La ecuación de Pell

Trabajo Fin de Grado

Autora:
María Morales Cruz

Tutor:
Juan Cuadra Díaz

Grado en Matemáticas

Junio, 2020
Universidad de Almería

Abstract in English

Let d be a positive integer that is not a square. The equation $x^2 - dy^2 = 1$ is called Pell's equation and it arises in different problems in number theory. This simple equation has a long and amazingly rich history, ranging from ancient Greece to the present day. It appears implicitly in Archimedes' cattle problem for the first time (251 B.C.) and it has been studied by mathematicians of all times, including Archimedes, Diophantus, Brahmagupta, Bhaskara II, Fermat, Brouncker, Euler, Lagrange and Lenstra. In 1768 Lagrange finally ended a long search when proving rigorously that this equation has infinitely many integer solutions, that all of them are obtained from the so called fundamental solution, and that the latter can be calculated by using an algorithm based on the expression of $\sqrt{d}$ as an infinite simple continued fraction. He proved so several conjectures on this equation formulated through history and found the reason why the different empirical methods known for resolution worked. Pell's equation is still today under research and there is a cryptosystem based on it.

In this work we explain in full detail how to solve Pell's equation by using the theory of continued fractions. We first discuss the relation between this equation and the ring $\mathbb{Z}[\sqrt{d}\,]$, arising from the factorization $x^2 - dy^2 = (x + y\sqrt{d})(x - y\sqrt{d})$. In this framework we prove that Pell's equation always admit a minimal positive integer solution, called the fundamental solution, and that any other positive solution is obtained by taking powers of it. Then we develop the necessary part of the theory of continued fractions to describe the link between the fundamental solution and the parameter d. We prove that the fundamental solution is a convergent of the infinite simple continued fraction expansion of $\sqrt{d}$ and show that this convergent is determined by the length of the period of such an expansion. Throughout this work we present the algorithms that allow us to calculate the solutions of Pell's equation and we implement them as computer programs using the software *Mathematica*.

Finally, as an application of the results and algorithms expounded here, we solve Archimedes' cattle problem, an ancient problem that took more than 2000 years to be solved and whose complete solutions could not be calculated in full until the first computers appeared.

Resumen en español

Sea d un número natural que no es un cuadrado. La ecuación $x^2 - dy^2 = 1$ recibe el nombre de ecuación de Pell y surge en diferentes problemas de teoría de números. Esta sencilla ecuación tiene una historia larga y asombrosamente rica, que va desde la antigua Grecia hasta nuestros días. Aparece por primera vez oculta en el problema del ganado del Arquímedes (251 a.C.) y ha sido estudiada por matemáticos de todas las épocas, que incluyen a Arquímedes, Diofanto, Brahmagupta, Bhaskara II, Fermat, Brouncker, Euler, Lagrange y Lenstra. Fue Lagrange el que en 1768 puso fin a un larga búsqueda, a afirmaciones injustificadas y métodos de resolución empíricos, al demostrar rigurosamente que la ecuación posee infinitas soluciones enteras, que todas ellas se obtienen a partir de la llamada solución fundamental y que esta última se puede calcular mediante un algoritmo basado en la expansión en fracciones continuas simples del radical $\sqrt{d}$. En la actualidad esta ecuación sigue siendo objeto de investigación y existe un criptosistema fundamentado en ella.

En este trabajo explicamos detalladamente cómo se resuelve la ecuación de Pell a través de la teoría de fracciones continuas. Analizamos en primer lugar la relación entre esta ecuación y el anillo $\mathbb{Z}[\sqrt{d}\,]$ derivada de la factorización $x^2-dy^2 = (x+y\sqrt{d})(x-y\sqrt{d})$. En este marco demostramos que la ecuación de Pell siempre admite una solución mínima positiva, denominada solución fundamental, y que cualquier otra solución positiva es potencia de ella. Desarrollamos después la parte necesaria de la teoría de fracciones continuas para describir el vínculo entre la solución fundamental y el parámetro d. Mostramos que la solución fundamental viene dada por un convergente de la expansión en fracciones continuas simples de $\sqrt{d}$ y que este convergente queda determinado por la longitud del periodo de la expansión. A lo largo del trabajo presentamos los algoritmos que permiten calcular las soluciones de la ecuación de Pell y los implementamos en el ordenador con el software *Mathematica*.

Finalmente, como aplicación de los resultados y algoritmos expuestos, resolvemos el problema del ganado de Arquímedes, un problema de la antigüedad que tardó más de 2000 años en ser resuelto y cuyas soluciones completas no pudieron ser calculadas hasta la aparición de los primeros ordenadores.

Índice general

Introducción

Ten siempre a Ítaca en tu mente.
Llegar allí es tu destino.
Mas no apresures nunca el viaje.
Mejor que dure muchos años
y atracar, viejo ya, en la isla,
enriquecido de cuanto ganaste en el camino
sin aguantar a que Ítaca te enriquezca.

Viaje a Ítaca
Constantino Cavafis (1863-1933),
poeta griego.

El problema del ganado de Arquímedes, que nos servirá de motivación para nuestro estudio de la ecuación de Pell, se inspira en el Canto XII de *La Odisea* de Homero, una de las grandes obras de la literatura universal. Este canto se titula *Las sirenas, Escila, Caribdis, las vacas del sol*. En él se relata el siguiente episodio del famoso viaje de regreso a Ítaca del legendario héroe griego Ulises:

Ulises y el rebaño de Helios, el dios Sol
Johannes Stradanus (in circa 1600-1605)

127 (Habla Circe.) Llegarás más tarde á la isla de Trinacria (actual Sicilia), donde pacen las muchas vacas y pingües ovejas del Sol. Siete son las vacadas, otras tantas las hermosas greyes de ovejas, y cada una está formada por cincuenta cabezas. […] Si á éstas las dejares indemnes, ocupándote tan sólo en preparar tu regreso, aún llegaríais á Ítaca, después de pasar muchos trabajos; pero, si les causares daño, desde ahora te anuncio la perdición de la nave y la de tus amigos. Y aunque tú escapes, llegarás tarde y mal á la patria, después de perder todos los compañeros.

320 (Habla Ulises.) ¡Oh amigos! Puesto que hay en la velera nave alimentos y bebida, abstengámonos de tocar esas vacas, á fin de que no nos venga ningún mal, porque tanto las vacas como las pingües ovejas son de un dios terrible, del Sol (Helios), que todo lo ve y todo lo oye.

324 Así les dije y su ánimo generoso se dejó persuadir. […] Eurílocо comenzó á hablar con los amigos, para darles este pernicioso consejo:

324 […] Todas las muertes son odiosas á los infelices mortales, pero ninguna es tan mísera como morir de hambre y cumplir de esta suerte el propio destino. Ea, tomemos las más excelentes de las vacas del Sol y ofrezcamos un sacrificio á los dioses que poseen el anchuroso cielo.

352 Tales palabras profirió Eurílocо y los demás compañeros las aprobaron. Seguidamente, habiendo echado mano á las más excelentes de entre las vacas del Sol, que estaban allí cerca –pues las hermosas vacas de retorcidos cuernos y ancha frente pacían á poca distancia de la nave de azulada proa– se pusieron á su alrededor y oraron á los dioses […] Terminada la plegaria, degollaron y desollaron las reses; […]

391 Llegado que hube á la nave y al mar, reprendí á mis compañeros –acercándome ora á éste, ora á aquél,– mas no pudimos hallar remedio alguno, porque ya las vacas estaban muertas. […]

397 Durante seis días mis fieles compañeros celebraron banquetes, para los cuales echaban mano á las mejores vacas del Sol; […]

407 […] No anduvo la embarcación largo rato, pues sopló en seguida el estridente Céfiro y, desencadenándose, produjo gran tempestad: un torbellino rompió los dos cables del mástil, que se vino hacia atrás, y todos los aparejos se juntaron en la sentina. El mástil, al caer en la popa, hirió la cabeza del piloto, aplastándole todos los huesos; […] Júpiter despidió un trueno y simultáneamente arrojó un rayo en nuestra nave: ésta se estremeció, al ser herida por el rayo de Júpiter, llenándose del olor del azufre; y mis hombres cayeron en el agua. Llevábalos el oleaje alrededor del negro bajel y un dios les privó de la vuelta á la patria.

420 Seguí andando por la nave, hasta que el ímpetu del mar separó los flancos de la quilla, la cual flotó sola en el agua; y el mástil se rompió en su unión con la misma. Sobre el mástil hallábase una soga hecha del cuero de un buey: até con ella mástil y quilla y, sentándome en ambos, dejéme llevar por los perniciosos vientos.

Unos 2300 años después de la composición homérica, en 1679, el escritor Gotthold E. Lessing, representante destacado de la ilustración alemana, es nombrado director de la biblioteca *Herzog August* de Wolfenbüttel (Alemania). En su trabajo como bibliotecario tradujo y comentó varios manuscritos griegos y latinos de la biblioteca. Entre ellos se halla un poema griego, procedente de un manuscrito árabe, que contiene un problema matemático en el que se pide calcular el número de reses del rebaño del dios Sol[1]. Se atribuye generalmente a Arquímedes[2]. El problema se propone en una carta dirigida a Eratóstenes de Cirene (276-194 a.C.), otro gran matemático de la antigüedad, coetáneo de Arquímedes, y bibliotecario de la famosa biblioteca de Alejandría. Dice[3] así:

> Si eres diligente y sabio, oh extranjero, calcula la cantidad de reses del dios Sol, que una vez pastaron en los campos de la isla trinacriana de Sicilia, divididas en cuatro rebaños de diferentes colores, uno blanco lechoso, otro negro brillante, el tercero amarillo y el último moteado. En cada rebaño había toros, un número imponente según estas proporciones: Entiende, extranjero, que los toros blancos eran iguales a la mitad y un tercio de los toros negros unidos con todos los amarillos, mientras que los negros eran iguales a la cuarta parte y un quinto de los moteados, unidos, una vez más, con todos los amarillos. Observa además que los toros restantes, los moteados, eran iguales a una sexta parte y a un séptimo de los blancos unidos a todos los amarillos. Estas eran las proporciones de las vacas: las blancas eran precisamente iguales a la tercera parte y un cuarto de todo el rebaño de las negras; mientras que el rebaño de las negras era igual una vez más a la cuarta parte y un quinto del rebaño moteado, cuando todos, incluyendo a los toros iban a pastar juntos. Ahora en las cuatro partes las moteadas eran iguales en número a una quinta parte y un sexto del rebaño amarillo. Finalmente, las amarillas eran iguales en número a una sexta parte y un séptimo del rebaño de color blanco. Si puedes con precisión decir, oh extranjero, el número de reses del dios Sol, dando por separado el número de los bien alimentados toros y también el número de hembras de cada color, no serías llamado incompetente o ignorante de los números, pero aún no contarás entre los sabios.
>
> Pero ven, entiende también todas estas condiciones sobre las vacas del Sol. Cuando los toros blancos unieron su número con los negros, se mantuvieron firmes, iguales en profundidad y anchura, rellenaron con su multitud las llanuras de Trinacria, que se extienden lejos en todas direcciones. De nuevo, cuando los toros amarillos y los moteados se juntaron en un mismo rebaño, se dispusieron de tal modo que su número, comenzando en uno, creció lentamente hasta que completó una figura triangular, no faltando ninguno y no habiendo toros de otros colores en medio de ellos. Si eres capaz, oh extranjero, de averiguar todas estas cosas y juntarlas en tu mente, dando todas las relaciones, saldrás coronado de gloria y sabiendo que has sido declarado perfecto en esta especie de sabiduría.

Sean x, y, z, t el número de toros blancos, negros, moteados y amarillos[4] respectivamente. Similarmente, sean x', y', z', t' el número de vacas de esos mismos colores. Las condiciones de la primera parte del problema se traducen en el sistema de ecuaciones lineales 3.4 de la página 41. Se trata de un sistema compatible indeterminado cuya solución en los números naturales, calculada en las páginas 41, 42 y 43, es:

$$\begin{aligned}(x, y, z, t) &= (10366482, 7460514, 7358060, 4149387)\mu,\\ (x', y', z', t') &= (7206360, 4893246, 3515820, 5439213)\mu, \qquad \mu \in \mathbb{N}.\end{aligned}$$

De aquí obtenemos que el número de toros es 29334443μ, el de vacas es 21054639μ y el número total de reses en el rebaño del dios Sol es 50389082μ. El sistema lo resolvemos

[1] En la sección A.1 del apéndice se incluyen una imagen del manuscrito original y de la transcripción de Lessing. Han sido tomadas de [W4].

[2] Existe controversia sobre si el problema fue realmente propuesto por Arquímedes. Aparece mencionado como *problema del ganado de Arquímedes* en un escolio al diálogo *Cármides* de Platón. En [9, Sección 2.1], [21, Sección 4.3] y [22, Sección 1.9] se da más información al respecto.

[3] Nosotros lo hemos traducido del inglés de [9, página 18]. Los autores lo reproducen de [20]. En internet véase [W4].

[4] El término usado en tauromaquia es "pelaje melocotón": amarillento leonado se llama al color.

hoy en décimas de segundo con la ayuda del ordenador. Resolverlo a mano es tedioso, por la magnitud de los números que van apareciendo en el proceso y la dificultad de operar con ellos. Precisamente con la intención de resaltar esto hemos incluido en la sección 3.2 la resolución detallada de esta primera parte. No sabemos si se podría hablar ya con esta solución de un «*número imponente*» de toros en cada rebaño.

¿Qué desafío esconde la segunda parte? Se pide que $x+y$ sea un número cuadrado y que $z+t$ sea un número triangular. Esto significa que $x+y=c^2$ y $z+t=\frac{m(m+1)}{2}$ para algunos $c,m\in\mathbb{N}$. La primera condición lleva a que el parámetro μ debe cumplir $\mu=4456749s^2$ para cierto $s\in\mathbb{N}$. Los detalles se explican en la página 43. Ahí también podemos ver cómo la segunda condición conduce a que $8(z+t)+1=r^2$ para algún $r\in\mathbb{N}$. Como $z+t=11507447\mu$, operando con lo anterior, obtenemos la ecuación

$$r^2-410286423278424s^2=1, \tag{1}$$

que debemos resolver. El número 410286423278424 es el resultado del producto de 8, 4456749 y 11507447. Aquí nos damos de bruces con un problema que resiste a nuestros intentos por resolverlo.

La ecuación anterior es un caso particular de la llamada ecuación de Pell, que es el objeto de estudio de esta memoria. Nuestro objetivo aquí será resolver completamente esta ecuación para, posteriormente, solucionar el problema del ganado. La herramienta matemática usada para resolver la ecuación de Pell es la teoría de fracciones continuas. Estas fracciones ya eran utilizadas de forma rudimentaria por los antiguos griegos para aproximar números irracionales mediante números racionales. El problema del ganado supone la primera aparición conocida, aunque implícita, de esta ecuación.

Sea $d\in\mathbb{N}$ que no es un cuadrado. La *ecuación de Pell* es la ecuación diofántica:

$$x^2-dy^2=1.$$

El adjetivo diofántico se refiere a que sólo nos interesan las soluciones enteras, es decir, valores enteros de x e y que cumplan la igualdad.

La ecuación de Pell aparece mencionada por primera vez en los trabajos del filósofo y matemático griego Teón de Esmirna (130 a.C.). En lenguaje actual, él afirma que los pares de números (x_n,y_n) definidos por las relaciones de recurrencia

$$(x_1,y_1)=(1,1),\qquad (x_{n+1},y_{n+1})=(x_n+2y_n,x_n+y_n),\qquad n\geq 1,$$

cumplen $x_n^2-2y_n^2=(-1)^n$. (Compárese con la proposición 3.2.) Así que las parejas de subíndice par son soluciones de la ecuación de Pell. Por otro lado, las fracciones $\frac{x_n}{y_n}$ surgidas de estas relaciones aproximan cada vez mejor al número irracional $\sqrt{2}$.

Si, en lugar de estas, tomamos

$$(x_1,y_1)=(2,1),\qquad (x_{n+1},y_{n+1})=(x_n+3y_n,x_n+y_n),\qquad n\geq 1,$$

entonces las fracciones $\frac{x_n}{y_n}$ se van aproximando cada vez más a $\sqrt{3}$. Ahora se cumple que $x_n^2-3y_n^2=(-1)^{n+1}$. Los pares con índice impar son soluciones de la ecuación de Pell. Para $n=8$ y $n=11$ se obtiene $(x_8,y_8)=(265,153)$ y $(x_{11},y_{11})=(1351,780)$. En el tratado de Arquímedes, *La medida del círculo*, aparece la desigualdad:

$$\frac{265}{153}<\sqrt{3}<\frac{1351}{780}.$$

Esto apunta a que Arquímedes podía estar familiarizado con algún método para construir soluciones de esta ecuación.

