

Project Euler Problem 700 - Eulercoin

Problem 700: Leonhard Euler was born on 15 April 1707. Consider the sequence $1504170715041707 \cdot n \pmod{4503599627370517}$. An element of this sequence is defined to be an Eulercoin if it is strictly smaller than all previously found Eulercoins.

For example, the first term is 1504170715041707 which is the first Eulercoin. The second term is 3008341430083414 which is greater than 1504170715041707 so is not an Eulercoin. However, the third term is 8912517754604 which is small enough to be a new Eulercoin.

The sum of the first 2 Eulercoins is therefore 1513083232796311. Find the sum of all Eulercoins.

Proof. It is easy by iteratively setting values for $n \in \mathbb{Z}$ to find the first 14 Eulercoins (the 14th one being $e_{14} = 428410324$, after that being computationally unmanagable).

Let $a = 1504170715041707$, $b = 4503599627370517$ and e denote the candidate Eulercoin. Notice that $(a, b) = 1$ so it's invertible in \mathbb{Z}_b , $\exists a^{-1}$ such that

$$a \cdot a^{-1} \pmod{b} \equiv 1 = e_1$$

where e_1 is the second smallest Eulercoin (the first one being $e_0 = 0$). By the extended Euclidean Algorithm one finds $a^{-1} = 3451657199285664$.

$$\begin{aligned} a \cdot n \pmod{b} = e &\Rightarrow an \equiv e \pmod{b} \Rightarrow \\ n &\equiv a^{-1}e \pmod{b} \end{aligned} \tag{1}$$

From this we can keep a list of the first 14 Eulercoins, start from the (second) smallest Eulercoin e_1 and iteratively increase the possible Eulercoin and if n is smaller than all the previous Eulercoins, append to the list of Eulercoins, until we reach e_{14} .

□