Universidad Autónoma de Chiapas

Facultad de Ciencias en física y matemáticas

Descripción de un método para resolver algunas ecuaciones diofánticas exponenciales usando formas lineales en logaritmos

TESIS

QUE PARA OBTENER EL GRADO DE:

Maestro en Ciencias Matemáticas

PRESENTA:

Luis Elesban Santos Cruz

Asesor:
Dr. Sergio Guzmán Sánchez

Tuxtla Gutiérrez, Chiapas. 20 de Mayo del 2019.

UNIVERSIDAD AUTÓNOMA DE CHIAPAS
FACULTAD DE CIENCIAS EN FÍSICA Y MATEMÁTICAS
DIRECCIÓN
CONTROL ESCOLAR POSGRADO

Tuxtla Gutiérrez, Chiapas
07 de mayo de 2019
Oficio No. FCFM/0202/19

Dr. Sergio Guzmán Sánchez
Presidente y Director de Tesis
Presente

Por este medio me permito informarle que una vez efectuada la revisión de la tesis denominada:

"DESCRIPCIÓN DE UN MÉTODO PARA RESOLVER ALGUNAS ECUACIONES DIOFÁNTICAS EXPONENCIALES USANDO FORMAS LINEALES EN LOGARITMOS".

Ha sido aceptado para sustentar el Examen de Grado de Maestro en Ciencias Matemáticas del **Lic. Luis Elesban Santos Cruz** con matrícula escolar: PS800.

Se autoriza su impresión en virtud de cumplir con los requisitos correspondientes.

Atentamente

"Por la conciencia de la necesidad de servir"

UNACH FÍSICA Y MATEMÁTICAS DIRECCIÓN FCFM

Dr. Sendic Estrada Jiménez
Director

C.c.p. Dr. Florencio Corona Vázquez, Secretario Académico de la FCFM.
CP. Juan Manuel Aguiar Gámez.- Encargado de Posgrado FCFM
Archivo / Minutario
SEJ /jmag

FCFM- UNACH – Ciudad Universitaria, Carretera Emiliano Zapata Km 8, Rancho San Francisco, Tuxtla Gutiérrez, Chiapas. C. P. 29050.
Correo electrónico: fcfm.posgrado@gmail.com Tel. 61 7 80 00 ext. 8104

Agradecimientos.

Quiero expresar mi más sincero agradecimiento al Dr. Sergio Guzmán por su esfuerzo, dedicación y por todas y cada una de sus atenciones e indicaciones así como su infinita paciencia durante el desarrollo de este trabajo, por orientarme tanto en el ámbito profesional como en la personal, por sus consejos, por inculcarme disciplina, así como responsabilidad en las acciones de la vida. Sin duda le estaré siempre agradecido.

Por otra parte, agradezco al jurado, Dr. Aarón Quiñones, Dra. Rosario Soler, Dr. Saúl Campos y Dr. Jhon J. Bravo, por la revisión, corrección y sus valiosos y muy acertados comentarios que hicieron para mejorar este trabajo.

Agradezco especialmente Deysi por alentarme en esta aventura que no fue nada fácil, además de ofrecerme su apoyo incondicional en todo momento. Muchas gracias por estar ahí cuando te necesitaba, tu apoyo fue indispensable.

Quiero agradecer a mi madre Maria y mi padre Elesban, a ellos les debo la vida y les estaré eternamente agradecido por eso. A mis hermanas Yaneth y Gloria y a mi hermano Santiago por ser un soporte cuando los necesité. A mi abuela que es mi segunda madre y a quien le debo la gran parte de mi ser. Gracias por todo.

También quiero agradecer a todos los profesores de la FCFM. En especial a los profesores Dr. Armando Mendoza, Dr. Saúl Campos, Dra. Rosario Soler, Dra. Eddaly Guerra y Dr. Aarón Quiñones por esforzarse en todo momento para impartir sus cursos en los que tuve la oportunidad de ser su estudiante.

A mis compañeros de la maestría Lupita, Fatima y Herón con los cuales tuve el gusto de tomar algunos de los cursos de la maestría. En especial a Herón con el cual compartí momentos de alegría y enojos desde los primeros días en los que decidí tomar este reto.

A todos aquelos que fueron parte fundamental para conclusión de esta etapa muy importante de mi vida. Muchas gracias.

Finalmente, gracias a ti amigo(a) lector(a) por interesarte en leer este trabajo, espero te pueda servir de ayuda.

Resumen.

En este trabajo presentamos un método donde usamos la teoría de formas lineales en logaritmos para resolver ciertas ecuaciones diofánticas del tipo exponencial, dichas ecuaciones involucran sucesiones linealmente recurrentes que cumplen con algunas características. Dicho método lo explicamos resolviendo un par de ejemplos.

Índice general

Notación

deg	Grado de un polinomio.
$\deg_K(\alpha)$	Grado de α sobre K.
$\lfloor x \rfloor$	Mayor entero menor o igual a x.
$\|\| \cdot \|\|$	Distancia al entero más cercano.
$h(\alpha)$	Altura logarítmica del número algebraico α.
$\mathbb{A}$	Conjunto de números algebraicos.
$\mathbb{P}$	Conjunto de números primos.
$[a_0, \ldots, a_n]$	Fracción continua finita.
$C_k := [a_0, \ldots, a_k]$, $0 \leq k \leq n$	k-ésima convergente de $[a_0, \ldots, a_n]$.
$[a_0, a_1, a_2, \ldots]$	Fracción continua infinita.
$\mathrm{Irr}_K(\alpha)$	Polinomio mínimo de α sobre K.
$\mathrm{fld}_K(\alpha)$	Polinomio de campo de α sobre K.
log	Logaritmo natural.

Introducción

La temática central del trabajo es la teoría de formas lineales en logaritmos. Esta teoría tuvo su auge en el año de 1966 gracias al matemático britanico A. Baker[1], él en sus trabajos "Linear forms in logarithms of algebraic numbers I,II III" ([4], [5], [6]) presentó una cota inferior efectiva para el valor absoluto de una forma lineal en logaritmos no cero de números algebraicos. A partir del resultado de Baker se empezaron a resolver problemas diofánticos del tipo exponencial que aún, en ese momento, no eran resueltos. Gracias a su trabajo A. Baker ganó la medalla Fields en 1970.

Matemáticos como Wűstholz[2], Matveev[3] y hasta el mismo A. Baker estuvieron trabajando en mejorar la cota inferior, no fue si no hasta el año 2000 que Matveev en sus trabajos "An explicit lower bound for a homogeneous rational linear form in the logarithms of algebraic numbers. I, II" ([29], [30]) presentó una cota inferior que es la más efectiva, hasta el día de hoy, según Yann Bugeaud (ver [14]). En este trabajo usamos la cota presentada por Matveev y damos una forma de aplicarla para resolver algunas ecuaciones del tipo exponenciales.

El teorema de Matveev como se menciona en el párrafo anterior proporciona una cota inferior no trivial para el valor absoluto de una forma lineal en logaritmos; en realidad, el resultado lo usamos para ver que, cierta ecuación diofántica, tiene una cantidad finita de soluciones dando una cota sobre las variables involucradas en nuestro problema diofántico. Por lo general, al aplicar el teorema de Matveev, la cota obtenida es muy alta, por ello, lo que hacemos es aplicar un método de reducción; en este

[1] Alan Baker(1939-2018).
[2] Gisbert Wűstholz(1948), matemático Alemán.
[3] Eugene Mikhailovich Matveev (1955), matemático Ruso.

caso usamos un resultado de Dujella[4] y Pethő[5] ([18]).

Para esta tesis, se necesita que el lector esté familiarizado con resultados básicos de fracciones continuas y teoría algebraica de números así como también, tener noción de algunos conceptos de teoría de campos, sin embargo, en el capítulo uno, se repasan algunas definiciones y resultados básicos, esencialmente para fijar la notación. El trabajo está diseñado de tal forma que sea autocontenido; está distribuido en dos capítulos y dos apéndices.

El primer capítulo lo dedicamos a presentar resultados básicos, iniciando con nociones sobre fracciones continuas, las cuales nos ayudan a sentar las bases para presentar el lema de Dujella y Pethő. Continuamos esta parte con conceptos de sucesiones linealmente recurrentes que son de utilidad para el tipo de problemas que presentamos pues están muy relacionados a ellos. Aquí también damos algunos preliminares sobre números algebraicos y trascendentes mismos que son necesarios para entender el teorema de Matveev.

En el capítulo dos presentamos dos ejemplos en los cuales explicamos una manera de usar el teorema de Matveev para resolver ciertos tipos de problemas. En los mismos ejemplos mostramos como el lema de Dujella y Pethő es eficiente para reducir cotas.

Por último, en los apéndices se incluyen temas sobre campos de números algebraicos y el código que hemos usado para reducir las cotas de las variables de los ejemplos del capítulo dos.

El orden de la presentación del contenido está relacionado con la comprensión que adquirimos sobre la teoría en formas lineales en logaritmos. Tratamos de presentar ejemplos de la mayoría de los conceptos para que queden claros y así hacer un trabajo comprensible.

[4]Andrej Dujella (1966), matemático Croata.
[5]Attila Pethő (1950), matemático Hungaro.

Capítulo 1 Preliminares

Este primer capítulo, incluye algunos conceptos básicos de teoría de números como lo son fracciones continuas y sucesiones linealmente recurrentes así como números algebraicos y trascendentes, además de incluir algunos resultados de formas lineales en logaritmos.

1.1 Fracciones continuas

El objetivo de esta sección es presentar un lema que usaremos en las secciones 2.2 y 2.3 como método de reducción de cota. Para su demostración daremos algunos conceptos y resultados básicos sobre fracciones continuas. Si el lector está interesado en saber más sobre este tema le sugerimos ver [24], [37], [16] y [21].

Definición 1.1.1. Una fracción continua finita es una expresión de la forma

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cdots + \cfrac{1}{a_{n-1} + \cfrac{1}{a_n}}}} \tag{1.1}$$

donde cada $a_i \in \mathbb{R}$ y $a_i > 0$ para $1 \leq i \leq n$. Usaremos la notación $[a_0, \ldots, a_n]$ para denotar la expresión anterior.

Cuando $a_i \in \mathbb{Z}$ para todo $0 \leq i \leq n$ la fracción continua se llama simple. La fracción continua $C_k = [a_0, \ldots, a_k]$, $0 \leq k \leq n$ se llama la k-ésima convergente de $[a_0, \ldots, a_n]$.

Observe que cada fracción continua simple finita representa un número racional. Recíprocamente, usando el algoritmo de Euclides, se puede demostrar que cada número racional se puede expresar como una fracción

continua simple finita. En efecto, si $p, q \in \mathbb{P}$ son relativos y escribimos

$$\begin{aligned} p &= qa_0 + r_1, & 1 \leq r_1 < q; \\ q &= a_1 r_1 + r_2; & 1 \leq r_2 < r_1; \\ \vdots &= \vdots \\ r_{n-1} &= a_n r_n \end{aligned}$$

donde $n \geq 0$ es maximal en el sentido que $r_n \geq 1$. Es rutinario verificar que la expresión (1.1) es p/q. Notemos que el anterior proceso nos ayuda a encontrar la fracción continua de un número racional el cual usamos en el siguiente ejemplo.

Ejemplo 1.1.2. *La fracción continua de* $7/11$.

$$\begin{aligned} \frac{7}{11} &= 0 + \frac{1}{\frac{11}{7}} = 0 + \frac{1}{1 + \frac{4}{7}} = 0 + \frac{1}{1 + \frac{1}{\frac{7}{4}}} = 0 + \frac{1}{1 + \frac{1}{1 + \frac{3}{4}}} \\ &= 0 + \frac{1}{1 + \frac{1}{1 + \frac{1}{\frac{4}{3}}}} = 0 + \frac{1}{1 + \frac{1}{1 + \frac{1}{1 + \frac{1}{3}}}}, \end{aligned}$$

así, $\frac{7}{11} = [0, 1, 1, 1, 3]$.

La siguiente proposición enlista algunas propiedades importantes de las convergentes de las fracciones continuas.

Proposición 1.1.3. *Consideremos la fracción continua* $[a_0, \ldots, a_n]$. *Definamos las sucesiones* $p_0, \ldots, p_n$ *y* $q_0, \ldots, q_n$ *recursivamente como sigue:*

$$\begin{aligned} &p_0 = a_0 && q_0 = 1; \\ &p_1 = a_0 a_1 + 1 && q_1 = a_1; \\ &p_k = a_k p_{k-1} + p_{k-2} && q_k = a_k q_{k-1} + q_{k-2} \quad \textit{para } k \geq 2. \end{aligned}$$

Se tienen las siguientes igualdades:

(i) $C_k = p_k/q_k$.

(ii) $p_k q_{k-1} - p_{k-1} q_k = (-1)^{k-1}$ *para todo* $k \geq 1$.

(iii) $C_k - C_{k-1} = \dfrac{(-1)^{k-1}}{q_k q_{k-1}}$ *para* $1 \leq k \leq n$.

(iv) $C_k - C_{k-2} = \dfrac{(-1)^k a_k}{q_k q_{k-2}}$ *para* $2 \leq k \leq n$.

Demostración. Los incisos (i) y (ii) serán demostrados por inducción sobre k.

(i) Para $k = 0$ y $k = 1$ tenemos $C_0 = [a_0] = p_0/q_0$ y

$$C_1 = [a_0, a_1] = a_0 + \frac{1}{a_1} = \frac{a_0 a_1 + 1}{a_1} = \frac{p_1}{q_1},$$

respectivamente. Sea $k > 1$ y supongamos que la igualdad es cierta para $C_i = p_i/q_i$, $i \leq k$. Observemos que p_{k-2}, q_{k-2}, p_{k-1} y q_{k-1} dependen sólo de $a_0, a_1, \ldots, a_{k-1}$, por lo tanto,

$$C_{k+1} = [a_0, a_1, \ldots, a_{k-1}, a_k, a_{k+1}] = \left[a_0, a_1, \ldots, a_{k-1}, a_k + \frac{1}{a_{k+1}}\right].$$

Aplicando la hipótesis de inducción a la última expresión se tiene que

$$\begin{aligned} C_{k+1} &= \frac{\left(a_k + \frac{1}{a_{k+1}}\right) p_{k-1} + p_{k-2}}{\left(a_k + \frac{1}{a_{k+1}}\right) q_{k-1} + q_{k-2}} = \frac{a_{k+1}\left(a_k p_{k-1} + p_{k-2}\right) + p_{k-1}}{a_{k+1}\left(a_k q_{k-1} + q_{k-2}\right) + q_{k-1}} \\ &= \frac{a_{k+1} p_k + p_{k-1}}{a_{k+1} q_k + q_{k-1}} = \frac{p_{k+1}}{q_{k+1}}. \end{aligned}$$

(ii) Si $k = 1$ claramente,

$$p_1 q_0 - p_0 q_1 = (a_0 a_1 + 1)1 - a_0 a_1 = 1.$$

Supongamos que la igualdad se satisface para $n < k$ y demostremos que se cumple para $n = k$. En efecto,

$$\begin{aligned} p_k q_{k-1} - p_{k-1} q_k &= (a_k p_{k-1} + p_{k-2}) q_{k-1} - p_{k-1}(a_k q_{k-1} + q_{k-2}) \\ &= -(p_{k-1} q_{k-2} - p_{k-2} q_{k-1}) = -(-1)^{k-2} \\ &= (-1)^{k-1}. \end{aligned}$$

(iii) $C_k - C_{k-1} \underset{(i)}{=} \frac{p_k}{q_k} - \frac{p_{k-1}}{q_{k-1}} = \frac{p_k q_{k-1} - p_k q_k}{q_k q_{k-1}} \underset{(ii)}{=} \frac{(-1)^{k-1}}{q_k q_{k-1}}$.

(iv) Finalmente,

$$\begin{aligned} C_k - C_{k-2} &\underset{(i)}{=} \frac{p_k}{q_k} - \frac{p_{k-2}}{q_{k-2}} = \frac{p_k q_{k-2} - q_k p_{k-2}}{q_k q_{k-2}} \\ &= \frac{(a_k p_{k-1} + p_{k-2}) q_{k-2} - (a_k q_{k-1} + q_{k-2}) p_{k-2}}{q_k q_{k-2}} \\ &= \frac{a_k (p_{k-1} q_{k-2} - p_{k-2} q_{k-1})}{q_k q_{k-2}} \underset{(ii)}{=} \frac{(-1)^{k-2} a_k}{q_k q_{k-2}} = \frac{(-1)^k a_k}{q_k q_{k-2}}. \end{aligned}$$

Q.E.D.

De la proposición anterior podemos verificar que si $a_0 > 0$ entonces las sucesiones $(q_k)_{0 \leq k \leq n}$ y $(p_k)_{0 \leq k \leq n}$ son crecientes. Además, si $[a_0, \ldots, a_n]$ es una fracción continua simple de (iii) se tiene que p_k y q_k son primos relativos. También tenemos lo siguiente.

Observación 1.1.4. Si $k \geq 2$ es par entonces $C_k > C_{k-2}$ y si $k \geq 3$ es impar entonces $C_k < C_{k-2}$. Además

$$C_{2k} - C_{2k-1} = \frac{(-1)^{2k-1}}{q_{2k} q_{2k-1}} < 0.$$

Consecuentemente,

$$C_0 < C_2 < C_4 < C_6 < \cdots < C_5 < C_3 < C_1.$$

De la observación anterior se concluye que la sucesión de convergentes, con índices pares, es creciente, mientras que la sucesión de convergentes, con índices impares, es decreciente; más aún, toda convergente de índice par es menor que cualquier convergente de índice impar.

