Ejercicio 7

David García Curbelo

Toma tu número $n = 42306590867920578696052923567 91$ 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:

- $\left(\frac{5}{n}\right) = 1$
- $\left(\frac{-7}{n}\right) = 1$
- $\left(\frac{9}{n}\right) = 1$
- $\left(\frac{-11}{n}\right) = 1$
- $\left(\frac{13}{n}\right) = -1$

Hemos encontrado el valor de $d = 13$ que nos interesa. Así podemos hayar la forma explícita de $P = 1$ y $Q = -3$. De la misma manera podemos hayar la forma explícita de $\Delta = P^2 - 4Q = 13$ y por tanto obtener $\alpha = \frac{P+\sqrt{\Delta}}{2} = \frac{1+\sqrt{13}}{2}$.

Las sucesiones de lucas asociadas son las siguientes:

- $V_n = P \cdot V_{n-1} - Q \cdot V_{n-2} = V_{n-1} + 3 \cdot V_{n-2}$
- $U_n = P \cdot U_{n-1} - Q \cdot U_{n-2} = U_{n-1} + 3 \cdot U_{n-2}$

Con $V_0 = 2$, $V_1 = P$, $U_0 = 0$, $U_1 = 1$.

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***?***

Si tomamos n suponiendo que es primo, por la tercera versión del TPF para elementos cuadráticos tenemos que, como $\left(\frac{\Delta}{n}\right) = -1$ por definición, tienen que cumplirse las siguientes ecuaciones:

$$\begin{cases} U_{n-\left(\frac{\Delta}{n}\right)} \equiv 0 \pmod{n} & \Rightarrow \quad U_{n+1} \equiv 0 \pmod{n} \\ V_{n-\left(\frac{\Delta}{n}\right)} \equiv 2Q \pmod{n} & \Rightarrow \quad V_{n+1} \equiv -6 \pmod{n} \end{cases}$$

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***?***
Factorizamos $r = n+1 = 42306590867920578696052923567 92 = 2^3 \cdot 52883238584900723370066154459 9$. Desconocemos si $m_1 = 52883238584900723370066154459 9$ es primo o no. Para saberlo aplicamos el test de composición de Fermat y obtenemos que $2^{m_1-1} \not\equiv 1 \pmod{m_1}$ (algoritmo de exponenciación rápida) con lo que obtenemos un certificado de composición. Ahora factorizando mediante el algoritmo ρ de Polard, obtenemos un divisor 4349 en 46 iteraciones, quedando por tanto $52883238584900723370066154459 9 = 4349 \cdot 12159861711864962835149725 1$.

Veamos a continuación si $m_2 = 12159861711864962835149725 1$ es primo o no. Para saberlo aplicamos el test de composición de Fermat y obtenemos que $2^{m_2-1} \not\equiv 1 \pmod{m_2}$ (algoritmo de exponenciación rápida) con lo que obtenemos un certificado de composición. Ahora factorizando mediante el algoritmo ρ de Polard, obtenemos un divisor 62347 en 46 iteraciones, quedando por tanto $12159861711864962835149725 1 = 62347 \cdot 1950352336417945183433$.

Repetimos el mismo proceso para $m_3 = 1950352336417945183433$. Aplicando el test de composición de Fermat, obtenemos que $2^{m_3-1} \not\equiv 1 \pmod{m_3}$ (algoritmo de exponenciación rápida) con lo que obtenemos un certificado de composición. Ahora factorizando mediante el algoritmo ρ de Polard, obtenemos un divisor 1924630699 en 26395 iteraciones, quedando por tanto $1950352336417945183433 = 1924630699 \cdot 1013364453467$.

Veamos por último si $m_4 = 1013364453467$ es primo o no. se puede ver que dicho número pasa el test de Solovay-Strassen para las bases 2, 3, 5, 7 y 11, por lo que tenemos altas probabilidades de que dicho número sea primo. Busquemos ahora un elemento primitivo de m_4. Para ello factorizamos primero el número $m_4 - 1 = 1013364453466 = 2 \cdot 506682226733$.

Veamos si $m_{4,1} = 506682226733$ es primo o no. Aplicamos de nuevo el test de composición de Fermat y obtenemos que $2^{m_{4,1}-1} \not\equiv 1 \pmod{m_{4,1}}$ (algoritmo de exponenciación rápida) con lo que obtenemos un certificado de composición. Busquemos ahora sus factores primos mediante el algoritmo ρ de Polard, con el que obtenemos un divisor 73 en solo 6 iteraciones, quedando por tanto $506682226733 = 73 \cdot 6940852421$.

Tomando ahora $m_{4,2} = 6940852421$ veamos si es primo. Vemos que pasa el test de Solovay-Strassen para las bases 2, 3, 5, 7 y 11, por lo que tenemos altas probabilidades de que dicho número sea primo. Busquemos ahora un elemento primitivo de $m_{4,2}$. Para ello factorizamos primero el número $m_{4,2} - 1 = 6940852420 = 2^2 \cdot 5 \cdot 347042621$.

Veamos si $m_{4,2,1} = 347042621$ es primo o no. Vemos que pasa el test de Solovay-Strassen para las bases 2, 3, 5, 7 y 11, por lo que tenemos altas probabilidades de que dicho número sea primo. Aplicamos de nuevo el algoritmo de Lucas-Lehmer para ver si $m_{4,2,1}$ es primo o no. Para ello factorizamos $m_{4,2,1} - 1 = 2^2 \cdot 5 \cdot 17352131$, y veamos si $m_{4,2,1,1} = 17352131$ es primo o no.

