CUERPOS CUADRÁTICOS Y SUC. DE LUCAS

¿Cómo certificar primalidad con suc. de Lucas?

1. Números algebraicos

Los números de Lucas o sucesiones de Lucas se definen en el contexto del anillo de enteros de un cuerpo cuadrático. Por tanto, antes de dar siquiera su definición, daremos algunas definiciones más generales.

Definición 1. *Decimos que $\alpha \in \mathbb{C}$ es **algebraico** si es la raíz de un polinomio con coeficientes racionales. O sea, si existe $g(x) = a_n x^n + \cdots + a_0 \in \mathbb{Q}[x]$ tal que $g(\alpha) = a_n \alpha^n + \cdots + a_0 = 0$. En otro caso, decimos que α es **trascendente**.*

El conjunto, $I_\alpha = \{g(x) \in \mathbb{Q}[x] : g(\alpha) = 0\}$,de todos los polinomios que tienen a α como raíz es un subgrupo aditivo y es lícito para la multiplicación. Así, es un ideal de $\mathbb{Q}[x]$. Como $\mathbb{Q}$ es cuerpo, el anillo de polinomios es un DE⇒ DIP⇒ DFU⇒ DI. Todo ideal es principal en $\mathbb{Q}[x]$ y por tanto

$$I_\alpha = \big(f(x)\big) = \{\lambda(x) f(x) : \lambda(x) \in \mathbb{Q}[x]\}$$

Como los múltiplos escalares de un polinomio tienen las mismas raíces, podemos tomar $f(x)$ con coeficiente líder 1 (**mónico**). A ese generador único

Definición 2. *Le llamamos el **polinomio mínimo** de α, $f(x) = polmin(\alpha)$.*

Como podemos multiplicar por el mcm (mínimo común múltiplo) de los denominadores de los coeficientes del polmin$(\alpha) \in \mathbb{Q}[x]$, siempre existe un polinomio entero, $f(x) \in \mathbb{Z}$, de grado mínimo tal que $f(\alpha) = 0$.

Definición 3. *Si el mcd de sus coeficientes es 1, le llamamos el* ***polinomio primitivo mínimo*** *de α. Si el polmin(α) es entero, entonces es el polinomio primitivo mínimo. En este caso, decimos que α es un* ***entero algebraico***.

El lema de Gauss sobre polinomios primitivos nos asegura que si α es raíz de un polinomio entero mónico también lo es su polinomio mínimo. Por tanto,

Lema 1. *α es entero algebraico $\Leftrightarrow$ es raíz de un polinomio entero mónico.*

Definición 4. *Los más sencillos son raíces de polinomios cuadráticos irreducibles en $\mathbb{Z}[x]$ y los llamamos* ***enteros cuadráticos***.

Ejemplo 1. *$\alpha = i$ y $\beta = -i$ son enteros algebraicos porque*

$$\left.\begin{array}{l}\alpha+\beta=0\\ \alpha\beta=-(i)^2=1\end{array}\right\}\Rightarrow polmin(\alpha)=polmin(\beta)=x^2+1\in\mathbb{Z}[x]$$

Ejemplo 2. *$\alpha = 1+\sqrt{2}$ y $\beta = 1-\sqrt{2}$ son enteros algebraicos porque*

$$\left.\begin{array}{l}\alpha+\beta=2\\ \alpha\beta=1^1-(\sqrt{2})^2=-1\end{array}\right\}\Rightarrow polmin(\alpha)=polmin(\beta)=x^2-2x-1\in\mathbb{Z}[x]$$

Ejemplo 3. *$\alpha = \frac{1+i\sqrt{3}}{2}$ y $\beta = \frac{1-i\sqrt{3}}{2}$ son enteros algebraicos porque*

$$\left.\begin{array}{l}\alpha+\beta=1\\ \alpha\beta=\frac{1^1-(i\sqrt{3})^2}{4}=\frac{4}{4}=1\end{array}\right\}\Rightarrow polmin(\alpha)=polmin(\beta)=x^2-x+1\in\mathbb{Z}[x]$$

Como vemos, los enteros cuadráticos van a pares y son de dos tipos.

2. Irracionales cuadráticos

Si $P, Q, \Delta \in \mathbb{Z}$ con Δ no cuadrado perfecto, $\alpha = \frac{P+\sqrt{\Delta}}{Q}$ y $\beta = \frac{P-\sqrt{\Delta}}{Q}$. Entonces,

$$\left.\begin{array}{l} a = \alpha + \beta = \frac{2P}{Q} \in \mathbb{Q} \\ b = \alpha\beta = \frac{P^2-\Delta}{Q^2} \in \mathbb{Q} \end{array}\right\} \Longrightarrow f(x) = x^2 - ax + b \in \mathbb{Q}[x] \text{ es irreducible}$$

$\alpha, \beta \in \mathbb{C}$ son irracionales y son las raíces de $f(x)$. Además,

Lema 2. *α es entero algebraico si y sólo si β lo es si y sólo si $a, b \in \mathbb{Z}$.*

Los enteros algebraicos los clasificamos en dos grupos:

Tipo I) Si Q es impar,

$$\left.\begin{array}{l} aQ = 2P \\ bQ^2 = P^2 - \Delta \end{array}\right\} \Rightarrow \left.\begin{array}{l} P = a'Q \Rightarrow bQ^2 = a'^2Q^2 - \Delta \Rightarrow \\ \Delta = (a'^2 - b)Q^2 \Rightarrow \sqrt{\Delta} = Q\sqrt{d} \end{array}\right\} \Rightarrow \left.\begin{array}{l} \alpha = \frac{P+\sqrt{\Delta}}{Q} = a' + \sqrt{d} \\ \beta = \frac{P-\sqrt{\Delta}}{Q} = a' - \sqrt{d} \end{array}\right\}$$

Tipo II) Si Q par, $Q = 2Q'$, entonces

$$\left.\begin{array}{l} P^2 - \Delta = bQ^2 = b4Q'^2 \\ 2P = aQ \Rightarrow P = aQ' \end{array}\right\} \Rightarrow \left.\begin{array}{l} a^2Q'^2 - \Delta = b4Q'^2 \Rightarrow \\ \Delta = (a^2 - 4b)Q'^2 \end{array}\right\} \Rightarrow \sqrt{\Delta} = Q'\sqrt{d'}$$

con $d' = a^2 - 4b$ y entonces $\left.\begin{array}{l} \alpha = \frac{P+\sqrt{\Delta}}{Q} = \frac{a+\sqrt{d'}}{2} \\ \beta = \frac{P-\sqrt{\Delta}}{Q} = \frac{a-\sqrt{d'}}{2} \end{array}\right\}$

Como las dos raíces de todo polinomio cuadrático irreducible se pueden expresar como $\alpha = \frac{P+\sqrt{\Delta}}{Q}$ y $\beta = \frac{P-\sqrt{\Delta}}{Q}$, tenemos

Lema 3. *Los enteros cuadráticos son de dos tipos o bien* $a \pm \sqrt{\Delta}$ *o bien* $\frac{a\pm\sqrt{\Delta}}{2}$, *donde en este último caso* $\Delta = a^2 - 4b$ *y* $\Delta \equiv 1 \pmod 4$.

Demostración: Para los de tipo II, como $\Delta = a^2 - 4b$ implica que Δ es un cuadrado módulo 4, $\Delta \equiv 1 \pmod 4$ o bien $\Delta \equiv 0 \pmod 4$.

Pero si $\Delta = a^2 - 4b = n^2 d$ con d entero libre de cuadrados, entonces a y n tienen la misma paridad y los e.c. de tipo II, se pueden escribir como

$$\frac{a \pm n\sqrt{d}}{2} = \frac{a-n}{2} + n\frac{1 \pm \sqrt{d}}{2} = m + n\frac{1 \pm \sqrt{d}}{2}$$

Como $\Delta \equiv 0 \pmod 4 \Leftrightarrow n$ par $\Leftrightarrow \frac{n}{2} = \mu \in \mathbb{Z}$. En este caso, los e.c. son $\lambda \pm \mu\sqrt{d}$ con λ, μ enteros y no son tipo II. Absurdo que implica $\Delta \equiv 1 \pmod 4$.