Sin embargo, es la matemática hindú la que más información aporta sobre el conocimiento de la ecuación de Pell en la antigüedad. Los documentos que han llegado a nuestros días indican que la estudiaron con mayor profundidad que los griegos. El matemático y astrónomo hindú Brahmagupta (598-660 d.C.) nos deja esta curiosa cita: *Cualquiera capaz de resolver* $x^2 - 92y^2 = 1$ *en el plazo de un año, es un matemático.* A él se debe la siguiente identidad, que lleva su nombre:

$$(a_1^2 - db_1^2)(a_2^2 - db_2^2) = (a_1a_2 + db_1b_2)^2 - d(a_1b_2 + b_1a_2)^2.$$

Esta identidad permite operar soluciones para producir una nueva. Usando esto, Brahmagupta construyó soluciones de manera ingeniosa. Por ejemplo, para $x^2 - 92y^2 = 1$ calcula del siguiente modo. Parte de $8 = 10^2 - 92 \cdot 1^2$. Opera con la identidad y llega a $64 = 192^2 - 92 \cdot 20^2$. Divide por 64 y obtiene $1 = 24^2 - 92 \cdot (5/2)^2$. Opera de nuevo esta solución (racional) y obtiene $1 = 1151^2 - 92 \cdot 120^2$.

Bhaskara II (1114-1185 d.C.) perfeccionó las ideas de Brahmagupta e inventó un método de resolución llamado *Chakravala*[5]. Se basa en la siguiente identidad, conocida como lema de Bhaskara II:

$$\text{Si } a^2 - db^2 = k \text{ y } m \in \mathbb{Q}, \text{ entonces } \left(\frac{ma + db}{k}\right)^2 - d\left(\frac{a + bm}{k}\right)^2 = \frac{m^2 - d}{k}.$$

Mediante este método encontró la solución $(1766319049, 226153980)$ de la ecuación $x^2 - 61y^2 = 1$. En este método ya están presentes varias de las ideas que permitieron resolver finalmente la ecuación de Pell. Para más información véase [W2].

En los tiempos modernos, la ecuación de Pell, como muchas otras cuestiones de teoría de números, reaparece en el trabajo del matemático y jurista francés Pierre de Fermat (1607-1665). En 1657 propone el siguiente reto:

> Dado un número cualquiera que no es un cuadrado, existe un número infinito de cuadrados tal que, si el cuadrado es multiplicado por el número dado y la unidad es añadida al producto, el resultado es un cuadrado.

A este desafío añade su interés por tres casos particulares: $d = 109, 149, 433$. Curiosamente, los dos primeros son los más complejos entre todos los d menores que 200. No sabemos si Fermat disponía o no de un método para resolver la ecuación de Pell.

Los matemáticos ingleses John Wallis (1606-1713) y William Brouncker (1620-1684) recogieron el testigo de Fermat. De la correspondencia entre los tres aflora una técnica de resolución atribuida a Brouncker. Con ella Brouncker resolvió el caso $d = 433$. Un logro notable puesto que el valor de y en la solución posee 19 dígitos.

La técnica de Brouncker llegó más tarde a manos de Leonhard Euler (1707-1783). Él estableció su relación con las fracciones continuas y vaticinó que estas proporcionarían un algoritmo eficiente para resolver la ecuación de Pell. Sin embargo, no fue él, sino Joseph-Louis Lagrange (1736-1813) el que puso final a una larga búsqueda. En un trabajo de 1768 prueba, usando fracciones continuas, que la ecuación de Pell posee infinitas soluciones, presenta el algoritmo que empleamos actualmente y demuestra correctamente que funciona. La tecnología matemática necesaria para la resolución del problema del ganado de Arquímedes estaba finalmente disponible.

[5] En sánscrito, *chakra* significa rueda. Aquí se refiere al carácter cíclico del método.

En 1880 el matemático alemán August Amthor (1845-1916) pasó a contarse «*entre los sabios*» y se «*coronó de gloria habiendo sido declarado perfecto en esta especie de sabiduría*». En [1] resuelve el problema del ganado casi 2000 años después de haber sido propuesto. Amthor redujo primero con astucia la resolución de la ecuación 1 a la de $x^2 - 4729494y^2 = 1$. (Véase la página 44.) Con obstinación y paciencia calculó la expansión en fracciones continuas simples de $\sqrt{4729494}$, que resultó tener longitud 92. Luego, deshizo el camino en la reducción, ayudándose de argumentos teóricos, y volvió a sumergirse en un mar de cálculos. La solución más pequeña apareció, efectivamente, en forma de «*número imponente*». Un gigante de 206545 dígitos, del que calculó los cuatro primeros. Eran: 7766. El cuarto dígito resultaría ser incorrecto.

En 1895 Bell publica en [3] una solución más detallada. Calcula los primeros 31 dígitos y los últimos 12 del número de reses de cada color[6]. La solución completa fue calculada por primera vez, con ayuda del ordenador, en 1965 por Williams, German y Zarnke. Exponen sus resultados en [23]. La solución fue publicada íntegramente por primera vez en 1981 en [14]. Ocupa 12 páginas a tamaño reducido. Es, abreviadamente:

$$77602714\ldots237983357\ldots55081800.$$

Cada punto indica la omisión de 34420 dígitos. En internet puede verse completa en [W4]. Ilan Vardi da en [21] esta otra representación de este astronómico número:

$$\left\lceil \frac{25194541}{184119152}\left(109931986732829734979866232821433543901088049 + 50549485234315033074477819735540408986340\sqrt{4729494}\right)^{4658}\right\rceil.$$

Aquí $\lceil \cdot \rceil$ denota la parte entera por exceso. Una representación más abreviada es dada por Hendrik Lenstra en [12]. La reproducimos en la página 46. Antti Nygrén resuelve el problema en [16] con una aproximación diferente que no usa fracciones continuas.

Tras la introducción a los contenidos que estudiaremos, describimos ahora cómo está organizado este trabajo. Se divide en cuatro capítulos y un apéndice. El primer capítulo contiene un análisis preliminar de la ecuación de Pell. Esta ecuación se comprende mejor recurriendo al anillo $\mathbb{Z}[\sqrt{d}\,]$, formado por números reales del tipo $a + b\sqrt{d}$ con $a, b \in \mathbb{Z}$. Dos nociones importantes en este anillo son la de norma y conjugado. Mostraremos en la proposición 1.2 que existe una biyección entre el conjunto $\mathcal{S}$ de soluciones de la ecuación y el conjunto $\mathcal{U}$ de elementos inversibles en $\mathbb{Z}[\sqrt{d}\,]$ con norma 1. Cada solución (a, b) se identifica con $a + b\sqrt{d}$. La forma conocida de operar soluciones corresponde entonces al hecho de que $\mathcal{U}$ es un grupo abeliano. Por otro lado, toda solución no trivial, es decir, distinta de $(\pm 1, 0)$, se obtiene por cambio de signo de una solución positiva (ambas incógnitas toman valores positivos). En el teorema 1.7 probaremos que la ecuación de Pell admite una solución no trivial. Esto implicará la existencia de una solución mínima positiva, denominada solución fundamental. Finalmente, veremos en el teorema 1.10 que toda solución positiva se obtiene mediante potencias de la solución fundamental. Así el problema de hallar todas las soluciones de la ecuación de Pell se reduce al de calcular la solución fundamental.

La teoría de fracciones continuas facilita las herramientas necesarias para el cálculo de la solución fundamental de la ecuación de Pell. A esta teoría dedicaremos el segundo capítulo, que constituye el núcleo principal de este trabajo, abarcando casi la mitad

[6] Incluimos el artículo en la sección A.8 del apéndice. Allí menciona que los cálculos fueron realizados entre 1889 y 1893 por el club matemático de Hillsboro (Illinois, EEUU) formado por Bell, Fish y Richard.

del mismo. Nuestra exposición de este tema sigue la ruta estándar marcada por los manuales básicos de referencia, como [10], [17], [15], [18] y [6]. Este segundo capítulo consta de seis secciones. En la primera se presentará la noción de fracción continua simple, única que usaremos en este trabajo, y se distinguirá entre fracción continua finita e infinita. En la segunda sección veremos que todo número racional se expresa de manera única como una fracción continua finita mediante el algoritmo de Euclides.

La tercera sección introduce una pieza fundamental dentro de esta teoría: los convergentes asociados a una fracción continua. Se muestra aquí que forman una sucesión convergente (de ahí su nombre) cuyo límite es el valor de la fracción continua. En la cuarta sección se prueba que, en las fracciones continuas infinitas, este límite es un número irracional, teorema 2.12. Y también que, recíprocamente, teorema 2.13, todo número irracional ξ se puede expresar de manera única como una fracción continua infinita y simple (expresión abreviada como EFCS de ξ). Esto da un método para aproximar un número irracional por números racionales. En la quinta sección se establecen cotas para el error cometido al realizar tal aproximación. Aquí se demostrará el teorema 2.18, que será clave en la resolución de la ecuación de Pell. Este teorema da una cota que sirve de condición suficiente para reconocer una aproximación racional de un número irracional como un convergente de su EFCS. De él deduciremos que si (a, b) es una solución positiva de $x^2 - dy^2 = 1$, entonces $\frac{a}{b}$ es un convergente de la EFCS de $\sqrt{d}$. Así, deberemos buscar la solución fundamental entre los convergentes de la EFCS de $\sqrt{d}$.

La sexta sección se ocupa del estudio de la EFCS de un número irracional cuadrático. Aquí surgirá la noción de fracción continua periódica. Veremos que un número irracional cuadrático queda caracterizado por la propiedad de que su EFCS es periódica. Presentaremos un algoritmo, sencillo de implementar en ordenador, para calcular la EFCS de este tipo de números. Terminaremos este capítulo con otro resultado clave en la resolución de la ecuación de Pell, el teorema de Lagrange, teorema 2.22, que revela un vínculo entre la longitud del periodo de la EFCS de $\sqrt{d}$ y $\lfloor \sqrt{d} \rfloor$.

El tercer capítulo culmina todo el trabajo realizado previamente. Presentaremos aquí la resolución completa de la ecuación de Pell, que aparece en el teorema 3.4. Sea ℓ el periodo de la EFCS de $\sqrt{d}$ y $\left\{\frac{p_n}{q_n}\right\}_{n\in\mathbb{N}}$ su sucesión de convergentes. Veremos que la solución fundamental vendrá dada por $(p_{\ell-1}, q_{\ell-1})$ si ℓ es par y $(p_{2\ell-1}, q_{2\ell-1})$ si ℓ es impar. Acabaremos este capítulo con la resolución del problema del ganado de Arquímedes.

En el cuarto capítulo nos ocupamos del apartado conclusiones requerido en la normativa de trabajos de fin de estudios de la Facultad de Ciencias Experimentales. Aquí reflexionamos sobre qué ha supuesto la realización de este trabajo en nuestra formación como estudiante de matemáticas. Mencionamos también varios resultados y aplicaciones que hemos estudiado sobre fracciones continuas y ecuación de Pell, pero que no hemos incluido por la limitación a 50 páginas exigida.

Por último, el apéndice contiene:

- Una imagen del manuscrito hallado en la biblioteca de Wolfenbüttel y la transcripción de Lessing del mismo de 1773.
- Una tabla con las soluciones fundamentales de la ecuación de Pell para $d < 100$.
- La implementación en *Mathematica* de los algoritmos expuestos en el trabajo; en particular, el usado para calcular la solución fundamental.
- Los cálculos realizados para la resolución del problema del ganado.
- El artículo de Bell de 1895.

1 Análisis preliminar de la ecuación

No basta examinar, hay que contemplar:
impregnemos de emoción y simpatía las cosas observadas,
hagámoslas nuestras, tanto por el corazón como por la inteligencia.
Sólo así nos entregarán su secreto.

Santiago Ramón y Cajal (1852-1934),
histólogo español.

En este capítulo realizamos un análisis preliminar de la ecuación de Pell. Explicaremos la estrecha relación existente entre esta ecuación y el anillo $\mathbb{Z}[\sqrt{d}\,]$. Demostraremos que la ecuación de Pell siempre admite una solución mínima positiva, a la que se denomina solución fundamental, y que cualquier otra solución positiva es potencia de ella. De esta manera, el problema de calcular todas las soluciones de la ecuación de Pell se reducirá al de calcular la solución fundamental.

1.1 Observaciones iniciales

Sea $d \in \mathbb{N}$. Supongamos que d no es un cuadrado[1]. La *ecuación de Pell*[2] es la ecuación diofántica:

$$x^2 - dy^2 = 1. \tag{1.1}$$

Como dijimos antes, el adjetivo diofántico indica que sólo nos interesan las soluciones enteras, es decir, valores enteros de x e y que cumplan la igualdad. A menudo escribiremos simplemente soluciones, sobreentendiendo su condición de enteras.

A primera vista nos damos cuenta de lo siguiente:

- El par $(1,0)$ es solución. La llamaremos *solución trivial*;
- No hay soluciones en las que x tome el valor 0;
- De cada solución (a,b), con $b \neq 0$, surgen otras tres por cambio de signo: $(-a,b)$, $(a,-b)$ y $(-a,-b)$;
- Las soluciones $(\pm 1, 0)$ son las únicas en las que y toma el valor 0.

Al igual que ocurre con otras ecuaciones diofánticas[3], esta ecuación se entiende mejor recurriendo a un anillo apropiado que sea una extensión de $\mathbb{Z}$. La factorización

$$1 = x^2 - dy^2 = \left(x + y\sqrt{d}\right)\left(x - y\sqrt{d}\right) \tag{1.2}$$

[1] Si d es un cuadrado, las únicas soluciones de la ecuación de Pell son $(\pm 1, 0)$. Supongamos que $d = c^2$ y $(a,b) \in \mathbb{Z} \times \mathbb{Z}$ es una solución. Entonces, $1 = a^2 - db^2 = a^2 - c^2b^2 = (a+cb)(a-cb)$. Hay dos posibilidades: $a + bc = a - bc = 1$ o $a + bc = a - bc = -1$. La primera da $(a,b) = (1,0)$ y la segunda $(a,b) = (-1,0)$.

[2] John Pell (1611-1685), matemático inglés. La mayoría de fuentes afirman que Euler atribuyó esta ecuación a Pell incorrectamente al referirse al trabajo de Brouncker. En la biografía de Pell en [W5] se presenta una prueba de quizá Euler no estaba equivocado.

[3] El anillo $\mathbb{Z}[i]$ de enteros gaussianos permite probar que las soluciones de la ecuación $y^2 + 4 = x^3$ son $(x,y) = (2, \pm 2)$ y $(x,y) = (5, \pm 11)$, véase [19, Teorema 4.20]. La demostración de que las únicas soluciones de $y^2 + 2 = x^3$ son $(x,y) = (3, \pm 5)$ se realiza en $\mathbb{Z}[\sqrt{-2}]$, véase [19, páginas 80-81]. Para el teorema de Ramanujan-Nagell, que da las soluciones de $x^2 + 7 = 2^n$, se trabaja en $\mathbb{Z}\left[\frac{1+\sqrt{-7}}{2}\right]$, véase [19, Teorema 4.21]. La clave de la demostración en todos estos ejemplos es que el anillo involucrado tiene la propiedad de factorización única.

sugiere el anillo $\mathbb{Z}[\sqrt{d}\,]$, cuyos elementos son números reales de la forma $a+b\sqrt{d}$ con $a,b\in\mathbb{Z}$. Se suman y multiplican de forma habitual, lo que da las siguientes fórmulas:

- *Suma:* $(a+b\sqrt{d}\,)+(a'+b'\sqrt{d}\,)=(a+a')+(b+b')\sqrt{d}$;
- *Multiplicación:* $(a+b\sqrt{d}\,)(a'+b'\sqrt{d}\,)=(aa'+dbb')+(ab'+ba')\sqrt{d}$.