Teorema 1.1.5. *Sea $(a_n)_{n \geq 0}$ una sucesión infinita de enteros con $a_i > 0$ para $i \geq 1$ y sea $C_k = [a_0, \ldots, a_k]$. Se tiene:*

(i) La sucesión $(C_{2n+1})_{n \geq 0}$ es decreciente y acotada y por lo tanto convergente.

(ii) La sucesión $(C_{2n})_{n \geq 0}$ es creciente y acotada y por lo tanto convergente.

(iii) La sucesión $C_{2n} - C_{2n+1}$ tiende a cero.

Demostración.

(i) Tenemos $C_1 > C_3 > C_5 > \cdots$, se tiene también que $C_{2n+1} > C_0$. La sucesión $(C_{2n+1})_{n\geq 0}$ es entonces decreciente y acotada inferiormente por C_0, por lo tanto converge.

(ii) Tenemos también que $C_0 < C_2 < C_4 < \cdots$ y que $C_{2n} < C_1$. La sucesión $(C_{2n})_{n\geq 0}$ es entonces creciente y acotada superiormente por C_1, por lo tanto converge.

(iii) Sean $\alpha_1 = \lim_{n\to\infty} C_{2n}$ y $\alpha_2 = \lim_{n\to\infty} C_{2n+1}$. Queremos ver que $\alpha_1 = \alpha_2$. En efecto, como cada $a_i \geq 1$ para $i \geq 1$ y $q_0, q_1 \geq 1$, se puede probar fácilmente por inducción sobre k que

$$q_k = a_k q_{k-1} + q_{k-2} \geq 2k - 3.$$

Aplicando el inciso (iii) de la proposición 1.1.3 se tiene

$$C_{2n+1} - C_{2n} = \frac{1}{q_{2n+1}q_{2n}} \leq \frac{1}{(4n-1)(4n-3)} \underset{n\to\infty}{\longrightarrow} 0,$$

por lo tanto, ambas sucesiones convergen al mismo límite, que es lo que se quería ver.

Q.E.D.

Notése que del inciso (iii) del teorema 1.1.5 se concluye que $(C_n)_{n\geq 0}$ es convergente. Esto nos permite definir correctamente las fracciones continuas infinitas, antes presentamos un lema sin demostración que nos será útil. La demostración puede ser encontrada en [34].

Lema 1.1.6. *Un número real α es irracional si y sólo si existe una cantidad infinita de números racionales p/q tales que*

$$\left|\alpha - \frac{p}{q}\right| \leq \frac{1}{q^2}.$$

Definición 1.1.7. Sea $(a_n)_{n\geq 0}$ una sucesión infinita de enteros con $a_n > 0$ para $n \geq 1$. Definimos la fracción continua infinita como el límite de las fracciones continuas finitas

$$[a_0, a_1, \ldots] := \lim_{n\to\infty} C_n.$$

Sea $\alpha = \lim_{n\to\infty} C_n$. Observe que si n es par entonces se tiene:

$$\begin{aligned} C_n < \alpha < C_{n+1} &\Rightarrow 0 < \alpha - C_n < C_{n+1} - C_n \\ &\Rightarrow 0 < |\alpha - C_n| < |C_{n+1} - C_n|\,. \end{aligned}$$

y si n es impar se tiene:

$$\begin{aligned} C_n > \alpha > C_{n+1} &\Rightarrow 0 > \alpha - C_n > C_{n+1} - C_n \\ &\Rightarrow 0 < C_n - \alpha < C_n - C_{n+1} \\ &\Rightarrow 0 < |C_n - \alpha| < |C_n - C_{n+1}|\,. \end{aligned}$$

Por lo tanto, para todo n se tiene

$$|\alpha - C_n| < |C_{n+1} - C_n|\,,$$

o de manera equivalente,

$$\left|\alpha - \frac{p_n}{q_n}\right| < \left|\frac{p_{n+1}}{q_{n+1}} - \frac{p_n}{q_n}\right|.$$

Luego, del inciso (ii) de la proposición 1.1.3 se tiene que

$$\left|\frac{p_{n+1}}{q_{n+1}} - \frac{p_n}{q_n}\right| = \frac{1}{q_n q_{n+1}},$$

pero como $q_n < q_{n+1}$ entonces

$$\left|\alpha - \frac{p_n}{q_n}\right| < \frac{1}{q_n^2},$$

para todo n. Como p_n y q_n son primos relativos hemos encontrado una cantidad infinita de números racionales p/q tales que

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^2},$$

y así, por el lema 1.1.6, α es irracional. Podemos concluir entonces que las fracciones continuas infinitas representan siempre números irracionales. De manera recíproca, cualquier número irracional α se puede expresar como fracción continua infinita. Ésto nos lleva a la siguiente proposición.

Proposición 1.1.8. *Dado $\alpha = \alpha_0 \in \mathbb{R} \setminus \mathbb{Q}$ definimos la sucesión $(a_n)_{n\geq 0}$ dada por*

$$a_k = \lfloor \alpha_k \rfloor, \qquad \alpha_{k+1} = \frac{1}{\alpha_k - a_k} \qquad \text{para todo } k \geq 0.$$

Se cumple entonces que $\alpha = [a_0, a_1, \ldots]$.

Demostración. Claramente se tiene

$$\alpha = \alpha_0 = a_0 + \frac{1}{\alpha_1} = [a_0, \alpha_1] = [a_0, a_1, \alpha_2] = \cdots = [a_0, a_1, \ldots, a_k, \alpha_{k+1}];$$

luego, por (i) de la proposición 1.1.3 tenemos

$$\alpha = \frac{\alpha_{k+1} p_k + p_{k-1}}{\alpha_{k-1} q_k + q_{k-1}},$$

y por lo tanto

$$\begin{aligned} |\alpha - C_k| &= \left| \frac{\alpha_{k+1} p_k + p_{k-1}}{\alpha_{k+1} q_k + q_{k-1}} - \frac{p_k}{q_k} \right| = \left| \frac{-(p_k q_{k-1} - q_k p_{k-1})}{(\alpha_{k+1} q_k + q_{k-1}) q_k} \right| \\ &= \frac{1}{(\alpha_{k+1} q_k + q_{k-1}) q_k} < \frac{1}{q_k^2}. \end{aligned}$$

Como $q_k > 1$ para $k > 1$, tenemos que $1/q_k^2 \to 0$ cuando $k \to \infty$, lo que termina la demostración. Q.E.D.

Ejemplo 1.1.9. *La fracción continua infinita de $\sqrt{2}$ es $[1, 2, 2, 2, 2, \ldots]$.*

La siguiente proposición la usaremos para demostrar una propiedad de las convergentes.

Proposición 1.1.10. *Sean $\alpha \in \mathbb{R} \setminus \mathbb{Q}$ y $C_j = p_j/q_j$, $j \geq 1$, las convergentes de la fracción continua de α. Si $r, s \in \mathbb{Z}$ con $s > 0$ y k es un entero positivo tal que*

$$|s\alpha - r| < |q_k \alpha - p_k|$$

entonces $s \geq q_{k+1}$.

Demostración. La demostración la haremos por contradicción. Supongamos que $1 \leq s < q_{k+1}$. Para cada $k \geq 1$ consideremos el sistema de ecuaciones lineales

$$\begin{aligned} p_k x + p_{k+1} y &= r \\ q_k x + q_{k+1} y &= s \end{aligned} \tag{1.2}$$

Utilizando eliminación gaussiana obtenemos:

$$\begin{aligned} (p_k q_{k+1} - p_{k+1} q_k) x &= r q_{k+1} - s p_{k+1} \\ (p_{k+1} q_k - p_k q_{k+1}) y &= r q_k - s p_k \end{aligned}$$

Ahora, como $p_k q_{k+1} - p_{k+1} q_k = (-1)^{k+1}$ se tiene que la solución del sistema es única y está dada por:

$$\begin{aligned} x &= (-1)^{k+1}(r q_{k+1} - s p_{k+1}) \\ y &= (-1)^{k+1}(s p_k - r q_k). \end{aligned}$$

Probaremos ahora que x e y son no nulos y además que son de distinto signo. Si $x = 0$ entonces $s p_{k+1} = r q_{k+1}$, como $(p_{k+1}, q_{k+1}) = 1$ y $s > 1$ se tiene que $q_{k+1} | s$ y esto implica que $q_{k+1} \leq s$, lo cual es una contradicción, pues hemos supuesto que $1 \leq s < q_{k+1}$ y por lo tanto $x \neq 0$. Ahora si $y = 0$, del sistema de ecuaciones (1.2) se tiene que $r = p_k x$ y $s = q_k x$ y así,

$$|s\alpha - r| = |x| \cdot |q_k \alpha - p_k| \geq |q_k \alpha - p_k|$$

lo cual también es una contradicción; por tanto $y \neq 0$.

Veamos que x e y son de signos opuestos. En el caso en que $y < 0$, como $q_k x = s - q_{k+1} y$ con $q_j > 0$, tenemos que $x > 0$. Ahora si $y > 0$ entonces $q_{k+1} y \geq q_{k+1} > s$, luego $q_k x = s - q_{k+1} y < 0$ y así $x < 0$. Por lo tanto $xy < 0$. Recordemos que

$$\begin{aligned} &\tfrac{p_k}{q_k} < \alpha < \tfrac{p_k+1}{q_{k+1}} \quad \text{si } k \equiv 0 \bmod 2; \\ \text{y} \quad &\tfrac{q_{k+1}}{q_{k+1}} < \alpha < \tfrac{p_k}{q_k} \quad \text{si } k \equiv 1 \bmod 2. \end{aligned}$$

En ambos casos, $q_k \alpha - p_k$ y $q_{k+1}\alpha - p_{k+1}$ tienen signos opuestos y por lo tanto $x(q_k \alpha - p_k)$ y $y(q_{k+1}\alpha - p_{k+1})$ tiene el mismo signo. Obtenemos así

que

$$\begin{aligned} |s\alpha - r| &= |(q_k x + q_{k+1} y)\alpha - (p_k x + p_{k+1} y)| \\ &= |x(q_k\alpha - p_k) + y(q_{k+1}\alpha - p_{k+1})| \\ &= |x| \cdot |q_k\alpha - p_k| + |y||q_{k+1}\alpha - p_{k+1}| \\ &> |x| \cdot |q_k\alpha - p_k| \geq |q_k\alpha - p_k|. \end{aligned}$$

Se tiene entonces que $|s\alpha - r| > |q_k\alpha - p_k|$, lo cual es una contradicción y por lo tanto $s \geq q_{k+1}$. **Q.E.D.**

La siguiente proposición se conoce como el criterio de Legendre y se usa para saber si un número racional r/s es una convergente de α.

Proposición 1.1.11. *Si α es un número irracional y r/s es un número racional con $s > 0$ tal que*

$$\left|\alpha - \frac{r}{s}\right| < \frac{1}{2s^2}.$$

Se tiene cumple que r/s es un convergente de la fracción continua de α.

Demostración. Procedamos por contradicción. Supongamos que r/s no es una convergente de la fracción continua de α, es decir, $r/s \neq p_j/q_j$ para toda j. Sea k el entero más grande tal que $s \geq q_k$. Como $q_0 = 1$ y $q_k \to \infty$ cuando $k \to \infty$, este entero existe. Tenemos que $q_k \leq s < q_{k+1}$ y por la proposición anterior se tiene

$$|q_k\alpha - p_k| \leq |s\alpha - r| = s\left|\alpha - \frac{r}{s}\right| < \frac{1}{2s}$$

y por lo tanto,

$$\left|\alpha - \frac{p_k}{q_k}\right| < \frac{1}{2sq_k}.$$

Como $r/s \neq p_k/q_k$, se tiene que $|sp_k - rq_k| \geq 1$ y por tanto

$$\frac{1}{sq_k} \leq \frac{|sp_k - rq_k|}{sq_k} = \left|\frac{p_k}{q_k} - \frac{r}{s}\right| \leq \left|\frac{p_k}{q_k} - \alpha\right| + \left|\alpha - \frac{r}{s}\right| < \frac{1}{2sq_k} + \frac{1}{2s^2};$$

esto implica que

$$\frac{1}{2sq_k} < \frac{1}{2s^2}, \qquad \text{de donde} \qquad q_k > s,$$

lo cual es una contradicción, pues hemos supuesto que $s \geq q_k$. Concluimos por lo tanto que r/s es una convergente de α. Q.E.D.

La siguiente definición nos sirve para determinar cuando un número racional está cerca a un número real α.

Definición 1.1.12. Una fracción a/b con $b > 0$ es llamada una **mejor aproximación de segundo tipo** de un número α si para todo $c, d \in \mathbb{Z}$ con $0 < d \leq b$ y $c/d \neq a/b$ se tiene que

$$|d\alpha - c| > |b\alpha - a|.$$

Ejemplo 1.1.13. *Tomando $\alpha = \sqrt{2}$ se tiene que $a/b = 3/2$ es una mejor aproximación de segundo tipo. Para ver esto, sean $c, d \in \mathbb{Z}$ con $0 < d \leq 2$ y $c/d \neq 3/2$. Analicemos los casos para d, que son $d = 1$ y $d = 2$. Supongamos primero que $d = 1$, debemos ver que*

$$\left|\sqrt{2} - c\right| > \left|2\sqrt{2} - 3\right|.$$

Notemos que como $\sqrt{2} \approx 1.4142$, tenemos que el entero c que hace que la diferencia

$$\left|\sqrt{2} - c\right|$$

sea mínima es 1, entonces

$$\left|\sqrt{2} - c\right| \geq \left|\sqrt{2} - 1\right| > 0.4.$$

Como $|2\sqrt{2} - 3| < 0.18$ se tiene que, para el caso $d = 1$ se satisface

$$\left|\sqrt{2} - c\right| > |2\sqrt{2} - 3| \quad \textit{para todo } c \in \mathbb{Z}.$$

Veamos el segundo caso, supongamos ahora que $d = 2$. En este caso, como $c/2 \neq 3/2$, se tiene que $c \neq 3$. Nuevamente el entero $c \neq 3$ tal que $|2\sqrt{2} - c|$ es mínimo es $c = 2$, entonces

$$|2\sqrt{2} - c| \geq |2\sqrt{2} - 2| > 0.8.$$

Por lo tanto,

$$|2\sqrt{2} - c| > |2\sqrt{2} - 3| \quad \textit{para todo } c \in \mathbb{Z} \setminus \{3\}.$$

Concluimos así que $3/2$ es una mejor aproximación de segundo tipo de $\sqrt{2}$.

Observe que si a/b es una mejor aproximación de segundo tipo de α se satisface que

$$\left|\alpha - \frac{c}{d}\right| > \left|\alpha - \frac{a}{b}\right|, \quad \text{para } c, d \in \mathbb{Z} \text{ con } 0 < d \leq b \text{ y } \frac{c}{d} \neq \frac{a}{b}.$$

Así, si a/b es una mejor aproximación de segundo tipo entonces el número racional a/b está más cerca al número real α que c/d. Podemos hacer una afirmación aún más fuerte, mediante el siguiente teorema, el cual no demostraremos en este trabajo pero si el lector está interesado en la prueba puede verla en [21].

Teorema 1.1.14. *Cualquier mejor aproximación de segundo tipo de un número α, es una convergente de α.*

Observación 1.1.15. Dado que p_k/q_k es una convergente de un número irracional α se tiene que p_k/q_k es una mejor aproximación de segundo tipo. Para ver esto, sean $c, d \in \mathbb{Z}$ tales que $0 < d \leq q_k$ y $c/d \neq p_k/q_k$. Como $d < q_{k+1}$, por la proposición 1.1.10, se tiene que

$$|d\alpha - c| \geq |q_k\alpha - p_k|.$$

Note que la igualdad no es posible por ser α irracional y por lo tanto p_k/q_k es una mejor aproximación de segundo tipo.

Si en la definición 1.1.12 se toma el caso $d = b$, se tiene que

$$|b\alpha - c| > |b\alpha - a|, \quad \text{para } c \neq a.$$

Lo anterior nos dice que, para cualquier entero $c \neq a$, el entero más cercano a $b\alpha$ es a. Lo anterior motiva a la siguiente definición.

Definición 1.1.16. Sea $x \in \mathbb{R}$. Se define y se denota la **distancia de x al entero más cercano** como $\|x\| := \min\{|x - n| : n \in \mathbb{Z}\}$.

Del teorema 1.1.14 y de la observación 1.1.15 se tiene el siguiente corolario.

Corolario 1.1.17. *Si p/q es una convergente de la fracción continua del irracional α entonces*

$$||q\alpha|| = |q\alpha - p|.$$

El siguiente resultado es una variación de un lema de Dujella y Pethő [18].