Ejemplo 4. *Como* $-3 \equiv 1 \pmod 4$ *y el conjugado* $\frac{1-\sqrt{-3}}{2} = 1 - \frac{1+\sqrt{-3}}{2}$, *el conjunto de todos los e.c. pertenecientes al cuerpo* $\mathbb{Q}\left(\sqrt{-3}\right)$ *es el subanillo*

$$\mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right] = \left\{m + n\frac{1+\sqrt{-3}}{2} : \ m, n \in \mathbb{Z}\right\} \subset \mathbb{Q}\left(\sqrt{-3}\right)$$

Ejemplo 5. *El conjunto de todos los e.c. en* $\mathbb{Q}(\sqrt{-4}) = \mathbb{Q}(i)$ *es*

$$\mathbb{Z}[i] = \{m + ni : \ m, n \in \mathbb{Z}\} \subset \mathbb{Q}(i)$$

3. Una caracterización de algebraico

Si existen $\theta_1,\ldots,\theta_n \in \mathbb{C}$ tales que los productos, $\alpha\theta_j$, son combinaciones racionales, $\alpha\theta_j = a_{j1}\theta_1 + \cdots + a_{jn}\theta_n$. Entonces, para todo j,

$$0 = a_{j1}\theta_1 + \cdots + (a_{jj} - \alpha)\theta_j + \cdots + a_{jn}\theta_n$$

Así, el sistema lineal de n ecuaciones con n incógnitas tiene solución

$$a_{j1}x_1 + \cdots + (a_{jj} - \alpha)x_j + \cdots + a_{jn}x_n = 0$$

distinta de la trivial y por tanto el determinante de sus coeficientes es cero.

$$\begin{vmatrix} a_{11} - \alpha & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{nn} - \alpha \end{vmatrix} = 0 \Rightarrow \alpha^n + b_1\alpha^{n-1} + \cdots + b_n = 0$$

Como los b_i se obtienen de los coeficientes a_{ij} usando sólo sumas y multiplicaciones, se tiene que $b_i \in \mathbb{Q}$ para todo i y si $a_{ij} \in \mathbb{Z}$, también los $b_i \in \mathbb{Z}$. O sea, α es algebraico si los $a_{ij} \in \mathbb{Q}$ son racionales y si los $a_{ij} \in \mathbb{Z}$ entonces α es raíz de un polinomio $f(x) = x^n + b_1x^{n-1} + \cdots + b_n \in \mathbb{Z}$ entero mónico y por el lema de Gauss su polinomio mínimo también es entero mónico. Así,

Lema 4. *α es algebraico si los coeficientes son racionales, $a_{ij} \in \mathbb{Q}$, y es un entero algebraico si además son enteros, $a_{ij} \in \mathbb{Z}$.*

Observamos que el polinomio encontrado desarrollando el determinante no es el polmin salvo que sea irreducible sobre los racionales.

4. Estructura de los números algebraicos

Ahora, si $\alpha, \beta \in \mathbb{C}$ son e.a., satisfacen dos polinomios enteros mónicos.

$$\alpha^r + a_{r-1}\alpha^{r-1} + \cdots + a_0 = 0 \Rightarrow \alpha^r = -a_{r-1}\alpha^{r-1} - \cdots - a_0$$
$$\beta^s + b_{s-1}\alpha^{s-1} + \cdots + b_0 = 0 \Rightarrow \beta^s = -b_{r-1}\beta^{r-1} - \cdots - b_0$$

Y si consideramos los $n = rs$ productos $\theta_{ij} = \alpha^i \beta^j$ con $i \in \{0, \ldots, r-1\}$ y $j \in \{0, \ldots, s-1\}$, numerados en cualquier orden (por ej., lexicográfico de parejas), tenemos n números complejos θ_{ij}.

Usando las igualdades anteriores se demuestra que los productos $\alpha\theta_{ij}$ y $\beta\theta_{ij}$ se pueden escribir como combinaciones lineales enteras de los θ_{ij}. Por tanto, también su suma $(\alpha + \beta)\theta_{ij}$ es una c.l. entera de los θ_{ij}.

Usando el lema anterior, $\alpha + \beta$ satisface un polinomio entero mónico. Así,

Lema 5. *Si α y β son números o enteros algebraicos también lo es $\alpha + \beta$.*

También $-\alpha$ es una c.l. de los θ_{ij}. O sea, $-\alpha$ es e.a. si lo es α. Por tanto,

Lema 6. *Los conjuntos de n.a. y de los e.a. son subgrupos aditivos de $\mathbb{C}$.*

Usando recursivamente las igualdades iniciales, también los productos $\alpha\beta\theta_{ij}$ se pueden poner como c.l. enteras o racionales de los θ_{ij}. Así,

Lema 7. *Si α y β son n.a. o e.a. también lo es $\alpha\beta$. Por tanto, los conjuntos de los números o enteros algebraicos son subanillos de los complejos.*

Multiplicando por el inverso α^{-1}, r veces se tiene que α^{-1} es algebraico

$$\alpha^r + a_{r-1}\alpha^{r-1} + \cdots + a_0 = 0 \Rightarrow 1 + a_{r-1}\alpha^{-1} - \cdots - a_0\alpha^{-r} = 0$$

pero en general no es un entero algebraico. Así,

Lema 8. *El conjunto de todos los n.a. es un subcuerpo, K_A, de los complejos mientras que el de los e.a. es sólo un subanillo, $A \subset \mathbb{C}$.*

Un elemento $0 \neq a \in R$ en un DI, se dice **irreducible** si no es una unidad y no admite factorizaciones propias. Pero si $0 \neq \alpha \in \mathbb{C}$, siempre existe su raíz cuadrada y se tiene $\alpha = (\sqrt{\alpha})^2$. Además, si α es un e.a. existe $f(x) \in \mathbb{Z}[x]$ tal que $f(\alpha) = 0$ y entonces $g(\sqrt{\alpha}) = 0$ para $g(x) = f(x^2) \in \mathbb{Z}[x]$. O sea,

Lema 9. *El anillo de los e.a. A no tiene elementos irreducibles.*

Sin embargo, cuando $K/\mathbb{Q}$ es una extensión finita el subanillo, $O_K = A \cap K$, de los e.a. en K tiene infinitos irreducibles[1]. Además todo elemento de O_K factoriza en irreducibles. Cuando lo hace de forma única, O_K es un DFU.

El ejemplo más sencillo es el anillo de los enteros de Gauss que es un DE[2].

Ejemplo 6. *El anillo $\mathbb{Z}[i]$ tiene infinitos irreducibles que con $a \pm bi$ son $a, b \in \mathbb{Z}$ enteros tales que $a^2 + b^2 = p \in \mathbb{Z}$ primo, $p \equiv 1 \pmod 4$ y todos los primos enteros $p \not\equiv 1 \pmod 4$.*

[1] Como consecuencia de que la norma, $N : O_K \to \mathbb{Z}$, es multiplicativa.

[2] DE $\Rightarrow$ DIP $\Rightarrow$ DFU. Por tanto, $\mathbb{Z}[i]$ tiene factorización única.

5. Extensiones algebraicas

El cuerpo de todos los n.a. es un cuerpo, intermedio entre $\mathbb{Q}$ y $\mathbb{C}$, demasiado grande[3]. Es mejor trabajar en subcuerpos más pequeños.

Dado cualquier subcuerpo K de los complejos, tenemos $\mathbb{Q} \subset K \subset \mathbb{C}$.

Lema 10. *Escribimos $K/\mathbb{Q}$ y decimos que K es una extensión de $\mathbb{Q}$. Claramente, K es un espacio vectorial sobre $\mathbb{Q}$, a su dimensión le llamamos*

$$gr(K/\mathbb{Q}) = dim_{\mathbb{Q}}(K)$$

grado de la extensión. *$K/\mathbb{Q}$ una* ***extensión finita cuando su grado es finito***.

Si $K/\mathbb{Q}$ es una extensión de grado n, y $a \in K$ las potencias $1, a, a^2, \ldots, a^n$ son $\mathbb{Q}$-l.d. Por tanto, a satisface un polinomio racional y K está formado por n.a. O sea,

Lema 11. *Toda extensión finita es algebraica.*

Entre los elementos de K, algunos son e.a. Como todo $a \in \mathbb{Z}$ satisface $f(x) = x - a$, todos los números enteros son enteros algebraicos.

Como la intersección de subanillos es un subanillo, el conjunto, O_K, de los e.a. contenidos en K es un subanillo de K ya que es la intersección del subanillo de todos los enteros algebraicos con K. Por tanto,

[3] Tiene dimensión infinita sobre $\mathbb{Q}$ ya que por ej. el conjunto $\{\sqrt[p]{2}\}_{p \text{ primo}}$ son $\mathbb{Q}$-l.i.

Definición 5. *$O_K = \{\alpha \in K : \ \alpha$ e.a.$\}$ es el mayor subanillo de e.a. en K, $\mathbb{Z} \subset O_K \subset K$. Le llamamos, la* ***clausura entera*** *de $\mathbb{Z}$ en K.*

Ejemplo 7. *Como vimos en 4, la clausura entera de $\mathbb{Z}$ en $\mathbb{Q}[\sqrt{-3}]$ es*

$$O_{\mathbb{Q}[\sqrt{-3}]} = \mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right] = \left\{m + n\frac{1+\sqrt{-3}}{2} : \ m, n \in \mathbb{Z}\right\}$$

Ejemplo 8. *Como vimos en 5, la clausura entera de $\mathbb{Z}$ en $\mathbb{Q}[\sqrt{-1}]$ es*

$$O_{\mathbb{Q}[i]} = \mathbb{Z}[i] = \{m + ni : \ m, n \in \mathbb{Z}\}$$

A veces, es difícil encontrar el anillo de enteros de un c.n., $K/\mathbb{Q}$, cuando su grado es mayor que 2. Un criterio útil es calcular el discriminante de una base entera conocida y comprobar si es un entero libre de cuadrados.

En ese caso, por el teorema de estructura de grupos abelianos libres, el valor absoluto del discriminante es mínimo y esa base genera al anillo de enteros.