Como d no es un cuadrado, se tiene que $a+b\sqrt{d}=0$ si y sólo si $a=b=0$. Si $a+b\sqrt{d}=0$ y fuese $b\neq 0$, llegaríamos a que $\sqrt{d}$ sería racional pues $\sqrt{d}=-a/b$. Por tanto $b=0$ y, en consecuencia, $a=0$. Así que $a+b\sqrt{d}=a'+b'\sqrt{d}$ si y sólo si $a=a'$ y $b=b'$.

Sea $(a,b)\in\mathbb{Z}\times\mathbb{Z}$. La igualdad 1.2 expresa que (a,b) es solución de la ecuación de Pell si y sólo si $a+b\sqrt{d}$ es inversible y su inverso es $a-b\sqrt{d}$. Esto lleva a fijar nuestra atención en los elementos inversibles de $\mathbb{Z}[\sqrt{d}\,]$. Para describir tales elementos necesitamos introducir dos conceptos: el conjugado y la norma.

Sea $z=a+b\sqrt{d}\in\mathbb{Z}[\sqrt{d}\,]$:

- Llamaremos *conjugado* de z, denotado por $\overline{z}$, al número $a-b\sqrt{d}$. Se comprueba fácilmente que la aplicación conjugación $\overline{\cdot}:\mathbb{Z}[\sqrt{d}\,]\to\mathbb{Z}[\sqrt{d}\,]$ es biyectiva y preserva la suma y el producto; es decir, es un automorfismo de anillos de $\mathbb{Z}[\sqrt{d}\,]$.
- La *norma* de z, denotada por $\mathrm{N}(z)$, es el número entero a^2-db^2. La factorización $a^2-db^2=(a+b\sqrt{d})(a-b\sqrt{d})$ toma entonces la forma $\mathrm{N}(z)=z\overline{z}$. La aplicación norma $\mathrm{N}:\mathbb{Z}[\sqrt{d}\,]\to\mathbb{Z}$ es multiplicativa, es decir, $\mathrm{N}(zz')=\mathrm{N}(z)\mathrm{N}(z')$. Esto se deduce de que la conjugación es compatible con la multiplicación:

  $$\mathrm{N}(zz')=(zz')(\overline{zz'})=(zz')(\overline{z}\,\overline{z'})=(z\overline{z})(z'\overline{z'})=\mathrm{N}(z)\mathrm{N}(z').$$

  Poniendo $z'=a'+b'\sqrt{d}$ y usando la fórmula para la multiplicación, vemos que la anterior igualdad es precisamente la identidad de Brahmagupta:

  $$(a^2-db^2)(a'^2-db'^2)=(aa'+dbb')^2-d(ab'+ba')^2. \tag{1.3}$$

Ya podemos afirmar:

Lema 1.1. *El número $z=a+b\sqrt{d}\in\mathbb{Z}[\sqrt{d}\,]$ es inversible si y sólo si $\mathrm{N}(z)=\pm 1$. Además, si z es inversible, entonces*

$$z^{-1}=\frac{1}{\mathrm{N}(z)}\,\overline{z}. \tag{1.4}$$

Demostración. Supongamos que z es inversible. Sea $w\in\mathbb{Z}[\sqrt{d}\,]$ tal que $zw=1$. Aplicamos la norma a esta igualdad y usamos que es multiplicativa. Queda:

$$1=\mathrm{N}(1)=\mathrm{N}(zw)=\mathrm{N}(z)\mathrm{N}(w).$$

Como $\mathrm{N}(z),\mathrm{N}(w)\in\mathbb{Z}$, debe ser $\mathrm{N}(z)=\pm 1$.

Recíprocamente, si $\mathrm{N}(z)=\pm 1$, entonces $\dfrac{1}{\mathrm{N}(z)}\,\overline{z}\in\mathbb{Z}[\sqrt{d}\,]$ y además:

$$\left(\frac{1}{\mathrm{N}(z)}\,\overline{z}\right)z=\frac{1}{\mathrm{N}(z)}\,\overline{z}z=\frac{1}{\mathrm{N}(z)}\,\mathrm{N}(z)=1.$$

Esto prueba también la fórmula para el inverso. ∎

Lo anterior tiene las siguientes consecuencias para la ecuación de Pell.

Proposición 1.2. *La asignación $(a,b) \mapsto a + b\sqrt{d}$ establece una biyección entre el conjunto de soluciones de la ecuación de Pell y los elementos inversibles de $\mathbb{Z}[\sqrt{d}]$ con norma 1.*

Demostración. Basta usar el lema previo y que $\mathrm{N}(a + b\sqrt{d}) = a^2 - db^2$. ■

Proposición 1.3. *El conjunto de soluciones de la ecuación de Pell tiene estructura de grupo abeliano con la operación definida por*

$$(a,b) \cdot (a',b') = (aa' + dbb', ab' + ba'). \tag{1.5}$$

El elemento neutro es la solución trivial $(1,0)$ y el inverso de (a,b) es $(a,-b)$.

Demostración. Sea $\mathcal{U}$ el conjunto de elementos inversibles de $\mathbb{Z}[\sqrt{d}]$, que es un grupo abeliano bajo la multiplicación. Llamemos $\mathcal{V}$ al subconjunto de $\mathcal{U}$ formado por los elementos con norma 1. Se tiene que $\mathcal{V} \neq \emptyset$ pues $1 \in \mathcal{V}$. Como la norma es multiplicativa, dados $z, z' \in \mathcal{V}$, se tiene $\mathrm{N}(zz') = \mathrm{N}(z)\mathrm{N}(z') = 1$. Además, $z^{-1} = \overline{z}$ según (1.4), luego $\mathrm{N}(z^{-1}) = 1$. Esto muestra que $\mathcal{V}$ es un subgrupo de $\mathcal{U}$. Podemos llevar la estructura de grupo de $\mathcal{V}$ al conjunto de soluciones de la ecuación de Pell a través de la biyección anterior. Pongamos $z = a + b\sqrt{d}$ y $z' = a' + b'\sqrt{d}$. Su producto es:

$$zz' = (aa' + dbb') + (ab' + ba')\sqrt{d}.$$

El elemento neutro es $1 = 1 + 0\sqrt{d}$ y el inverso de z es $\overline{z} = a - b\sqrt{d}$. ■

Observación 1.4. *Aunque aquí sólo trabajaremos con soluciones enteras, hemos de reseñar que la ley de grupo 1.5 es válida para el conjunto de todos los puntos de la hipérbola $\mathcal{H}$ de ecuación $x^2 - dy^2 = 1$. Esta ley además se puede interpretar geométricamente. Sean $P_1(x_1, y_1)$ y $P_2(x_2, y_2)$ dos puntos de $\mathcal{H}$. Consideremos la recta determinada por ellos. Sea r la recta paralela a esta que pasa por el punto $E(1,0)$ de $\mathcal{H}$. El punto $P_1 \cdot P_2$ con coordenadas $(x_1x_2 + dy_1y_2, x_1y_2 + y_1x_2)$ es el otro punto de corte de r y $\mathcal{H}$.*

1.2 La solución fundamental

Una vez establecida la relación entre las soluciones de la ecuación de Pell y los elementos inversibles de $\mathbb{Z}[\sqrt{d}]$, nuestro siguiente objetivo es demostrar que esta ecuación siempre admite una solución no trivial. Necesitaremos antes dos resultados técnicos:

Lema 1.5. *Sean $d, t \in \mathbb{Z}^+$, donde d no es un cuadrado. Existen $a, b \in \mathbb{Z}$ tales que:*

$$0 < \left| a - b\sqrt{d} \right| < \frac{1}{t} \leq \frac{1}{|b|}.$$

Demostración. Para cada $b \in \mathbb{Z}$ con $0 \leq b \leq t$ consideremos $a = \lceil b\sqrt{d} \rceil$. Entonces, $0 < a - b\sqrt{d} < 1$. Partimos el intervalo $]0,1[$ en t subintervalos de longitud $1/t$. Como hay $t+1$ números del tipo $a - b\sqrt{d}$ y t subintervalos, por el principio del palomar, dos de estos números, digamos $a_1 - b_1\sqrt{d}$ y $a_2 - b_2\sqrt{d}$, caen en el mismo subintervalo. Estos números son distintos ya que b_1 y b_2 lo son. Al pertenecer al mismo subintervalo, distan menos de $1/t$. Es decir,

$$0 < \left| (a_1 - a_2) - (b_1 - b_2)\sqrt{d} \right| < \frac{1}{t}.$$

Del mismo modo, como $0 \leq b_1, b_2 \leq t$ y $b_1 \neq b_2$, se tiene $0 < |b_1 - b_2| \leq t$. Por tanto,

$$0 < \left|(a_1 - a_2) - (b_1 - b_2)\sqrt{d}\right| < \frac{1}{t} \leq \frac{1}{|b_1 - b_2|}.$$

La afirmación se obtiene tomando $a = a_1 - a_2$ y $b = b_1 - b_2$. ■

Proposición 1.6. *Existen infinitos pares $(a, b) \in \mathbb{Z} \times \mathbb{Z}$ tales que*

$$0 < \left|a - b\sqrt{d}\right| < \frac{1}{|b|}.$$

Demostración. Consideremos el conjunto

$$\mathcal{C} = \left\{(a, b) \in \mathbb{Z} \times \mathbb{Z} \,:\, 0 < \left|a - b\sqrt{d}\right| < \frac{1}{|b|}\right\}.$$

Por el lema 1.5, se tiene que $\mathcal{C} \neq \emptyset$. Supongamos, razonando por reducción al absurdo, que $\mathcal{C}$ es finito. Podemos elegir pues $M \in \mathbb{Z}^+$ tal que

$$\frac{1}{M} < \text{mín}\left\{\left|a - b\sqrt{d}\right| \,:\, (a, b) \in \mathcal{C}\right\}.$$

Aplicamos el lema 1.5 para $t = M$. Existirán $a', b' \in \mathbb{Z}$ que cumplen:

$$\left|a' - b'\sqrt{d}\right| < \frac{1}{M} \leq \frac{1}{|b'|}.$$

Esta desigualdad contradice nuestra elección de M pues, por un lado, significa que $(a', b') \in \mathcal{C}$, y, por otro, que $\left|a' - b'\sqrt{d}\right|$ es menor que $1/M$. Por tanto, $\mathcal{C}$ es infinito. ■

Ya estamos en condiciones de demostrar el primer teorema de esta sección:

Teorema 1.7. *La ecuación de Pell posee al menos una solución no trivial.*

Demostración. Seguimos trabajando con el conjunto $\mathcal{C}$ anterior. Tomemos $(u, v) \in \mathcal{C}$ arbitrario. Usando la desigualdad triangular, obtenemos:

$$0 < \left|u + v\sqrt{d}\right| = \left|u - v\sqrt{d} + 2v\sqrt{d}\right| \leq \left|u - v\sqrt{d}\right| + \left|2v\sqrt{d}\right| < \frac{1}{|v|} + 2|v|\sqrt{d}.$$

Con esto, calculamos otra vez:

$$0 < \left|u^2 - dv^2\right| = \left|u - v\sqrt{d}\right|\left|u + v\sqrt{d}\right| < \frac{1}{|v|}\left(\frac{1}{|v|} + 2|v|\sqrt{d}\right) = \frac{1}{v^2} + 2\sqrt{d} \leq 1 + 2\sqrt{d}.$$

Luego, $|u^2 - dv^2|$ es un número natural entre 0 y $1 + 2\sqrt{d}$.

El conjunto $\mathcal{C}$ es infinito por la proposición 1.6. Por otro lado, hay una cantidad finita de números naturales menores que $1 + 2\sqrt{d}$. Por el principio del palomar, existirán $n \in \mathbb{N}$ con $0 < n < 1 + 2\sqrt{d}$ e infinitos pares $(a, b) \in \mathcal{C}$ tales que $|a^2 - db^2| = n$. Existen pues infinitos pares $(a, b) \in \mathcal{C}$ tales que $a^2 - db^2 = n$ o $a^2 - db^2 = -n$. Reducimos módulo n las componentes de los pares. Una vez más, la infinitud de pares y el principio del palomar aseguran que existen $(a_1, b_1), (a_2, b_2) \in \mathcal{C}$ tales que $a_1 \equiv_n a_2, b_1 \equiv_n b_2, a_1 \neq \pm a_2$ y $b_1 \neq \pm b_2$.

Aplicando la identidad 1.3, obtenemos:

$$n^2 = \left(a_1^2 - db_1^2\right)\left(a_2^2 - db_2^2\right) = (a_1a_2 - db_1b_2)^2 - d(a_1b_2 - a_2b_1)^2.$$

Como $a_1 \equiv_n a_2$ y $b_1 \equiv_n b_2$, podemos afirmar que n divide a $a_1b_2 - a_2b_1$. Junto a la igualdad anterior, esto da que n divide a $a_1a_2 - db_1b_2$. Entonces,

$$1 = \left(\frac{a_1a_2 - db_1b_2}{n}\right)^2 - d\left(\frac{a_1b_2 - a_2b_1}{n}\right)^2,$$

y los números dentro de los paréntesis son ambos enteros. Hemos conseguido así una solución entera de la ecuación $x^2 - dy^2 = 1$.

Veamos finalmente que esta solución es distinta de $(\pm 1, 0)$. Supongamos que fuesen iguales. Entonces, $a_1b_2 - a_2b_1 = 0$ y $a_1a_2 - db_1b_2 = \pm n$. Multiplicamos esta igualdad por b_1. Queda: $a_1a_2b_1 - db_1^2b_2 = \pm nb_1$. Sustituimos aquí a_2b_1 por a_1b_2 y queda $(a_1^2 - db_1^2)b_2 = \pm nb_1$. Como $a_1^2 - db_1^2 = \pm n$, llegamos a $b_2 = \pm b_1$, lo que contradice la elección de (a_1, b_1) y (a_2, b_2). Por tanto, la solución antes encontrada no es trivial. ■

El teorema anterior da sentido a la siguiente definición: una solución (a, b) de la ecuación de Pell es *positiva* si $a, b > 0$. *Llamaremos $\mathcal{S}$ al conjunto de soluciones de la ecuación de Pell y $\mathcal{S}^+$ al subconjunto de soluciones positivas.* Seguidamente veremos que en $\mathcal{S}$ hay un orden natural para el que $\mathcal{S}^+$ posee mínimo. Identificando el par (a, b) con el número real $a + b\sqrt{d}$, inducimos en $\mathcal{S}$ el orden de los números reales. Denotemos a este orden por $\preceq$. Dados $(a, b), (a', b') \in \mathcal{S}$, tenemos $(a, b) \preceq (a', b')$ si $a + b\sqrt{d} \leq a' + b'\sqrt{d}$. Puesto que los números reales están totalmente ordenados, la relación $\preceq$ establece un orden total en $\mathcal{S}$. En esta argumentación no hemos usado que (a, b) sea solución de la ecuación, es decir, que $a^2 - db^2 = 1$. Añadiendo esta condición podemos afirmar más:

Lema 1.8. *Se tiene que $(a, b) \preceq (a', b')$ si y sólo si $a \leq a'$ y $b \leq b'$.*

Demostración. Es claro que si $a \leq a'$ y $b \leq b'$, entonces $a + b\sqrt{d} \leq a' + b'\sqrt{d}$. Recíprocamente, supongamos que $(a, b) \preceq (a', b')$, es decir, que $a + b\sqrt{d} \leq a' + b'\sqrt{d}$. Como (a, b) y (a', b') son soluciones de la ecuación, los inversos de $a + b\sqrt{d}$ y $a' + b'\sqrt{d}$ son $a - b\sqrt{d}$ y $a' - b'\sqrt{d}$ respectivamente. Entonces:

$$a' - b'\sqrt{d} = \frac{1}{a' + b'\sqrt{d}} \leq \frac{1}{a + b\sqrt{d}} = a - b\sqrt{d}.$$

Sumando esta desigualdad y

$$-a' - b'\sqrt{d} \leq -a - b\sqrt{d}$$

resulta $-2b'\sqrt{d} \leq -2b\sqrt{d}$. De aquí, $b \leq b'$. La desigualdad inicial da ahora $a \leq a'$. ■

Sea $\mathcal{S}_x^+$ el conjunto formado por las componentes en x de los elementos de $\mathcal{S}^+$. Gracias a que $\mathbb{N}$ está bien ordenado, podemos tomar $(u, v) \in \mathcal{S}^+$ tal que $u = \text{mín}(\mathcal{S}_x^+)$. Como el orden en $\mathcal{S}$ es total, tenemos $(u, v) = \text{mín}(\mathcal{S}^+)$. Así que existe una solución mínima positiva de la ecuación de Pell. Nótese que, según el lema precedente, hubiésemos obtenido la misma solución mínima mediante el conjunto $\mathcal{S}_y^+$ de componentes en y.