Lema 1.1.18. *Sean M un entero positivo, p/q una convergente de la fracción continua del irracional γ, A, B y μ números reales con $A > 0$ y $B > 1$. Finalmente, sea $\epsilon = \|\mu q\| - M\|\gamma q\|$. Si $\epsilon > 0$ entonces no hay ninguna solución de la desigualdad*

$$0 < |m\gamma - n + \mu| < AB^{-k}$$

en enteros positivos m, n y k con

$$\frac{\log(Aq/\epsilon)}{\log B} \leq k \qquad y \qquad m \leq M.$$

Demostración. Procedamos por contradicción. Supongamos que

$$0 < |m\gamma - n + \mu| < AB^{-k},$$

multiplicando por q, sumando $mp - mp$ y agrupando se obtiene,

$$|m(\gamma q - p) + mp - nq + \mu q| < qAB^{-k}.$$

Como p/q es una convergente de γ entonces por el corolario 1.1.17 tenemos que $\|\gamma q\| = |\gamma q - p|$, por lo tanto

$$qAB^{-k} > |\mu q - (nq - mp)| - m\|\gamma q\| \geq \|\mu q\| - M\|\gamma q\| = \epsilon,$$

esto implica que

$$k < \frac{\log(Aq/\epsilon)}{\log B},$$

lo cual es una contradicción. **q.e.d.**

El lema 1.1.18 es el que usamos como método de reducción de cota en nuestro trabajo.

Nota 1.1.19. En todos los trabajos en los que investigamos, el denominador q de la convergente de la fracción continua del número irracional γ del lema 1.1.18 se toma mayor a $6M$, pues en la práctica para $q \leq 6M$ el valor numérico de ε es negativo. Es por esto que en nuestro trabajo usaremos esta condición sobre el denominador q.

Ejemplo 1.1.20. *Se desean encontrar todos los enteros no negativos que satisfacen la desigualdad*

$$0 < |x \log 2 - y \log 3 + \log 5| < 40e^{-z}, \tag{1.3}$$

donde $z = max\{x, y\} \leq 10^{30}$.

Como $z < 10^{30}$ *y* $x, y \leq z$, *tomando* $M = 10^{30}$, *se tiene* $x \leq M$. *Supongamos que*

$$x \log 2 - y \log 3 + \log 5 > 0.$$

Luego, dividiendo por $\log 3$ *la ecuación* (1.3) *tenemos,*

$$0 < x\frac{\log 2}{\log 3} - y + \frac{\log 5}{\log 3} < \frac{40}{\log 3}e^{-z}.$$

Ahora, definamos

$$\gamma = \frac{\log 2}{\log 3}, \quad \mu = \frac{\log 5}{\log 3}, \quad A = \frac{40}{\log 3}, \quad B = e.$$

Observe que $A > 0$ *y* $B > 1$. *Calculando una convergente* p/q *de la fracción continua del número irracional* γ *de tal forma que satisfaga* $q > 6M$ *(condición de la nota 1.1.19) y* $\varepsilon = ||\mu q|| - M||\gamma q|| > 0$ *y aplicando el lema 1.1.18 se tiene que*

$$z < \frac{\log (Aq/\varepsilon)}{\log B} \approx 77.4746. \tag{1.4}$$

Podemos por lo tanto buscar los pares (x, y) *que satisfacen las desigualdades* (1.4) *y* (1.3). *Usando Mathematica tenemos que los pares que satisfacen* (1.3) *son,*

$$(0,0), (0,1), (1,0), (1,1), (1,2), (2,0),$$
$$(2,1), (2,2), (3,0), (3,1), (3,2), (3,3), (4,3).$$

Supongamos ahora que

$$x \log 2 - y \log 3 + \log 5 < 0,$$

luego

$$0 < y \log 3 - x \log 2 - \log 5.$$

Dividiendo (1.3) *por* $\log 2$ *tenemos*

$$0 < y\frac{\log 3}{\log 2} - x - \frac{\log 5}{\log 2} < \frac{40}{\log 2}e^{-z}.$$

Tomando

$$\gamma = \frac{\log 3}{\log 2}, \quad \mu = \frac{\log 5}{\log 2}, \quad A = \frac{40}{\log 2}, \quad B = e,$$

tenemos que $A > 0$ *y* $B > 1$. *Nuevamente calculando la convergente* p/q *de* γ *tal que* $q > 6M$ *y* $\varepsilon > 0$ *obtenemos* $z < 89$. *Haciendo la búsqueda de los pares* (x, y) *que satisfacen* $z < 89$ *y* (1.3) *encontramos que son*

$$(0,2), (0,3), (1,3), (2,3), (2,4), (3,4), (4,4), (5,5).$$

Nota 1.1.21. Para la aplicación del lema 1.1.18 se busca una convergente p_k/q_k de tal manera que su denominador cumpla que $q_k > 6M$. Sin embargo, puede suceder que $\varepsilon < 0$, si llega a pasar lo que uno puede hacer para intentar obtener un $\varepsilon > 0$ es buscar una convergente "mayor", es decir, buscar una convergente p_r/q_r con $r > k$. El denominador sigue cumpliendo que $q_r > 6M$ pues la sucesión $(q_n)_{n\geq 0}$ es creciente. Cabe señalar que el proceso de buscar una convergente "mayor" no asegura que en algún momento se tenga que $\varepsilon > 0$.

1.2 Sucesiones linealmente recurrentes

En esta sección presentamos definiciones y resultados básicos sobre sucesiones linealmente recurrentes que nos servirán en el tipo de problemas que trabajamos. Para ver más de esto sugerimos ver [27] y [35].

Definición 1.2.1. Sea $k \geq 1$ un entero. Una sucesión $(u_n)_{n\geq 0} \subset \mathbb{C}$ se llama **linealmente recurrente de orden** k si la recurrencia

$$u_{n+k} = a_1 u_{n+k-1} + a_2 u_{n+k-2} + \cdots + a_k u_n$$

se satisface para todo $n \geq 0$ con algunos coeficientes fijos $a_1, \ldots, a_k \in \mathbb{C}$ con $a_k \neq 0$.

Ejemplo 1.2.2. *La sucesión de Fibonacci* $(F_n)_{n\geq 0}$ *está dada por* $F_0 = 0$, $F_1 = 1$ *y* $F_{n+2} = F_{n+1} + F_n$ *para todo* $n \geq 0$. *Por lo tanto, la sucesión de Fibonacci es linealmente recurrente de orden* 2.

Observación 1.2.3. Sea $(u_n)_{n\geq 0}$ una sucesión linealmenemte recurrente de orden k. Si $a_1, \ldots, a_k \in \mathbb{Z}$ y $u_0, \ldots u_{k-1} \in \mathbb{Z}$ entonces se puede ver por inducción que u_n es un entero para todo $n \geq 0$.

El polinomio

$$f(X) = X^k - a_1 X^{k-1} - \cdots - a_k \in \mathbb{C}[X]$$

se denomina el **polinomio característico** de la sucesión $(u_n)_{n\geq 0}$ de la definición 1.2.1.

Del ejemplo 1.2.2 se tiene que el polinomio característico de la sucesión de Fibonacci es

$$f(X) = X^2 - X - 1.$$

Estamos interesados en encontrar una fórmula del n-ésimo término de la sucesión linealmente recurrente en función de las potencias de las raíces de su respectivo polinomio característico, para esto supongamos primero que

$$f(X) = \prod_{i=1}^{s} (X - \alpha_i)^{\sigma_i},$$

con $\alpha_1, \ldots, \alpha_s$ las raíces de $f(X)$ con multiplicidades $\sigma_1, \ldots, \sigma_s$ respectivamente. La siguiente proposición garantiza la existencia de elementos en cierto campo para poder expresar a la sucesión como combinación lineal de potencias de las raíces de su respectivo polinomio característico.

Proposición 1.2.4. *Si $f(X) \in \mathbb{Z}[X]$ tiene raíces distintas $\alpha_1, \ldots, \alpha_k$ entonces existen constantes $c_1, \ldots, c_k \in \mathbb{K} = \mathbb{Q}(\alpha_1, \ldots, \alpha_k)$ tales que*

$$u_n = \sum_{i=1}^{k} c_i \alpha_i^n \qquad \text{para todo } n \geq 0. \tag{1.5}$$

Demostración. Sea

$$u(z) = \sum_{n\geq 0} u_n z^n.$$

Note que

$$\begin{aligned} u(z)(1 - a_1 z - \cdots - a_k z^k) &= u_0 + (u_1 - u_0 a_1)z + (u_2 - a_1 u_1 - a_2 u_0)z^2 \\ &+ \cdots + \sum_{m\geq k} (u_m - a_1 u_{m-1} - \cdots - a_k u_{m-k}) z^m \\ &:= P(z) \end{aligned}$$

de donde por el hecho de que $(u_n)_{n\geq 0}$ es recurrente de orden k se tiene

$$P(z) = \sum_{m=0}^{k-1}(u_m - a_1u_{m-1} - \cdots - a_mu_0)z^m \in \mathbb{C}[z];$$

por lo tanto,

$$\begin{aligned} u(z) &= \frac{P(z)}{1 - a_1z - \cdots - a_kz^k} = \frac{P(z)}{z^k f(1/z)} = \frac{P(z)}{z^k \prod_{i=1}^k (1/z - \alpha_i)} \\ &= \frac{P(z)}{\prod_{i=1}^k (1 - z\alpha_i)} = \sum_{i=1}^k \frac{c_i}{1 - z\alpha_i} \end{aligned}$$

para algunos coeficientes $c_i \in \mathbb{K}$. Para el último paso hemos usado la teoría de las fracciones parciales junto con el hecho de que $\alpha_1, \ldots, \alpha_k$ son distintos y el grado de $P(z)$ es menor que k. Si

$$|z| < \rho = \min\{|\alpha_i|^{-1} : i = 1, \ldots, k\}$$

entonces podemos escribir

$$\frac{1}{1 - z\alpha_i} = \sum_{n\geq 0}(z\alpha_i)^n = \sum_{n\geq 0}\alpha_i^n z^n \qquad \text{para todo } n \geq 0;$$

por lo tanto, para $|z| < \rho$ se tiene que $\sum_{n\geq 0}\alpha_i^n z^n$ converge y así tenemos

$$\sum_{n\geq 0} u_n z^n = u(z) = \sum_{i=1}^k c_i \sum_{n\geq 0}\alpha_i^n z^n = \sum_{n\geq 0}\left(\sum_{i=1}^k c_i\alpha_i^n\right) z^n,$$

converge. Identificando coeficientes obtenemos

$$u_n = \sum_{i=1}^k c_i\alpha_i^n.$$

Q.E.D.

A la ecuación (1.5) la llamaremos **fórmula tipo Binet** de la sucesión linealmente recurrente. Cuando el orden de la sucesión $(u_n)_{n\geq 0}$ es $k = 2$

entonces la sucesión se llama **recurrente binaria**; en este caso, el polinomio característico es de la forma

$$f(X) = X^2 - a_1X - a_2 = (X - \alpha_1)(X - \alpha_2). \tag{1.6}$$

Un ejemplo de sucesión recurrente binaria es la de Fibonacci. Si en (1.6) suponemos que $\alpha_1 \neq \alpha_2$, la proposición 1.2.4 nos dice que

$$u_n = c_1\alpha_1^n + c_2\alpha_2^n \qquad \text{para todo } n \geq 0.$$

Ejemplo 1.2.5. *Tomemos el ejemplo 1.2.2. Como hemos visto su polinomio característico es*

$$f(x) = x^2 - x - 1 = (x - \alpha)(x - \beta),$$

donde $\alpha = (1 + \sqrt{5})/2$ *y* $\beta = (1 - \sqrt{5})/2$. *Como* $\alpha \neq \beta$ *entonces por la proposición 1.2.4 te tiene que existen* $c_1, c_2 \in \mathbb{Q}(\alpha, \beta)$ *tales que*

$$F_n = c_1\alpha^n + c_2\beta^n \qquad \textit{para todo } n \geq 0.$$

Para encontrar c_1 *y* c_2 *damos a* n *los valores de* 0 *y* 1 *y obtenemos el sistema*

$$\begin{aligned} 0 &= F_0 = c_1 + c_2, \\ 1 &= F_1 = c_1\alpha + c_2\beta. \end{aligned}$$

Resolviendo este sistema, tenemos que

$$c_1 = 1/\sqrt{5} \quad y \quad c_2 = -1/\sqrt{5}.$$

Como $\sqrt{5} = (\alpha - \beta)$ *entonces la fórmula de Binet de la sucesión de Fibonacci es*

$$F_n = \frac{\alpha^n - \beta^n}{\alpha - \beta}, \qquad \textit{para todo } n \geq 0. \tag{1.7}$$

Algunas de las propiedades que se satisfacen de la sucesión de Fibonacci y que usaremos más adelante son:

1) $(\alpha\beta)^n = (-1)^n$ y $|\beta| < 1 < |\alpha|$.

2) $\alpha^{n-2} \leq F_n \leq \alpha^{n-1}$ para todo $n \geq 1$.

La demostración del punto 1 es inmediata. La segunda parte puede demostrarse por inducción sobre n y usar el hecho que $(\alpha^{-2} + \alpha^{-1}) = 1$.

Se sabe que la sucesión de Fibonacci tiene una gran variedad de propiedades así como muchas aplicaciones en ciencias de la computación, matemáticas y teoría de juegos así como en configuraciones biológicas, como por ejemplo en la crianza de conejos, las ramas de los arboles, en la disposición de las hojas en el tallo y en la flora de la alcachofa por mencionar algunos. Otra sucesión muy relacionada a la sucesión de Fibonacci es la sucesión de números de Lucas, la cual satisface la siguiente propiedad.

Ejemplo 1.2.6. *La sucesión de números de Lucas $(L_n)_{n\geq 0}$ está dada por $L_0 = 2$, $L_1 = 1$ y $L_{n+2} = L_{n+1} + L_n$ para todo $n \geq 0$. Esta sucesión tiene el mismo polinomio característico que la sucesión de Fibonacci y por lo tanto existen dos constantes d_1 y d_2 tales que*

$$L_n = d_1\alpha^n + d_2\beta^n \qquad \text{para todo } n \geq 0.$$

Evaluando en $n = 0, 1$ y resolviendo el sistema obtenido se tiene que $d_1 = d_2 = 1$ y así

$$L_n = \alpha^n + \beta^n \qquad \text{para todo } n \geq 0.$$

Haciendo uso de las fórmulas de Binet de las sucesiones de Fibonacci y de los números de Lucas se puede obtener que $L_n^2 - 5F_n^2 = 4(-1)^n$.

Otra sucesión menos conocida y con propiedades matemáticas similares a la sucesión de Fibonacci es la sucesión de Narayana, la cual estudiamos a continuación.

1.3 Sucesión de Narayana.

La sucesión de Narayana fue introducida por el matemático hindú Narayana en el siglo XIV mientras estudiaba el siguiente problema de una manada de vacas y terneros: *Una vaca tiene anualmente una cría. Cada una de ellas, cuando ya es novilla a los cuatro años, también tiene una cría anual ¿Cuántas vacas habrá a los 20 años?* ([2]).

Este problema puede ser resuelto de la misma manera que el problema de Fibonacci acerca de conejos ([23]). Si r es el año entonces el problema de Narayana puede ser modelado por la recurrencia:

$$N_0 = 0; \quad N_1 = N_2 = 1 \quad \text{y} \quad N_{r+1} = N_r + N_{r-2} \quad \text{para } r \geq 2. \quad (1.8)$$

Los primeros términos son:

$$\{0, 1, 1, 1, 2, 3, 4, 6, 9, 13, 19, 28, 41, 60, \cdots\}$$

Esta sucesión es llamada **sucesión de Narayana**. Si el lector está interesado en saber mas sobre esta sucesión le recomendamos ver [33], [8] y [2]. Por otro lado, de acuerdo con la definición (1.2.1) se tiene que la sucesión de Narayana es de orden 3 y por lo tanto su polinomio característico es de grado 3, a saber,

$$f(x) = x^3 - x^2 - 1, \quad (1.9)$$

las raíces de este polinomio son,

$$\begin{aligned} \alpha &= \frac{1}{3}\left[1 + \left(\frac{29}{2} - \frac{3\sqrt{93}}{2}\right)^{1/3} + \left(\frac{29}{2} + \frac{3\sqrt{93}}{2}\right)^{1/3}\right] \quad \text{y} \\ \beta, \gamma &= \frac{1}{3} - \frac{1}{6}\left\{\left(1 \pm i\sqrt{3}\right)\sqrt[3]{\tfrac{29}{2} - \tfrac{3\sqrt{93}}{2}} - \left(1 \mp i\sqrt{3}\right)\sqrt[3]{\tfrac{29}{2} + \tfrac{3\sqrt{93}}{2}}\right\}. \end{aligned}$$

En las secciones 2.2 y 2.3 serán útiles algunas desigualdades donde se involucran las raíces de norma mayor. Dos de ellas están en la siguiente observación.

Observación 1.3.1. α, β y γ satisfacen:

- $1 < \alpha < 3/2$, $|\beta| = |\gamma| < 1$ y entonces $|\beta| = |\gamma| < \alpha^{1/2}$
- $\alpha^{r-2} \leq N_r \leq \alpha^{r-1}$, para todo $r \geq 1$.