Ejemplo 9. *$f_1 = x^3 - x - 1$ y $f_2 = x^3 + x - 1$ son ambas irreducibles en $\mathbb{Q}[x]$ y tienen discriminante libre de cuadrados $\Delta_{f_1} = -4(-1)^3 - 27(-1)^2 = -23$ y $\Delta_{f_1} = -4 * 1^3 - 27(-1)^2 = -31$. Y ambos c.n. $K = \mathbb{Q}(\alpha)$ tienen $O_K = \mathbb{Z}[\alpha]$.*

Ejemplo 10. *$x^5 - x - 1$ y $x^5 - x + 1$ son ambas irreducibles en $\mathbb{Q}[x]$ y tienen el mismo discriminante libre de cuadrados $\Delta_{x^5-x\pm1} = 5^5 - 4^4 = 2869 = 19 * 151$. Por tanto, ambos c.n. $K = \mathbb{Q}(\alpha)$ tienen $O_K = \mathbb{Z}[\alpha]$.*

6. Cuerpos cuadráticos

Dada una extensión de cuerpos $K/\mathbb{Q}$,

Definición 6. *Decimos que $K/\mathbb{Q}$ es una extensión cuadrática si $gr(K/\mathbb{Q}) = 2$.*

En ese caso, existe una base, $B_{K/\mathbb{Q}} = \{\theta_1, \theta_2\}$ de tal forma que para todo $\alpha \in K$, existen escalares únicos $\lambda_1, \lambda_2 \in \mathbb{Q}$, con $\alpha = \lambda_1\theta_1 + \lambda_2\theta_2$.
Por la misma razón, existen racionales a_{ij} tales que

$$\left.\begin{array}{l} \alpha\theta_1 = a_{11}\theta_1 + a_{12}\theta_2 \\ \alpha\theta_2 = a_{21}\theta_1 + a_{22}\theta_2 \end{array}\right\} \Rightarrow \begin{vmatrix} a_{11}-\alpha & a_{12} \\ a_{21} & a_{22}-\alpha \end{vmatrix} = 0 \Rightarrow (a_{11}-\alpha)(a_{22}-\alpha) - a_{12}a_{21} = 0$$

Si $\alpha \notin \mathbb{Q}$, entonces el polinomio

$$f(x) = (x-a_{11})(x-a_{22}) - a_{12}a_{21} = x^2 - (a_{11}+a_{22})x + a_{11}a_{22} - a_{12}a_{21} = x^2 - Px + Q$$

es irreducible en $\mathbb{Q}[x]$ ya que en caso contrario, α satisface un polinomio lineal racional y α sería racional. O sea, $f(x)$ es el polinomio mínimo de α. Y α es algebraico. Si los a_{ij} enteros, α sería un entero algebraico (e.a.).

Si α no es racional, $\mathbb{Q}(\alpha)$ es un subcuerpo de K distinto de $\mathbb{Q}$ y como $\mathbb{Q}$-esp. vect. tiene dimensión 2 ya que el conjunto $\{1, \alpha\}$ es $\mathbb{Q}$-l.i., es una base de $\mathbb{Q}(\alpha)$ como $\mathbb{Q}$-esp. vect. y $K = \mathbb{Q}(\alpha)$, que tiene la misma dimensión.

Multiplicando por el mcm de los denominadores de P, Q en $f(x)$ se encuentra un polinomio entero $ax^2 + bx + c \in \mathbb{Z}$ que tiene a α, como raíz.

Así, $\alpha = \frac{-b+\sqrt{\Delta}}{2a}$ o $\alpha = \frac{-b-\sqrt{\Delta}}{2a}$, y se tiene que $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{\Delta})$, con $\Delta = b^2 - 4ac$.

Como se puede factorizar el discriminante $\Delta = m^2 d$ con d un entero libre de cuadrados, se tiene finalmente que una base de la extensión es $\{1, \sqrt{d}\}$ que es entera porque el polinomio mínimo de $\sqrt{d}$ es $x^2 - d \in \mathbb{Z}[x]$. Por tanto,

$$K = \mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{\Delta}) = \mathbb{Q}(\sqrt{d})$$

Lema 12. *Todo cuerpo cuadrático es el menor cuerpo que contiene a una raíz cuadrada de un entero libre de cuadrados.*

La representación $K = \mathbb{Q}(\sqrt{d})$, con d un entero libre de cuadrados, es única ya que si $\mathbb{Q}(\sqrt{d}) = \mathbb{Q}(\sqrt{d'})$ existen $a, b \in \mathbb{Z}$ tales que $\sqrt{d} = a + b\sqrt{d'}$ y aplicando $tr : \mathbb{Q}(\sqrt{d}, \sqrt{d'}) \to \mathbb{Q}$ se llega a que $a = 0$ y $d = b^2 d'$ implica $b = 1$.

Como $\{1, \sqrt{d}\}$ es una base de $\mathbb{Q}(\sqrt{d})$ como $\mathbb{Q}$-esp. vect., se tiene que

$$\mathbb{Q}(\sqrt{d}) = \left\{ \lambda_0 + \lambda_1 \sqrt{d} : \ \lambda_0, \lambda_1 \in \mathbb{Q} \right\}$$

Ejemplo 11. *Como* $12 = 2^2 * 3$, *para el cuerpo cuadrático* $\mathbb{Q}[\sqrt{-12}]$ *se tiene* $\mathbb{Q}[\sqrt{-12}] = \mathbb{Q}[\sqrt{-3}]$ *y una base de la extensión es* $\{1, \sqrt{-3}\}$. *Por tanto,*

$$\mathbb{Q}[-12] = \left\{ \lambda_0 + i\lambda_1 \sqrt{3} : \ \lambda_0, \lambda_1 \in \mathbb{Q} \right\}$$

Ejemplo 12. *Si* α *es una raíz compleja del polinomio* $f(x) = x^2 + x + 1$[4]. *Entonces, también se tiene que* $\mathbb{Q}[\alpha] = \mathbb{Q}[\sqrt{-3}]$

[4] O sea, α es una raíz primitiva cúbica de la unidad.

7. Enteros cuadráticos

Como los enteros cuadráticos son de dos tipos:

Tipo I) $a \pm \sqrt{\Delta}$ con a y Δ enteros, Δ no cuadrado perfecto. Como $\Delta = b^2 d$ con $b, d \in \mathbb{Z}$ y d libre de cuadrados, se tiene que $\mathbb{Q}(\sqrt{d})$ contiene siempre enteros algebraicos de este tipo, $a + b\sqrt{d} \in \mathbb{Q}(\sqrt{d})$ con a, b enteros arbitrarios.

Tipo II) Si $d \equiv 1 \pmod 4 \Leftrightarrow d = 4k+1$, también $\frac{1+\sqrt{d}}{2}$ es un entero algebraico en $\mathbb{Q}(\sqrt{d})$ y contiene a todos los de la forma $m + n\frac{1+\sqrt{d}}{2}$ con $m, n \in \mathbb{Z}$.

Por tanto, si d es libre de cuadrados, $d \not\equiv 0 \pmod 4$ y el subanillo de enteros cuadráticos de $\mathbb{Q}(\sqrt{d})$ es de uno de los dos tipos siguientes:

$$O_{\sqrt{d}} = \begin{cases} \left\{a + b\sqrt{d} : \ a, b \in \mathbb{Z}\right\} = \mathbb{Z}\left[\sqrt{d}\right] & \text{Si } d \equiv 2,3 \pmod 4 \\ \left\{m + n\frac{1+\sqrt{d}}{2} : \ m, n \in \mathbb{Z}\right\} = \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right] & \text{Si } d \equiv 1 \pmod 4 \end{cases}$$

Ejemplo 13.

$$O_{\mathbb{Q}[\sqrt{2}]} = \mathbb{Z}\left[\sqrt{2}\right], \quad O_{\mathbb{Q}[\sqrt{3}]} = \mathbb{Z}\left[\sqrt{3}\right], \quad O_{\mathbb{Q}[\sqrt{5}]} = \mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right]$$

En cualquier caso, dado el irracional cuadrático $\alpha = \frac{P+\sqrt{\Delta}}{Q}$ con P, Q enteros, la mejor forma de comprobar si es un e.a. es comprobando si los racionales $a = \alpha + \beta = \frac{2P}{Q}$, $b = \alpha\beta = \frac{P^2 - \Delta}{Q^2}$ son enteros.

8. Conjugados y normas

Dado un c.c. $\mathbb{Q}(\sqrt{d})$ siempre existe una aplicación, $\mathbb{Q}(\sqrt{d}) \to \mathbb{Q}(\sqrt{d})$, definida por $\overline{\lambda_0 + \lambda_1\sqrt{d}} = \lambda_0 - \lambda_1\sqrt{d}$ para todo $\lambda_0, \lambda_1 \in \mathbb{Q}$.

Claramente, lleva sumas en sumas y también lleva productos en productos:

$$\begin{aligned}
&\overline{(\lambda_0 + \lambda_1\sqrt{d})(\mu_0 + \mu_1\sqrt{d})} = \overline{\lambda_0\mu_0 + d\lambda_1\mu_1 + (\lambda_0\mu_1 + \lambda_1\mu_0)\sqrt{d}} = \\
&= \lambda_0\mu_0 + d\lambda_1\mu_1 - (\lambda_0\mu_1 + \lambda_1\mu_0)\sqrt{d} = (\lambda_0 - \lambda_1\sqrt{d})(\mu_0 - \mu_1\sqrt{d}) = \\
&= \left(\overline{\lambda_0 + \lambda_1\sqrt{d}}\right)\left(\overline{\mu_0 + \mu_1\sqrt{d}}\right)
\end{aligned}$$

Por tanto, es un endomorfismo de cuerpos y es necesariamente biyectivo.

Definición 7. *La llamamos* ***conjugación algebraica****. Con esta definimos la* ***norma algebraica*** *como* $N(\alpha) = \alpha\overline{\alpha} \in \mathbb{Q}$*, explícitamente*

$$N(\lambda_0 + \lambda_1\sqrt{d}) = (\lambda_0 + \lambda_1\sqrt{d})(\lambda_0 - \lambda_1\sqrt{d}) = \lambda_0^2 - d\lambda_1^2 \in \mathbb{Q}$$

La norma hereda la propiedad multiplicativa del endomorfismo conjugación.