Definición 1.9. *La solución mínima positiva de la ecuación de Pell se denomina solución fundamental.*

El siguiente teorema muestra la importancia de esta solución. Afirma que todas las soluciones positivas se pueden generar a partir de ella mediante el producto en (1.5).

Teorema 1.10. *Consideremos la ecuación de Pell*

$$x^2 - dy^2 = 1. \tag{1.6}$$

Sea (x_1, y_1) su solución fundamental. Entonces, toda solución entera y positiva de (1.6) es de la forma (x_n, y_n), donde x_n e y_n están definidos por la siguiente fórmula en $\mathbb{Z}[\sqrt{d}]$:

$$x_n + y_n\sqrt{d} = \left(x_1 + y_1\sqrt{d}\right)^n, \quad n \in \mathbb{N}. \tag{1.7}$$

Esta expresión se puede describir recursivamente como:

$$\begin{cases} x_{n+1} = x_n x_1 + d y_n y_1, \\ y_{n+1} = x_n y_1 + y_n x_1, \qquad n \in \mathbb{N}. \end{cases} \tag{1.8}$$

Demostración. Realizamos la demostración en dos pasos:

(1) *El par (x_n, y_n) definido por la fórmula 1.7 es solución.* Para establecer esta afirmación, observamos primero que

$$x_n - y_n\sqrt{d} = \left(x_1 - y_1\sqrt{d}\right)^n$$

porque la conjugación en $\mathbb{Z}[\sqrt{d}]$ es un homomorfismo de anillos. Ahora operamos del siguiente modo:

$$\begin{aligned} x_n^2 - dy_n^2 &= \left(x_n + y_n\sqrt{d}\right)\left(x_n - y_n\sqrt{d}\right) \\ &= \left(x_1 + y_1\sqrt{d}\right)^n \left(x_1 - y_1\sqrt{d}\right)^n \\ &= \left(\left(x_1 + y_1\sqrt{d}\right)\left(x_1 - y_1\sqrt{d}\right)\right)^n \\ &= \left(x_1^2 - dy_1^2\right)^n \\ &= 1. \end{aligned}$$

Aquí hemos usado respectivamente: la definición de (x_n, y_n); la observación anterior; que el producto en $\mathbb{Z}[\sqrt{d}]$ es conmutativo y que (x_1, y_1) es solución de (1.6).

(2) *Toda solución entera y positiva (a, b) viene dada por la fórmula 1.7.* Llamemos $\mathcal{G}$ al conjunto de soluciones $\{(x_n, y_n) : n \in \mathbb{N}\}$ generadas por (1.7). Supongamos, razonando por reducción al absurdo, que $(a, b) \notin \mathcal{G}$. Los números reales $x_1 + y_1\sqrt{d}$ y $a + b\sqrt{d}$ son mayores que 1. Por ser (x_1, y_1) la solución mínima positiva, tenemos:

$$1 < x_1 + y_1\sqrt{d} < a + b\sqrt{d}.$$

Definimos el conjunto

$$\mathcal{I} = \left\{ r \in \mathbb{N} : a + b\sqrt{d} < \left(x_1 + y_1\sqrt{d}\right)^r \right\}.$$

Este conjunto no es vacío porque la sucesión $\left\{\left(x_1+y_1\sqrt{d}\right)^n\right\}_{n\in\mathbb{N}}$ diverge. Así que $\mathcal{I}$ posee mínimo. Pongamos $m=\min(\mathcal{I})-1$. Entonces:

$$\left(x_1+y_1\sqrt{d}\right)^m < a+b\sqrt{d} < \left(x_1+y_1\sqrt{d}\right)^{m+1}. \tag{1.9}$$

Nótese que las desigualdades son estrictas. Si se diese alguna igualdad, (a,b) sería una solución de la forma (x_n,y_n) y pertenecería a $\mathcal{G}$, en contra de nuestra hipótesis. Puesto que $x_1-y_1\sqrt{d}$ es el inverso de $x_1+y_1\sqrt{d}$, sabemos que:

$$\frac{1}{\left(x_1+y_1\sqrt{d}\right)^m} = \left(x_1-y_1\sqrt{d}\right)^m.$$

Multiplicamos (1.9) por $\left(x_1-y_1\sqrt{d}\right)^m$. Usando lo anterior, resulta:

$$1 < \left(a+b\sqrt{d}\right)\left(x_1-y_1\sqrt{d}\right)^m < x_1+y_1\sqrt{d}.$$

Sean $u,v\in\mathbb{Z}$ tales que:

$$u+v\sqrt{d} = \left(a+b\sqrt{d}\right)\left(x_1-y_1\sqrt{d}\right)^m.$$

Aplicamos a estos elementos la conjugación en $\mathbb{Z}\left[\sqrt{d}\right]$. Por ser un homomorfismo de anillos da:

$$u-v\sqrt{d} = \left(a-b\sqrt{d}\right)\left(x_1+y_1\sqrt{d}\right)^m.$$

Ahora calculamos como sigue:

$$\begin{aligned} u^2-dv^2 &= \left(u+v\sqrt{d}\right)\left(u-v\sqrt{d}\right) \\ &= \left(a+b\sqrt{d}\right)\left(x_1-y_1\sqrt{d}\right)^m\left(a-b\sqrt{d}\right)\left(x_1+y_1\sqrt{d}\right)^m \\ &= \left(a^2-db^2\right)\left(x_1^2-dy_1^2\right)^m \\ &= 1. \end{aligned}$$

Esto prueba que (u,v) es una solución entera de la ecuación 1.6. Vamos a comprobar que además es positiva. La línea anterior a la definición de u y v nos dice que $1<u+v\sqrt{d}<x_1+y_1\sqrt{d}$. De aquí, sabiendo que $u-v\sqrt{d}$ es el inverso de $u+v\sqrt{d}$, se sigue que $0<u-v\sqrt{d}<1$. Las dos desigualdades juntas implican que u y v son positivos:

$$\begin{aligned} u &= \frac{1}{2}\left(u+v\sqrt{d}\right)+\frac{1}{2}\left(u-v\sqrt{d}\right) > 0+0 = 0, \\ v &= \frac{1}{2}\left(u+v\sqrt{d}\right)-\frac{1}{2}\left(u-v\sqrt{d}\right) > \frac{1}{2}-\frac{1}{2} = 0. \end{aligned}$$

Hemos hallado pues una solución (u,v) entera y positiva y menor que (x_1,y_1). Esto contradice la minimalidad de (x_1,y_1). Por tanto, $(a,b)\in\mathcal{G}$.

Finalmente, la descripción de (1.7) mediante la ley de recurrencia 1.8 se prueba fácilmente por inducción sabiendo cómo se multiplican los elementos de $\mathbb{Z}\left[\sqrt{d}\right]$. ■

La regla de recurrencia 1.8 se puede expresar matricialmente como:

$$\begin{pmatrix} x_{n+1} \\ y_{n+1} \end{pmatrix} = \begin{pmatrix} x_1 & dy_1 \\ y_1 & x_1 \end{pmatrix}\begin{pmatrix} x_n \\ y_n \end{pmatrix}, \qquad n\in\mathbb{N}.$$

Que (x_1,y_1) es solución de la ecuación de Pell se traduce en que la anterior matriz 2×2 tiene determinante 1.

Ejemplos 1.11. *Para los primeros valores de d la solución fundamental se calcula fácilmente por tanteo. Escribimos* $1 + dy^2 = x^2$ *y damos valores a y hasta encontrar uno para el que* $1 + dy^2$ *sea un cuadrado. La siguiente tabla muestra las* 5 *primeras soluciones positivas de la ecuación de Pell para* $d = 2, 3, 5, 6$*:*

$d \setminus i$	1	2	3	4	5
2	(3, 2)	(17, 12)	(99, 70)	(577, 408)	(3363, 2378)
3	(2, 1)	(7, 4)	(26, 15)	(97, 56)	(362, 209)
5	(9, 4)	(161, 72)	(2889, 1292)	(51841, 23184)	(930249, 416020)
6	(5, 2)	(49, 20)	(485, 198)	(4801, 1960)	(47525, 19402)

El teorema 1.10 y nuestras observaciones iniciales reducen el cálculo de todas las soluciones de la ecuación de Pell al cálculo de su solución fundamental. Para valores pequeños o particulares de d la estrategia de tanteo puede funcionar. Sin embargo, rápidamente se revela ineficaz. Por ejemplo, para $d = 13$, la solución fundamental es $(649, 180)$. Con la ayuda del ordenador podemos llevar más lejos esta aproximación por fuerza bruta, pero unos pocos experimentos con los valores adecuados también nos muestran su limitación.

La herramienta matemática apropiada para el cálculo de la solución fundamental de la ecuación de Pell son las fracciones continuas. La relación existente entre la solución fundamental de $x^2 - dy^2 = 1$ y el parámetro d se oculta en la expansión en fracciones continuas simples del radical $\sqrt{d}$. En el capítulo 2 desarrollaremos la parte de la teoría de fracciones continuas necesaria para hacer visible esta relación.

Notas bibliográficas

La presentación de la ecuación de Pell hecha en la introducción de este trabajo la hemos adaptado a nuestro formato de [9, Capítulo 2], dándole varios toques personales. Esa introducción es mucho más profusa y se la recomendamos al lector interesado en los aspectos históricos de la ecuación de Pell. Ahí se explica con detalle, por ejemplo, el método de la *Chakravala* y la técnica de resolución de Brouncker. Para la *Chakravala* recomendamos también [W2]. Otra fuente fundamental para la parte histórica es [22]. El Canto XII de *La Odisea* lo hemos extraído de la versión en línea [W3]. Para la exposición del problema del ganado de Arquímedes hemos utilizado [9, Sección 2.1], [12], [21], [3] y [W4].

En la elaboración de este primer capítulo hemos usado los libros [9, Sección 1.2], [15, Sección 7.8] y [19, Capítulo 4]. La observación sobre la interpretación geométrica del producto de soluciones de la ecuación de Pell aparece en [5, página 349].

Créditos fotográficos

La imagen de la pintura *Ulises y el rebaño de Helios, el dios Sol*, del pintor flamenco Johannes Stradanus, que aparece en la primera página, está tomada de [W1].

2 Fracciones continuas simples

Podríamos llamar al algoritmo de Euclides
el abuelo de todos los algoritmos, porque es el algoritmo
no trivial más antiguo que ha sobrevivido hasta nuestros días.

Donald Knuth (1938-),
matemático e informático estadounidense.

En este capítulo, que constituye el núcleo principal del trabajo, desarrollamos aquellos aspectos de la teoría de fracciones continuas necesarios para calcular la solución fundamental de la ecuación de Pell. Los objetivos que perseguimos son: explicar la noción de expansión en fracciones continuas simples (EFCS) de un número y definir los convergentes asociados; mostrar que la EFCS de un número irracional cuadrático es periódica y presentar el algoritmo para calcularla; dar un criterio que permite reconocer una aproximación racional de un número irracional como un convergente de su EFCS y, finalmente, demostrar el teorema de Lagrange, que desvela la forma de la EFCS de $\sqrt{d}$.

2.1 Notación, terminología e hipótesis

Presentamos nuestro objeto de estudio a través de la siguiente definición:

Definición 2.1. *Una fracción continua infinita y simple es una expresión algebraica de la forma*

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots}}} \tag{2.1}$$

donde $a_0, a_1, a_2, \ldots$ son números enteros, todos positivos excepto quizá a_0.

En la teoría general de fracciones continuas se permiten otros conjuntos para los valores de la sucesión $a_0, a_1, a_2, \ldots$ El adjetivo simple se emplea para referirse a la condición anterior. A lo largo de este trabajo trataremos principalmente con fracciones simples. (En algún punto abusaremos de la definición al permitir que algún a_i sea un número real.) La expresión 2.1 la denotaremos de manera abreviada como $[a_0; a_1, a_2, \ldots]$.

Podemos considerar un número finito de términos, en lugar de infinitos, y tendríamos una expresión de la forma

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots + \cfrac{1}{a_{n-2} + \cfrac{1}{a_{n-1} + \cfrac{1}{a_n}}}}}} \tag{2.2}$$

La llamaremos *fracción continua finita y simple* y escribiremos $[a_0; a_1, a_2, \ldots, a_n]$. Desde un punto de vista puramente formal, la fracción infinita $[a_0; a_1, a_2, \ldots]$ se puede ver como

el límite de las fracciones finitas $[a_0;a_1,a_2,\ldots,a_n]$ cuando n tiende a infinito. Esto lo justificaremos debidamente en la sección 2.3.

Sea $k \in \mathbb{N}$. Llamaremos a la fracción

$$[a_0;a_1,\ldots,a_k]$$

el *k-ésimo convergente* de la fracción continua infinita 2.1. Nos referiremos a

$$s_k := [a_k;a_{k+1},a_{k+2},\ldots]$$

como el *k-ésimo resto* de (2.1). Se tiene entonces la relación:

$$[a_0;a_1,a_2,\ldots] = [a_0;a_1,\ldots,a_k,s_k].$$

Nótese que esta igualdad y las definiciones anteriores también tienen sentido para la fracción finita 2.2 tomando $0 \leq k \leq n$. En ese caso, el resto s_k es finito.

2.2 Números racionales y fracciones continuas finitas

Toda fracción continua finita y simple es un número racional. En esta sección veremos que, recíprocamente, todo número racional se puede expresar de manera única como una fracción continua finita y simple. El procedimiento para el cálculo de esta expresión lo proporciona el algoritmo de Euclides. Comenzamos recordándolo.

Sean $a,b \in \mathbb{Z}$ con $b \neq 0$. El teorema de la división afirma que existen $q,r \in \mathbb{Z}$ únicos (cociente y resto) tales que $a = bq + r$ con $0 \leq r < |b|$. El algoritmo de Euclides calcula el máximo común divisor de a y b aplicando este teorema sucesivamente a divisor y resto hasta obtener un resto nulo. El último resto no nulo es precisamente $\mathrm{mcd}(a,b)$. Escribimos de la siguiente forma este proceso de divisiones sucesivas:

$$\begin{aligned}
a &= bq_0 + r_0, && 0 < r_0 < |b|,\\
b &= r_0q_1 + r_1, && 0 < r_1 < r_0,\\
r_0 &= r_1q_2 + r_2, && 0 < r_2 < r_1,\\
&\vdots\\
r_{n-2} &= r_{n-1}q_n + r_n, && 0 < r_n < r_{n-1},\\
r_{n-1} &= r_nq_{n+1} + r_{n+1}, && 0 = r_{n+1}.
\end{aligned} \tag{2.3}$$

Entonces, $r_n = \mathrm{mcd}(a,b)$. Nótese que $q_i > 0$ para todo i excepto quizá q_0 y q_1. Además, $q_1 > 0$ si y sólo si $b > 0$.

Teorema 2.2. *Todo número racional se puede expresar de manera única como una fracción continua finita y simple.*

Demostración. Probaremos primero la expresión y después la unicidad.

(1) *Expresión.* Sea $\frac{a}{b} \in \mathbb{Q}$. Veamos cómo expresar $\frac{a}{b}$ mediante fracciones continuas usando el algoritmo de Euclides. Podemos suponer que $\frac{a}{b}$ es irreducible, esto es, que $\mathrm{mcd}(a,b) = 1$. Y que $b > 0$ cambiando de signo a si fuese necesario. Aplicamos el algoritmo a a y b. Adaptaremos antes nuestra notación a la usada para fracciones continuas. Pongamos $h_0 = a$, $h_1 = b$ y $h_i = r_{i-2}$ para $i = 2,\ldots,n+3$. Pongamos $a_j = q_j$ para $j = 0,\ldots,n+1$. Las igualdades 2.3 se expresan ahora como:

$$\begin{aligned} h_i &= h_{i+1}a_i + h_{i+2}, \qquad 0 < h_{i+2} < h_{i+1}, \qquad i = 0,\dots,n, \\ h_{n+1} &= h_{n+2}a_{n+1} + h_{n+3}, \qquad 0 = h_{n+3}. \end{aligned} \tag{2.4}$$

Entonces, $h_{n+2} = r_n = \mathrm{mcd}(a,b) = 1$. Nótese que $a_j > 0$ para todo j excepto quizá a_0.