El primer punto es directo calculando explícitamente las normas de α, β y γ. Para el punto dos procedamos por inducción sobre r. Notemos que del punto uno tenemos que $1/\alpha < 1 = N_1 \leq \alpha^0 = 1$, por lo tanto la desigualdad se cumple para $r = 1$. Supongamos entonces que la desigualdad es válida para $1 \leq k < r$ y demostremos que se cumple para $k = r$. Para esto primero observe que $(\alpha^{-1} + \alpha^{-3}) = 1$ pues

$$\frac{1}{\alpha} + \frac{1}{\alpha^3} = \frac{1}{\alpha^3}\left(\alpha^2 + 1\right) = \frac{1}{\alpha^3}\alpha^3 = 1,$$

donde hemos usado que $\alpha^3 = \alpha^2 + 1$. Por hipótesis de inducción se tiene que

$$\alpha^{r-3} \leq N_{r-1} \leq \alpha^{r-2} \qquad \text{y} \qquad \alpha^{r-5} \leq N_{r-3} \leq \alpha^{r-4}.$$

Sumando ambas desigualdades obtenemos

$$\alpha^{r-3} + \alpha^{r-5} \leq N_{r-1} + N_{r-3} \leq \alpha^{r-2} + \alpha^{r-4},$$

pero usando que $N_r = N_{r-1} + N_{r-3}$ y $\alpha^{-1} + \alpha^{-3} = 1$ obtenemos

$$\alpha^{r-2} \leq N_r \leq \alpha^{r-1},$$

que es lo que se quería demostrar.

Otra cosa importante es obtener la fórmula tipo Binet de la sucesión de Narayana, para ello podemos recurrir al trabajo de Ramírez, que en [33], usando el método descrito en [22], encontró dicha fórmula, la cual es,

$$N_r = a_1\alpha^r + a_2\beta^r + a_3\gamma^r,$$

donde

$$a_1 = \frac{\alpha}{(\alpha-\beta)(\alpha-\gamma)},\ a_2 = \frac{\beta}{(\beta-\alpha)(\beta-\gamma)} \text{ y } a_3 = \frac{\gamma}{(\gamma-\alpha)(\gamma-\beta)}.$$

Una manera alterna de obtener dicha fórmula es usando la proposición (1.2.4). Primero observe que el polinomio (1.9) pertenece a $\mathbb{Z}[x]$ y además que sus raíces son diferentes, por lo tanto existen $b_1, b_2, b_3 \in \mathbb{Q}(\alpha, \beta, \gamma)$ tales que

$$N_r = b_1\alpha^r + b_2\beta^r + b_3\gamma^r \qquad \text{para todo } r \geq 0.$$

Dándole a r los valores de $0, 1$ y 2 se tiene el siguiente sistema

$$\begin{aligned} 0 &= N_0 = b_1 + b_2 + b_3 \\ 1 &= N_1 = b_1\alpha + b_2\beta + b_3\gamma \\ 1 &= N_2 = b_1\alpha^2 + b_2\beta^2 + b_3\gamma^2. \end{aligned}$$

Resolviendo el sistema se tiene que $b_1 = a_1$, $b_2 = a_2$ y $b_3 = a_3$.

En nuestro trabajo, usaremos la fórmula,

$$N_r = C_\alpha\alpha^{r+2} + C_\beta\beta^{r+2} + C_\gamma\gamma^{r+2}, \tag{1.10}$$

donde $C_X = 1/(X^3+2)$. Esta notación para C_X se nos hace más fácil de escribir y usar en la práctica. Para obtener la ecuación (1.10) recordemos que

$$f(x) = x^3 - x^2 - 1 = (x-\alpha)(x-\beta)(x-\gamma).$$

Multiplicando la parte derecha se tiene

$$x^3 - x^2 - 1 = x^3 - x^2(\alpha+\beta+\gamma) + x(\beta\gamma+\alpha\gamma+\alpha\beta) - \alpha\beta\gamma.$$

Por lo tanto

$$\alpha+\beta+\gamma = 1, \quad \beta\gamma+\alpha\gamma+\alpha\beta = 0 \quad \text{y} \quad \alpha\beta\gamma = 1. \tag{1.11}$$

Por otro lado, multiplicando a_1 por α^{-2}, a_2 por β^{-2}, a_3 por γ^{-2} y usando las relaciones (1.11) se tiene que

$$C_\alpha = \frac{1}{\alpha^3+2}, \quad C_\beta = \frac{1}{\beta^3+2} \quad \text{y} \quad C_\gamma = \frac{1}{\gamma^3+2}. \tag{1.12}$$

1.4 Números algebraicos y trascendentes

En esta sección presentaremos definiciones y resultados de teoría algebraica de números. Iniciaremos con el concepto de número algebraico y continuaremos con el de polinomio mínimo para más adelante, presentar la definición de campo de números algebraicos. El lector interesado en profundizar en estos temas puede consultar [1], [32], [37] y [17].

Iniciemos recordando que, dados dos dominios enteros A y B con $A \subset B$, se dice que un elemento b de B es **entero** sobre A si satisface una ecuación de la forma

$$x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 = 0,$$

donde $a_0, a_1, \ldots, a_{n-1} \in A$. Observemos que cualquier elemento $a \in A$ es entero sobre A pues es raíz de $x - a \in A[x]$. Diremos que un número complejo z es un **entero algebraico** si z es entero sobre $\mathbb{Z}$. Si A es campo y $b \in B$ es entero sobre A entonces se dice que b es **algebraico** sobre A.

Un concepto importante es el de número algebraico, el cual presentamos a continuación.

Definición 1.4.1. Un número complejo que es algebraico sobre $\mathbb{Q}$ es llamado **número algebraico**. Un número que no es algebraico se llama trascendente o trascendental.

Ejemplo 1.4.2. *Todos los números racionales son algebraicos pues toda fracción de la forma a/b con $a, b \in \mathbb{Z}$ es solución de $bx - a = 0$.*

Ejemplo 1.4.3. *El irracional $\sqrt{2}$ es algebraico pues es solución de $x^2 - 2 = 0$.*

En los ejemplos de arriba se exhiben números algebraicos, la pregunta natural es, ¿hay números trascendentes?, la respuesta a esta pregunta es afirmativa. Primero recordemos que los números reales forman un conjunto no numerable (ver [3, Teorema 2.17]), como el conjunto de los números algebraicos es numerable (ver [31, Teorema 4.17]) se debe tener que el conjunto de los números trascendentes es no numerable y por lo tanto existen. Por otro lado, decidir si un número particular es o no trascendente es un problema más difícil. A continuación presentamos algunos ejemplos de números transcendentes.

Ejemplo 1.4.4. *Hermite*[1] *probó en* 1873 *que e es trascendente; la prueba se puede encontrar en [7] y en [19].*

Ejemplo 1.4.5. *Lindemann*[2] *demostró en* 1882 *que π es transcendente; la demostración se puede encontrar en [26].*

Definición 1.4.6. Sean K un subcampo de $\mathbb{C}$ y α un algebraico sobre K, se define el **polinomio mínimo** $p(x)$ **de** α **sobre** K, denotado $\mathrm{Irr}_K(\alpha)$, como el único polinomio mónico irreducible de grado mínimo tal que $p(\alpha) = 0$.

Los elementos que son algebraicos sobre K y tienen el mismo polinomio mínimo son llamados **conjugados sobre** K**.** El siguiente ejemplo nos será de gran utilidad en las secciones 2.2 y 2.3.

Ejemplo 1.4.7. *Sea α la raíz real del polinomio mónico*

$$f(x) = x^3 - x^2 - 1,$$

el cual es el polinomio característico de la sucesión de Narayana. Claramente se tiene que $\alpha \in \mathbb{C}$ y que es algebraico sobre $\mathbb{Q}$. Veamos que $f(x)$

[1] Charles Hermite (1822-1901) matemático Francés.
[2] Ferdinand von Lindemann (1852-1939) matemático Alemán.

es irreducible en $\mathbb{Q}[x]$. *Supongamos que es reducible. Note que* $f(x)$ *no tiene factores lineales pues si los tuviera, como* $\deg(f(x)) = 3$ *entonces existiría* $c = r/s \in \mathbb{Q}$ *tal que* $f(c) = 0$ *y usando el criterio de la raíz racional se tendría que* $c = \pm 1$ *pero* $f(\pm 1) \neq 0$. *Por lo tanto,* $f(x)$ *es irreducible en* $\mathbb{Q}[x]$ *y en consecuencia* $f(x)$ *es el polinomio mínimo de* α *sobre* $\mathbb{Q}$, *i.e.,* $Irr_{\mathbb{Q}}(\alpha) = f(x)$.

Considere el polinomio mínimo

$$x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0,$$

de un número algebraico α sobre $\mathbb{Q}$, entonces multiplicando por el mínimo común múltiplo de los denominadores de los coeficientes a_i, $i = 0, \ldots, a_{n-1}$, obtenemos un único polinomio P con $P(\alpha) = 0$ que tiene la forma

$$P(x) = b_n x^n + b_{n-1}x^{n-1} + \cdots + b_1 x + b_0,$$

donde los coeficientes b_i, $i = 0, \ldots, n$, son enteros primos relativos y $b_n > 0$. Llamaremos a $P(x)$ el **polinomio mínimo de** α **sobre** $\mathbb{Z}$**.** Note que el polinomio mínimo de α del ejemplo 1.4.7 sobre $\mathbb{Z}$ en este caso coincide con $f(x)$.

Definición 1.4.8. Sean K un subcampo de $\mathbb{C}$ y $\alpha \in \mathbb{C}$ algebraico sobre K. El **grado de** α **sobre** K, denotado por $\deg_K(\alpha)$, está dado por

$$\deg_K(\alpha) = \deg(\mathrm{Irr}_K(\alpha)).$$

Recordemos que si F y K son campos, entonces todo morfismo de campos $\varphi : F \to K$ (por definición $\varphi(1) = 1$) es inyectivo ya que $\ker \varphi \subset F$ y como F es campo sus únicos ideales son el 0 y el total, y como $\varphi(1) = 1 \neq 0$ entonces $\ker \varphi = 0$.

Definición 1.4.9. Una **extensión de campos** es un monomorfismo de campos $\varphi : F \to K$.

Observe que como $\varphi : F \to \varphi(F) \subset K$ es un isomorfismo de campos, entonces dentro de K se encuentra una copia de F, a saber, $\varphi(F) \subset K$.

Definición 1.4.10. Si K y F son campos tal que $F \subset K$ y las operaciones $(+, \cdot)$ de F son las mismas que las de K, entonces diremos que F es un **subcampo** de K o que K es una **extensión** de F y lo denotaremos por $F \leq K$ o K/F.

Se puede mostrar que si f es un polinomio irreducible sobre el campo F, entonces existe una extensión K del campo F y $\alpha \in K$ tal que

$$f(\alpha) = 0.$$

Por lo tanto, la extensión del campo inicial F se puede obtener del campo F adjuntando una raíz α de un polinomio no constante f sobre el campo F; en este caso el mínimo campo conteniendo a α y F es denotado por $F(\alpha)$. Al campo $F(\alpha)$ se le llama **extensión algebraica simple de F.** El siguiente resultado clásico nos dice como es una extensión algebraica simple.

Teorema 1.4.11. *Sean K un subcampo de $\mathbb{C}$, $\alpha \in \mathbb{C}$ algebraico sobre K y $n = \deg Irr_K(\alpha)$. Se tiene que*

$$K(\alpha) = \left\{ a_0 + b_1\alpha + \cdots + b_{n-1}\alpha^{n-1} | a_i \in K \right\}.$$

El teorema 1.4.11 muestra que $K(\alpha)$ puede ser visto como un espacio vectorial n-dimensional sobre K con base $\{1, \alpha, \ldots, \alpha^{n-1}\}$; esto motiva a la siguiente definición.

Definición 1.4.12. Sean K un subcampo de $\mathbb{C}$ y $\alpha \in \mathbb{C}$ algebraico sobre K de grado n (i.e. $n = \deg_K(\alpha)$). **El grado de la extensión $K(\alpha)$ sobre K**, denotado $[K(\alpha) : K]$, es definido por

$$[K(\alpha) : K] := n.$$

El hecho de tomar un algebraico $\alpha \in \mathbb{C}$ sobre K y considerar el campo $K(\alpha)$ se puede generalizar para una cantidad finita de elementos (no necesariamente algebraicos), es decir, si consideramos K un subcampo de $\mathbb{C}$ y $\alpha_1, \ldots, \alpha_k \in \mathbb{C}$, se define $K(\alpha_1, \ldots, \alpha_k)$ como el menor subcampo de $\mathbb{C}$ que contiene tanto a K como a los $\alpha_1, \ldots, \alpha_k$. Al campo $K(\alpha_1, \ldots, \alpha_k)$ se le llama **extensión múltiple de** K si $k \geq 2$. El siguiente resultado presenta un hecho importante cuando $\alpha_1, \ldots, \alpha_k \in \mathbb{C}$ son algebraicos sobre K. La demostración no la presentamos para no desviarnos del objetivo de este trabajo. Si el lector está interesado en la demostración de este resulado puede consultar [1].

Teorema 1.4.13. *[Teorema del elemento primitivo] Sean K un subcampo de $\mathbb{C}$ y $\alpha_1, \ldots, \alpha_k \in \mathbb{C}$ algebraicos sobre K. Existe entonces $\alpha \in \mathbb{C}$ algebraico sobre K tal que*

$$K(\alpha_1, \ldots, \alpha_k) = K(\alpha).$$

Observe que el teorema nos está diciendo que toda extensión múltiple es simple. A continuación presentamos el concepto más importante de esta sección.

Definición 1.4.14. Un **campo de números algebraicos** es un subcampo de $\mathbb{C}$ de la forma $\mathbb{Q}(\alpha_1, \ldots, \alpha_k)$, donde $\alpha_1, \ldots, \alpha_k$ son números algebraicos.

Una consecuencia directa del teorema 1.4.13 es que si $\mathbb{L}$ es un campo de números algebraicos entonces existe un número algebraico α tal que $\mathbb{L} = \mathbb{Q}(\alpha)$, por lo tanto $[\mathbb{L} : \mathbb{Q}]$ es el grado de α sobre $\mathbb{Q}$.

1.5 Formas lineales en logaritmos

El objetivo de esta sección es presentar un teorema que juega un papel muy importante en nuestro trabajo. Antes de eso daremos una motivación de como surgió dicho teorema, así como nociones básicas sobre formas lineales en logaritmos. Si el lector está interesado en saber más sobre los temas puede consultar [14], [37] y [36].

Recuerde que dados $\alpha_1, \ldots, \alpha_n$ números reales (o complejos), se dice que $\alpha_1, \ldots, \alpha_n$ son **linealmente dependientes** sobre los racionales (equivalentemente enteros) si existen números racionales (números enteros) $r_1, \ldots, r_n$ no todos ceros tales que

$$r_1\alpha_1 + r_2\alpha_2 + \cdots + r_n\alpha_n = 0.$$

Si $\alpha_1, \ldots, \alpha_n$ no son linealmente dependientes sobre los racionales (enteros), decimos que son **linealmente independientes** sobre los racionales (enteros).

Los problemas del matemático alemán D. Hilbert forman una lista de veintitrés problemas en matemáticas recopilados, propuestos y publicados en 1900. El séptimo problema de Hilbert, titulado "irrationality and transcendence of certain numbers", se trata de la trascendencia del número α^β para $\alpha \neq 0, 1$ y β algebraico irracional. Concretamente presentó el siguiente problema (ahora teorema).

Teorema 1.5.1. *Sean $\alpha, \beta \in \mathbb{A}$. Si $\alpha \neq 1, 0$ y $\beta \notin \mathbb{Q}$ entonces α^β es trascendente.*

Éste teorema fue demostrado de manera independiente por Gelfond[3] y Schneider[4] en 1935. Ellos probaron el siguiente resultado más general.

Teorema 1.5.2. *Sean* α_1, $\alpha_2 \in \mathbb{A}$. *Si* α, β *son no nulos tales que* $\log\alpha$ *y* $\log\beta$ *son linealmente independientes sobre* $\mathbb{Q}$ *entonces* $\log\alpha$ *y* $\log\beta$ *son linealmente independientes sobre* $\mathbb{A}$.

Para ver que el teorema 1.5.2 implica el teorema 1.5.1, supongamos que α^β es algebraico y mostremos que $\alpha = 0$ o $\alpha = 1$ o $\beta \in \mathbb{Q}$. Primero, si $\alpha = 0$ o $\alpha = 1$ no hay nada que hacer. Si $\alpha \neq 0, 1$ entonces debemos ver que $\beta \in \mathbb{Q}$. Supongamos que $\beta \neq 0$, si no $\beta \in \mathbb{Q}$. Observe que $\log\alpha^\beta$ y $\log\alpha$ son linealmente dependientes sobre $\mathbb{A}$ entonces por teorema 1.5.2 se tiene que $\log\alpha^\beta$ y $\log\alpha$ son linealmente dependientes sobre $\mathbb{Q}$, es decir, existen $x, y \in \mathbb{Q}$ no ceros tales que

$$x\log\alpha^\beta + y\log\alpha = 0.$$

Esto último implica que $x\beta + y = 0$ y por lo tanto $\beta = \frac{-y}{x} \in \mathbb{Q}$ que es lo que queriamos. Posterior al resultado de Gelfond y Schneider se conjeturó que se podía obtener un teorema análogo para una suma de más logaritmos de números algebraicos. Esta conjetura fue probada por A. Baker[5] en 1966, él probó el siguiente teorema del cual no presentamos su demostración pero si el lector está interesado en ver una prueba puede consultar [4] ó [5].