Ejemplo 14. $\alpha = \frac{3+\sqrt{5}}{2} \in \mathbb{Q}(\sqrt{5})$ *es un entero algebraico porque* $\alpha + \overline{\alpha} = 3$ *y* $\alpha\overline{\alpha} = \frac{9-5}{4} = 1$ *por tanto* α *es raíz del polinomio entero mónico* $x^2 - 3x + 1$ *que es su polmin. Además, la última igualdad nos dice que* α *y* $\overline{\alpha}$ *son inversos*[5] *mutuamente en el anillo de enteros,* $O_{\sqrt{5}} = \mathbb{Z}\left(\frac{1+\sqrt{5}}{2}\right) = \{m + n\frac{1+\sqrt{5}}{2} : \ m, n \in \mathbb{Z}\}$

[5] En realidad, $\left(\frac{1+\sqrt{5}}{2}\right)^2 = \frac{3+\sqrt{5}}{2}$ y sus potencias sucesivas son de nuevo unidades.

9. Recurrencia de los coeficientes de las potencias

Para el i.c. anterior, $\alpha = \frac{3+\sqrt{5}}{2}$, como

$$\alpha^2 = 3\alpha - 1 \Longrightarrow \alpha^n = 3\alpha^{n-1} - \alpha^{n-2}$$

si llamamos $\alpha^i = \frac{V_i}{2} + \frac{U_i}{2}\sqrt{5}$, se tiene $V_0 = 2$, $U_0 = 0$, $V_1 = 3$, $U_1 = 1$ y además

$$\alpha^n = 3\left(\frac{V_{n-1}}{2} + \frac{U_{n-1}}{2}\sqrt{5}\right) - \left(\frac{V_{n-2}}{2} + \frac{U_{n-2}}{2}\sqrt{5}\right) =$$

$$= \frac{3V_{n-1} - V_{n-2}}{2} + \frac{3U_{n-1} - U_{n-2}}{2}\sqrt{5} \Longrightarrow \begin{cases} V_n = 3V_{n-1} - V_{n-2} \\ U_n = 3U_{n-1} - U_{n-2} \end{cases}$$

V_n y U_n son enteros que satisfacen la misma ec. en recurrencia de segundo orden con distintos parámetros iniciales.

Ejemplo 15. *Para el e.a.* $\alpha = \frac{3+\sqrt{5}}{2} \in \mathbb{Q}(\sqrt{5})$ *es fácil de calcular sus potencias sucesivas con las ecuaciones en recurrencia anteriores*[6]*. Así,*

V_i	2	3	7	18	47	123	322	843	2207	5778	15127	…
U_i	0	1	3	8	21	55	144	377	987	2584	6765	…

De forma que por ejemplo se tiene $\alpha^{10} = \frac{V_{10}+U_{10}\sqrt{5}}{2} = \frac{15127+6765\sqrt{5}}{2}$

[6] Se puede acelerar su cálculo con un algoritmo como el de la exponenciación rápida.

10. Caso general. Sucesiones de Lucas

Dados $P, Q \in \mathbb{Z}$ con $\Delta = P^2 - 4Q$ no cuadrado perfecto, el irracional $\alpha = \frac{P+\sqrt{\Delta}}{2}$ es un e.a. en el cuerpo $\mathbb{Q}(\sqrt{\Delta})$ ya que satisface el polinomio

$$f_\alpha(x) = x^2 - Px + Q \in \mathbb{Z}[x]$$

Como $\alpha^2 = P\alpha - Q$, multiplicando por α^{n-2}, se tiene $\alpha^n = P\alpha^{n-1} - Q\alpha^{n-2}$. Si llamamos $\alpha^i = \frac{V_i}{2} + \frac{U_i}{2}\sqrt{\Delta}$, se tiene $V_0 = 2$, $U_0 = 0$, $V_1 = P$, $U_1 = 1$ y además

$$\alpha^n = P\left(\frac{V_{n-1}}{2} + \frac{U_{n-1}}{2}\sqrt{\Delta}\right) - Q\left(\frac{V_{n-2}}{2} + \frac{U_{n-2}}{2}\sqrt{\Delta}\right) =$$

$$= \frac{PV_{n-1} - QV_{n-2}}{2} + \frac{PU_{n-1} - QU_{n-2}}{2}\sqrt{\Delta} \Rightarrow \begin{cases} V_n = PV_{n-1} - QV_{n-2} \\ U_n = PU_{n-1} - QU_{n-2} \end{cases}$$

V_n y U_n son enteros que satisfacen la misma ec. en recurrencia de segundo orden con distintos parámetros iniciales.

Ejemplo 16. *Para el e.a.* $\alpha = \frac{1-\sqrt{5}}{2} \in \mathbb{Q}(\sqrt{5})$ *las ecuaciones en recurrencia anteriores son las de la suc. de Fibonacci con distintos parámetros iniciales.*

V_i	2	1	3	4	7	11	18	29	47	76	123	…
U_i	0	1	1	2	3	5	8	13	21	34	55	…

11. Teorema pequeño de Fermat para enteros cuadráticos

Dados $P, Q, p \in \mathbb{Z}$, con $\Delta = P^2 - 4Q$ no cuadrado perfecto, p **primo impar** tal que $(p, \Delta) = 1$, entonces el irracional $\alpha = \frac{P+\sqrt{\Delta}}{2}$ y el entero p ambos pertenecen al mismo anillo de e.c. O sea, $\alpha, p \in O_{\sqrt{\Delta}}$.

Este anillo es DI porque es un subanillo de $\mathbb{C}$, por tanto la relación de divisibilidad funciona bien (verifica la cancelativa del producto). Como es usual,

Definición 8. *En un DI, se dice que dos elementos son congruentes módulo c cuando su diferencia es múltiplo de c. Esta relación contiene a la de $\mathbb{Z}$.*

O sea, dados $a, b \in \mathbb{Z}$, si $a \equiv b \pmod{p}$ en $\mathbb{Z}$ también es cierta en $O_{\sqrt{\Delta}}$.
Y si existe el inverso de a módulo p en $\mathbb{Z}$, también es inverso módulo p en $O_{\sqrt{\Delta}}$. Por tanto, existe el inverso de 2 módulo p en $O_{\sqrt{\Delta}}$ y es un entero usual.
Como el TPF, dice que $a^n \equiv a \pmod{p}$ para todo $a \in \mathbb{Z}$, se tiene

$$\alpha^p = \left(\frac{P}{2} + \frac{\sqrt{\Delta}}{2}\right)^p \equiv \left(\frac{P}{2}\right)^p + \left(\frac{\sqrt{\Delta}}{2}\right)^p \equiv \frac{P}{2} + \frac{\sqrt{\Delta}^p}{2} \equiv \frac{P}{2} + \frac{\Delta^{(p-1)/2}\sqrt{\Delta}}{2} \pmod{p}$$

como además $\Delta^{(p-1)/2} \equiv \left(\frac{\Delta}{p}\right) \pmod{p}$ por ser p primo impar, tenemos

$$\textbf{TPF para e.c.} \quad \alpha^p \equiv \begin{cases} \alpha \pmod{p}, & \text{Si } \left(\frac{\Delta}{p}\right) = 1 \\ \overline{\alpha} \pmod{p}, & \text{Si } \left(\frac{\Delta}{p}\right) = -1 \end{cases}$$

Ejemplo 17. ***Exponenciación rápida para enteros cuadráticos modulares*** *Para* $P = 3$, $Q = -1$, *se tiene* $\Delta = P^2 - 4Q = 13$ *y* $\alpha = \frac{3+\sqrt{13}}{2}$. *Vamos a ver si se verifiva el TPF para el ent. cuad.* α *y el primo* $p = 11$.

Como $\Delta = 13$, *se tiene* $\left(\frac{13}{11}\right) = \left(\frac{2}{11}\right) = -1$ *(porque* $11 \equiv 3 \pmod 8$*). Entonces,* $r = p - \left(\frac{13}{11}\right) = 11 + 1 = 12$, *y el TPF para* α *dice que*

$$\alpha^{11} \equiv \overline{\alpha} \pmod{11} \Rightarrow \alpha^{12} \equiv \alpha\overline{\alpha} = Q = -1 \equiv 10 \pmod{11}$$

Ahora, aplicaremos el algoritmo de la exponenciación rápida para calcular α^{12}. *Como* $12 = 1100\_2$ *en base dos, el algoritmo tiene 4 pasos. Además, como* $2 * 6 \equiv 1 \pmod{11} \Leftrightarrow 2^{-1} \equiv 6 \pmod{11}$, *por tanto se tiene: Paso 1) Primer bit a la izquierda* $e = 1$,

$$acu \equiv \alpha \equiv 6 * 3 + 6\sqrt{13} \equiv 7 + 6\sqrt{13} \pmod{11}$$

Paso 2) Segundo bit por la izquierda $e = 1$,

$$acu \equiv acu^2\alpha = (517 + 84\sqrt{13})(7 + 6\sqrt{13}) \equiv 7\sqrt{13}(7 + 6\sqrt{13}) \equiv$$
$$\equiv 546 + 49\sqrt{13} \equiv 7 + 5\sqrt{13} \pmod{11}$$

Paso 3) Tercer bit por la izquierda $e = 0$,

$$acu \equiv acu^2 = (7 + 5\sqrt{13})^2 = 374 + 70\sqrt{13} \equiv 4\sqrt{13} \pmod{11}$$

Paso 4) Cuarto bit por la izquierda $e = 0$,

$$acu \equiv acu^2 = (4\sqrt{13})^2 = 208 \equiv 10 \pmod{11}$$

O sea, $\alpha^{11} \equiv 10 \pmod{11}$ *como queríamos demostrar.*

Ejemplo 18. *Para* $P=3$, $Q=1$, *se tiene* $\Delta = P^2-4Q = 5$ *y* $\alpha = \frac{3+\sqrt{5}}{2}$. *Vamos a ver si se verifiva el TPF para el ent. cuad.* α *y el primo* $p=11$.