Escribiendo

$$f_i = \frac{h_i}{h_{i+1}}, \qquad i = 0,\dots,n+1,$$

las igualdades 2.4 nos dan las siguientes:

$$\begin{aligned} f_i &= a_i + \frac{1}{f_{i+1}}, \qquad i = 0,\dots,n, \\ f_{n+1} &= a_{n+1}. \end{aligned} \tag{2.5}$$

Sustituyendo sucesivamente $f_0, f_1, \dots, f_{n+1}$ obtenemos:

$$\frac{a}{b} = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots \; + \cfrac{1}{a_{n-1} + \cfrac{1}{a_n + \cfrac{1}{a_{n+1}}}}}}} \tag{2.6}$$

Esto muestra que $\frac{a}{b}$ se puede expresar como la fracción continua finita y simple $[a_0; a_1, \dots, a_{n+1}]$, donde los a_i son los cocientes que surgen al aplicar el algoritmo de Euclides a a y b. Queda así demostrada la expresión.

(2) *Unicidad.* Antes de tratar la unicidad es necesario poner de manifiesto lo siguiente. Si $a_{n+1} \geq 2$, en vista de (2.6), hay dos posibles expresiones de la misma fracción continua, a saber:

$$[a_0; a_1, \dots, a_{n+1}] = [a_0; a_1, \dots, a_n, a_{n+1} - 1, 1].$$

Por unicidad entenderemos unicidad salvo este hecho. Si $\frac{a}{b} \in \mathbb{Z}$, esto es, si $b \mid a$, es inevitable. Siempre tenemos $[a_0] = [a_0 - 1; 1]$. Podemos descartarlo fijando la siguiente regla: *la expresión en fracciones continuas finitas y simples de $z \in \mathbb{Z}$ tendrá un sólo término*, es decir, $z = [a_0]$ con $a_0 = z$. Si $\frac{a}{b} \notin \mathbb{Z}$, es decir, si $b \nmid a$, la expresión de $\frac{a}{b}$ tendrá varios términos. En este caso, siempre podemos suponer que el último es mayor que 1. Si fuese $a_{n+1} = 1$, tomamos como último término $a_n + 1$ que cumplirá $a_n + 1 > 1$. Esta será la otra regla que fijaremos: *en la expresión en fracciones continuas finitas y simples de un número racional no entero el último término siempre será mayor que* 1.

Procedemos a demostrar la unicidad, que formulamos como sigue. Consideremos dos fracciones continuas finitas y simples

$$\alpha = [a_0; a_1, \dots, a_n] \quad \text{y} \quad \alpha' = [a'_0; a'_1, \dots, a'_{n'}]. \tag{2.7}$$

Supongamos que $\alpha = \alpha'$. Entonces, $n = n'$ y $a_i = a'_i$ para todo $i = 0, 1, \dots, n$.

Haremos la demostración suponiendo que n' es arbitrario y procediendo por inducción sobre n. En el caso $n = 0$ se aplica la primera regla fijada. Obsérvese que no puede ocurrir que $n' > 0$. Si fuese así, tendríamos

$$a_0 = \alpha = \alpha' = a'_0 + \frac{1}{s'_1},$$

con $s'_1 = [a'_1; a_2, \ldots, a_{n'}]$. Como $a_0, a'_0 \in \mathbb{Z}$, debe ser $s'_1 = 1$, posibilidad ya descartada. Por tanto, $n' = n = 0$ y $a_0 = a'_0$.

Supongamos pues en (2.7) que $n, n' \geq 1$ y que $a_n, a_{n'} > 1$. Antes de abordar la inducción, necesitamos deducir de esta hipótesis una condición sobre los restos de α y α'. Para cada $1 \leq i \leq n$, consideremos el i-ésimo resto de α:

$$s_i = [a_i; a_{i+1}, \ldots, a_n].$$

Sabemos que $a_i \in \mathbb{Z}^+$ para todo i excepto quizá a_0. Así que $a_i \geq 1$ para $i = 1, \ldots, n-1$. Y por hipótesis, $a_n > 1$. Esto implica que $0 < \frac{1}{s_i} < 1$ para $i = 1, \ldots, n$. El mismo razonamiento vale para α'. Pongamos $s'_j = [a'_j; a'_{j+1}, \ldots, a'_{n'}]$ para cada $1 \leq j \leq n'$. Entonces, $0 < \frac{1}{s'_j} < 1$ para $j = 1, \ldots, n'$.

Ya estamos preparados para la argumentación por inducción:

- *Caso inicial.* Supongamos que $n = 1$. Tenemos:

$$a_0 + \frac{1}{a_1} = \alpha = \alpha' = a'_0 + \frac{1}{s'_1}.$$

Como $a_0, a'_0 \in \mathbb{Z}$ y $0 < \frac{1}{a_1}, \frac{1}{s'_1} < 1$, tomando parte entera en la anterior igualdad obtenemos $a_0 = a'_0$. De ella se deduce ahora que $a_1 = s'_1$. Esto implica que no puede ser $n' \geq 2$. Si lo fuese tendríamos:

$$a_1 = a'_1 + \frac{1}{s'_2}$$

Esto es un absurdo ya que $a_1, a'_1 \in \mathbb{Z}$ y $0 < \frac{1}{s'_2} < 1$. Entonces, $n' = 1$ y $a_1 = a'_1$.

- *Hipótesis de inducción.* Supongamos que la afirmación es cierta para $n > 1$.
- *Paso de inducción.* Lo demostramos para $n + 1$. Partimos de la siguiente igualdad:

$$a_0 + \frac{1}{s_1} = s_0 = \alpha = \alpha' = s'_0 = a'_0 + \frac{1}{s'_1}.$$

Como $a_0, a'_0 \in \mathbb{Z}$, usando nuestra observación inicial, extraemos de aquí:

$$a_0 = \lfloor s_0 \rfloor = \lfloor s'_0 \rfloor = a'_0.$$

Volviendo atrás, esto implica $s_1 = s'_1$. Las fracciones s_1 y s'_1 tienen n y $n' - 1$ términos respectivamente. Podemos aplicar la hipótesis de inducción a s_1. Entonces, $n = n' - 1$ y $a_i = a'_i$ para todo $i = 1, \ldots, n + 1$. Queda así establecida la parte de la unicidad. ■

En el ejemplo siguiente se pone en práctica el procedimiento descrito para expresar un número racional como una fracción continua finita y simple.

Ejemplo 2.3. *Consideremos el número* $-\frac{431}{124}$. *Aplicamos el algoritmo de Euclides a* -431 *y* 124. *El proceso de divisiones sucesivas nos da las igualdades de la izquierda. Tomando los cocientes obtenemos la fórmula de la derecha:*

$$\begin{aligned} -431 &= 124\cdot(-4)+65,\\ 124 &= 65\cdot 1+59,\\ 65 &= 59\cdot 1+6,\\ 59 &= 6\cdot 9+5,\\ 6 &= 5\cdot 1+1,\\ 5 &= 1\cdot 5. \end{aligned} \qquad -\frac{431}{124} = -4+\cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{9+\cfrac{1}{1+\cfrac{1}{5}}}}}$$

La expresión de $-\frac{431}{124}$ *en fracciones continuas finitas y simples es* $[-4;1,1,9,1,5]$.

Programación. *En la sección A.3 del apéndice aparece el código del programa que hemos realizado con el software* Mathematica *para calcular la expresión en fracciones continuas simples de un número racional.*

2.3 Fracciones continuas infinitas

En esta sección justificaremos que la fracción continua infinita y simple 2.1 está bien definida ya que, como veremos, se trata del límite de una sucesión convergente.

Sea $\{a_n\}_{n\in\mathbb{N}}$ una sucesión de números enteros todos positivos salvo quizá a_0. Consideremos la fracción continua infinita y simple asociada 2.1. Sea ahora $k\in\mathbb{N}$ y tomemos el k-ésimo convergente

$$r_k := [a_0;a_1,\ldots,a_k].$$

Como $r_k\in\mathbb{Q}$, existen $p_k,q_k\in\mathbb{Z}$, con $q_k\neq 0$, tales que $r_k=\frac{p_k}{q_k}$. A continuación mostramos que p_k y q_k se pueden calcular a partir de $a_0,a_1,\ldots,a_k$ mediante una relación de recurrencia de segundo orden.

Partiendo de la sucesión $\{a_n\}_{n\in\mathbb{N}}$ definimos recursivamente otras dos sucesiones de números enteros $\{p_n\}_{n\geq -2}$ y $\{q_n\}_{n\geq -2}$ del siguiente modo:

$$\begin{aligned} &p_{-2}=0, \quad p_{-1}=1, \quad p_i=a_ip_{i-1}+p_{i-2},\\ &q_{-2}=1, \quad q_{-1}=0, \quad q_i=a_iq_{i-1}+q_{i-2}, \quad i\geq 0. \end{aligned} \tag{2.8}$$

Obsérvese que $q_0=1$ y $q_1=a_1q_0\geq q_0$. Como $a_i\in\mathbb{Z}^+$ para $i\geq 1$ se ve fácilmente por inducción que $q_i>q_{i-1}$ para todo $i\geq 2$. La sucesión $\{q_n\}_{n\geq -2}$ cumple pues:

$$0<q_0\leq q_1<q_2<q_3<\ldots<q_n<\ \ldots \tag{2.9}$$

El crecimiento de esta sucesión será una pieza fundamental en la demostración de los teoremas principales de esta y las posteriores secciones. Es sencillo probar que para $n\geq 2$ se cumple que $q_n\geq 2^{\lfloor\frac{n-1}{2}\rfloor}$, lo que da información sobre su ratio de crecimiento.

El siguiente resultado da una regla para la formación de convergentes en función de las sucesiones que acabamos de definir:

Proposición 2.4. *Sean $n \in \mathbb{N}$ y $x \in \mathbb{R}^+$. Entonces:*

$$[a_0; a_1, \ldots, a_n, x] = \frac{xp_n + p_{n-1}}{xq_n + q_{n-1}}. \tag{2.10}$$

Demostración. Procedemos por inducción sobre n.

- *Caso inicial:* $n = 0$. Tenemos:

$$[x] = x = \frac{x \cdot 1 + 0}{x \cdot 0 + 1} = \frac{xp_{-1} + p_{-2}}{xq_{-1} + q_{-2}}.$$

- *Hipótesis de inducción.* Supongamos que (2.10) es cierta para n y para todo $x \in \mathbb{R}^+$.
- *Paso de inducción.* La siguiente cadena de igualdades demuestra la afirmación para $n+1$. En la primera usamos la definición de fracción continua, en la segunda la hipótesis de inducción, con $a_{n+1} + \frac{1}{x}$ en vez de x, y en la última la definición (2.8). Tenemos:

$$\begin{aligned}
[a_0; a_1, \ldots, a_n, a_{n+1}, x] &= \left[a_0; a_1, \ldots, a_n, a_{n+1} + \frac{1}{x}\right] = \frac{\left(a_{n+1} + \frac{1}{x}\right)p_n + p_{n-1}}{\left(a_{n+1} + \frac{1}{x}\right)q_n + q_{n-1}} \\
&= \frac{(xa_{n+1} + 1)p_n + xp_{n-1}}{(xa_{n+1} + 1)q_n + xq_{n-1}} = \frac{x(a_{n+1}p_n + p_{n-1}) + p_n}{x(a_{n+1}q_n + q_{n-1}) + q_n} \\
&= \frac{xp_{n+1} + p_n}{xq_{n+1} + q_n}.
\end{aligned}$$

■

Como consecuencia:

Proposición 2.5. *Para $n \in \mathbb{N}$ se tiene*

$$r_n = [a_0; a_1, \ldots, a_n] = \frac{p_n}{q_n}.$$

Demostración. Poniendo $x = a_n$ en la proposición 2.4 y usando las igualdades 2.8 obtenemos:

$$r_n = [a_0; a_1, \ldots, a_n] = \frac{a_n p_{n-1} + p_{n-2}}{a_n q_{n-1} + q_{n-2}} = \frac{p_n}{q_n}.$$

■

Las siguientes afirmaciones describen la diferencia entre un convergente y los dos inmediatamente anteriores. Recordando que la sucesión $\{q_n\}_{n\in\mathbb{N}}$ es creciente, (2.9), se sigue que la sucesión de convergentes es de Cauchy y, por tanto, convergerá.

Proposición 2.6.

(i) Para $i \geq 1$ se cumple:

$$p_i q_{i-1} - p_{i-1} q_i = (-1)^{i-1} \qquad y \qquad r_i - r_{i-1} = \frac{(-1)^{i-1}}{q_i q_{i-1}}.$$

(ii) Para $i \geq 2$ se cumple:

$$p_i q_{i-2} - p_{i-2} q_i = (-1)^i a_i \qquad y \qquad r_i - r_{i-2} = \frac{(-1)^i a_i}{q_i q_{i-2}}.$$

Además, la fracción $\frac{p_i}{q_i}$ es irreducible.

Demostración. (i) Probamos la primera igualdad por inducción sobre i:

- *Caso inicial:* $i = 1$. Según (2.8), tenemos:

$$p_0 = a_0 p_{-1} + p_{-2} = a_0 \cdot 1 + 0 = a_0, \qquad p_1 = a_1 p_0 + p_{-1} = a_1 a_0 + 1,$$
$$q_0 = a_0 q_{-1} + q_{-2} = a_0 \cdot 0 + 1 = 1, \qquad q_1 = a_1 q_0 + q_{-1} = a_1 \cdot 1 + 0 = a_1.$$

  Ahora:
$$p_1 q_0 - p_0 q_1 = (a_1 a_0 + 1) \cdot 1 - a_0 a_1 = 1 = (-1)^{1-1}.$$

- *Hipótesis de inducción.* Supongamos que la afirmación es cierta para i.
- *Paso de inducción.* Lo demostramos para $i + 1$:

$$\begin{aligned} p_{i+1} q_i - p_i q_{i+1} &\overset{(2.8)}{=} (a_{i+1} p_i + p_{i-1}) q_i - p_i (a_{i+1} q_i + q_{i-1}) \\ &= a_{i+1} p_i q_i + p_{i-1} q_i - p_i a_{i+1} q_i - p_i q_{i-1} \\ &= -(p_i q_{i-1} - p_{i-1} q_i) \\ &\overset{\text{H.I.}}{=} (-1)(-1)^{i-1} \\ &= (-1)^{(i+1)-1}. \end{aligned}$$

La segunda igualdad se obtiene a partir de la primera dividiendo por $q_i q_{i-1}$ y aplicando la proposición 2.5.

(ii) Probamos la primera igualdad usando el apartado anterior:

$$\begin{aligned} p_i q_{i-2} - p_{i-2} q_i &\overset{(2.8)}{=} (a_i p_{i-1} + p_{i-2}) q_{i-2} - p_{i-2} (a_i q_{i-1} + q_{i-2}) \\ &= a_i (p_{i-1} q_{i-2} - p_{i-2} q_{i-1}) + p_{i-2} q_{i-2} - p_{i-2} q_{i-2} \\ &\overset{(i)}{=} a_i (-1)^{i-2} \\ &= a_i (-1)^i. \end{aligned}$$

La otra igualdad se obtiene a partir de esta dividiendo por $q_i q_{i-2}$ y empleando la proposición 2.5.

Finalmente, probamos que la fracción $\frac{p_i}{q_i}$ es irreducible. Sea $e = \operatorname{mcd}(p_i, q_i)$. Como $e \mid p_i$ y $e \mid q_i$, tenemos que $e \mid p_i q_{i-1} - p_{i-1} q_i$. Esto último es ± 1 por el apartado (i). Por tanto, $e = 1$. ■

Disponemos ya de todo lo necesario para explicar por qué la fracción continua infinita y simple 2.1 determina un número real.

Teorema 2.7. *Consideremos la sucesión $\{r_n\}_{n \in \mathbb{N}}$ definida anteriormente. Entonces:*

(i) La sucesión $\{r_{2n}\}_{n \in \mathbb{N}}$ es creciente.

(ii) La sucesión $\{r_{2n+1}\}_{n \in \mathbb{N}}$ es decreciente.

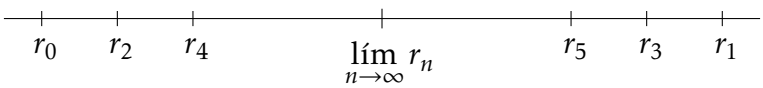
(iii) Para todo $i, j \in \mathbb{N}$ se cumple $r_{2i} < r_{2j+1}$.