Teorema 1.5.3. *Sean* $\alpha_1, \ldots, \alpha_n$ *números algebraicos diferentes de cero tales que* $\log\alpha_1, \ldots \log\alpha_n$ *son linealmente independientes sobre los racionales, entonces* $1, \log\alpha_1, \ldots, \log\alpha_n$ *son linealmente independientes sobre el campo de los números algebraicos.*

A una expresión de la forma

$$\beta_0 + \beta_1\log\alpha_1 + \cdots + \beta_n\log\alpha_n$$

donde $\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_n$ son números algebraicos diferentes de cero y β_0 es algebraico se le llama **forma lineal en logaritmos**. El teorema 1.5.3 muestra que cualquier forma lineal en logaritmos toma el valor cero sólo en caso trivial.

[3]Alexander Osipovich Gelfond (1906-1968), matemático Ruso.
[4]Theodor Schneider (1911-1988), matemático Alemán.
[5]Alan Baker (1939-2018), matemático Ingles.

Una pregunta natural es: ¿Podemos acotar inferiormente el valor absoluto de dicha expresión por un valor positivo?. Respondamos a esta pregunta para cuando los algebraicos involucrados son todos racionales. Para cada $j = 1, \ldots, n$, sean x_j/y_j números racionales diferentes de cero, b_j enteros no ceros y definamos

$$B := \max\{|b_1|, \ldots, |b_n|\} \quad \text{y} \quad A_j := \max\{2, |x_j|, |y_j|\}.$$

Consideremos el número racional

$$\Lambda := \left(\frac{x_1}{y_1}\right)^{b_1} \cdots \left(\frac{x_n}{y_n}\right)^{b_n} - 1. \tag{1.13}$$

Como la hipótesis del teorema 1.5.3 dice que los logaritmos de los números racionales son linealmente independientes sobre $\mathbb{Q}$ no es difícil mostrar que Λ es diferente de cero y por lo tanto una cota inferior

$$\begin{aligned}
\log|\Lambda| &= \log\left|\left(\frac{x_1}{y_1}\right)^{b_1} \cdots \left(\frac{x_n}{y_n}\right)^{b_n} - 1\right| = \log\left|\frac{x_1^{b_1}\cdots x_n^{b_n} - y_1^{b_n}\cdots y_n^{b_n}}{y_1^{b_n}\cdots y_n^{b_n}}\right| \\
&= \log|x_1^{b_1}\cdots x_n^{b_n} - y_1^{b_n}\cdots y_n^{b_n}| - \log|y_1^{b_n}\cdots y_n^{b_n}| \\
&\geq -\log|y_1^{b_n}\cdots y_n^{b_n}| = -\sum_{i=1}^{n} b_i \log|y_i| \geq -B\sum_{i=1}^{n}\log A_i.
\end{aligned}$$

Observe que la dependencia de las A_i's es muy satisfactoria a diferencia de la dependencia de B. Sin embargo, para resolver muchos problemas diofánticos necesitamos una mejor dependencia de B, incluso si la dependencia de las A_i's no es la mejor posible. El primero en establecer tal resultado fue A. Baker en 1966 en sus artículos "Linear forms in logarithms of algebraic numbers I, II, III" (ver [4], [5] y [6]) y gracias a este trabajo ganó la medalla Fields en 1970. Después de que Baker presentó dicho resultado muchos matemáticos trabajaron en refinarlo pero no fue hasta el 2000 que Matveev en [29] probó, bajo las hipótesis anteriores (que los algebraicos son racionales), que

$$\log|\Lambda| \geq -30^{n+4}(n+1)^6(\log A_1)\cdots\log(A_n)(\log B).$$

De manera general, Matveev presentó cotas inferiores análogas cuando se sustituyen los x_i/y_i por números algebraicos α_i deferentes de cero y los números reales A_i se expresan en términos de la altura logarítmica de α_i. Dicho resultado es el teorema 1.5.9 y lo presentamos al final de esta sección, para poder hacer esto se necesitan algunos conceptos básicos que presentaremos a continuación.

Definición 1.5.4. Sea α un número algebraico de grado d con polinomio mínimo sobre los enteros dado por

$$p(x) = a_0x^d + a_1x^{d-1} + \cdots + a_{d-1}x + a_d = a_0\prod_{i=1}^{d}(x - \alpha^{(i)}),$$

donde el coeficiente líder a_0 es positivo y los $\alpha^{(i)}$'s son los conjugados de α. Se define la **altura logarítmica de** α mediante

$$h(\alpha) := \frac{1}{d}\left(\log|a_0| + \sum_{i=1}^{d}\log\max\{|\alpha^{(i)}|, 1\}\right).$$

En las aplicaciones que presentamos en el capítulo 2 usaremos los siguientes ejemplos.

Ejemplo 1.5.5. *Sea* $\eta = \frac{p}{q} \in \mathbb{Q}$ *con* $q > 0$ *tal que* $(p, q) = 1$, *entonces* $h(\eta) = \log max\{|p|, q\}$.

En efecto, observe que el polinomio mínimo de η *sobre* $\mathbb{Q}$ *y el polinomio mínimo de* η *sobre* $\mathbb{Z}$ *son*

$$f(x) = x - p/q \qquad y \qquad p(x) = qx - p,$$

respectivamente, por lo tanto

$$h(\eta) = \log q + \log max\{|p/q|, 1\}.$$

Si $|p/q| < 1$ *entonces* $|p| < |q| = q$ *y así* $h(\eta) = \log q + 0 = \log q$. *En caso contrario, si* $|p/q| > 1$ *entonces* $|p| > q$ *y así*

$$h(\eta) = \log q + \log(|p/q|) = \log|p|,$$

por tanto, $h(\eta) = max\{|p|, q\}$.

Ejemplo 1.5.6. *Sea* α *como en el ejemplo 1.4.7. Anteriormente se vió que el polinomio mínimo de* α *sobre* $\mathbb{Z}$ *es*

$$f(x) = x^3 - x^2 - 1$$

y que sus conjugados son β *y* γ. *Además, de la observación 1.3.1 se tiene que* $|\beta| = |\gamma| < 1$, *por lo tanto,* $h(\alpha) = \log\alpha/3$.

Ejemplo 1.5.7. *Sea C_α como en* (1.12)*. Haciendo uso de Mathematica se puede ver que el polinomio mínimo de C_α sobre $\mathbb{Z}$ es*

$$g(x) = 31x^3 - 31x^2 + 10x - 1$$

y además que todas las raíces de $g(x)$ tienen norma menor a 1; así que $h(C_\alpha) = \log 31/3$.

La altura de un elemento algebraico es muy importante pero muchas veces no es fácil encontrar el polinomio mínimo sobre los enteros de dicho elemento. Sin embargo, en la práctica no es necesario tenerlo, pues lo que interesa es la altura del elemento, así que basta con dar una cota superior de la altura. Una forma de hacerlo es usando el polinomio de campo del elemento (ver apéndice A).

Presentamos la forma de llevar a cabo ésto para el elemento C_α. Considere el campo de números algebraicos $\mathbb{L} = \mathbb{Q}(\alpha)$ entonces $[\mathbb{L} : \mathbb{Q}] = 3$ y $C_\alpha \in \mathbb{L}$. De los teoremas A.1.2 y A.1.6 se tiene que los $\mathbb{L}$-conjugados de C_α son 3, a saber C_α, C_β y C_γ. Sea $g(x)$ el polinomio de campo de C_α sobre $\mathbb{L}$, es decir,

$$\begin{aligned} g(x) &= (x - C_\alpha)(x - C_\beta)(x - C_\gamma) \\ &= \left(x - \frac{1}{\alpha^3 + 2}\right)\left(x - \frac{1}{\beta^3 + 2}\right)\left(x - \frac{1}{\gamma^3 + 2}\right). \end{aligned}$$

Por teorema A.1.8 se tiene que $g(x) \in \mathbb{Q}[x]$. Como α, β y γ son enteros algebraicos entonces los elementos

$$(\alpha^3 + 2), \quad (\beta^3 + 2), \quad (\gamma^3 + 2)$$

son algebraicos, de hecho cualquier producto de ellos también lo es. Luego, multiplicando $g(x)$ por el entero algebraico

$$\eta := (\alpha^3 + 2)(\beta^3 + 2)(\gamma^3 + 2)$$

se tiene que $h(x) := \eta g(x) \in \mathbb{Q}[x]$. Más aún, tenemos que los coeficientes de $h(x)$ son enteros algebraicos, por lo tanto $h(x) \in \mathbb{Z}[x]$. En consecuencia, el coeficiente líder a_0 del polinomio mínimo de C_α sobre $\mathbb{Z}$ divide a

$$(\alpha^3 + 2)(\beta^3 + 2)(\gamma^3 + 2).$$

Por otro lado, por teorema A.1.9 se tiene que $\mathrm{Irr}_{\mathbb{Q}}(C_\alpha)|g(x)$ entonces $\deg Irr_{\mathbb{Q}}(C_\alpha) = 1$ ó 3, pero como $C_\alpha \notin \mathbb{Q}$ se sigue que

$$\deg Irr_{\mathbb{Q}}(C_\alpha) = 3.$$

Por lo tanto, las raíces de $\mathrm{Irr}_{\mathbb{Q}}(C_\alpha)$ son las mismas raíces de $g(x)$. Tenemos así

$$\begin{aligned} h(C_\alpha) &= \frac{1}{3}\left(\log a_0 + \sum_{i=1}^{3} \log \max\{|C_{\alpha_i}|, 1\}\right) \\ &\leq \frac{1}{3}\left(\log\left(\left(\alpha^3+2\right)\right)\left(\beta^3+2\right)\left(\gamma^3+2\right)\right). \end{aligned}$$

A continuación presentamos, sin demostración, algunas propiedades sobre la altura logarítmica de números algebraicos.

Proposición 1.5.8. *Sean α y β números algebraicos. Las siguientes propiedades se satisfacen:*

- $h(\alpha \pm \beta) \leq h(\alpha) + h(\beta) + \log 2$,
- $h(\alpha\beta^{\pm 1}) \leq h(\alpha) + h(\beta)$,
- $h(\alpha^s) = |s|h(\alpha), \qquad s \in \mathbb{Z}$.

Con la proposición 1.5.8 se tiene,

$$\begin{aligned} h(C_\alpha) &= h\left(\frac{1}{\alpha^3+2}\right) \leq h(1) + h(\alpha^3+2) = h(\alpha^3+2) \\ &= h(\alpha^3) + h(2) + \log 2 = h(\alpha^3) + \log 2 + \log 2 \\ &= 3h(\alpha) + 2\log 2 \underset{Ejem.(1.5.6)}{=} \log\alpha + 2\log 2. \end{aligned}$$

El siguiente teorema se debe a Matveev ([30]) y es la consecuencia de varios años de trabajo en los que se había intentado mejorar la cota que presentó Baker en 1966 en sus trabajos [4], [5] y [6]. Es importante recalcar que el objetivo de nuestro trabajo es explicar como aplicar el teorema de Matveev para resolver algunos problemas diofánticos, es por ello, que dicho resultado es clave para nosotros. Sin embargo, a pesar que el teorema de Matveev es el más importante en nuestro trabajo, no daremos la demostración porque el desarrollo de la misma no tiene aporte en el

método que presentamos en la tesis, pues usa resultados de otras áreas además de ser notablemente extensa con más de 50 páginas.

Antes de enunciar el teorema sentaremos la notación usada para este. Sea $\mathbb{L}$ un campo de números algebraicos de grado D. Sean $\gamma_1, \ldots, \gamma_n$ elementos no nulos de $\mathbb{L}$ y $b_1, \ldots, b_n$ enteros. Definimos

$$B := \max\{|b_1|, \ldots, |b_n|\} \qquad \text{y} \qquad \Lambda := \prod_{i=1}^{n} \gamma_i^{b_i} - 1.$$

Sean $A_1, \ldots, A_n$ enteros positivos tales que

$$A_j \geq h'(\gamma_j) := \max\{Dh(\gamma_j), |\log \alpha_j|, 0.16\} \qquad j = 1, \ldots, n. \quad (1.14)$$

Teorema 1.5.9. *(**Matveev**,2000)*
Si $\Lambda \neq 0$ *y* $\mathbb{L} \subset \mathbb{R}$ *entonces*

$$\log|\Lambda| > (-1.4)30^{n+3}n^{4.5}D^2(1+\log D)(1+\log B)A_1A_2\cdots A_n.$$

Por último, presentamos un lema que nos permite encontrar una cota absoluta para x cuando tenemos una cota de la forma $x < T\log x$ con $T > 3$. Esto nos servirá en las aplicaciones que presentamos en el capítulo 2.

Lema 1.5.10. *Si* $T \geq 3$ *y* $\frac{x}{\log x} < T$ *entonces* $x < 2T\log T$.

Demostración. Procedamos por contradicción, supongamos que

$$x \geq 2T\log T,$$

entonces $x > e$ pues $T > e$ y así $2T\log T > 6 > e$. Como $x \mapsto x/\log x$ es creciente para todo $x > e$ tenemos que

$$\frac{x}{\log x} \geq \frac{2T\log T}{\log(2T\log T)},$$

pero esto implica que $2\log T > T$, lo cual es una contradicción para $T \geq 3$. **Q.E.D.**

Capítulo 2 Aplicación

2.1 Introducción

Recordemos que una ecuación diofántica es una ecuación algebraica en dos o mas variables en donde las soluciones sólo son enteras, es decir, las incógnitas toman valores enteros. Una ecuación diofántica lineal es una suma de dos o mas monomios donde cada uno de ellos tiene grado uno en las variables. Un ejemplo de ecuación diofántica es

$$3x + 2y = 1.$$

Una ecuación diofántica exponencial es la que tiene las variables en los exponentes. Un ejemplo de ecuación diofántica exponencial es

$$3^m + 2^n = 5^k.$$

En este capítulo se explicará como usar las herramientas del capítulo 1 para resolver algunas ecuaciones diofánticas del tipo exponencial. Las herramientas son básicamente dos resultados, el primero tiene que ver con una cota inferior de una forma lineal en logaritmos y se debe a Matveev, el segundo es el lema de Dujella y Pethő que lo usamos como un método de reducción de cota sobre alguna variable.

Tratamos aquí algunas ecuaciones diofánticas exponenciales porque al tomar logaritmos de dicha ecuación, en muchos casos, se puede llevar a una forma lineal en logaritmos, la cual podemos resolver usando la teoría en formas lineales en logaritmos. Muchas ecuaciones que involucran sucesiones linealemente recurrentes resultan ser de este tipo al usar su fórmula de Binet.

La siguiente definición es muy útil para poder referirnos a una de las variables con cierta característica.

Definición 2.1.1. Sean $k \in \mathbb{Z}$ y $f(x_1, \ldots, x_n) = 0$ una ecuación diofántica. Diremos que x_j con $1 \leq j \leq n$ es **variable dominante** si para cualesquiera $a_1, \ldots, a_n \in \mathbb{Z}_{\geq k}$ tales que

$$f(a_1, \ldots, a_n) = 0$$

se tiene que $a_j \geq a_i$ para $i = 1, \ldots, n$.

Un ejemplo donde existe una variable dominante es el siguiente.

Ejemplo 2.1.2. *Consideremos la ecuación diofántica*

$$2^m - 3^n = 1,$$

las variables son m y n. La variable dominante en este caso es m. Para ver ésto, observe que si $a, b \geq 1$ satisfacen que $2^a - 3^b = 1$ entonces $2^a > 3^b$, tomando logaritmos tenemos que

$$a > b\frac{\log 3}{\log 2} > b.$$

En la práctica resulta complicado determinar si cierta ecuación tiene o no variable dominante. La pregunta natural es: ¿existen ecuaciones diofánticas que no tengan variables dominantes?. La respuesta es sí y lo mostramos en el siguiente ejemplo.

Ejemplo 2.1.3. *Consideremos la ecuación diofántica*

$$F_n + 4F_m = 2F_k + 3F_l. \tag{2.1}$$

Las variables son n, m, k y l. Para ver que la ecuación (2.1) no tiene variables dominantes, basta con exhibir cuádruplas que sean soluciones y que en al menos una de ellas, las variables no son las mayores. En efecto, representemos por (a_1, a_2, a_3, a_4) las soluciones de la ecuación (2.1). Presentamos por casos las cuádruplas que verifican que cada una de las variables no es variable dominante. Para $a \in \mathbb{N}$,

***Caso 1**: La cuádrupla $(a, a+3, a+2, a+3)$ es solución de (2.1) pues*

$$F_a + 4F_{a+3} = 3F_{a+3} + F_a + F_{a+2} + F_{a+1} = 2F_{a+2} + 3F_{a+3},$$

pero n no es variable dominante puesto que $a_1 < a_j$ para $j = 2, 3, 4$.

***Caso 2**: Observe que $(a+3, a, a+2, a)$ también es solución de la ecuación (2.1) ya que*

$$F_{a+3} + 4F_a = F_{a+2} + F_{a+1} + F_a + 3F_a = 2F_{a+2} + F_a.$$

Sin embargo, las variables m y l no son dominantes debido a que tanto a_2 como a_4 son menores que a_1 y a_3.

***Caso 3**: Finalmente para verificar que la variable k no es dominante, consideremos la cuádrupla $(a+3, a+2, a, a+3)$, la cual es solución de (2.1) pues*

$$2F_a + 3F_{a+3} = 2F_a + F_{a+3} + 2F_{a+2} + 2F_{a+1} = F_{a+3} + 4F_{a+2}.$$

Además, es claro que $a_3 < a_j$ para $j = 1, 2, 4$.