Como $\Delta = 5 \equiv 1 \pmod 4$, *se tiene* $\left(\frac{5}{11}\right) = \left(\frac{11}{5}\right) = \left(\frac{1}{5}\right) = 1$. *Entonces,* $r = p - \left(\frac{5}{11}\right) = 11-1 = 10$, *y el TPF para* α *dice que*

$$\alpha^{11} \equiv \alpha \pmod{11} \Rightarrow \alpha^{10} \equiv 1 \pmod{11}$$

Ahora, aplicaremos el algoritmo de la exponenciación rápida para calcular α^{10}. *Como* $10 = 1010\_2$ *en base dos, el algoritmo tiene 4 pasos. Además, como* $2*6 \equiv 1 \pmod{11} \Leftrightarrow 2^{-1} \equiv 6 \pmod{11}$, *por tanto se tiene:*

Paso 1) Primer bit a la izquierda $e=1$,

$$acu \equiv \alpha \equiv 6*3+6\sqrt{5} \equiv 7+6\sqrt{5} \pmod{11}$$

Paso 2) Segundo bit por la izquierda $e=0$,

$$acu \equiv acu^2 = \alpha^2 = 229+84\sqrt{5} \equiv 9+7\sqrt{5} \pmod{11}$$

Paso 3) Tercer bit por la izquierda $e=1$,

$$acu \equiv acu^2 * \alpha = (326+126\sqrt{5})(7+6\sqrt{5}) \equiv (7+5\sqrt{5})(7+6\sqrt{5}) =$$
$$= 199+77\sqrt{5} \equiv 1 \pmod{11}$$

Paso 4) Cuarto bit por la izquierda $e=0$,

$$acu \equiv acu^2 = 1^2 = 1 \pmod{11}$$

O sea, $\alpha^{10} \equiv 1 \pmod{11}$ *como queríamos demostrar.*

12. Otra versión del TPF para enteros cuadráticos

Si p primo impar, $(p,\Delta) \neq 1$, entonces $\Delta \equiv 0 \pmod{p}$ y de la demostración anterior sale $\alpha^p \equiv P/2 \pmod{p}$.

Si $(Q,\Delta) = 1$, como $\alpha\overline{\alpha} = Q$, entonces existe el inverso de α módulo p.

$$\alpha^{-1} \equiv \overline{\alpha}Q^{-1} \Rightarrow \alpha^p \equiv \alpha \Rightarrow \alpha^{p-1} \equiv 1 \pmod{p}$$

Resumiendo, si p es un primo entero tal que $(p,2Q) = 1$, entonces se tiene

Teorema 1. *[2ª versión del TPF para e.c.]*

$$\alpha^{p-\left(\frac{\Delta}{p}\right)} \equiv \begin{cases} 1 \pmod{p}, & Si \left(\frac{\Delta}{p}\right) = 1 \\ Q \pmod{p}, & Si \left(\frac{\Delta}{p}\right) = -1 \\ P/2 \pmod{p}, & Si \left(\frac{\Delta}{p}\right) = 0 \end{cases}$$

Si se exige la hipótesis $(p,2Q\Delta) = 1$, entonces sobra la tercera alternativa.

Y recordando la definición, $\alpha^i = \frac{V_i}{2} + \frac{U_i}{2}\sqrt{\Delta}$, de las sucesiones de Lucas, si $(p,2Q) = 1$, entonces (si p no verifica el corolario, entonces es compuesto)

Corolario 1. *[3ª versión del TPF para e.c.]*

$$U_{p-\left(\frac{\Delta}{p}\right)} \equiv 0 \pmod{p}, \quad V_{p-\left(\frac{\Delta}{p}\right)} \equiv \begin{cases} 2 \pmod{p}, & Si \left(\frac{\Delta}{p}\right) = 1 \\ 2Q \pmod{p}, & Si \left(\frac{\Delta}{p}\right) = -1 \\ P \pmod{p}, & Si \left(\frac{\Delta}{p}\right) = 0 \end{cases}$$

Ejemplo 19. *Para* $P=3$, $Q=1$, *se tiene* $\Delta = P^2-4Q = 5$ *y* $\alpha = \frac{3+\sqrt{5}}{2}$. *Las ec. en recurrencia para* $\{V_n\}_{n\in\mathbb{N}}$, $\{U_n\}_{n\in\mathbb{N}}$, *tales que* $\alpha^n = \frac{V_n}{2} + \frac{U_n}{2}\sqrt{\Delta}$ *son* $a_n = 3a_{n-1} - a_{n-2}$. *Recordamos sus primeros valores*

Paso	0	1	2	3	4	5	6	7	8	9	10	11
U_i	0	1	3	8	21	55	144	377	987	2584	6765	17711
V_i	2	3	7	18	47	123	322	843	2207	5778	15127	39603

Con el primo $p=11$, *como* $\Delta = 5 \equiv 1 \pmod 4$, *se tiene* $\left(\frac{5}{11}\right) = \left(\frac{11}{5}\right) = \left(\frac{1}{5}\right) = 1$. *El TPF dice* $U_{10} = U_{p-1} \equiv 0 \pmod{11}$ $V_{10} = V_{p-1} \equiv 2 \pmod{11}$ *y*

$$U_{10} = 6765 \equiv 0 \pmod{11} \quad V_{10} = 15127 \equiv 2 \pmod{11}$$

Ejemplo 20. *Para* $P=3$, $Q=-1$, *se tiene* $\Delta = P^2-4Q = 13$ *y* $\alpha = \frac{3+\sqrt{13}}{2}$. *Las ec. en recurrencia para* $\{V_n\}_{n\in\mathbb{N}}$, $\{U_n\}_{n\in\mathbb{N}}$, *tales que* $\alpha^n = \frac{V_n}{2} + \frac{U_n}{2}\sqrt{\Delta}$ *son* $a_n = 3a_{n-1} + a_{n-2}$. *Si calculamos algunos de sus primeros valores*

i	2	3	4	5	6	7	8	9	10	11	12
U_i	3	10	33	109	360	1189	3927	12970	42837	141481	467280
V_i	11	36	119	393	1298	4287	14159	46764	154451	510117	1684802

Para el primo $p=11$, *como* $\Delta = 13$, *se tiene* $\left(\frac{13}{11}\right) = \left(\frac{2}{11}\right) = -1$ *(porque* $11 \equiv 3 \pmod 8$*). Y el TPF dice* $U_{12} = U_{p+1} \equiv 0 \pmod{11}$ $V_{12} = V_{p+1} \equiv 2Q = -2 \pmod{11}$ *y en efecto se tiene*

$$U_{12} = 467280 \equiv 0 \pmod{11} \quad V_{12} = 1684802 \equiv 9 \equiv -2 \pmod{11}$$

13. Propiedades de las sucesiones de Lucas

Dados $P, Q \in \mathbb{Z}$ con $\Delta = P^2 - 4Q$ no cuadrado perfecto, el irracional $\alpha = \frac{P+\sqrt{\Delta}}{2}$ tiene de polmin, $f_\alpha(x) = x^2 - Px + Q \in \mathbb{Z}[x]$ y es un e.a. en el cuerpo $\mathbb{Q}(\sqrt{\Delta})$.

Como $\alpha^2 = P\alpha - Q$, multiplicando por α^{n-2}, se tiene $\alpha^n = P\alpha^{n-1} - Q\alpha^{n-2}$.Y si llamamos $\alpha^i = \frac{V_i}{2} + \frac{U_i}{2}\sqrt{\Delta}$, se tiene $V_0 = 2$, $U_0 = 0$, $V_1 = P$, $U_1 = 1$ y los siguientes coeficientes son

$$\alpha^n = P(\tfrac{V_{n-1}}{2} + \tfrac{U_{n-1}}{2}\sqrt{\Delta}) - Q(\tfrac{V_{n-2}}{2} + \tfrac{U_{n-2}}{2}\sqrt{\Delta}) = \tfrac{PV_{n-1} - QV_{n-2}}{2} + \tfrac{PU_{n-1} - QU_{n-2}}{2}\sqrt{\Delta} \Rightarrow$$
$$\Rightarrow \begin{cases} V_n = PV_{n-1} - QV_{n-2} \\ U_n = PU_{n-1} - QU_{n-2} \end{cases}$$

V_n y U_n son enteros que satisfacen la misma ec. en recurrencia de segundo orden con distintos parámetros iniciales. Ahora, $\forall k, e \in \mathbb{N}$, se tiene

$$\left.\begin{array}{l} \alpha^e = \frac{V_e}{2} + \frac{U_e}{2}\sqrt{\Delta} \\ \alpha^{ke} = \frac{V_{ke}}{2} + \frac{U_{ke}}{2}\sqrt{\Delta} \end{array}\right\} \Rightarrow V_{ke} + U_{ke}\sqrt{\Delta} = 2\alpha^{ke} = (2\alpha^e)^k 2^{1-k} = (V_e + U_e\sqrt{\Delta})^k 2^{1-k}$$

Y como $\{1, \sqrt{\Delta}\}$ son $\mathbb{Q} - l.i.$
Si U_e es divisible por un entero m impar, m divide a U_{ke}.