Vemos que pasa el test de Solovay-Strassen para las bases 2, 3, 5, 7 y 11, por lo que tenemos altas probabilidades de que dicho número sea primo. Aplicamos de nuevo el algoritmo de Lucas-Lehmer para ver si $m_{4,2,1,1}$ es primo o no. Para ello factorizamos $m_{4,2,1,1} - 1 = 2 \cdot 5 \cdot 1735213$, y veamos si $m_{4,2,1,1,1} = 1735213$ es primo o no.

Aplicando el test de composición de Fermat, obtenemos que $2^{m_{4,2,1,1,1}-1} \not\equiv 1 \pmod{m_{4,2,1,1,1}}$ (algoritmo de exponenciación rápida) con lo que obtenemos un certificado de composición. Aplicamos el algoritmo ρ de Polard para obtener un divisor 19 en solo 4 iteraciones, quedando por tanto $1735213 = 19 \cdot 91327$.

Veamos de nuevo si $m_{4,2,1,1,2} = 91327$ es primo o no. Aplicando el test de composición de Fermat, obtenemos que $2^{m_{4,2,1,1,2}-1} \not\equiv 1 \pmod{m_{4,2,1,1,2}}$ (algoritmo de exponenciación rápida) con lo que obtenemos un certificado de composición. Aplicamos el algoritmo ρ de Polard para obtener un divisor 271 en solo 9 iteraciones, quedando por tanto $91327 = 271 \cdot 337$, quedando así completamente descompuesto.

Tenemos por tanto $m_{4,2,1,1} - 1 = 2 \cdot 5 \cdot 5 \cdot 19 \cdot 271 \cdot 337$, por lo que estamos preparados para buscar un elemento primitivo de $m_{4,2,1,1} = 17352131$.

- $2^{m_{4,2,1,1}-1} \equiv 1 \pmod{m_{4,2,1,1}}$
- $2^{(m_{4,2,1,1}-1)/2} \not\equiv 1 \pmod{m_{4,2,1,1}}$

- $2^{(m_{4,2,1,1}-1)/5} \not\equiv 1 \pmod{m_{4,2,1,1}}$
- $2^{(m_{4,2,1,1}-1)/19} \not\equiv 1 \pmod{m_{4,2,1,1}}$
- $2^{(m_{4,2,1,1}-1)/271} \not\equiv 1 \pmod{m_{4,2,1,1}}$
- $2^{(m_{4,2,1,1}-1)/337} \not\equiv 1 \pmod{m_{4,2,1,1}}$

Y así hemos obtenido un elemento primitivo, luego podemos afirmar que $m_{4,2,1,1} = 17352131$ es primo.

Con este resultado obtenemos la factorización en primos de $m_{4,2,1} - 1 = 2^2 \cdot 5 \cdot 17352131$, por lo que estamos preparados para buscar un elemento primitivo de $m_{4,2,1} = 347042621$.

- $3^{m_{4,2,1}-1} \equiv 1 \pmod{m_{4,2,1}}$
- $3^{(m_{4,2,1}-1)/2} \not\equiv 1 \pmod{m_{4,2,1}}$
- $3^{(m_{4,2,1}-1)/5} \not\equiv 1 \pmod{m_{4,2,1}}$
- $3^{(m_{4,2,1}-1)/17352131} \not\equiv 1 \pmod{m_{4,2,1}}$

Y así hemos obtenido un elemento primitivo, luego podemos afirmar que $m_{4,2,1} = 347042621$ es primo.

Con este resultado obtenemos la factorización en primos de $m_{4,2} - 1 = 2^2 \cdot 5 \cdot 347042621$, por lo que estamos preparados para buscar un elemento primitivo de $m_{4,2} = 6940852421$.

- $3^{m_{4,2}-1} \equiv 1 \pmod{m_{4,2}}$
- $3^{(m_{4,2}-1)/2} \not\equiv 1 \pmod{m_{4,2}}$
- $3^{(m_{4,2}-1)/5} \not\equiv 1 \pmod{m_{4,2}}$
- $3^{(m_{4,2}-1)/347042621} \not\equiv 1 \pmod{m_{4,2}}$

Y así hemos obtenido un elemento primitivo, luego podemos afirmar que $m_{4,2} = 6940852421$ es primo.

Con este resultado obtenemos la factorización en primos de $m_4 - 1 = 2 \cdot 73 \cdot 6940852421$, por lo que estamos preparados para buscar un elemento primitivo de $m_4 = 1013364453467$.

- $2^{m_4-1} \equiv 1 \pmod{m_4}$
- $2^{(m_4-1)/2} \not\equiv 1 \pmod{m_4}$
- $2^{(m_4-1)/73} \not\equiv 1 \pmod{m_4}$
- $2^{(m_4-1)/6940852421} \not\equiv 1 \pmod{m_4}$

Y así hemos obtenido un elemento primitivo, luego podemos afirmar que $m_4 = 1013364453467$ es primo. Con ello hemos obtenido finalmente una factorización total del número $r = n + 1$ en factores primos, que son los siguientes:

$p_1 = 2^3$

$p_2 = 4349$

$p_3 = 62347$

$p_4 = 1924630699$

$p_5 = 1013364453467$

Calculemos a continuación $U_{r/p}$ para cada p en la lista anterior.