Es importante mencionar que la cota inferior, que proporciona el teorema de Matveev, está en función de la variable dominante de nuestro problema diofántico. El método que usamos se describe a continuación.

1.- Acotar las variables en función de una de ellas si es posible, es decir, determinar la existencia de una variable dominante.

2.- Llevar nuestra ecuación diofántica a una forma lineal en logaritmos y después acortarla superiormente por una función del tipo exponencial del negativo de la variable dominante.

3.- Aplicar el teorema de Matveev para tener una cota inferior de nuestra forma lineal en función de la variable dominante.

4.- Comparar las cotas de los pasos 2 y 3 para obtener una cota superior numérica de la variable dominante y por lo tanto de todas las variables de nuestro problema.

En la práctica, muchas veces, la cota numérica de las variables son altas y lo que hacemos es aplicar el siguiente paso.

5.- Aplicar el método de reducción de cota (lema 1.1.18).

6.- Con la nueva cota numérica obtenida en el paso 5, encontrar las soluciones de nuestro problema diofántico.

Veamos con un par de ejemplos como llevar a cabo este método.

2.2 Números de Narayana como potencia de 2

Sea $k \geq 2$ un entero. Consideremos una generalización de la sucesión de Fibonacci llamada sucesión k-generalizada de Fibonacci $F_n^{(k)}$ definida como

$$F_n^{(k)} = F_{n-1}^{(k)} + F_{n-2}^{(k)} + \cdots + F_{n-k}^{(k)} \qquad \text{para todo } n \geq 2, \tag{2.2}$$

con condiciones iniciales

$$F_{-(k-2)}^{(k)} = F_{-(k-3)}^{(k)} = \cdots = F_{-1}^{(k)} = F_0^{(k)} = 0, \quad \text{y} \quad F_1^{(k)} = 1. \tag{2.3}$$

Luca y Bravo en [10] consideraron la ecuación diofántica

$$F_n^{(k)} = 2^m \qquad m \geq 0. \tag{2.4}$$

Ellos demostraron que la única solución no trivial de (2.4) es

$$(n, k, m) = (6, 2, 3).$$

En este ejemplo trabajaremos el mismo problema con la sucesión de Narayana $(N_r)_{r\geq 0}$ expuesta en la sección 1.3. Recordemos que tal sucesión está dada por $N_0 = 0$, $N_1 = N_2 = 1$,

$$N_{r+1} = N_r + N_{r-2} \quad \text{para todo } r \geq 0.$$

Los primeros términos de la sucesión (1.8) son

$$0, 1, 1, 1, 2, 3, 4, 6, 9, 13, 19, 28, 41, 60, \cdots .$$

Nosotros estamos interesados en saber para qué enteros positivos (r, m) se satisface que $N_r = 2^m$. Tenemos el siguiente resultado.

Teorema 2.2.1. *Los únicos pares de enteros positivos (r, m) con $r \geq 4$ que satisfacen*

$$N_r = 2^m$$

son $(4, 1)$ y $(6, 2)$.

Demostraremos el teorema 2.2.1 llevando a cabo los pasos descritos al final de la sección anterior.

Paso 1: Lo primero que haremos es identificar cuál es la variable dominante entre r y m en caso de que alguna lo sea. Para esto primero observe que para $r = 1, 2$ y 3 tenemos

$$N_1 = N_2 = N_3 = 2^0,$$

así que consideraremos estos casos las soluciones triviales. Supongamos entonces que $r \geq 4$. Como $\alpha^{r-2} \leq N_r \leq \alpha^{r-1}$ y $N_r = 2^m$ entonces

$$\alpha^{r-2} \leq 2^m \leq \alpha^{r-1}.$$

Tomando logaritmos de la segunda desigualdad tenemos

$$m \leq (r-1)\frac{\log \alpha}{\log 2}.$$

Recuerde que $1 < \alpha < 3/2$ y así $\log \alpha / \log 2 < 1$ entonces

$$m + 1 < r. \tag{2.5}$$

Hemos concluido nuestro primer objetivo que era identificar la variable dominante, en este caso es r.

Paso 2: De (1.10) se tiene

$$|N_r - C_\alpha \alpha^{r+2}| = |C_\beta \beta^{r+2} + C_\gamma \gamma^{r+2}| \leq |C_\beta \beta^{r+2}| + |C_\gamma \gamma^{r+2}|.$$

Como $|\gamma| = |\beta|$ entonces de (1.12) se tiene $|C_\gamma| = |C_\beta|$ y además se cumple que

$$|C_\beta \beta^{r+2}| \leq |C_\beta \beta^3| < 1/4 \quad \text{para } r \geq 1,$$

entonces

$$|N_r - C_\alpha \alpha^{r+2}| < 1/2 \qquad \forall r \geq 1. \tag{2.6}$$

La ecuación (2.6) nos dice que la contribución de las raíces complejas β y γ es muy pequeña. Como $N_r = 2^m$, de (2.6) tenemos

$$|2^m - C_\alpha \alpha^{r+2}| < \frac{1}{2},$$

dividiendo entre $C_\alpha \alpha^{r+2}$ y tomando en cuenta que

$$(2 \cdot C_\alpha \cdot \alpha^{r+2})^{-1} < (2 \cdot C_\alpha \cdot \alpha)^{-1} < 18/10$$

se tiene

$$|2^m \alpha^{-(r+2)} C_\alpha^{-1} - 1| < \frac{18}{10} \alpha^{-(r+1)}. \tag{2.7}$$

Aquí nuestra forma lineal en logaritmos es

$$2^m \alpha^{-(r+2)} C_\alpha^{-1} - 1$$

y la cota superior, que es función del tipo exponencial del negativo de r, es $\frac{18}{10}\alpha^{-(r+1)}$.

Paso 3: En este paso lo que haremos es aplicar el teorema de Matveev 1.5.9 a nuestra forma lineal

$$2^m \alpha^{-(r+2)} C_\alpha^{-1} - 1.$$

Para esto, tomemos $\mathbb{L} := \mathbb{Q}(\alpha)$, $\gamma_1 = 2$, $\gamma_2 = \alpha$, $\gamma = C_\alpha$, $b_1 = m$, $b_2 = -(r+2)$ y $b_3 = -1$, se tiene entonces que $D := [\mathbb{L} : \mathbb{Q}] = 3$ y $B := r + 2$.
Sea $\Lambda = 2^m \alpha^{-(r+2)} C_\alpha^{-1} - 1$. Para aplicar el teorema de 1.5.9 es necesario demostrar que $\Lambda \neq 0$. Para ello, procedamos por contradicción, supongamos que $\Lambda = 0$ se tiene

$$2^m = \alpha^{r+2} C_\alpha.$$

Pero si $\Lambda = 0$ en $\mathbb{L}$ entonces $\Lambda = 0$ en $\mathbb{L}(\beta)$. Luego, usando el monomorfismo $\sigma : \mathbb{L}(\beta) \to \mathbb{C}$ que asigna $\sigma(\alpha) = \beta$ se tiene que

$$2^m = \beta^{r+2} C_\beta.$$

Tomando normas de ambos lados de la igualdad anterior tenemos en particular

$$2 < 2^m = \left|\beta^{r+2}\right| |C_\beta| < \frac{1}{2},$$

lo cual es una contradicción; por lo tanto $\Lambda \neq 0$ en $\mathbb{L}(\beta)$ y así lo es en $\mathbb{L}$. Otra cosa más que necesitamos para aplicar el teorema 1.5.9 es calcular

los A_j de (1.14). Para esto, de los ejemplos 1.5.6, 1.5.7 y 1.5.5 tenemos que

$$\begin{aligned} h(\gamma_1) &= h(2) = \frac{\log 2}{2} \quad \Rightarrow \quad A_1 := \frac{3\log 2}{2} \\ h(\gamma_2) &= h(\alpha) = \frac{\log \alpha}{3} \quad \Rightarrow \quad A_2 := \log \alpha \\ h(\gamma_3) &= h(C_\alpha) = \frac{1}{3}\log 31 \quad \Rightarrow \quad A_3 := \log 31 \end{aligned}$$

Con todo lo anterior, aplicando el Teorema 1.5.9 tenemos

$$\log |\Lambda| > -t \cdot (1 + \log(r+2)), \tag{2.8}$$

donde

$$\begin{aligned} t &= 1.4 \cdot 30^6 \cdot 3^{4.5} \cdot 3^2(1+\log 3) \cdot 3 \cdot \log 2 \cdot 2 \cdot \log \alpha \cdot 2 \cdot \log 31 \\ &\approx 1.62769 \times 10^{15} < 1.7 \times 10^{15}. \end{aligned}$$

Hemos terminado el paso tres, el cuál era aplicar el teorema de Matvevv.

Paso 4**:** Comparando (2.5) y (2.8) tenemos

$$(r+1)\log \alpha + \log 10 - \log 18 < 3.2 \times 10^{14}(1 + \log(r+2))$$

lo cual implica que

$$r < 4.44741 \times 10^{15} \log r.$$

Luego, usando el lema 1.5.10 se tiene que

$$r < 3.3 \times 10^{17}.$$

En este caso la cota superior numérica para la variable r es 3.3×10^{17}, la cual también es cota de m pues $m < r$.

Es importante mencionar que, hasta aquí, hemos demostrado que hay una cantidad finita de soluciones por lo que el paso siguiente sería calcular las soluciones dándole a r los valores desde 4 a 3.3×10^{17}, pero observe que 3.3×10^{17} es un número muy grande, por lo que llevarlo a cabo requiere del cálculo de muchas operaciones y nos llevaría mucho tiempo. Por ello, debemos aplicar el paso 5.

Paso 5**:** En este paso lo que debemos hacer es reducir la cota numérica de r, para hacerlo aplicaremos el lema 1.1.18. Antes de aplicar el lema, debemos hacer algunas observaciones. Sea

$$\Gamma = m\log 2 - (r+2)\log\alpha - \log C_\alpha,$$

entonces $\Lambda = e^\Gamma - 1$. Lo primero que buscamos es obtener una cota superior, en función de r, del tipo exponencial negativo del valor absoluto de Γ. Recuerde que en el paso dos lo que se buscaba era encontrar una cota superior del tipo exponencial negativo que dependía de nuestra cota del primer paso, así que usando la identidad $\Gamma < e^\Gamma - 1$ obtenemos de manera directa lo que se quiere. Para esto, veamos que si $\Gamma > 0$ entonces $|e^\Gamma - 1| > 0$ y como $\Gamma < e^\Gamma - 1$ tenemos que

$$0 < \Gamma < e^\Gamma - 1 = \Lambda < \frac{9}{5}\alpha^{-(r+1)}.$$

Pero si $\Gamma < 0$, como $r \geq 4$ tenemos que $9\alpha^{-(r+1)}/5 < 1/2$ entonces $|e^\Gamma - 1| < 1/2$ y por lo tanto $e^{|\Gamma|} < 2$, pero esto implica que

$$0 < |\Gamma| < e^{|\Gamma|} - 1 = e^{|\Gamma|}|e^\Gamma - 1| < 2 \cdot \frac{9}{5} \cdot \alpha^{-(r+1)} = \frac{18}{5}\alpha^{-(r+1)}.$$

Así que, sin importar el signo de Γ obtenemos

$$0 < |m\log 2 - (r+2)\log\alpha - \log C_\alpha| = |\Gamma| < \frac{18}{5}\alpha^{-(r+1)}.$$

Lo que queremos ahora es obtener una expresión similar al del lema 1.1.18, es decir, que m o $-(r+2)$ no aparezcan multiplicándose por otro término, pero esto se logra dividiendo entre $\log\alpha$, pues obtenemos

$$0 < |m\gamma - (r+2) + \mu| < A \cdot B^{-k},$$

donde

$$\gamma = \frac{\log 2}{\log\alpha}, \quad \mu = -\frac{\log C_\alpha}{\log\alpha}, \quad A = \frac{18}{5 \cdot \log\alpha}, \quad B = \alpha \quad \text{y} \quad k = r+2.$$

Para aplicar el lema 1.1.18 tomemos $M := 3.3 \times 10^{17}$, calculamos la convergente p/q de la fracción continua del irracional γ que satisface $q > 6M$ (condición de la nota 1.1.19) y $\epsilon = ||\mu q|| - M||\gamma q|| > 0$. Como

$m \leq M$, usando la contrapositiva del lema 1.1.18, se tiene $r + 1 \leq 121$. Por hipótesis tenemos que $r \geq 4$ entonces,

$$4 \leq r \leq 120.$$

Paso 6**:** Hallar las soluciones de nuestra ecuación diofántica dándole a r los valores de 4 hasta 120. Esto lo hacemos con ayuda de Mathematica y hemos obtenido que las únicas soluciones no triviales son

$$(r, m) \in \{(4, 1), (6, 2)\},$$

que es lo que se quería demostrar.

2.3 Coincidencias de las sucesiones de Fibonacci y Narayana.

En este ejemplo trabajaremos con la muy conocida sucesión de Fibonacci $(F_n)_{n\geq 0}$ y con la sucesión de Narayana $(N_m)_{m\geq 0}$ que fue presentada en la sección anterior.

Bravo y Luca en [11] trabajaron en encontrar coincidencias en la sucesión $k-$generalizada de Fibonacci, es decir, resolvieron la ecuación

$$F_n^{(k)} = F_m^{(l)},$$

en enteros no negativos n, k, m, l con $k, l \geq 2$; encontraron que las únicas soluciones no triviales son

$$(n, k, m, l) \in \{(6, 3, 7, 2), (11, 7, 12, 3)\} \cup \{(6, 2, 5, t) \ : t \geq 4\}.$$

Nosotros estamos interesados en estudiar qué números de Fibonacci coinciden con números de Narayana, es decir, queremos determinar todas las soluciones de la ecuación diofántica

$$N_m = F_n, \tag{2.9}$$

en enteros positivos $n, m \geq 1$.

Notemos que los primeros tres números de la sucesión de Narayana y los primeros dos números de la sucesión de Fibonacci son uno,

$$1 = N_1 = N_2 = N_3 = F_1 = F_2. \tag{2.10}$$

Las soluciones de (2.10) las llamaremos **soluciones triviales.** Tenemos el siguiente resultado.

Teorema 2.3.1. *Las únicas soluciones no triviales de la ecuación* (2.9) *en enteros positivos* m, n *con* $m \geq 4$ *y* $n \geq 3$ *son*

$$(m, n) = (4, 3), (5, 4) \quad y \quad (9, 7).$$

Demostraremos el teorema siguiendo la estrategia descrita al inicio del capítulo. Las variables involucradas son m y n.

Paso 1: Lo primero que haremos es ver quien es la variable dominante. Para esto, note que $N_r < F_r$ para $r \geq 3$. En efecto, si $r = 3$ entonces

$$1 = N_3 < F_3 = 2.$$

Supongamos que esto es válido para $3 \leq s < r$, entonces

$$N_r = N_{r-1} + N_{r-3} < F_{r-1} + F_{r-3} \leq F_{r-1} + F_{r-2} = F_r. \tag{2.11}$$

La desigualdad (2.11) muestra que si $N_m = F_n$ entonces $m > n$. Hemos así cumplido con el paso uno.

Paso 2: Usando (1.7) y (1.10) tenemos

$$\begin{aligned} \left| \frac{\alpha^n}{\sqrt{5}} - C_{\alpha_*}\alpha_*^{m+2} \right| &= \left| \frac{\beta^n}{\sqrt{5}} + C_{\beta_*}\beta_*^{m+2} + C_{\gamma_*}\gamma_*^{m+2} \right| \\ &\leq \frac{1}{\sqrt{5}}|\beta^n| + |C_{\beta_*}||\beta_*^{m+2}| + |C_{\gamma_*}||\gamma_*^{m+2}| \\ &= \frac{1}{\sqrt{5}}\frac{1}{|\alpha^n|} + 2|C_{\beta_*}||\beta_*^{m+2}|, \end{aligned}$$

donde α_*, β_* y γ_* son las raíces del polinomio característico de la sucesión de Narayana y donde hemos usado el hecho que $(\alpha\beta)^n = (-1)^n$ y $|\beta_*| = |\gamma_*|$, los cuales son fáciles de comprobar. Ahora, como $n \geq 3$ y $m \geq 4$ entonces

$$\frac{1}{\sqrt{5}|\alpha^n|} < \frac{1}{\sqrt{5}|\alpha^3|} \approx 0.10 < \frac{2}{10} \quad \text{y} \quad |\beta_*^{m+2}| \leq |\beta_*^6| \approx 0.31 < \frac{1}{3}.$$

Como además $\|C_{\beta_*}\| \approx 0.40 < 4/9$, se tiene

$$\left| \frac{\alpha^n}{\sqrt{5}} - C_{\alpha_*}\alpha_*^{m+2} \right| < \frac{2}{10} + 2 \cdot \frac{4}{9} \cdot \frac{1}{3} = \frac{67}{135} < \frac{1}{2}. \tag{2.12}$$

Dividiendo ambos lados de la ecuación 2.12 por $C_{\alpha_*}\alpha_*^{m+2}$ obtenemos

$$|\alpha^n(\sqrt{5})^{-1}(C_{\alpha_*})^{-1}\alpha_*^{-(m+2)} - 1| < \frac{1}{2}\cdot\frac{1}{C_{\alpha_*}}\cdot\frac{1}{\alpha_*^{m+2}} < \frac{1}{\alpha_*^{m-1}}, \qquad (2.13)$$

donde en la última desigualdad hemos usado el hecho que $1/(2\cdot C_{\alpha_*}) < \alpha_*^3$. Aquí nuestra forma lineal en logaritmos es

$$\alpha^n(\sqrt{5})^{-1}(C_{\alpha_*})^{-1}\alpha_*^{-(m+2)} - 1$$

y la cota superior del tipo exponencial en términos de m es $\alpha_*^{-(m-1)}$.

