{D_1}$$

Comprobación del algoritmo modificado.

Antes de seguir, vamos a comprobar las modificaciones, con el caso K_1=69/15. Las columnas sombreadas en gris se incluyen para cotejar con el algoritmo original, pero no se usan en los cálculos.

N_i	D_i	K_i	E_i	d_i	$1/d_i$	P_i
$N_i = D_{i-1}$	$D_i = P_{i-1}$	$K_i = \frac{N_i}{D_i}$	$E_i = Ent\left\{\frac{N_i}{D_i}\right\}$	$d_i = Dec\{K_i\}$		$P_i = N_i - E_i D_i$
69	15	4,6	4	0,6	1,666666667	9
15	9	1,666666667	1	0,666666667	1,5	6
9	6	1,5	1	0,5	2	3
6	3	2	2	0		0

Los cálculos de A y B que dan la fracción irreducible serían:

$$A = \prod_{i=1}^{n} \frac{N_i}{D_i} = \frac{\prod_{i=1}^{n} N_i}{\prod_{i=1}^{n} D_i} = \frac{69 \cdot 15 \cdot 9 \cdot 6}{15 \cdot 9 \cdot 6 \cdot 3} = \frac{55.980}{2.430} = 23$$

$$B = \prod_{i=2}^{n} \frac{N_i}{D_i} = \frac{\prod_{i=1}^{n} N_i}{\prod_{i=1}^{n} D_i} = \frac{15 \cdot 9 \cdot 6}{9 \cdot 6 \cdot 3} = \frac{810}{162} = 5$$

Y efectivamente, 23/5 es la fracción irreducible de 69/15. Aquí vemos ya la clave de la demostración. Multiplicar los K_i como número decimal equivale a multiplicarlos como fracciones, dadas por N_i/D_i. Pero en la secuencia, cada N_i se anula con el denominador de la fila anterior D_{i-1}, cuyos valores coinciden, y solo nos quedamos con el primer numerador y el último denominador. Para el caso de A, en este ejemplo, serían 69 y 3. Para el caso de B, que empieza en la fila con numerador 15, serían 15 y 3. Los valores 69 y 15, en naranja en la tabla, son los datos de partida, y el 3, en verde en la tabla, sería el último Pi diferente de cero. Este parece ser el máximo divisor de los valores iniciales (69 y 15).

Demostración de que A/B es una forma reducida de N_1/D_1.

Extendámoslo, más formalmente, al caso general:

$$A = \frac{\prod_{i=1}^{n} N_i}{\prod_{i=1}^{n} D_i} = \frac{N_1 \cdot \prod_{i=2}^{n} N_i}{D_n \cdot \prod_{i=1}^{n-1} D_i} = \frac{N_1 \cdot \prod_{i=2}^{n} D_{i-1}}{D_n \cdot \prod_{i=1}^{n-1} D_i} = \frac{N_1 \cdot \prod_{i=1}^{n-1} D_i}{D_n \cdot \prod_{i=1}^{n-1} D_i} = \frac{N_1}{D_n}$$

$$B = \frac{\prod_{i=2}^{n} N_i}{\prod_{i=2}^{n} D_i} = \frac{N_2 \cdot \prod_{i=3}^{n} N_i}{D_n \cdot \prod_{i=2}^{n-1} D_i} = \frac{N_2 \cdot \prod_{i=3}^{n} D_{i-1}}{D_n \cdot \prod_{i=2}^{n-1} D_i} = \frac{N_2 \cdot \prod_{i=2}^{n-1} D_i}{D_n \cdot \prod_{i=2}^{n-1} D_i} = \frac{N_2}{D_n}$$

Como además, $N_2 = D_1$ y $D_n = P_{n-1}$, tendremos:

$$A = \frac{N_1}{P_{n-1}} \qquad B = \frac{D_1}{P_{n-1}} \qquad \frac{A}{B} = \frac{N_1}{D_1}$$

Esto demuestra que A/B es una fracción equivalente a N_1/D_1. Además, es en general, una fracción más reducida, ya que recordemos que P_{n-1} es un valor entero. Pero no hemos demostrado que sea la forma más reducida. Esto solo sería si P_{n-1} es el máximo común divisor de N_1 y D_1

Redefiniendo el algoritmo.

Vamos a enfocar el problema a hallar el máximo común divisor de números enteros, lo que nos soluciona el problema original. Lo formulamos así:

Sean N_1 y D_1 dos números enteros. Entonces, si aplicamos el algoritmo dado por las fórmulas siguientes hasta obtener un valor $P_n=0$, el valor P_{n-1} es el máximo común divisor de N_1 y D_1.

$$N_i = D_{i-1} \qquad D_i = P_{i-1} \qquad E_i = Ent\left\{\frac{N_i}{D_i}\right\} \qquad P_i = N_i - E_i D_i$$

A mi juicio, lo que queda por hacer es:

- Demostrar que siempre se alcanza un valor de $P_n=0$
- Demostrar que en ese caso, P_{n-1} es el máximo común divisor de N_1 y D_1.

Y si es así, ya podemos ponernos a reventar los sistemas de seguridad de la CIA.