RESOLUCION SISTEMA DE CONGRUENCIAS

Autor: Daniel Pérez Ruiz

1. ENUNCIADO DEL PROBLEMA

- Sea $d = 12345678$. Sea $u = d \mod 100$, $v = \frac{d-u}{100} \mod 100$, $w = \frac{d-100v-u}{10000} \mod 100$
- Resuelve el siguiente sistema de ecuaciones:
  - $x \equiv u \mod 101$.
  - $x \equiv v \mod 102$.
  - $x \equiv w \mod 103$.

2. SOLUCIÓN

2.1 PREPARACIÓN DE LOS DATOS

- Tenemos que $u = 12345678 \mod 100 = 78$, $v = 56$, $w = 34$.
- Ademas tenemos que:
  - $mcd(101, 102) = 1$
  - $mcd(101, 103) = 1$ (Obvio, puesto que son primos).
  - $mcd(102, 103) = 1$
- Llamemos $n_1 = 101, n_2 = 102, n_3 = 103$. Vamos a hallar los s_i , con $i \in \{1, 2, 3\}$ tal que $s_i \cdot \frac{n}{n_i} \equiv 1 \mod n_i$, donde $n = n_1 \cdot n_2 \cdot n_3 = 1061106$

2.2 CÁLCULO DE LOS s_i

- Para s_1:

$$s_1 \cdot \frac{1061106}{101} \equiv 1 \mod 101 \Rightarrow s_1 \cdot 10506 \equiv 1 \mod 101 \Rightarrow 2 \cdot s_1 \equiv 1 \mod 101 \Rightarrow s_1 = 51$$

- Para s_2:

$$s_2 \cdot \frac{1061106}{102} \equiv 1 \mod 102 \Rightarrow s_2 \cdot 10403 \equiv 1 \mod 102 \Rightarrow 101 \cdot s_2 \equiv 1 \mod 102 \Rightarrow s_2 = 101$$

- Para s_3:

$$s_3 \cdot \frac{1061106}{103} \equiv 1 \mod 103 \Rightarrow s_3 \cdot 10302 \equiv 1 \mod 103 \Rightarrow 2 \cdot s_3 \equiv 1 \mod 103 \Rightarrow s_3 = 52$$

2.3 CÁLCULO DEL ENTERO a

- Una vez hemos calculado los s_i, tenemos todo lo necesario para calcular el valor de x, que se calcula de la siguiente forma:

$$a = \sum_{i=1}^{3} b_i \cdot s_i \cdot \frac{n}{n_i}$$

- Donde $b_1 = u, b_2 = v, b_3 = w$.
- Procedamos a calcular a:

$$a = 78 \cdot 51 \cdot 10506 + 56 \cdot 101 \cdot 10403 + 43 = 100632279$$

2.4 CÁLCULO DE x

- Ahora sólo nos falta calcular x. Para ello en primer lugar tenemos que $x \equiv a \mod 1061106 = 888315$
- Sin embargo, ésta solución no es única, por lo que $x = 888315 + 1061106 \cdot m, m \in \mathbb{Z}$.

3. COMPROBACIÓN

- Vamos a comprobar la validez y veracidad de este resultado:
  - $888315 \mod 101 = 78$
  - $888315 \mod 102 = 56$
  - $888315 \mod 103 = 34$