Para m primo con $2Q$, lo siguiente tiene sentido módulo m

$$\alpha\overline{\alpha} = Q \Rightarrow \alpha^{-1} = Q^{-1}\overline{\alpha} \Rightarrow \alpha^{-ke} = Q^{-ke}\overline{\alpha}^{ke}$$

Ahora, si existe el menor $e \in \mathbb{N}^*$ tal que $m|U_e$, entonces $m|U_r \Rightarrow e|r$.

Elegimos $k \in \mathbb{N}$ tal que $ke \leq r < (k+1)e$, entonces

$$V_{r-ke} + U_{r-ke}\sqrt{\Delta} = 2\alpha^{r-ke} = 2\alpha^r Q^{-ke}(2\overline{\alpha}^e)^k 2^{-k} = \\ = 2^{-k}Q^{-ke}(V_r + U_r\sqrt{\Delta})(V_e + U_e\sqrt{\Delta})^k$$

Ahora, como m divide a U_r y U_e también divide a U_{r-ke}, pero como $r - ke < e$ entonces $r - ke = 0 \iff r = ke$.

Entonces, para cualquier sucesión de Lucas $\{U_i\}_{i\in\mathbb{N}}$.

Teorema 2. *Si m primo con $2Q$ y existe el menor natural no nulo e tal que $m|U_e$, entonces $m|U_r$ si y sólo si $e|r$.*

Definición 9. *Al menor menor natural no nulo $e = w(m)$, tal que $m|U_e$, le llamamos el **rango de Lucas** de m en $\{U_i\}_{i\in\mathbb{N}}$.*

Por el TPF para e.c., 1, si $p \in \mathbb{N}$ primo, $(p, 2Q\Delta) = 1$, entonces $p|U_{p-\left(\frac{\Delta}{p}\right)}$.
Por tanto, si p es primo tal que $(p, 2Q\Delta) = 1$,

Corolario 2. *Existe el menor natural no nulo $e = w(p)$ tal que $p|U_e$.Puede ser $e = p - \left(\frac{\Delta}{p}\right)$. En caso contrario, existe un divisor propio $d|e$ tal que $p|U_d$.*

13.1. Mas propiedades. Como

$$V_{2k} + U_{2k}\sqrt{d} = 2\alpha^{2k} = (2\alpha^k)^2 2^{-1} = \frac{(V_k + U_k\sqrt{d})^2}{2}$$

entonces

$$V_{2k} = \frac{V_k^2 + dU_k^2}{2} = \frac{V_k^2 + V_k^2 - 4Q^k}{2} = V_k^2 - 2Q^k, \quad U_{2k} = U_k V_k$$

Ahora, $\alpha^{k+1} = \alpha\alpha^k$ implica que

$$\frac{V_{k+1} + U_{k+1}}{2} = \frac{(P + \sqrt{d})(V_k + U_k\sqrt{d})}{4} = \frac{PV_k + dU_k + (V_k + PU_k)\sqrt{d}}{4}$$

entonces

$$V_{k+1} = \frac{PV_k + dU_k}{2}, \quad U_{k+1} = \frac{V_k + PU_k}{2} \Leftrightarrow V_k = 2U_{k+1} - PU_k$$

y por tanto

$$U_{2k} = U_k V_k = U_k(2U_{k+1} - PU_k) = 2U_k U_{k+1} - PU_k^2$$

por otro lado

$$V_{k+1} = \frac{PV_k + dU_k}{2} = \frac{P(2U_{k+1} - PU_k) + dU_k}{2} =$$
$$= \frac{2PU_{k+1} - (P^2 - d)U_k}{2} = PU_{k+1} - 2QU_k$$

Como $\alpha^{2k+1} = \alpha^k \alpha^{k+1}$ implica que

$$\frac{V_{2k+1}+U_{2k+1}}{2} = \frac{(V_k+U_k\sqrt{d})(V_{k+1}+U_{k+1}\sqrt{d})}{4} = \\ = \frac{V_kV_{k+1}+dU_kU_{k+1}+(V_kU_{k+1}+U_kV_{k+1})\sqrt{d}}{4}$$

entonces

$$V_{2k+1} = \frac{V_kV_{k+1}+dU_kU_{k+1}}{2}, \quad U_{2k+1} = \frac{V_kU_{k+1}+U_kV_{k+1}}{2}$$

y por tanto

$$U_{2k+1} = \frac{V_kU_{k+1}+U_kV_{k+1}}{2} = \\ = \frac{(2U_{k+1}-PU_k)U_{k+1}+U_k(PU_{k+1}-2QU_k)}{2} = U_{k+1}^2 - QU_k^2$$

Por otro lado,

$$U_{2k+2} = U_{2(k+1)} = 2U_{k+1}U_{k+2} - PU_{k+1}^2 = \\ = 2U_{k+1}(PU_{k+1}-QU_k) - PU_{k+1}^2 = PU_{k+1}^2 - 2QU_kU_{k+1}$$

Resumiendo lo anterior, hemos demostrado las fórmulas que se usan en el cálculo iterativo de izquierda a derecha.

Teorema 3. *[U-fórmulas binarias y V-fórmula en función de U]*

$$\begin{cases} U_{2k} = 2U_kU_{k+1} - PU_k^2 \\ U_{2k+1} = U_{k+1}^2 - QU_k^2 \\ U_{2k+2} = PU_{k+1}^2 - 2QU_kU_{k+1} \\ V_k = 2U_{k+1} - PU_k \end{cases}$$

14. Cálculo de las sucesiones de Lucas

Como las ecuaciones en recurrencia equivalen a una igualdad matricial

$$U_n = PU_{n-1} - QU_{n-2} \Longleftrightarrow \begin{pmatrix} U_{n-1} \\ U_n \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ -Q & P \end{pmatrix} \begin{pmatrix} U_{n-2} \\ U_{n-1} \end{pmatrix}$$

para el cálculo basta hacer potencias de la misma matriz.
Si se parte de la pareja $(U_0, U_1) = (0, 1)$, se tiene por inducción

$$\begin{pmatrix} U_1 \\ U_2 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ -Q & P \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

$$\begin{pmatrix} U_n \\ U_{n+1} \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ -Q & P \end{pmatrix} \begin{pmatrix} U_{n-1} \\ U_n \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ -Q & P \end{pmatrix} \begin{pmatrix} 0 & 1 \\ -Q & P \end{pmatrix}^{n-1} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ -Q & P \end{pmatrix}^{n} \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

Así, se puede aplicar el algoritmo de la exponenciación rápida izda-drcha para el cálculo de la pareja (U_n, U_{n+1}).

Calcular cuadrados (si el bit es cero), equivale a partir de la pareja (U_k, U_{k+1}) calcular (U_{2k}, U_{2k+1}) que podemos hacerlo por las dos primeras U-fórmulas.

Y calcular un cuadrado multiplicado por la matriz de la recurrencia (si el bit es 1), equivale a calcular la pareja (U_{2k+1}, U_{2k+2}) a partir de la pareja (U_k, U_{k+1}), que podemos hacerlo por las dos últimas U-fórmulas binarias. En realidad, no necesitamos calcular potencias matriciales en absoluto.

15. Algoritmo de izquierda a derecha

Si $n = e_1 \dots e_r|_2$ está en base dos, daremos r-pasos.

Input: la pareja $(U_0, U_1) = (0, 1)$. O sea, al principio $k = 0$.

En cada paso, tenemos una pareja (U_k, U_{k+1}).

Si $e = 0$, entonces calculamos $(U_{2k}, U_{2k+1}) = \left(2U_kU_{k+1} - PU_k^2,\ U_{k+1}^2 - QU_k^2\right)$.

Si $e = 1$, entonces calculamos $(U_{2k+1}, U_{2k+2}) = \left(U_{k+1}^2 - QU_k^2,\ PU_{k+1}^2 - 2QU_kU_{k+1}\right)$.

Output: La pareja (U_n, U_{n+1}) y a partir de ella, también $V_n = 2U_{n+1} - PU_n$.

Observaciones:
En el primer paso $k = 0$, y el primer bit de la izquierda es $e_1 = 1$, tenemos

Paso 1) $(U_1, U_2) = \left(U_1^2 - QU_0^2,\ PU_1^2 - 2QU_0U_1\right) = \left(U_1^2,\ PU_1^2\right) = (1,\ P)$

Además, en los ejemplos que importan siempre calculamos módulo n. De forma que los números, (U_k, U_{k+1}), estarán acotados por el número n a testar si es primo o compuesto.

Ejemplo 21. *Para $P = 3$, $Q = -1$, vamos a ver si se verifiva el TPF para el e.c. α y el primo $p = 11$.*

Como $\Delta = 13$, se tiene $\left(\frac{13}{11}\right) = -1$. Entonces, $r = p - \left(\frac{13}{11}\right) = 11 + 1 = 12$.
Como $12 = 1100_2$ en base dos, el algoritmo tiene 4 pasos.

