Ejercicio 7

David García Curbelo

Toma tu número $n = 4230659086792057869605292356791$ de la lista publicada para el ejercicio 3. Sea d el primer elemento de la sucesión $5, -7, 9, -11, 13, \ldots$ que satisface que el símbolo de Jacobi es $(d|n) = -1$.

Apartado I. ***Con*** $P = 1$***,*** $Q = (1-d)/4$***, define el e.c.*** α ***y sus sucesiones de Lucas asociadas.*** Calculamos primero el valor de d mediante el símbolo de Jacobi:

$d = 5$ $\left(\frac{5}{n}\right) = \left(\frac{n}{5}\right)$ por ser $5 \equiv 1 \pmod 4$. Pero ahora vemos que $n \equiv 1 \pmod 5$, luego tenemos $\left(\frac{n}{5}\right) = \left(\frac{1}{5}\right) = 1$.

$d = -7$ $\left(\frac{-7}{n}\right) = \left(\frac{-1}{n}\right)\left(\frac{7}{n}\right) = -(-1)^{(n-1)/2}\left(\frac{7}{n}\right) = \left(\frac{7}{n}\right)$ por ser $7 \equiv 3 \pmod 4$. Pero ahora vemos que $n \equiv 1 \pmod 7$, luego tenemos $\left(\frac{n}{-7}\right) = \left(\frac{1}{7}\right) = 1$.

$d = 9$ $\left(\frac{9}{n}\right) = \left(\frac{n}{9}\right)$ por ser $9 \equiv 1 \pmod 4$. Pero ahora vemos que $n \equiv 7 \pmod 9$, luego tenemos $\left(\frac{n}{9}\right) = \left(\frac{7}{9}\right)$. Ahora, $\left(\frac{7}{9}\right) = -\left(\frac{9}{7}\right)$ porque $7 \equiv 3 \pmod 4$. Vemos que $9 \equiv 2 \pmod 7$, luego tenemos $-\left(\frac{9}{7}\right) = -\left(\frac{2}{7}\right)$. Comprobamos a continuación que $7 \equiv -1 \pmod 8$, luego concluimos $-\left(\frac{2}{7}\right) = -1$.

Hemos encontrado el valor de $d = 9$ que nos interesa. Así podemos hayar la forma explícita de $P = 1$ y $Q = -2$. De la misma manera podemos hayar la forma explícita de $\Delta = P^2 - 4Q = 9$ y $\alpha = P + Q$.

Apartado II. ***Si*** n ***primo, ¿Qué debería pasarle a*** V_r, U_r, ***módulo*** n***? ¿Y a*** $V_{r/2}$, $U_{r/2}$***? Calcula los términos*** V_r, U_r, $V_{r/2}$, $U_{r/2}$ ***módulo*** n, ***de las sucesiones de Lucas. ¿Tu*** n ***verifica el TPF para el entero cuadrático*** α***?***

Apartado III. ***Factoriza*** $r = n + 1$ ***y para cada factor primo*** p ***suyo, calcula*** $U_{r/p}$***. ¿Cuál es el rango de Lucas*** $w(n)$***? ¿Qué deduces sobre la primalidad de tu*** n***?***