(iv) La sucesión $\{r_n\}_{n \in \mathbb{N}}$ es convergente.

(v) Para cada $j \in \mathbb{N}$ se tiene:

$$r_{2j} < \lim_{n \to \infty} r_n < r_{2j+1}.$$

El siguiente gráfico ilustra bien todas estas afirmaciones:



La sucesión $\{r_n\}_{n\in\mathbb{N}}$ converge oscilando alrededor del límite. Los términos de índice par se sitúan a la izquierda de este y los de índice impar a la derecha.

Demostración. (i) Veamos que $r_{2(n+1)} > r_{2n}$. Usando la proposición 2.6(ii), obtenemos:

$$r_{2(n+1)} - r_{2n} = \frac{(-1)^{2(n+1)} a_{2(n+1)}}{q_{2(n+1)} q_{2n}} = \frac{a_{2(n+1)}}{q_{2(n+1)} q_{2n}} > 0.$$

Para la desigualdad hemos utilizado (2.9) y que $a_n > 0$ para todo $n \geq 1$.

(ii) Análogamente se muestra que $r_{2n+1} < r_{2n-1}$:

$$r_{2n+1} - r_{2n-1} = \frac{(-1)^{2n+1} a_{2n+1}}{q_{2n+1} q_{2n-1}} = -\frac{a_{2n+1}}{q_{2n+1} q_{2n-1}} < 0.$$

(iii) Procedemos como en (i) y (ii), pero ahora usando la proposición 2.6(i):

$$r_{2(n+1)} - r_{2n+1} = \frac{(-1)^{(2n+1)-1}}{q_{2(n+1)} q_{2n+1}} = -\frac{1}{q_{2(n+1)} q_{2n+1}} < 0.$$

Sean $i, j \in \mathbb{N}$. Combinando las tres desigualdades anteriores obtenemos:

$$r_{2i} < r_{2(i+j+1)} < r_{2(i+j)+1} < r_{2j+1}.$$

(iv) De los apartados previos sabemos que la sucesión $\{r_{2n}\}_{n\in\mathbb{N}}$ es creciente y está acotada superiormente por r_1 y que la sucesión $\{r_{2n+1}\}_{n\in\mathbb{N}}$ es decreciente y está acotada inferiormente por r_0. Por tanto, ambas son convergentes. Pongamos:

$$L_0 = \lim_{n\to\infty} r_{2n} \qquad y \qquad L_1 = \lim_{n\to\infty} r_{2n+1}.$$

Mostramos a continuación que $L_0 = L_1$. Vimos en (2.9) que la sucesión $\{q_n\}_{n\in\mathbb{N}}$ es creciente, así que la sucesión $\left\{\frac{1}{q_n}\right\}_{n\in\mathbb{N}}$ tiende a 0. Sea $\varepsilon > 0$. Existe pues $n_1 \in \mathbb{N}$ tal que para $n > n_1$ se cumple:

$$|r_{2n+1} - r_{2n}| = \frac{1}{q_{2n+1} q_{2n}} < \frac{\varepsilon}{2}.$$

En la primera igualdad hemos usado la proposición 2.6(i). Por otro lado, existe $n_2 \in \mathbb{N}$ tal que para $n > n_2$ se cumple:

$$|r_{2n} - L_0| < \frac{\varepsilon}{2}.$$

Sea $m = \max\{n_1, n_2\}$. Para $n > m$ se tiene:

$$|r_{2n+1} - L_0| = |r_{2n+1} - r_{2n} + r_{2n} - L_0| \leq |r_{2n+1} - r_{2n}| + |r_{2n} - L_0| < \frac{\varepsilon}{2} + \frac{\varepsilon}{2} = \varepsilon.$$

Esto muestra que la sucesión $\{r_{2n+1}\}_{n\in\mathbb{N}}$ converge a L_0. De la unicidad del límite obtenemos $L_0 = L_1$. Pongamos $L = L_0 = L_1$. La sucesión $\{r_n\}_{n\in\mathbb{N}}$ converge a L ya que cada

uno de sus términos es, o bien un término de $\{r_{2n}\}_{n\in\mathbb{N}}$ o bien uno de $\{r_{2n+1}\}_{n\in\mathbb{N}}$, y ambas sucesiones convergen a L.

(v) Es consecuencia de la argumentación anterior. ■

El teorema precedente y la proposición 2.5 dan sentido a la siguiente definición:

Definición 2.8. *Sea $\{a_n\}_{n\in\mathbb{N}}$ una sucesión de números enteros, todos positivos excepto quizá a_0. El valor de la fracción continua infinita y simple $[a_0;a_1,a_2,\ldots]$ se define como*

$$[a_0;a_1,a_2,\ldots] = \lim_{n\to\infty} [a_0;a_1,a_2,\ldots,a_n].$$

A la vista de esta definición cabe preguntarse: ¿pueden dos sucesiones distintas $\{a_n\}_{n\in\mathbb{N}}$ y $\{a'_n\}_{n\in\mathbb{N}}$ definir la misma fracción continua infinita y simple? Probamos seguidamente que la respuesta es negativa. Necesitamos antes dos resultados técnicos.

Lema 2.9. *Sea $\beta = [b_0;b_1,b_2,\ldots]$ una fracción continua infinita y simple. Entonces, $b_0 = \lfloor\beta\rfloor$.*

Demostración. Tomamos los convergentes correspondientes $\{r_n\}_{n\in\mathbb{N}}$. Tenemos $r_0 = b_0$ y $r_1 = b_0 + \frac{1}{b_1}$. Como $b_1 \geq 1$, obtenemos $r_1 = b_0 + \frac{1}{b_1} \leq b_0 + 1$. Por el teorema 2.7 sabemos que $r_0 < \beta < r_1$. Así que $b_0 < \beta < b_0 + 1$. Luego, $b_0 = \lfloor\beta\rfloor$. ■

Proposición 2.10. *Sea $\alpha = [a_0;a_1,a_2,\ldots]$ una fracción continua infinita y simple. Para cada $m \geq 0$ sea $\alpha_m = [a_m;a_{m+1},a_{m+2},\ldots]$. Entonces, $a_m = \lfloor\alpha_m\rfloor$.*

Demostración. Pongamos $b_0 = a_m$, $b_1 = a_{m+1}$ y, en general, $b_i = a_{m+i}$ para todo $i \geq 0$. Así, $\alpha_m = [b_0;b_1,b_2,\ldots]$. Por el lema anterior, $a_m = b_0 = \lfloor\alpha_m\rfloor$. ■

Ya estamos en condiciones de demostrar lo que pretendíamos.

Teorema 2.11. *Sean $[a_0;a_1,a_2,\ldots]$ y $[a'_0;a'_1,a'_2,\ldots]$ dos fracciones continuas infinitas y simples. Supongamos que $[a_0;a_1,a_2,\ldots] = [a'_0;a'_1,a'_2,\ldots]$. Entonces, $a_n = a'_n$ para todo $n \geq 0$.*

Demostración. Pongamos $\alpha = [a_0;a_1,a_2,\ldots]$ y $\alpha' = [a'_0;a'_1,a'_2,\ldots]$. Por hipótesis, $\alpha = \alpha'$. Probaremos la afirmación por inducción sobre n.

▪ *Caso inicial:* $n = 0$. Veamos que $a_0 = a'_0$ y $\alpha_1 = \alpha'_1$. El lema 2.9 da $a_0 = \lfloor\alpha\rfloor = \lfloor\alpha'\rfloor = a'_0$. Por otro lado, tenemos:

$$a_0 + \frac{1}{\alpha_1} = \alpha = \alpha' = a'_0 + \frac{1}{\alpha'_1}.$$

Como $a_0 = a'_0$, esta igualdad implica $\alpha_1 = \alpha'_1$.

▪ *Hipótesis de inducción:* Supongamos que $a_n = a'_n$ y $\alpha_{n+1} = \alpha'_{n+1}$.

▪ *Paso de inducción.* Mostraremos que $a_{n+1} = a'_{n+1}$ y $\alpha_{n+2} = \alpha'_{n+2}$. Aplicamos la proposición anterior a $\alpha_{n+1} = \alpha'_{n+1}$. Da $a_{n+1} = \lfloor\alpha_{n+1}\rfloor = \lfloor\alpha'_{n+1}\rfloor = a'_{n+1}$. Por otro lado, tenemos:

$$a_{n+1} + \frac{1}{\alpha_{n+2}} = \alpha_{n+1} = \alpha'_{n+1} = a'_{n+1} + \frac{1}{\alpha'_{n+2}}.$$

Como $a_{n+1} = a'_{n+1}$, se sigue de esto que $\alpha_{n+2} = \alpha'_{n+2}$. ■

La demostración anterior proporciona un método para recuperar, mediante la función parte entera, los términos de la sucesión $a_0, a_1, a_2, \ldots$ a partir del valor de la fracción continua infinita y simple $[a_0;a_1,a_2,\ldots]$.

2.4 Números irracionales y fracciones continuas infinitas

En la sección 2.2 vimos que toda fracción continua finita y simple define un número racional y, recíprocamente, que todo número racional se puede expresar de manera única como una fracción continua finita y simple. Las fracciones continuas infinitas permiten dar el salto a los números irracionales. En esta sección mostraremos que el mismo resultado es válido cambiando finito por infinito y racional por irracional.

Empezamos con la afirmación más sencilla.

Teorema 2.12. *Toda fracción continua infinita y simple* $[a_0;a_1,a_2,\ldots]$ *es un número irracional.*

Demostración. Escribimos $\alpha = [a_0;a_1,a_2,\ldots]$. Sabemos, por el teorema 2.7(v), que $r_{2n} < \alpha < r_{2n+1}$ para todo $n \in \mathbb{N}$. Luego, $0 < |\alpha - r_{2n}| < |r_{2n+1} - r_{2n}|$. Multiplicando esta desigualdad por q_{2n} y usando la proposición 2.6(i), obtenemos:

$$0 < |\alpha - r_{2n}|q_{2n} < |r_{2n+1} - r_{2n}|q_{2n} = \frac{1}{q_{2n+1}q_{2n}}q_{2n} = \frac{1}{q_{2n+1}}.$$

Recordemos, de la proposición 2.5, que $r_{2n} = \frac{p_{2n}}{q_{2n}}$. Supongamos, razonando por reducción al absurdo, que $\alpha \in \mathbb{Q}$. Pongamos $\alpha = \frac{u}{v}$, con $u,v \in \mathbb{Z}$ y $v > 0$. En la inecuación anterior reemplazamos r_{2n} por $\frac{p_{2n}}{q_{2n}}$, α por $\frac{u}{v}$ y operamos. Resulta:

$$0 < |uq_{2n} - vp_{2n}| < \frac{v}{q_{2n+1}}.$$

La sucesión $\{q_{2n+1}\}_{n\in\mathbb{N}}$ es creciente según (2.9). Existe pues $m \in \mathbb{N}$ tal que $v < q_{2m+1}$. Entonces:

$$0 < |uq_{2m} - vp_{2m}| < 1.$$

Esto es una contradicción ya que $|uq_{2m} - vp_{2m}| \in \mathbb{Z}$. Por tanto, α es irracional. ■

Recíprocamente:

Teorema 2.13. *Todo número irracional* ξ *se puede expresar de manera única como una fracción continua infinita y simple* $[a_0;a_1,a_2,\ldots]$ *definida recursivamente del siguiente modo:*

$$\xi_0 = \xi, \qquad a_i = \lfloor \xi_i \rfloor, \qquad \xi_{i+1} = \frac{1}{\xi_i - a_i}, \quad i \geq 0. \tag{2.11}$$

Además, se tiene:

$$\xi = [a_0;a_1,\ldots,a_{n-1},\xi_n] \quad y \quad \xi_n = [a_n;a_{n+1},a_{n+2},\ldots], \quad n \geq 0.$$

Demostración. Mostramos, en primer lugar, la simplicidad de la sucesión $\{a_n\}_{n\in\mathbb{N}}$. Nótese que, por construcción, $a_i \in \mathbb{Z}$ para todo $i \geq 0$. Despejando ξ_i de (2.11), tenemos:

$$\xi_i = a_i + \frac{1}{\xi_{i+1}}, \quad i \geq 0. \tag{2.12}$$

Como ξ_0 es irracional y $a_i \in \mathbb{Z}$, se ve fácilmente por inducción a partir de esta igualdad que ξ_i es irracional para todo i. Entonces, $a_i < \xi_i < a_i + 1$. (La irracionalidad asegura que las desigualdades son estrictas.) En consecuencia, $0 < \xi_i - a_i < 1$. Por tanto,

$$\xi_{i+1} = \frac{1}{\xi_i - a_i} > 1.$$

Esto da que $a_{i+1} = \lfloor \xi_{i+1} \rfloor \geq 1$ para todo $i \geq 0$. Queda así probado que los a_i son números enteros, todos positivos excepto quizá a_0.

Mostraremos que ξ es el valor de la fracción continua $[a_0; a_1, a_2, \ldots]$ definida mediante (2.11) probando que ξ es el límite de la correspondiente sucesión de convergentes. Necesitaremos para ello varias afirmaciones previas. Comenzamos demostrando por inducción sobre n la siguiente igualdad, que es parte del enunciado:

$$\xi = [a_0; a_1, \ldots, a_n, \xi_{n+1}]. \tag{2.13}$$

- *Caso inicial:* $n = 1$. La igualdad 2.12 para $i = 0$ da:

$$\xi = \xi_0 = a_0 + \frac{1}{\xi_1} = [a_0; \xi_1].$$

- *Hipótesis de inducción:* Supongamos que (2.13) es cierta.
- *Paso de inducción.* El siguiente cálculo lo demuestra para $n+1$:

$$\xi = [a_0; a_1, \ldots, a_n, \xi_{n+1}] = \left[a_0; a_1, \ldots, a_n, a_{n+1} + \frac{1}{\xi_{n+2}}\right] = [a_0; a_1, \ldots, a_n, a_{n+1}, \xi_{n+2}].$$

En él hemos usado: primero la hipótesis de inducción, después la igualdad 2.12 para $i = n$ y finalmente la definición de fracción continua.

Ahora aplicamos a (2.13) la proposición 2.4. Obtenemos:

$$\xi = [a_0; a_1, \ldots, a_n, \xi_{n+1}] = \frac{\xi_{n+1} p_n + p_{n-1}}{\xi_{n+1} q_n + q_{n-1}}. \tag{2.14}$$

En el siguiente cálculo hallamos la diferencia entre ξ y el convergente r_n. Usamos en él: la igualdad 2.14 y las proposiciones 2.5 y 2.6(i):

$$\begin{aligned} \xi - r_n &= \frac{\xi_{n+1} p_n + p_{n-1}}{\xi_{n+1} q_n + q_{n-1}} - \frac{p_n}{q_n} = \frac{\xi_{n+1} p_n q_n + p_{n-1} q_n - \xi_{n+1} p_n q_n - p_n q_{n-1}}{(\xi_{n+1} q_n + q_{n-1}) q_n} \\ &= -\frac{p_n q_{n-1} - p_{n-1} q_n}{(\xi_{n+1} q_n + q_{n-1}) q_n} = -\frac{(-1)^{n-1}}{(\xi_{n+1} q_n + q_{n-1}) q_n} = \frac{(-1)^n}{(\xi_{n+1} q_n + q_{n-1}) q_n}. \end{aligned}$$

Sabemos que $a_{n+1} < \xi_{n+1}$. Entonces, usando (2.9), queda:

$$q_{n+1} = a_{n+1} q_n + q_{n-1} < \xi_{n+1} q_n + q_{n-1}.$$

Juntando esto con el cálculo anterior, obtenemos:

$$|\xi - r_n| = \frac{1}{(\xi_{n+1} q_n + q_{n-1}) q_n} < \frac{1}{q_{n+1} q_n} < \frac{1}{q_n^2}. \tag{2.15}$$

Como la sucesión $\left\{\frac{1}{q_n}\right\}_{n \in \mathbb{N}}$ converge a 0, la sucesión $\{r_n\}_{n \in \mathbb{N}}$ converge a ξ. Por tanto, $\xi = [a_0; a_1, a_2, \ldots]$.