Paso 3: El siguiente paso es aplicar el teorema 1.5.9 de Matveev , para esto tomemos $\mathbb{L} := Q(\alpha, \alpha_*)$, $\gamma_1 = \alpha$, $\gamma_2 = \alpha_*$, $\gamma_3 = \sqrt{5}$, $\gamma_4 = C_{\alpha_*}$, $b_1 = n$, $b_2 = -(m+2)$, $b_3 = -1$ y $b_4 = -1$. Tenemos que $D = 6$ y $B := m+2$. Tomemos $\Lambda = \alpha^n(\sqrt{5})^{-1}(C_{\alpha_*})^{-1}\alpha_*^{-(m+2)} - 1$. Para aplicar el teorema de Matveev necesitamos probar que $\Lambda \neq 0$, para ello procedamos por contradicción, supongamos que $\Lambda = 0$, entonces

$$\alpha^n = \sqrt{5}C_{\alpha_*}\alpha_*^{m+2}.$$

Luego, tomando el monomorfismo $\sigma : \mathbb{L} \to \mathbb{C}$ que asigna $\alpha_* \mapsto \beta_*$ y deja fijas a las demás raíces, tenemos que

$$\alpha^n = \sqrt{5}C_{\beta_*}\beta_*^{m+2},$$

luego tomando normas ambos lados tenemos

$$|\alpha^n| = |\sqrt{5}C_{\beta_*}||\beta_*^{m+2}|,$$

lo cual es imposible pues el lado izquierdo es mayor a $3/2$ y el lado derecho es menor a 1. Por lo tanto $\Lambda \neq 0$. Ahora calculemos los A_j; para hacer esto usamos las propiedades de las alturas, tenemos

$$\begin{aligned}
h(\gamma_1) &= \frac{1}{2}\log\alpha, \qquad h(\gamma_2) = \frac{1}{3}\log\alpha_*, \qquad h(\gamma_3) = \log\sqrt{5} \\
h(\gamma_4) &= h\left(\frac{1}{\alpha_*^3+2}\right) \leq h(1) + h(\alpha_*^3+2) = h(\alpha_*^3+2) \\
&\leq h(\alpha_*^3) + h(2) + \log 2 = 3h(\alpha_*) + 2\log 2 \\
&= \log\alpha_* + 2\log 2 < 4\log 2.
\end{aligned}$$

Tenemos entonces $A_1 = 3\log\alpha$, $A_2 = 2\log\alpha_*$, $A_3 = 6\log\sqrt{5}$ y $A_4 = 24\log 2$. Aplicando el teorema 1.5.9 se tiene

$$\begin{aligned}\log|\Lambda| &> -1.4\cdot 30^7\cdot 4^{4.5}\cdot 6^2(1+\log 6)\cdot 864\cdot\log\alpha\cdot\log\alpha_* \\ &\quad\cdot\log\sqrt{5}\cdot\log 2\cdot(1+\log(m+2)) \\ &> -1.4\times 10^{17}(1+\log(m+2)).\end{aligned}$$

Con esto hemos culminado el paso dos.

Paso 3: Comparando la desigualdad anterior con (2.13) tenemos

$$(m-1)\log\alpha_* < 1.4\times 10^{17}(1+\log(m+2)).$$

Esto implica que $m < 9.6\times 10^{17}\log m$, así,

$$\frac{m}{\log m} < 9.6\times 10^{17}. \tag{2.14}$$

Usando el lema 1.5.10 en (2.14) obtenemos

$$m < 8\times 10^{19}.$$

Hemos obtenido hasta aquí una cota superior numérica de la variable dominante que es m. Note que, nuevamente esta cota es muy alta, por lo que procederemos a aplicar una reducción de cota.

Paso 5: Sea

$$\Gamma = n\log\alpha - \log\sqrt{5} - \log C_{\alpha_*} - (m+2)\log\alpha_*,$$

entonces $\Lambda = e^{\Gamma} - 1$; en particular $\Gamma \neq 0$ pues $\Lambda \neq 0$. Como en el ejemplo anterior, queremos hallar una cota superior en términos de m del tipo exponencial negativo del valor absoluto de Γ; para esto, nótese que si $\Gamma > 0$ entonces

$$0 < \Gamma \leq e^{\Gamma} - 1 < 1/\alpha_*^{m-1}.$$

Por el contrario, si $\Gamma < 0$, como $|\Lambda| = |e^{\Gamma} - 1| < 1/2$ cuando $m \geq 4$ entonces $e^{|\Gamma|} < 2$, así

$$0 < |\Gamma| \leq e^{|\Gamma|} - 1 = e^{|\Gamma|}|e^{\Gamma} - 1| < 2\cdot\frac{1}{\alpha_*^{m-1}} < \frac{1}{\alpha_*^{m-3}},$$

En cualquier caso, se tiene que

$$0 < |n \log \alpha - \log \sqrt{5} - \log C_{\alpha_*} - (m+2) \log \alpha_*| = |\Gamma| < \frac{1}{\alpha_*^{m-3}}. \quad (2.15)$$

El objetivo es ahora obtener una expresión similar al del lema 1.1.18, así que dividiendo entre $\log \alpha_*$ y usando que $1/\log \alpha_* < 3$ obtenemos de lo anterior que

$$0 < |n\gamma - (m+2) + \mu| < A \cdot B^{-k},$$

donde

$$\gamma = \frac{\log \alpha}{\log \alpha_*}, \quad \mu = -\frac{\log \sqrt{5} + \log C_{\alpha_*}}{\log \alpha_*}, \quad A = 3 \quad \text{y} \quad B = m - 3.$$

Para aplicar el teorema 1.1.18 tomemos $M := 8 \times 10^{19}$, calculamos la convergente p/q de la fracción continua del irracional γ que satisface $q > 6M$ (condición de la nota 1.1.19) y $\epsilon := ||\mu q|| - M|\gamma q| > 0$. Observe que $m \leq M$, usando entonces la contrapositiva del lema 1.1.18 se tiene que $m - 3 \leq 131$. Como $m \geq 4$ entonces

$$4 \leq m \leq 134.$$

Paso 6: Lo siguiente es calcular las soluciones de nuestro problema. Con ayuda de Mathematica comparando N_m y F_n para $4 \leq m \leq 134$ y $3 \leq n \leq 133$ obtenemos que las únicas soluciones son

$$(m, n) = (4, 3), (5, 4) \quad \text{y} \quad (9, 7).$$

2.4 Observaciones adicionales del método.

En nuestros ejemplos algunos pasos del método no fueron complicados llevarlos a cabo, sin embargo, en otros no es el caso, por ejemplo en [13] Bravo, Luca y Yazán encuentran todos los enteros c que tiene al menos dos representaciones como diferencia entre una potencia de 2 y un número de Tribonacci, la cual está definida como $T_0 = T_1 = 0$, $T_2 = 1$ y $T_{n+2} = T_{n+1} + T_n$, concretamente resuelven la ecuación diofántica

$$T_n - 2^m = T_{n_1} - 2^{m_1}$$

para enteros no negativos n, m, n_1, m_1 con $n_1 < n$ y $m_1 < m$. En el primer paso encontraron que la *variable dominante* es n. Para el segundo paso su forma lineal es

$$\Lambda = C_\alpha \alpha^{n-1} 2^{-m} - 1,$$

donde α es la raíz del polinomio característico de la sucesión de Tribonacci y C_α es la constante que acompaña a α en la fórmula de Binet de la sucesión de Tribonacci. Sin embargo, no les fue fácil acotarla superiormente por una función del tipo exponencial del negativo que sólo dependiera de n, así que decidieron dejar esa cota en función de todas las variables, concretamente la cota que ellos dieron fue

$$\max\{\alpha^{n_1-n+6}, 2^{m_1-m+1}\}. \tag{2.16}$$

Después de aplicar el teorema de Matveev, ellos obtuvieron

$$\log|\Lambda| > -1.3 \times 10^{13}(1 + \log n). \tag{2.17}$$

Luego, compararon las cotas (2.16) y (2.17), usaron propiedades de mínimo y máximo y obtuvieron

$$\min\{(n - n_1)\log\alpha, (m - m_1)\log 2\} < 1.4 \times 10^{13}(1 + \log n).$$

Analizan cada uno de los casos y obtienen que $n < 4 \times 10^{45}$. Después aplican el método de reducción de Dujella y Pethő para poder encontrar todas las soluciones. Se sugiere consultar el trabajo hecho por Bravo, Luca y Yazán para más detalle.

Podemos observar que en caso de no tener el paso dos, se puede intentar trabajar el problema dejando la cota superior en función de más de una variable incluyendo la variable dominante como lo hicieron Bravo, Luca y Yazán en [13] buscando el objetivo del paso 4.

Uno de los objetivos del paso dos, es acotar superiormente la forma lineal en logaritmos por una función del tipo exponencial del negativo de la variable dominante. Para llevarlo a cabo usamos una característica muy importante que cumplen el tipo de problemas que trabajamos, esto es que, de las raíces del polinomio característico de la sucesión en turno, sólo una de ellas tenga norma mayor a 1. Antes de mencionar por qué la anterior característica es importante, recordemos que en nuestro trabajo tratamos el tipo de ecuaciones que involucran sucesiones linealmente

recurrentes ya que, por medio de su fórmula de tipo Binet, obtenemos una ecuación diofántica del tipo exponencial. Después de obtener dicha ecuación, pasamos a uno de los miembros los términos de norma mayor a uno y del otro los de norma menor a uno. Luego, tomamos valor absoluto en ambos miembros; como en uno de los miembros de la ecuación están las raíces del polinomio característico con norma menor a 1, entonces podemos acortarlo por una constante. En importante aclarar que si se tienen dos o más raíces con norma mayor a 1, se debe hacer un análisis para obtener la cota superior de la forma lineal en logaritmos, es por eso que considerar problemas con esta característica es muy importante para nuestro trabajo. Finalmente, después de acotar el miembro que tiene los valores con norma menor a uno, se divide por el término que involucre a la variable dominante y así cumplimos nuestro paso 2. El anterior proceso se puede ver en ambos ejemplos que presentamos.

El teorema de Matveev juega un papel muy importante en este tipo de problemas ya que gracias a el, pasamos de buscar en una infinidad de valores enteros no negativos para las variables de nuestra ecuación diofántica, a hacerlo en un conjunto finito de enteros, i.e., hacemos la búsqueda hasta la cota superior numérica de las variables. La cota está directamente relacionada con la constante numérica $1.4 \cdot 30^{n+3} \cdot n^{4.5}$, así el hecho de obtener una cota pequeña depende de la cantidad de elementos de nuestra forma lineal en logaritmos, sin embargo, aún cuando sean pocos elementos en nuestra forma lineal la cota que arroja el teorema de Matveev no es pequeña, por ejemplo, para los valores de $n = 2$ y $n = 3$ se tiene que

$$1.4 \cdot 30^{n+3} \cdot n^{4.5} \approx 7.7 \times 10^8 \qquad \text{y} \qquad 1.4 \cdot 30^{n+3} \cdot n^{4.5} \approx 1.5 \times 10^{11}.$$

En ambos casos no se tomó en cuenta el grado de extensión del campo ni el valor de las alturas logarítmicas de los números algebraicos, así que considerándolos, la cota puede ser aún mayor. En la práctica se ha visto que para formas lineales de dos o tres logaritmos, el teorema de Matveev proporciona una constante numérica alrededor de 10^{12} y 10^{14}.

Cabe mencionar que cuando se trabaja con una forma lineal de exactamente dos logaritmos se puede hacer uso de otros resultados que entregan una cota inferior mucho mejor que Matveev, tales resultados se deben a Laurent, Mignotte y Nesterenko (ver [27], [25]). Hasta el momento se desconoce si hay resultados para exactamente tres, cuatro o más loga-

ritmos que entreguen mejores cotas inferiores a las que proporciona el teorema de Matveev. Es importante aclarar que en nuestro trabajo tenemos problemas que son de al menos tres formas en logaritmos por lo que no usamos los resultados de Laurent, Mignotte y Nesterenko pero decidimos mencionarlo por si el lector está interesado.

Como mencionamos en uno de los párrafos de arriba, en la práctica el teorema de Matveev proporciona una constante numérica alta y hacer la búsqueda de las soluciones implicarían muchas operaciones y esto llevaría mucho tiempo. Es por eso que es necesario aplicar una reducción a la cota numérica, para ello, empleamos el método de reducción de Dujella y Pethő, en el apéndice B hemos hecho un código que nos ayuda a reducir la cota. Es importante mencionar que se deben tener algunas consideraciones para poder aplicar el lema de Dujella y Pethő. La primera y la más importante es que μ sea un número real no entero, pues en caso contrario tendríamos que $\mu q \in \mathbb{Z}$ y así $||\mu q|| = 0$ para cualquier denominador q de la convergente de la fracción continua del irracional γ y por lo tanto ε siempre sería negativo. Además de lo anterior, se debe tener en cuenta que μ y γ no se puedan obtener uno del otro por medio de una traslación, es decir, que no sean de la forma $\mu = \gamma + k$ o $\gamma = \mu + k$ con $k \in \mathbb{Z}$. Si lo anterior pasa tendríamos que si $\gamma = \mu + k$ con $k \in \mathbb{Z}$ entonces

$$||\gamma q|| = ||(\mu + k)q|| = ||\mu q + kq)|| = ||\mu q||$$

y así $\varepsilon = ||\mu q|| - M||\gamma q|| = ||\mu q||(1 - M)$ será siempre negativo.

Una de las dificultades que uno tiene al aplicar el método de reducción es que ε es negativo, lo que se puede hacer es considerar una convergente mayor y verificar si ε cambia de signo. Lo anterior se puede hacer tantas veces como el usuario crea necesario. Otra cosa que el usuario puede hacer para obtener ε con signo positivo es manipular los valores de μ, para ello, note que la expresión $m\gamma - n + \mu$ es igual a $(m-1)\gamma - n + \mu'$ donde $\mu' = \mu + \gamma$, así que en lugar de aplicar el método de Dujella y Pethő a la primer expresión se le aplica a la segunda. Observe que el resultado que entrega el lema no cambia pues $m - 1 < m \leq M$. Es importante mencionar que hacer una o ambas cosas mencionadas arriba no garantizan que en algún momento se tenga lo deseado.

Capítulo 3 Conclusión

En este trabajo presentamos un método para resolver algunas ecuaciones diofánticas usando la teoría de formas lineales en logaritmos. Después de analizar el método que empleamos en este trabajo, podemos concluir que es muy efectivo para resolver ecuaciones diofánticas exponenciales, muchas ecuaciones que involucran sucesiones linealmente recurrentes de algún orden pueden tratarse como las de este tipo, pues por medio de su fórmula tipo binet obtenemos una ecuación diofántica exponencial. Los ejemplos que mostramos en las secciones 2.2 y 2.3 involucran sucesiones recurrentes. Otros problemas con esta característica y que usan el mismo método que presentamos aquí pueden ser encontrados en [9], [11], [28], [15], [13], [12] por mencionar algunos. Es importante mencionar que los problemas que presentamos en el capítulo 2 son completamente de nuestra autoría.

Apéndice A Resultados de campo de números algebraicos.

En este apéndice daremos algunos resultados de campos de números algebraicos que usamos en el trabajo, sólo pondremos algunas demostraciones si consideramos que son importantes. Si el lector está interesado en estos resultados puede consultarlos en [1], que es la referencia básica sobre la cual está basada la sección.

A.1 Campo de números algebraicos.

En toda esta sección $\mathbb{L}$ será un campo de números algebraicos, es decir, $\mathbb{L} = \mathbb{Q}(\alpha_1, \ldots, \alpha_n)$ donde $\alpha_1, \ldots, \alpha_n$ son números algebraicos. Del teorema 1.4.13 se tiene que $\mathbb{L} = \mathbb{Q}(\alpha)$ donde α es un número algebraico. Una consecuencia del teorema 1.4.11 para un campo de números algebraicos es el siguiente.

Teorema A.1.1. *Sea n el grado del polinomio $Irr_{\mathbb{Q}}(\alpha)$. Cualquier elemento de $\mathbb{L}$ se puede expresar de manera única de la forma*

$$c_0 + c_1\alpha + \cdots + c_{n-1}\alpha^{n-1},$$

donde $c_0, c_1, \ldots, c_{n-1} \in \mathbb{Q}$.

Un resultado importante es saber el número de monomorfismos

$$\sigma : \mathbb{L} \to \mathbb{C}.$$

Por ejemplo, si $\mathbb{L} = \mathbb{Q}(\sqrt{2})$ entonces

$$\sigma_1(x + y\sqrt{2}) = x + y\sqrt{2} \quad (x, y \in \mathbb{Q})$$

y

$$\sigma_2(x + y\sqrt{2}) = x - y\sqrt{2} \quad (x, y \in \mathbb{Q})$$

son dos monomorfismos de $\mathbb{L}$ a $\mathbb{C}$. El siguiente teorema nos dice la cantidad de monomorfismos que existen.