Paso 1) Primer bit a la izquierda $e = 1$, $(U_1, U_2) = (1,\ P) = (1, 3)$

Paso 2) Segundo bit $e = 1,\ k = 1 \Rightarrow (U_{2k+1}, U_{2k+2}) = (U_3, U_4)$. *Así*

$$(U_3, U_4) = \left(U_2^2 - QU_1^2,\ PU_2^2 - 2QU_1U_2\right) = (3^2 + 1, 3 * 3^2 + 2 * 3) =$$
$$= (10, 33) \equiv (10, 0) \pmod{11}$$

Paso 3) Tercer bit $e = 0,\ k = 3 \Rightarrow (U_{2k}, U_{2k+1}) = (U_6, U_7)$. *Así*

$$(U_6, U_7) = \left(2U_3U_4 - PU_3^2,\ U_4^2 - QU_3^2\right) = (-3 * 10^2, 10^2) =$$
$$= (-300, 100) \equiv (8, 1) \pmod{11}$$

Paso 4) Cuarto bit $e = 0,\ k = 6 \Rightarrow (U_{2k}, U_{2k+1}) = (U_{12}, U_{13})$. *Así*

$$(U_{12}, U_{13}) = \left(2U_6U_7 - PU_6^2,\ U_7^2 - QU_6^2\right) = (2 * 8 - 3 * 8^2, 1 + 8^2) =$$
$$= (-176, 65) \equiv (0, 10) \pmod{11}$$

En particular,

$$\begin{cases} U_{12} \equiv 0 \pmod{11} \\ V_{12} = 2U_{13} - PU_{12} = 20 \equiv -2 \pmod{11} \end{cases}$$

y $n = 11$ *verifica el QF-Test.*
O sea, satisface el TPF para la base $\alpha = \frac{3+\sqrt{13}}{2}$.

16. Rango de Lucas de un número arbitrario

Si $P, Q \in \mathbb{Z}$, con $d = P^2 - 4Q$ no cuadrado perfecto, sus s.L. se definen por las ecuaciones, con condiciones iniciales $V_0 = 2$, $U_0 = 0$, $V_1 = P$, $U_1 = 1$.

$$\begin{cases} V_n = PV_{n-1} - QV_{n-2} \\ U_n = PU_{n-1} - QU_{n-2} \end{cases}$$

Ahora, dado un entero n arbitrario, se define

Definición 10. *El rango $w(n)$ para $P, Q \in \mathbb{Z}$, con $d = P^2 - 4Q$ no cuadrado perfecto, es el primer índice e distinto de cero tal que $U_e \equiv 0 \pmod{n}$.*

La primera propiedad es que si existe $w(n)$, entonces $n|U_r \Leftrightarrow w(n)|r$.

Como vimos, si $p \in \mathbb{Z}$ es primo, el TPF para enteros cuadráticos nos asegura que existe $w(p)$ para todo P, Q, con $d = P^2 - 4Q$ no cuadrado perfecto, y debe ser un divisor de $p - \left(\frac{d}{p}\right)$.

A continuación demostraremos que existe $w(n)$ para todo $n \in \mathbb{Z}$ y que si existe una s.L., $\{U_i\}_{i \in \mathbb{N}}$, tal que $w(n) = p - \left(\frac{d}{n}\right)$ entonces n es primo (la s.L. es el análogo a un elemento primitivo para n).

16.1. Rango de una potencia de primo. Por inducción, para $t \geq 2$, suponemos que $w(p^{t-1})$ existe y que divide a $e = p^{t-2}\left(p - \left(\frac{d}{n}\right)\right)$. Como

$$\left(\frac{V_e + U_e\sqrt{d}}{2}\right)^p = \alpha^{ep} = \frac{V_{ep} + U_{ep}\sqrt{d}}{2} \Leftrightarrow$$

$$\Leftrightarrow 2^{p-1}\left(V_{ep} + U_{ep}\sqrt{d}\right) = \left(V_e + U_e\sqrt{d}\right)^p$$

Si desarrollamos la potencia p-ésima, vemos que el coeficiente de $\sqrt{d}$ es

$$pV_e^{p-1}U_e + \binom{p}{3}V_e^{p-3}U_e^3 d + \binom{p}{5}V_e^{p-5}U_e^5 d^2 + \cdots + U_e^p d^{(p-1)/2}$$

como cada coeficiente binomial es múltiplo de p (por ser primo), entonces cada sumando es múltiplo de p^t.

Como p no divide a 2^{p-1}, entonces p^t divide a U_{ep} y hemos demostrado el

Teorema 4. *Sea $\{U_i\}_{i\in\mathbb{N}}$ la s.L. determinada por P, Q y sea p primo, $(p, 2Q) = 1$. Entonces, $w(p^t)$ existe y divide a $p^{t-1}\left(p - \left(\frac{d}{n}\right)\right)$.*

16.2. Rango de un número compuesto. Si $\{U_i\}_{i\in\mathbb{N}}$ es una s.L. determinada por P, Q y $n = p_1^{e_1}\cdots p_r^{e_r}$, con$(n, 2Q) = 1$. Entonces, para cada i por el teorema anterior, $p_i^{e_i}$ divide a $U_{kp_i^{e_i-1}\left(p_i - \left(\frac{d}{n}\right)\right)}$ para todo $k > 1$.

Como son primos diferentes, n divide a U_s, donde s es el mínimo común múltiplo de los $p_i^{e_i-1}\left(p_i-\left(\frac{d}{n}\right)\right)$.

Por tanto, $w(n)$ existe y divide a ese mcm y hemos demostrado el

Lema 13. *Para cualquier s.L., si $n=p_1^{e_1}\cdots p_r^{e_r}$ es compuesto, $w(n)$ existe y divide al mcm de los $p_i^{e_i-1}\left(p_i-\left(\frac{d}{n}\right)\right)$.*

Ahora, podemos demostrar el

Teorema 5. ***[Lucas-caracterización de primalidad]*** *Si encontramos una s.L. $\{U_i\}_{i\in\mathbb{N}}$ determinada por P,Q, con $d=P^2-4Q$ no cuadrado perfecto y $n\in\mathbb{Z}$ satisface $(n,2Qd)=1$ y $w(n)=n\pm1$. Entonces, n es primo.*

Demostración:
Por reducción al absurdo, si n es divisible por 2 o mas primos, el corolario anterior nos dice que $w(n)<n-1\leq n\pm1$ que contradice la hipótesis.

Si $n=p^t$, con $t>1$, por el teorema 4, $w(n)$ es un divisor de $p^{t-1}\left(p-\left(\frac{d}{n}\right)\right)=p^t\pm p^{t-1}$. Pero $n\pm1=p^t\pm1$ no puede dividirlo. Y también contradice.

17. Primos en enteros cuadráticos

Si p es un primo impar y d no es un residuo cuadrático módulo p (i.e. $\left(\frac{d}{p}\right) = -1$). Si p divide a $(a+b\sqrt{d})(f+g\sqrt{d}) = af+bgd+(bf+ag)\sqrt{d}$, entonces también divide a $(a-b\sqrt{d})(f-g\sqrt{d}) = af+bgd-(bf+ag)\sqrt{d}$.

Por tanto, p^2 divide a $(a^2-db^2)(f^2-dg^2)$ y así p divide a uno de los dos, por ej a a^2-db^2. Ahora, si p no divide a b, existe el inverso de $b \pmod p$ y en consecuencia $(ab^{-1})^2 \equiv d \pmod p$ lo que contradice la hipótesis. Necesariamente, p divide a b y como divide a a^2-db^2, también dividirá a a como queríamos. Así,

Lema 14. *Si p primo impar con $\left(\frac{d}{p}\right) = -1$. Entonces, si p divide a $(a+b\sqrt{d})(f+g\sqrt{d})$ divide a uno de los dos factores.*

Corolario 3. *Si p primo impar con $\left(\frac{d}{p}\right) = -1$. Entonces, p sigue siendo primo en el anillo $A = O_{\sqrt{d}} = \mathbb{Z}[\frac{1+\sqrt{d}}{2}]$, de enteros cuadráticos en $\mathbb{Q}[\sqrt{d}]$. En particular, el anillo cociente $K = A/pA$ es cuerpo.*

17.1. El cuerpo cociente. Si p primo impar con $\left(\frac{d}{p}\right) = -1$. Entonces, como existe $2^{-1} \pmod p$, todo elemento del cuerpo cociente

$$K = \frac{O_{\sqrt{d}}}{(p)}$$

tiene un representante $a+b\sqrt{d}$, con $a,b \in \{0,1,\ldots,p-1\}$. Además, si

$$a+b\sqrt{d} \equiv f+g\sqrt{d} \pmod{p} \Leftrightarrow (a-f)+(b-g)\sqrt{d} = p(s+t\sqrt{d}) \Leftrightarrow$$

$$\Leftrightarrow \begin{cases} a-f = st \Leftrightarrow a \equiv f \pmod{p} \\ b-g = pt \Leftrightarrow b \equiv g \pmod{p} \end{cases}$$

Corolario 4. *Si p primo impar con $\left(\frac{d}{p}\right) = -1$. Entonces, el anillo cociente $K = \frac{O_{\sqrt{d}}}{(p)}$ es un cuerpo finito con p^2 elementos.*

Por lo anterior, el conjunto

$$K = \{a+b\sqrt{d} \in \mathbb{C} : \ 0 \leq a,b < p\}$$

con el producto usual módulo p es un modelo concreto para este cuerpo.

17.2. Existencia de elementos primitivos en cuerpos finitos. Como el grupo multiplicativo es $U(K) = K - \{0\}$, para $K = \frac{O_{\sqrt{d}}}{(p)}$ con p primo impar, $\left(\frac{d}{p}\right) = -1$ tenemos

$$|U(K)| = p^2 - 1 = (p-1)(p+1)$$

Por el teorema de Lagrange, el orden multiplicativo de cada elemento de K, debe ser un un divisor de p^2-1.

Si existe $\alpha \in K$ de orden multiplicativo r, entonces sus r potencias distintas $1, \alpha, \ldots, \alpha^{r-1} \in K$, todas satisfacen la ecuación $x^r - 1 = 0$. Esos son exactamente los elementos que tienen de orden un divisor de r ya que la ecuación $x^r - 1 \in K[x]$ tiene como máximo r raíces en K. Entre ellos $\varphi(r)$ tienen exactamente orden r.