Para finalizar la demostración solo resta probar que $\xi_n = [a_n; a_{n+1}, a_{n+2}, \ldots]$. Sabemos que ξ_n es irracional. Hagamos que ξ_n interprete el papel antes interpretado por ξ. La sucesión que resulta de aplicar (2.11) a ξ_n es $a_n, a_{n+1}, a_{n+2}, \ldots$ La afirmación anterior aplicada a ξ_n nos da $\xi_n = [a_n; a_{n+1}, a_{n+2}, \ldots]$. ■

Definición 2.14. *La fracción continua infinita y simple* $[a_0; a_1, a_2, \ldots]$ *obtenida al aplicar al número irracional* ξ *el algoritmo 2.11 recibe el nombre de expansión o expresión de* ξ *como una fracción continua simple. Nos referiremos a ella abreviadamente como la EFCS de* ξ.

El algoritmo 2.11 puede aplicarse también a un número racional. Si lo comparamos con las ecuaciones 2.5 vemos que se trata del mismo proceso expuesto allí para expresar un número racional como una fracción continua simple mediante el algoritmo de Euclides. En *Los elementos* de Euclides ya aparece el algoritmo de Euclides aplicado a números no necesariamente enteros. La proposición 2 del libro X dice:

> Si al restar continua y sucesivamente la menor de la mayor de dos magnitudes desiguales, la que queda nunca mide a la anterior, las magnitudes serán inconmensurables.

Véase [9, Sección 2.2] para una discusión más detallada. La conclusión que se extrae aquí es que los antiguos griegos ya conocían las fracciones continuas infinitas y sabían que daban lugar a números irracionales.

2.5 Aproximación mediante fracciones continuas

Sea ξ un número irracional y $[a_0; a_1, a_2, \ldots]$ su EFCS. Sabemos que la sucesión $\left\{\frac{p_n}{q_n}\right\}_{n\in\mathbb{N}}$ tiende a ξ. Así pues la EFCS da un método para aproximar ξ mediante números racionales. En esta sección presentaremos varios resultados que establecen cotas para el error cometido al aproximar ξ por $\frac{p_n}{q_n}$. Además veremos que este modo de aproximar ξ por números racionales es óptimo en un sentido que especificaremos más adelante.

Proposición 2.15. *Para todo* $n \in \mathbb{N}$ *se cumple:*

$$\frac{1}{2q_nq_{n+1}} < \frac{1}{q_n(q_n+q_{n+1})} < \left|\xi - \frac{p_n}{q_n}\right| < \frac{1}{q_nq_{n+1}} < \frac{1}{q_n^2},$$

$$\frac{1}{2q_{n+1}} < \frac{1}{q_n+q_{n+1}} < |\xi q_n - p_n| < \frac{1}{q_{n+1}} < \frac{1}{q_n}.$$

Demostración. La segunda cadena de desigualdades se obtiene a partir de la primera multiplicando por q_n, que es positivo. Así que nos centramos en probar la primera.

Recordemos que al final de la demostración del teorema 2.13 ya quedó establecida la parte derecha de la cadena, véase la ecuación 2.15:

$$\left|\xi - \frac{p_n}{q_n}\right| = \frac{1}{(\xi_{n+1}q_n + q_{n-1})q_n} < \frac{1}{q_{n+1}q_n} < \frac{1}{q_n^2}. \tag{2.16}$$

También en esa demostración vimos que $\xi_{n+1} < a_{n+1} + 1$. Entonces,

$$\xi_{n+1}q_n + q_{n-1} < (a_{n+1}+1)q_n + q_{n-1} = a_{n+1}q_n + q_{n-1} + q_n \overset{(2.8)}{=} q_{n+1} + q_n. \tag{2.17}$$

Usemos una vez más que la sucesión $\{q_n\}_{n\in\mathbb{N}}$ es creciente. Por tanto, $q_n < q_{n+1}$ y así $q_{n+1} + q_n < 2q_{n+1}$. Esta desigualdad y la anterior implican:

$$\frac{1}{2q_{n+1}q_n} < \frac{1}{(q_{n+1}+q_n)q_n} < \frac{1}{(\xi_{n+1}q_n + q_{n-1})q_n} = \left|\xi - \frac{p_n}{q_n}\right|,$$

lo que pone fin a la demostración. ∎

Mostramos ahora que cada convergente está más próximo a ξ que su predecesor.

Proposición 2.16. *Para $n \in \mathbb{N}$ arbitrario se cumple:*

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

Demostración. Probamos primero la desigualdad de la izquierda. Para ello, retomamos la desigualdad 2.17 de más arriba. Recordemos que $a_{n+2} \geq 1$. Lo unimos a lo anterior:

$$\xi_{n+1} q_n + q_{n-1} < q_{n+1} + q_n \leq a_{n+2} q_{n+1} + q_n \overset{(2.8)}{=} q_{n+2}.$$

Esta desigualdad, combinada con (2.16), da:

$$\frac{1}{q_{n+2} q_n} < \frac{1}{(\xi_{n+1} q_n + q_{n-1}) q_n} = \left|\xi - \frac{p_n}{q_n}\right|.$$

Multiplicamos esto por q_n y usamos el teorema anterior. Resulta:

$$|\xi q_{n+1} - p_{n+1}| < \frac{1}{q_{n+2}} < |\xi q_n - p_n|.$$

Finalmente mostramos cómo la desigualdad de la derecha se deduce de la ya probada. Recordemos que $q_n < q_{n+1}$. Tenemos:

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

■

El siguiente resultado revela que el convergente $\frac{p_n}{q_n}$ es la mejor aproximación[1] de ξ de entre todos los números racionales con denominador menor o igual que q_n.

Proposición 2.17. *Sea $\frac{a}{b} \in \mathbb{Q}$ con $b > 0$ tal que $|\xi b - a| < |\xi q_n - p_n|$ para algún $n \geq 0$. Entonces, $b \geq q_{n+1}$. Como consecuencia, si*

$$\left|\xi - \frac{a}{b}\right| < \left|\xi - \frac{p_n}{q_n}\right| \tag{2.18}$$

para algún $n \geq 1$, entonces $b > q_n$.

Demostración. Explicamos en primer lugar cómo deducir la segunda afirmación de la primera. Sea $\frac{a}{b} \in \mathbb{Q}$ con $b > 0$ tal que, para algún $n \geq 1$, se cumple (2.18). Supongamos que $b \leq q_n$. Tenemos:

$$|\xi b - a| = \left|\xi - \frac{a}{b}\right| b < \left|\xi - \frac{p_n}{q_n}\right| q_n = |\xi q_n - p_n|.$$

La primera afirmación da $b \geq q_{n+1} > q_n$, en contra de lo supuesto. Por tanto, $b > q_n$.

[1] En teoría de números, el estudio de la aproximación de números reales por números racionales recibe el nombre de *aproximación diofántica*. La noción de mejor aproximación se define aquí del siguiente modo, véase [10, página 21]. Dado $\alpha \in \mathbb{R}$, se dice que $\frac{a}{b} \in \mathbb{Q}$, con $b > 0$, es una *mejor aproximación de α* si $\left|\alpha - \frac{a}{b}\right| < \left|\alpha - \frac{a'}{b'}\right|$ para todo $\frac{a'}{b'} \in \mathbb{Q}$ tal que $\frac{a}{b} \neq \frac{a'}{b'}$ y $0 < b' \leq b$. También suele usarse la desigualdad $|\alpha b - a| < |\alpha b' - a'|$, que implica la anterior. En [6, Sección 1.4] se puede encontrar una definición mucho más técnica de mejor aproximación.

Probamos seguidamente la primera afirmación. Supongamos, razonando por reducción al absurdo, que:

$$|\xi b - a| < |\xi q_n - p_n| \quad \text{y} \quad b < q_{n+1}.$$

Consideremos el siguiente sistema de ecuaciones lineales con incógnitas x e y:

$$\begin{cases} p_{n+1}x + p_n y = a \\ q_{n+1}x + q_n y = b \end{cases}$$

El determinante de la matriz de coeficientes es $p_{n+1}q_n - p_n q_{n+1}$. Por la proposición 2.6(i), este es ± 1. Todos los coeficientes del sistema son números enteros. Resolviéndolo por la regla de Cramer obtenemos que $x, y \in \mathbb{Z}$.

Dividimos el resto de la demostración en varios pasos:

(1) *Mostramos que* $xy \neq 0$.

- Si $x = 0$, tenemos $a = p_n y$ y $b = q_n y$. Como $b > 0$ y $q_n > 0$, es $y > 0$ y, consecuentemente, $y \geq 1$. Entonces:

$$|\xi b - a| = |\xi q_n y - p_n y| = |\xi q_n - p_n| y \geq |\xi q_n - p_n|.$$

  Esto contradice nuestra suposición. Así que $x \neq 0$.
- Si $y = 0$, entonces $b = q_{n+1}x$. Como $b > 0$ y $q_{n+1} > 0$, es $x > 0$ y, consecuentemente, $x \geq 1$. Entonces, $b \geq q_{n+1}$, en contra de lo supuesto. Así que $y \neq 0$.

(2) *Mostramos que* x *e* y *tienen signos opuestos.*

- Supongamos que $x < 0$. Entonces, $q_n y = b - q_{n+1}x > 0$. Como $q_n > 0$, es $y > 0$.
- Supongamos que $x > 0$. Entonces $x \geq 1$ pues $x \in \mathbb{Z}$. Ahora, $q_{n+1}x \geq q_{n+1} > b$. Como $q_n y = b - q_{n+1}x$ y $q_n > 0$, es $y < 0$.

(3) *Mostramos que* $(\xi q_{n+1} - p_{n+1})x$ *y* $(\xi q_n - p_n)y$ *tienen el mismo signo.* Se deduce del paso (2) y de que $\xi q_n - p_n$ y $\xi q_{n+1} - p_{n+1}$ tienen distinto signo según el teorema 2.7(v).

(4) *Llegamos a una contradicción.* Tenemos:

$$\xi b - a = \xi(q_{n+1}x + q_n y) - (p_{n+1}x + p_n y) = (\xi q_{n+1} - p_{n+1})x + (\xi q_n - p_n)y.$$

Puesto que ambos sumandos son del mismo signo, podemos escribir:

$$|\xi b - a| = |(\xi q_{n+1} - p_{n+1})x| + |(\xi q_n - p_n)y|.$$

Como $x \neq 0$ y $\xi \neq \frac{p_{n+1}}{q_{n+1}}$, tenemos que $|(\xi q_{n+1} - p_{n+1})x| > 0$. Por otro lado, sabemos que $|y| \geq 1$. Continuamos desde la igualdad anterior:

$$|\xi b - a| = |\xi q_{n+1} - p_{n+1}||x| + |\xi q_n - p_n||y| > |\xi q_n - p_n||y| \geq |\xi q_n - p_n|.$$

Esto contradice nuestra hipótesis. Por tanto, $b \geq q_{n+1}$. ■

El siguiente resultado será la clave en la resolución de la ecuación de Pell.

Teorema 2.18. *Sea* ξ *un número irracional. Supongamos que existe* $\frac{a}{b} \in \mathbb{Q}$ *con* $b \geq 1$ *tal que*

$$\left|\xi - \frac{a}{b}\right| < \frac{1}{2b^2}.$$

Entonces, $\frac{a}{b}$ *es un convergente de la EFCS de* ξ.

Demostración. Sean $\left\{\frac{p_n}{q_n}\right\}_{n\in\mathbb{N}}$ los convergentes de la EFCS de ξ. Supongamos, razonando por reducción al absurdo, que $\frac{a}{b}$ no es uno de ellos. Como la sucesión $\{q_n\}_{n\in\mathbb{N}}$ es creciente, existe $m \in \mathbb{N}$ tal que $q_m \leq b < q_{m+1}$. Según la proposición 2.17, la desigualdad $|\xi b - a| < |\xi q_m - p_m|$ no es cierta. Así que, usando la cota del enunciado, tenemos:

$$|\xi q_m - p_m| \leq |\xi b - a| < \frac{1}{2b}.$$

De aquí, dividiendo por q_m, que es positivo, resulta:

$$\left|\xi - \frac{p_m}{q_m}\right| < \frac{1}{2bq_m}.$$

Tenemos que $bp_m - aq_m \in \mathbb{Z}$ y, por hipótesis, $\frac{a}{b} \neq \frac{p_m}{q_m}$. Luego, $|bp_m - aq_m| \geq 1$. Calculamos, usando todo lo anterior y la desigualdad triangular:

$$\frac{1}{bq_m} \leq \frac{|bp_m - aq_m|}{bq_m} = \left|\frac{p_m}{q_m} - \frac{a}{b}\right| = \left|\frac{p_m}{q_m} - \xi + \xi - \frac{a}{b}\right| \leq \left|\xi - \frac{p_m}{q_m}\right| + \left|\xi - \frac{a}{b}\right| < \frac{1}{2bq_m} + \frac{1}{2b^2}.$$

Multiplicando esta desigualdad por $2bq_m$, que es positivo, obtenemos que $b < q_m$, lo cual es una contradicción. Por tanto, $\frac{a}{b}$ es un convergente de la EFCS de ξ. ■

En el teorema 3.3 del siguiente capítulo veremos que si (a, b) es una solución positiva de $x^2 - dy^2 = 1$, entonces $\frac{a}{b}$ es una aproximación racional de $\sqrt{d}$ con error menor que $\frac{1}{2b^2}$. Así que $\frac{a}{b}$ será un convergente de la EFCS de $\sqrt{d}$ por el teorema anterior.

2.6 Expansión en fracciones continuas de un número irracional cuadrático

Un número irracional se dice *cuadrático* si es solución de una ecuación cuadrática con coeficientes enteros; en otros términos, si es de la forma $\frac{m+\sqrt{d}}{w}$, donde $m, w, d \in \mathbb{Z}$ y d es positivo y no cuadrado. En esta sección estudiaremos la EFCS de tales números. Veremos que se puede caracterizar por la propiedad de ser periódica. La demostración de este hecho proporciona un algoritmo sencillo de poner en práctica para calcularla. Acabaremos la sección con el importante teorema de Lagrange, que revela una curiosa relación entre la parte entera de $\sqrt{d}$ y la longitud del periodo de su EFCS.

Definición 2.19. *Una fracción continua infinita y simple $[a_0; a_1, a_2, \ldots]$ se dirá periódica si existen $l, m_l \in \mathbb{N}$ tal que $a_m = a_{m+l}$ para todo $m \geq m_l$. Al menor de tales l lo llamaremos longitud del periodo y lo denotaremos por ℓ. Cuando $m_l = 0$ decimos que la fracción continua es puramente periódica.*

Una fracción continua periódica será de la forma

$$[b_0; b_1, b_2, \ldots, b_n, a_0, a_1, \ldots, a_{\ell-1}, a_0, a_1, \ldots, a_{\ell-1}, \ldots],$$

donde la sucesión $a_0, a_1, \ldots, a_{\ell-1}$ se repetirá indefinidamente. Indicaremos esto abreviadamente con una línea sobre la parte que se repite. Así escribiremos:

$$[b_0; b_1, b_2, \ldots, b_n, \overline{a_0, a_1, \ldots, a_{\ell-1}}].$$

A las sucesiones de números $a_0, a_1, \ldots, a_{\ell-1}$ y $b_0, b_1, b_2, \ldots, b_n$ las llamamos *periodo* y *preperiodo* respectivamente. Obsérvese que, al ser la fracción simple y periódica, $a_0 \geq 1$. Las fracciones continuas puramente periódicas carecen de preperiodo.

Podemos abordar ya la caracterización que mencionamos antes:

Teorema 2.20. *Toda fracción continua infinita y simple que sea periódica es un número irracional cuadrático. Recíprocamente, la EFCS de un número irracional cuadrático es periódica.*

Demostración. Dividimos la demostración en dos partes, una para cada afirmación:

(1) *Toda fracción continua infinita y simple que sea periódica es un número irracional cuadrático.* Consideremos una fracción como en la hipótesis:

$$\xi = [b_0; b_1, \ldots, b_n, \overline{a_0, a_1, \ldots, a_{\ell-1}}].$$

Denotemos por θ a la parte que se repite. Tenemos entonces:

$$\theta = [\overline{a_0; a_1, \ldots, a_{\ell-1}}] = [a_0; a_1, \ldots, a_{\ell-1}, \theta].$$

La proposición 2.4 nos permite escribir:

$$\theta = [a_0; a_1, \ldots, a_{\ell-1}, \theta] = \frac{\theta p_{\ell-1} + p_{\ell-2}}{\theta q_{\ell-1} + q_{\ell-2}}.$$

Operando aquí obtenemos que θ es solución de la siguiente ecuación cuadrática con coeficientes enteros:

$$q_{\ell-1}x^2 + (q_{\ell-2} - p_{\ell-1})x - p_{\ell-2} = 0.$$

Por el teorema 2.12, θ es un número irracional. Luego,

$$\theta = \frac{m + \sqrt{d}}{w}$$

para ciertos $m, d, w \in \mathbb{Z}$ con $d > 0$. Expresamos ξ en función de θ del siguiente modo:

$$\xi = [b_0; b_1, \ldots, b_n, \theta] = \frac{\theta p'_n + p'_{n-1}}{\theta q'_n + q'_{n-1}},$$

siendo $\frac{p'_n}{q'_n}$ y $\frac{p'_{n-1}}{q'_{n-1}}$ los correspondientes convergentes. Como $p'_n, p'_{n-1} \in \mathbb{Z}$ y θ es un número irracional cuadrático, $\theta p'_n + p'_{n-1}$ y $\theta q'_n + q'_{n-1}$ también lo son. El inverso de un número irracional cuadrático es un número irracional cuadrático. El producto de dos números irracionales cuadráticos puede ser un número irracional cuadrático o un número racional. Esas dos posibilidades para ξ nos da la expresión anterior. Por el teorema 2.12, ξ es irracional, luego ξ es un número irracional cuadrático. Esto termina la primera parte.