Teorema A.1.2. *Si $n = [\mathbb{L} : \mathbb{Q}]$, entonces existen exactamente n diferentes monomorfismos $\sigma_k : \mathbb{L} \to \mathbb{C}$, $k = 1, \ldots, n$.*

Dado un campo de números algebraicos $\mathbb{L} = \mathbb{Q}(\alpha)$ se tiene que cada $\beta \in \mathbb{L}$ se puede expresar de manera única de la siguiente forma

$$\beta = a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1},$$

donde $a_0, \ldots, a_{n-1} \in \mathbb{Q}$. Así que los monomorfismos σ_k del teorema anterior se definen como

$$\sigma_k(a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1}) := a_0 + a_1\alpha_k + \cdots + a_{n-1}\alpha_k^{n-1},$$

donde α_k es el k-ésimo conjugado de $\alpha = \alpha_1$. Mostramos el siguiente ejemplo para dejar más claro, la manera en que son tomados los monomorfismos.

Ejemplo A.1.3. *Sea $\alpha = \sqrt[3]{2}$. Considere $\mathbb{L} = \mathbb{Q}(\alpha)$, note que $\mathbb{L}$ es campo de números algebraicos pues α es raíz del polinomio*

$$f(x) = x^3 - 2.$$

Más aún, $f(x)$ es el polinomio mínimo de α, entonces $[\mathbb{L} : \mathbb{Q}] = 3$. Los conjugados de α son los números complejos $\alpha_2 := \omega$ y $\alpha_3 := \overline{\omega}$. Luego, dado $\beta = 3 + 5\sqrt[3]{2} \in \mathbb{L}$ se tiene que los tres monomorfismos $\sigma_k : \mathbb{L} \to \mathbb{C}$ satisfacen:

$$\begin{aligned}
\sigma_1(\beta) &= \sigma_1(3 + 5\alpha) = 3 + 5\sigma_1(\alpha) \\
&= 3 + 5\alpha = \beta \\
\sigma_2(\beta) &= 3 + 5\alpha_2 = 3 + 5\omega \\
\sigma_3(\beta) &= 3 + 5\alpha_3 = 3 + 5\overline{\omega}.
\end{aligned}$$

Observe que para $k = 1, \ldots, n$ se tiene

$$\begin{aligned}
\text{Im } \sigma_k &= \sigma_k(\mathbb{L}) \\
&= \{\sigma_k(a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1}) \mid a_0, a_1, \ldots, a_{n-1} \in \mathbb{Q}\} \\
&= \{a_0 + a_1\alpha_k + \cdots + a_{n-1}\alpha_k^{n-1} \mid a_0, a_1, \ldots, a_{n-1} \in \mathbb{Q}\} \\
&= \mathbb{L}(\alpha_k)
\end{aligned}$$

por lo tanto $\sigma_k : \mathbb{L} = \mathbb{Q}(\alpha) \to \mathbb{Q}(\alpha_k)$ es un isomorfismo, de hecho es un $\mathbb{Q}$-isomorfismo y así todos lo campos $\mathbb{Q}(\alpha_k)$, $k = 1, \ldots, n$ son isomorfos. Ésto motiva a la siguiente definición.

Definición A.1.4. Los campos $\mathbb{L} = \mathbb{Q}(\alpha) = \mathbb{Q}(\alpha_1)$, $\mathbb{Q}(\alpha_2)$, ..., $\mathbb{Q}(\alpha_n)$ son llamados **campos conjugados de** $\mathbb{L}$.

Sea β un número algebraico de grado m sobre $\mathbb{Q}(\alpha)$, con conjugados $\beta_1, \ldots, \beta_m$ y sea $\mathbb{L} = \mathbb{Q}(\alpha_k)(\beta_l)$ con $l \in \{1, \ldots, m\}$. Como

$$\sigma_k : \mathbb{Q}(\alpha) \to \mathbb{Q}(\alpha_k)$$

es un isomorfismo, entonces una consecuencia de [20, Teorema 7.4] es que existe un único monomorfismo

$$\sigma_{k,l} : \mathbb{Q}(\alpha, \beta) \to \mathbb{L}$$

tal que $\sigma_{k,l}(\beta) = \beta_l$ y $\sigma_{k,l}|_{\mathbb{Q}(\alpha)} = \sigma_k$, es decir, $\sigma_{k,l}(\alpha) = \alpha_k$. De lo anterior se tiene que hay a $n \cdot m$ monomorfimos $\sigma_{k,l}$.

Ejemplo A.1.5. *Sea* $f(x) = x^2 - x - 1$ *y* $g(x) = x^3 - x^2 - 1$, *las raíces de* $f(x)$ *y* $g(x)$ *son* α_1, α_2 *y* $\beta_1, \beta_2, \beta_3$ *respectivamente. Los* 6 *monomorfismos*

$$\sigma_{k,l} : \mathbb{Q}(\alpha_1, \beta_1) \to \mathbb{C}$$

con $k = 1, 2$ *y* $l = 1, 2, 3$ *son tales que*

$$\begin{aligned}
\sigma_{1,1}(\alpha_1) &= \alpha_1 \qquad \sigma_{1,1}(\beta_1) = \beta_1 \\
\sigma_{1,2}(\alpha_1) &= \alpha_1 \qquad \sigma_{1,2}(\beta_1) = \beta_2 \\
\sigma_{1,3}(\alpha_1) &= \alpha_1 \qquad \sigma_{1,3}(\beta_1) = \beta_3 \\
\sigma_{2,1}(\alpha_1) &= \alpha_2 \qquad \sigma_{2,1}(\beta_1) = \beta_1 \\
\sigma_{2,2}(\alpha_1) &= \alpha_2 \qquad \sigma_{2,2}(\beta_1) = \beta_2 \\
\sigma_{2,3}(\alpha_1) &= \alpha_2 \qquad \sigma_{2,3}(\beta_1) = \beta_3.
\end{aligned}$$

Estos monoformismos juegan un papel muy importante en los ejemplos que presentamos en el capítulo dos. Por simplicidad denotaremos a $\sigma_{k,l}$ por σ.

De la definición A.1.4 se desprende que los campos conjugados de $\mathbb{L}$ pueden depender de la elección del número algebraico α tal que $\mathbb{L} = \mathbb{Q}(\alpha)$. El siguiente teorema muestra que este no es el caso.

Teorema A.1.6. *Sean $\alpha_1 = \alpha, \alpha_2, \ldots, \alpha_n$ los conjugados de α, sea también β otro número algebraico tal que $\mathbb{L} = \mathbb{Q}(\beta)$ y $c_0, c_1, \ldots, c_{n-1} \in \mathbb{Q}$ tales que*

$$\beta = c_0 + c_1\alpha + \cdots + c_{n-1}\alpha^{n-1}.$$

Para cada $k = 1, \ldots, n$ definamos

$$\beta_k = c_0 + c_1\alpha_k + \cdots + c_{n-1}\alpha_k^{n-1}.$$

Se tiene entonces que $\beta_1 = \beta, \beta_2, \ldots, \beta_n$ son conjugados de β sobre $\mathbb{Q}$ y $\mathbb{Q}(\alpha_k) = \mathbb{Q}(\beta_k)$, $k = 1, \ldots, n$.

Al conjunto $\{\beta_1 = \beta, \ldots, \beta_n\}$ del teorema A.1.6 se le llama **conjunto completo de conjugados de β relativos a $\mathbb{L}$** o brevemente **los $\mathbb{L}$-conjugados de β**. Observemos que los conjugados β relativos a $\mathbb{L}$ son obtenidos de β al aplicar el monomorfismo $\sigma_k : \mathbb{L} \to \mathbb{C}$ a β, así que es fácil ver que $\sigma_k(\beta) = \beta_k$. En la siguiente definición se ve la utilidad de los conjugados de β relativos a $\mathbb{L}$.

Definición A.1.7. Sean $\mathbb{L}$ un campo de números algebraicos de grado n y $\beta_1 = \beta, \beta_2, \ldots, \beta_n$ los $\mathbb{L}$-conjugados de β. El **polinomio de campo de β sobre $\mathbb{L}$** es el polinomio

$$\mathrm{fld}_{\mathbb{L}}(\beta) = \prod_{k=1}^{n}(x - \beta_k).$$

Claramente se tiene que $\mathrm{fld}_{\mathbb{L}}(\beta) \in \mathbb{C}[x]$ sin embargo en [1, página 118] se prueba el siguiente resultado.

Teorema A.1.8. *$fld_{\mathbb{L}}(\beta) \in \mathbb{Q}[x]$.*

Más aún, se tiene el siguiente teorema, el cual relaciona el polinomio de campo de β sobre $\mathbb{L}$ con el polinomio mínimo de β sobre $\mathbb{Q}$.

Teorema A.1.9. *$fld_{\mathbb{L}}(\beta) = (Irr_{\mathbb{Q}}(\beta))^s$, donde $s = n/\deg Irr_{\mathbb{Q}}(\beta)$ es un entero positivo.*

Apéndice B Código del método de reducción.

En este apéndice presentamos el algoritmo que seguimos para reducir la cota. La idea de hacer el algoritmo está basado en usar el Lema 1.1.18.

Algoritmo 1 Método de reducción

$M \leftarrow$ cota de las variables
$\gamma, \mu \leftarrow$ números reales de nuestra forma lineal
$A, B \leftarrow$ cotas superiores del valor absoluto de nuestra forma lineal
$q \leftarrow q_1$ ▷ q_1 denominador de la primer convergente de γ
$i \leftarrow 2$ ▷ contador para las convergentes
Mientras $q < 6M$ **hacer**
    $q \leftarrow q_i$
    $i \leftarrow i + 1$
end Mientras
$\varepsilon \leftarrow ||\mu q|| - M||\gamma q||$
Si $\varepsilon > 0$ **entonces**
    return $\frac{\log(Aq/\varepsilon)}{\log B}$
end Si

El algoritmo 1 se implementó en Mathematica; presentamos aquí el código que usamos en la sección 2.2 y después explicamos a detalle.

```
1  f[x_] := Abs[N[x - Round[x]]];
2  SOLnara = Solve[x^3 - x^2 - 1 == 0, x];
3  alfn = x /. SOLnara[[1]];
4  betn = x /. SOLnara[[2]];
5  gamn = x /. SOLnara[[3]];
6  m[x_] := 1/(x^3 + 2);
7  M = 5.8*10^16;
8  \[Gamma] = Log[2]/Log[alfn];                    γ del lema
9  \[Mu] = -(Log[m[alfn]]/Log[alfn]);              μ del lema
10 A = 18/(5*Log[alfn]);
11 B = alfn;
12 q2 = ContinuedFraction[\[Gamma], 1];
13 q1 = FromContinuedFraction[q2];
14 q = Denominator[q1];
15 i = 2;
16 While[q - 6*M < 0,
17          q2 = ContinuedFraction[\[Gamma], i];
18          q1 = FromContinuedFraction[q2];
19          q = Denominator[q1];
20          i++;
21 ]
22 distqgama = f[N[q*\[Gamma], 40]];
23 distqmu = f[N[q*\[Mu], 40]];
24 N[distqgama];
25 N[distqmu];
26 eps = distqmu - M*distqgama;
27 If[eps > 0,
28          Print[ IntegerPart[Log[A*q/eps]/Log[B]]]
29 ]
```

La función que definimos en la linea 1 es la que entrega la distancia de x al entero mas cercano. Las lineas $2-5$ son para poder trabajar con las raíces del polinomio característico de la sucesión de Narayana. La linea 6 es una función que evaluada en α, β y γ, entrega los coeficientes que acompañan a α^{r+2}, β^{r+2} y γ^{r+2} en la fórmula de Binet, respectivamente. De la linea 7 a la 11 son asignaciones de datos que se necesitan. Las lineas $12-21$ calculan la convergente de γ. Como trabajamos con números muy pequeños, necesitamos mucha precisión y en este caso hemos usado una precisión del orden 40. Lo anterior lo hemos hecho en las lineas $22-25$. La linea 27 es un condicional y verifica que la asignación de la linea 26 sea positiva.

Bibliografía

[1] Ş. Alaca and Kenneth. S. Williams. *Introductory Algebraic Number Theory*. Cambridge University Press, 2003.

[2] J. P. Allouche and J. Johnson. Narayana's cows and delayed morphisms. *Articles of 3rd Computer music conference JIM96, France*, 1996.

[3] Tom M. Apostol. *Mathematical analysis; 2nd ed.* Addison-Wesley Series in Mathematics. Addison-Wesley, Reading, MA, 1974.

[4] A. Baker. Linear forms in the logarithms of algebraic numbers I. *Mathematika J. Pure Appl. Math*, 13:204–216, 1966.

[5] A. Baker. Linear forms in the logarithms of algebraic numbers II. *Mathematika J. Pure Appl. Math*, 14:102–107, 1967.

[6] A. Baker. Linear forms in the logarithms of algebraic numbers III. *Mathematika J. Pure Appl. Math*, 14:220–228, 1967.

[7] Alan Baker. *Transcendental Number Theory*. Cambridge Mathematical Library. Cambridge University Press, 1975.

[8] G. Bilgici. The generalized order k-narayana's cows numbers. *Mathematica Slovaca*, 64(4):794–802, 2016.

[9] Eric Bravo, Jhon J. Bravo, and Florian Luca. Coincidences in generalized Lucas sequences. *Fibonacci Quarterly*, 52, 2014.

[10] Jhon J. Bravo and Florian Luca. Powers of Two in Generalized Fibonacci Sequences. *Revista Colombiana de Matemáticas*, 46:67 – 79, 2012.

[11] Jhon J. Bravo and Florian Luca. Coincidences in generalized Fibonacci sequences. *Journal of Number Theory*, 133(6):2121–2137, 2013.

[12] Jhon J. Bravo and Florian Luca. Repdigits in k-Lucas sequences. *Proceedings - Mathematical Sciences*, 124:141–154, 2014.

[13] Jhon J. Bravo, Florian Luca, and Yazán Karina. On pillai's problem with tribonacci numbers and powers of 2. *Bulletin of the Korean Mathematical Society*, pages 1069–1080, 2017.

[14] Yann Bugeaud. *Linear Forms in Logatithms and Applications*, volume 28. European Mathematical Society, 2018.

[15] Ana Chaves and Diego Marques. A Diophantine equation related to the sum of squares of consecutive k-generalized Fibonacci numbers. *Fibonacci Quarterly*, 52:70–74, 02 2014.

[16] H. Cohen. *Number Theory: Tools and Diophantine Equations*, volume Volume I. 2007.

[17] Harvey Cohn. *Advance number theory* . Dover Publications Inc., 1980.

[18] A. Dujella and A. Pethő. A generalization of a theorem of Baker and Davenport. *Quart. J. Math. Oxford Ser.*, 49(2):291–306, 1998.

[19] A.O. Gelfond and L.F. Boron. *Transcendental and Algebraic Numbers*. Dover Books on Mathematics. Dover Publications, 2015.

[20] D. J. H. Garling. *A course in galois theory*. Cambridge University Press, 03 2019.

[21] A. Ya. Khinchin. *Continued Fracions*. Dover Publications Inc., 1997.

[22] Emrah KiliÇ. Tribonacci sequences with certain indices and their sums. *Ars Combinatoria -Waterloo then Winnipeg*, 86:13–22, 01 2008.

[23] T. Koshy. *Fibonacci numbers and Lucas numbers with applications*. A Wiley-Interscience Publication, 2011.

[24] Serge Lang. *Introduction to Diophantine Approximations*. Springer-Verlag New York, 2 edition, 1995.

[25] Michel Laurent. Linear forms in two logarithms and interpolation determinants. *Acta Arithmetica*, 66(2):181–199, 1994.

[26] Lindemann. Ueber die Zahl π. *Mathematische Annalen*, 20:213–225, 1882.

[27] Florian Luca. *Ecuaciones Diofanticas*. 2008.

[28] Florian Luca and Roger Oyono. An exponential Diophantine equation related to powers of two consecutive Fibonacci numbers. *Proc. Japan Acad. Ser. A Math. Sci.*, 87(4):45–50, 2011.

[29] E. M. Matveev. An explicit lower bound for a homogeneous rational linear form in the logarithms of algebraic numbers. I. *Izvestiya: Mathematics*, 62(4):723–772, 1998.

[30] E. M. Matveev. An explicit lower bound for a homogeneous rational linear form in the logarithms of algebraic numbers. II. *Izvestiya: Mathematics*, 64(6):125–180, 2000.

[31] Steven J. Miller, Ramin Takloo-Bighash, and ONTENTS. Algebraic and transcendental numbers from an invitation to modern number theory. 2006.

[32] H. Pollard and Harold G. Diamond. *The theoryof algebraic numbers*. Dover Publications Inc., 1998.

[33] J. L. Ramirez and V. F. Sirvent. A note on the k-narayana sequence. *Annales mathematicae et informaticae*, 45:91–105, 2015.

[34] J. D. Sally and P. J. Sally Jr. *Roots to research: A vertical development of mathematics problems*. American Mathematical Society, 2007.

[35] T. N. Shorey and R. Tijdeman. *Exponential Diophantine Equations*. Cambridge Tracts in Mathematics. Cambridge University Press, 1986.

[36] Nigel P. Smart. *The algorithmic Resolution of Diophantine Equations*. Number 41. London Mathematical Society Student, 1998.

[37] Jörn Steuding. *Diophantine Analysis*. Birkhauser, 2016.