Como además, para todo $m \in \mathbb{N}$, $m = \sum_{r|m} \varphi(r)$, con $\varphi(r)$ la función de Euler, entonces la igualdad

$$p^2 - 1 = \sum_{r|p^2-1} \varphi(r) = \varphi(1) + \varphi(2) + \cdots + \varphi(p^2 - 1)$$

nos demuestra que tiene que haber en $U(K)$ elementos de orden cualquier divisor de $p^2 - 1$. En particular, existen $\varphi(p^2 - 1)$ elementos de orden máximo, $p^2 - 1$, y estos generan al grupo multiplicativo $U(K)$. O sea,

Teorema 6. *Si p primo impar con $\left(\frac{d}{p}\right) = -1$, el grupo multiplicativo de $K = \frac{O_{\sqrt{d}}}{(p)}$ es cíclico de orden $p^2 - 1$.*

17.3. Existencia de Lucas-certificado para un primo. Si p primo impar con $\left(\frac{d}{p}\right) = -1$, entre los $p^2 - 1$ elementos de $U(K)$,

$$a + b\sqrt{d} \in K, 1 \leq a < p, 0 \leq b < p$$

hay elementos de orden cualquier divisor de $p^2 - 1 = (p-1)(p+1)$.

Ahora, sea una s.L., $\{U_i\}_{i\in\mathbb{N}}$, definida por $P,Q \in \mathbb{Z}$, con $d = P^2 - 4Q$ no cuadrado perfecto, y $\alpha = \frac{P+\sqrt{d}}{2}$. Sea también p primo impar con $\left(\frac{d}{p}\right) = -1$. Por el TPF para ent. cuadr., la s.L. $\{U_i\}_{i\in\mathbb{N}}$ certifica que p es primo si y sólo si $p+1$ es la menor potencia de α que sale congruente, módulo p, con un entero racional. Esto es cierto, si en el cuerpo cociente la clase de α, módulo p, tiene de orden multiplicativo $(p^2-1)/t$ con t un divisor primo con $p+1$ (i.e., t divisor impar de $p-1$).

Recíprocamente, si $a+b\sqrt{d} \in K$ tiene de orden $(p^2-1)/t$ con t un divisor impar de $p-1$, entonces la s.L. asociada a $P = 2a$, $Q = a^2 - b^2 d \pmod p$ certifica la primalidad de p. Así

Teorema 7. *Existen al menos tantas s.L. que certifican la primalidad de p como elementos en K tienen orden $(p^2-1)/t$ con t un divisor impar de $p-1$.*

17.4. Probabilidad de un Lucas-certificado de primalidad. Como

$$\sum_{t|p-1,\ \text{t impar}} \varphi((p^2-1)/t) = (p-1)\varphi(p+1)$$

la probabilidad de encontrar una s.L.-certificado es $\frac{(p-1)\varphi(p+1)}{p^2-1} = \frac{\varphi(p+1)}{p+1}$

Ahora, si $\alpha = a+b\sqrt{d} \in K$ tiene orden $(p^2-1)/t$ con t un divisor impar de $p-1$, como existe $a^{-1} \pmod p$, también el elemento

$$\beta = (2a)^{-1}\alpha = (2a)^{-1}(a+b\sqrt{d}) = \frac{1+a^{-1}b\sqrt{d}}{2} = \frac{1+\sqrt{a^{-2}b^2 d}}{2}$$

tiene el mismo orden y su correspondiente s.L está asociada a $P = 1$, $Q \equiv (1 - a^{-2}b^2 d)/4 \pmod{p}$.

Por tanto, se tiene

Corolario 5. *La probabilidad de encontrar una s.L.-certificado es* $\frac{(p-1)\varphi(p+1)}{p^2-1} = \frac{\varphi(p+1)}{p+1}$ *y basta buscar entre las s.L.,* $\{U_i\}_{i\in\mathbb{N}}$*, definidas por* $P = 1, Q \in \mathbb{N}$*, con* $d = 1 - 4Q$ *no cuadrado perfecto, para certificar la primalidad de* p*.*

Ejemplo 22. ***Buscando un Lucas-certificado***
El número $n = 740580514804901$ *pasa el test Miller-Rabin y el de Solovay-Strassen para las bases* $2, 3, 5, 7, 11$*. Queremos certificar su primalidad encontrándole una s.L. Para eso necesitamos los factores primos de* $n + 1 = 740580514804902 = 2 * 370290257402451 = 2 * 3 * 123430085800817$.

El cofactor $m = 123430085800817$ *no pasa el test de primalidad de Fermat, ya que para la base* $a = 2$*, se tiene*

$$2^{m-1} \equiv 78526559169539 \pmod{m}$$

Como la potencia $2^{m-1} \not\equiv 1 \pmod{m}$*, m es un número compuesto y le podemos aplicar el método* ρ *de Pollard.*

Usando la función $f(x) = x^2 + 1$ *para iterar x, la variable y itera con la función* $f(f(y)) = y^4 + 2y^2 + 2$*. Calculando x, y módulo m y el mcd*$(x - y, m)$*,*

encontramos en 6 pasos el divisor 17

Paso	x	x	*mcd*
0	1	1	1
1	2	5	1
2	5	677	1
3	26	210066388901	1
4	677	115039510878259	1
5	458330	66454599203495	1
6	210066388901	91841093998594	17

Y obtenemos, la factorización $m = 123430085800817 = 17 * 7260593282401$

Análisis del cofactor. *El cofactor* $m_1 = 7260593282401$ *no pasa el test de Fermat, ya que para la base* $a = 2$*, se tiene*

$$2^{m_1-1} \equiv 1956858885248 \pmod{m_1}$$

Como la potencia 2^{m_1-1} *no da 1,* m_1 *es compuesto y le podemos aplicar el método ρ de Pollard.* Aquí ρ de Pollard es eficiente mientras que el método de factorización de Fermat no lo es (tarda demasiado). Esta vez en 115 iteraciones del ρ de Pollard, se encuentra la factorización*

$$m_1 = 7260593282401 = 4759 * 1525655239$$

y por tanto

$$n + 1 = 740580514804902 = 2 * 3 * 17 * 4759 * 1525655239$$

Como se comprueba que 4759 *es primo (p. ej., mirando en una tabla), nos queda analizar el cofactor*

$$m_2 = 1525655239$$

Análisis del segundo cofactor. $m_2 = 1525655239$ *pasa el test Miller-Rabin y el de Solovay-Strassen para las bases* $2,3,5,7,11$. *Vamos a certificar su primalidad encontrándole una s.L. Para eso, necesitamos factorizar* $m_2 + 1 = 1525655240 = 2^3 * 5 * 38141381$ *Pero el nuevo cofactor* 38141381 *no pasa el test de Fermat y lo factorizamos con el método* ρ *de Pollard. En* 28 *iteraciones, conseguimos*

$$38141381 = 967 * 39443$$

donde ambos factores son primos, 967 se mira en una tabla, y 39443 *se certifica que es primo porque* 2 *es un elemento primitivo. Por tanto,*

$$m_2 + 1 = 1525655240 = 2^3 * 5 * 967 * 39443$$

Ahora, buscando entre las s.L. para $Q = 2,3,4,\ldots$, *encontramos que la s.L. definida por P=1 y Q=6 el número* m_2 *tiene rango* m_2+1 *ya que calculando los términos*

$$\begin{cases} U_{m_2+1} \equiv 0 \pmod{m)_2} \\ U_{(m_2+1)/2} \equiv 959080291 \pmod{m)_2} \\ U_{(m_2+1)/5} \equiv 1335495812 \pmod{m)_2} \\ U_{(m_2+1)/967} \equiv 817967711 \pmod{m)_2} \\ U_{(m_2+1)/39443} \equiv 448183651 \pmod{m)_2} \end{cases}$$

Por tanto, se certifica que $m_2 = 1525655239$ *es primo.*

Lucas certificado final

Como $m_2 = 1525655239$ *es primo, tenemos la factorización en primos de*

$$n+1 = 740580514804902 = 2*3*17*4759*1525655239$$

y podemos empezar a buscar una s.L. para certificar que n *es primo.*

$$n = 740580514804901$$

Entre las s.L. para $Q = 2,3,4,\ldots$, *encontramos que la s.L. definida por P=1 y Q=31 el número* n *tiene rango* $w(n) = n+1$ *ya que calculando los términos*

$$\begin{cases} U_{n+1} \equiv 0 \pmod{n} \\ U_{(n+1)/2} \equiv 541879725150419 \pmod{n} \\ U_{(n+1)/3} \equiv 107159771256277 \pmod{n} \\ U_{(n+1)/17} \equiv 713517050696461 \pmod{n} \\ U_{(n+1)/4759} \equiv 251516807968421 \pmod{n} \\ U_{(n+1)/1525655239} \equiv 464091933503725 \pmod{n} \end{cases}$$

Y finalmente, se certifica que $n = 740580514804901$ *es primo.*

18. Ejercicios.

Ejercicio 1.

19. Referencias.

[1] David Bressoud, Stan Wagon: *A Course in Computational Number Theory*, John Wiley & Sons, Hoboken, NJ, USA, 2000.

[2] Hans Riesel: *Prime Numbers and Computer Methods for Factorization*, Springer Science+Business Media, LLC 2012, (first edition Birkhäuser, 1994).

[3] Samuel S. Wagstaff, Jr: *The joy of factoring*, AMS, Providence, Rhode island, 2013.

20. Test de repaso.