(2) *La EFCS de un número irracional cuadrático ξ es periódica*. Dividimos esta segunda parte en dos pasos:

(2.1) *Calculamos la EFCS de ξ*. Supongamos que

$$\xi = \frac{a + \sqrt{b}}{c}, \qquad \text{con} \quad a, b, c \in \mathbb{Z}, \quad b > 0 \quad \text{y} \quad c \neq 0.$$

Como ξ es irracional, b no es un cuadrado. Multiplicamos numerador y denominador por $|c|$ y, según el signo de c, obtenemos:

$$\xi = \frac{ac + \sqrt{bc^2}}{c^2} \quad \text{o} \quad \xi = \frac{-ac + \sqrt{bc^2}}{-c^2}.$$

Pongamos $\xi_0 = \xi$. Podemos expresar pues ξ_0 como

$$\xi_0 = \frac{m_0 + \sqrt{d}}{w_0},$$

donde $d, m_0, w_0 \in \mathbb{Z}$, w_0 es no nulo, d no es un cuadrado y w_0 divide a $d - m_0^2$. Probaremos que el algoritmo 2.11 para calcular la EFCS de ξ toma la siguiente forma en este caso:

$$a_i = \lfloor \xi_i \rfloor, \qquad \xi_i = \frac{m_i + \sqrt{d}}{w_i}, \qquad m_{i+1} = a_i w_i - m_i, \qquad w_{i+1} = \frac{d - m_{i+1}^2}{w_i}, \qquad i \geq 0, \tag{2.19}$$

donde $m_i, w_i \in \mathbb{Z}$, $w_i \neq 0$ y $w_i \mid d - m_i^2$. Realizamos la prueba por inducción sobre i.

- *Caso inicial:* $i = 0$. Ya lo hemos argumentado antes.
- *Hipótesis de inducción.* Supongamos que la afirmación es cierta para i.
- *Paso de inducción.* Lo probamos para $i + 1$. Por definición, $m_{i+1} = a_i w_i - m_i$. Ahora, $a_i \in \mathbb{Z}$, y $w_i, m_i \in \mathbb{Z}$ por hipótesis de inducción. Así que $m_{i+1} \in \mathbb{Z}$. Argumentamos sobre w_{i+1}. Tenemos:

$$w_{i+1} = \frac{d - m_{i+1}^2}{w_i} = \frac{d - (a_i w_i - m_i)^2}{w_i} = \frac{d - m_i^2}{w_i} + 2a_i m_i - a_i^2 w_i.$$

La hipótesis de inducción nos asegura que w_i divide a $d - m_i^2$ y que $m_i, w_i \in \mathbb{Z}$. Como $a_i \in \mathbb{Z}$, concluimos de la igualdad anterior que $w_{i+1} \in \mathbb{Z}$. Esto implica a su vez que w_{i+1} divide a $d - m_{i+1}^2$. Y obsérvese que $w_{i+1} \neq 0$ pues, en caso contrario, d sería un cuadrado. Finalmente, vemos que ξ_{i+1}, definido como en las ecuaciones 2.11, responde a la fórmula propuesta en (2.19). Tenemos:

$$\xi_{i+1} \overset{(2.11)}{=} \frac{1}{\xi_i - a_i} \overset{\text{H.I.}}{=} \frac{1}{\frac{m_i + \sqrt{d}}{w_i} - a_i} = \frac{w_i}{\sqrt{d} + m_i - a_i w_i} = \frac{w_i}{\sqrt{d} - m_{i+1}}$$

$$= \frac{w_i(\sqrt{d} + m_{i+1})}{(\sqrt{d} - m_{i+1})(\sqrt{d} + m_{i+1})} = \frac{w_i(\sqrt{d} + m_{i+1})}{d - m_{i+1}^2} \overset{(2.19)}{=} \frac{m_{i+1} + \sqrt{d}}{w_{i+1}}.$$

(2.2) *La EFCS de ξ antes calculada es periódica.* Necesitaremos usar el automorfismo conjugación de $\mathbb{Q}(\sqrt{d})$. Recordemos que $\mathbb{Q}(\sqrt{d})$ es el subcuerpo de $\mathbb{R}$ formado por números del tipo $z := s_0 + s_1\sqrt{d}$, con $s_0, s_1 \in \mathbb{Q}$. El conjugado de z se define como $\widehat{z} = s_0 - s_1\sqrt{d}$. Suele denotarse por $\overline{z}$, pero como aquí ya usamos la línea superior para el periodo, lo escribiremos así para evitar confusiones. La conjugación $\widehat{\cdot} : \mathbb{Q}(\sqrt{d}) \to \mathbb{Q}(\sqrt{d})$, $z \mapsto \widehat{z}$ es un $\mathbb{Q}$-automorfismo de $\mathbb{Q}(\sqrt{d})$. Esto significa que es biyectiva, respeta la suma y el producto y deja fijos a los elementos de $\mathbb{Q}$. Como consecuencia, lleva inversos en inversos.

Por lo visto en el paso anterior, para cada $i \geq 0$, tenemos:

$$\widehat{\xi_i} = \frac{m_i - \sqrt{d}}{w_i}.$$

Del teorema 2.13 y la proposición 2.4 sabemos que:

$$\xi_0 = \xi = [a_0; a_1, \ldots, a_{n-1}, \xi_n] = \frac{\xi_n p_{n-1} + p_{n-2}}{\xi_n q_{n-1} + q_{n-2}}.$$

Las propiedades de la conjugación especificadas permiten escribir:

$$\widehat{\xi_0} = \widehat{\xi} = [a_0; a_1, \ldots, a_{n-1}, \widehat{\xi_n}] = \frac{\widehat{\xi_n} p_{n-1} + p_{n-2}}{\widehat{\xi_n} q_{n-1} + q_{n-2}}.$$

Despejando de aquí $\widehat{\xi_n}$ obtenemos:

$$\widehat{\xi_n} = -\frac{q_{n-2}}{q_{n-1}} \left(\frac{\widehat{\xi_0} - \dfrac{p_{n-2}}{q_{n-2}}}{\widehat{\xi_0} - \dfrac{p_{n-1}}{q_{n-1}}} \right).$$

Sabemos que la sucesión $\left\{\frac{p_n}{q_n}\right\}_{n\in\mathbb{N}}$ converge a ξ_0. Como d no es un cuadrado, tenemos que $\widehat{\xi_0} \neq \xi_0$. La sucesión definida por el término entre paréntesis converge pues a 1. Luego existe $n_0 \in \mathbb{N}$ tal que para $n > n_0$ el correspondiente término entre paréntesis es positivo. Recordemos de (2.9) que la fracción $\frac{q_{n-2}}{q_{n-1}}$ es siempre positiva. Así que para $n > n_0$ será $\widehat{\xi_n} < 0$. Por otro lado, el teorema 2.13 nos dice que $\xi_n > 0$ para $n \geq 1$. Por tanto, $\xi_n - \widehat{\xi_n} > 0$ para $n > n_0$. Ahora bien, usando las fórmulas 2.19, encontramos que $\xi_n - \widehat{\xi_n} = \frac{2\sqrt{d}}{w_n}$. Por tanto, $w_n > 0$ para $n > n_0$. Como $w_n \in \mathbb{Z}$, debe ser $w_n \geq 1$ para $n > n_0$. De las ecuaciones 2.19 deducimos que para $n > n_0$ se cumple:

$$0 < w_n w_{n+1} = d - m_{n+1}^2 \leq d.$$

Esto implica:

$$0 < w_n \leq w_n w_{n+1} \leq d \qquad \text{y} \qquad 0 \leq m_{n+1}^2 < m_{n+1}^2 + w_n w_{n+1} = d.$$

De aquí extraemos:

$$0 < w_n \leq d \quad \text{y} \quad 0 \leq |m_{n+1}| < \sqrt{d} \qquad \forall n > n_0. \tag{2.20}$$

Como d es un número fijo y $m_n, w_n \in \mathbb{Z}$ para todo $n \in \mathbb{N}$, las cotas anteriores nos dicen que m_n y w_n sólo pueden tomar un número finito de valores para $n > n_0$. Existirán pues $j, k \in \mathbb{N}$, con $j < k$, tales que $m_j = m_k$ y $w_j = w_k$. Pongamos $l = k - j$. Demostraremos por inducción que $w_t = w_{t+l}$ y $m_t = m_{t+l}$ para todo $t \geq j$. Las fórmulas 2.19 nos darán que $\xi_t = \xi_{t+l}$ para todo $t \geq j$ y, en consecuencia, que $a_t = a_{t+l}$ para todo $t \geq j$. Así quedará demostrada la periodicidad de la EFCS de ξ.

- *Caso inicial:* $t = j$. Tenemos:

$$m_j = m_k = m_{j+(k-j)} = m_{j+l},$$
$$w_j = w_k = w_{j+(k-j)} = w_{j+l}.$$

- *Hipótesis de inducción.* Suponemos que la afirmación es cierta para t.
- *Paso de inducción.* Lo probamos para $t+1$. Calculamos:

$$m_{t+1} \overset{(2.19)}{=} a_t w_t - m_t \overset{\text{H.I.}}{=} a_{t+l} w_{t+l} - m_{t+l} \overset{(2.19)}{=} m_{(t+l)+1} = m_{(t+1)+l},$$

$$w_{t+1} \overset{(2.19)}{=} \frac{d - m_{t+1}^2}{w_t} \overset{\text{H.I.}}{=} \frac{d - m_{(t+1)+l}^2}{w_{t+l}} \overset{(2.19)}{=} w_{(t+l)+1} = w_{(t+1)+l}.$$

■

Algoritmo para el cálculo de la EFCS de un número irracional cuadrático. Las fórmulas 2.19 proporcionan un algoritmo sencillo de llevar a la práctica para calcular la EFCS de un número irracional cuadrático. Notése que, a diferencia de otros casos, el cálculo de la parte entera no plantea problemas ya que:

$$\left\lfloor \frac{m+\sqrt{d}}{w} \right\rfloor = \begin{cases} \left\lfloor \dfrac{m+\lfloor\sqrt{d}\rfloor}{w} \right\rfloor & \text{si} \quad w>0, \\ \left\lfloor \dfrac{m+\lceil\sqrt{d}\rceil}{w} \right\rfloor & \text{si} \quad w<0. \end{cases}$$

Programación. *En la sección A.4 del apéndice aparece nuestra implementación del algoritmo anterior en el software* Mathematica.

Fijamos ahora nuestra atención en las fracciones continuas puramente periódicas.

Teorema 2.21. *La EFCS de un número irracional cuadrático ξ es puramente periódica si y sólo si $\xi>1$ y $-1<\widehat{\xi}<0$.*

Demostración. Supongamos que la EFCS de ξ es puramente periódica. Pongamos $\xi=[\overline{a_0;a_1,\ldots,a_{\ell-1}}]$, donde $a_i\geq 1$ para $i=0,\ldots,\ell-1$. Obsérvese que $\xi>\lfloor\xi\rfloor=a_0\geq 1$. Probamos a continuación que $-1<\widehat{\xi}<0$. Por la proposición 2.4, tenemos:

$$\xi = [a_0;a_1,\ldots,a_{\ell-1},\xi] = \frac{\xi p_{\ell-1}+p_{\ell-2}}{\xi q_{\ell-1}+q_{\ell-2}}.$$

Operando aquí, vemos que ξ es raíz del siguiente polinomio cuadrático:

$$f(x) = q_{\ell-1}x^2+(q_{\ell-2}-p_{\ell-1})x-p_{\ell-2}.$$

Las raíces de $f(x)$ son pues ξ y $\widehat{\xi}$. Como $\xi>1$, basta mostrar que $f(x)$ posee una raíz en el intervalo abierto $]-1,0[$. Usaremos el teorema de Bolzano. Antes nótese que las fórmulas 2.8 nos dan que $p_n>0$ ya que $a_n\geq 1$ para todo $n\geq 0$. Evaluamos f en 0 y -1:

$$\begin{aligned} f(0) &= -p_{\ell-2}<0, \\ f(-1) &= q_{\ell-1}-q_{\ell-2}+p_{\ell-1}-p_{\ell-2} \overset{(2.8)}{=} a_{\ell-1}q_{\ell-2}+q_{\ell-3}-q_{\ell-2}+a_{\ell-1}p_{\ell-2}+p_{\ell-3}-p_{\ell-2} \\ &= (q_{\ell-2}+p_{\ell-2})(a_{\ell-1}-1)+q_{\ell-3}+p_{\ell-3} \;\geq\; q_{\ell-3}+p_{\ell-3} \;>0. \end{aligned}$$

Por tanto, $\widehat{\xi}\in]-1,0[$. Esto prueba la condición necesaria. Procedemos con la suficiente.

Supongamos que $\xi>1$ y $-1<\widehat{\xi}<0$. Calculamos la EFCS de ξ mediante el algoritmo 2.11. Aplicamos la conjugación a la relación de recurrencia. Obtenemos:

$$\widehat{\xi_0}=\widehat{\xi}, \qquad \widehat{\xi_i} = a_i+\frac{1}{\widehat{\xi_{i+1}}}, \qquad i\geq 0. \tag{2.21}$$

Sabemos que $a_i\geq 1$ para $i\geq 1$. También $a_0\geq 1$ pues, usando la hipótesis, $a_0=\lfloor\xi\rfloor\geq 1$. Demostramos por inducción que $-1<\widehat{\xi_i}<0$ para todo $i\geq 0$.

- *Caso inicial:* $i=0$. Supuesto por hipótesis.
- *Hipótesis de inducción.* Lo suponemos cierto para i.

▪ *Paso de inducción.* Mostramos que $-1 < \widehat{\xi_{i+1}} < 0$. Operando en la hipótesis de inducción, obtenemos:

$$\frac{1}{\widehat{\xi_{i+1}}} = \widehat{\xi_i} - a_i < -a_i \leq -1.$$

De aquí extraemos que $\widehat{\xi_{i+1}} < 0$, ya que su inverso lo es, y que $\widehat{\xi_{i+1}} > -1$. Así queda probada la afirmación.

Unida a la ecuación 2.21, dicha afirmación nos da:

$$0 < -a_i - \frac{1}{\widehat{\xi_{i+1}}} < 1.$$

Entonces,

$$a_i = \left\lfloor -\frac{1}{\widehat{\xi_{i+1}}} \right\rfloor.$$

Vimos en la demostración del teorema 2.20 que, cuando ξ es irracional y cuadrático, existen $j, k \in \mathbb{N}$ con $0 < j < k$ tales que $\xi_j = \xi_k$. Entonces, $\widehat{\xi_j} = \widehat{\xi_k}$, y, por tanto:

$$a_{j-1} = \left\lfloor -\frac{1}{\widehat{\xi_j}} \right\rfloor = \left\lfloor -\frac{1}{\widehat{\xi_k}} \right\rfloor = a_{k-1}.$$

Esto implica que:

$$\xi_{j-1} = a_{j-1} + \frac{1}{\xi_j} = a_{k-1} + \frac{1}{\xi_k} = \xi_{k-1}.$$

Así que $\xi_{j-1} = \xi_{k-1}$ y $\widehat{\xi_{j-1}} = \widehat{\xi_{k-1}}$. Aplicando otra vez el mismo razonamiento obtenemos que $\xi_{j-2} = \xi_{k-2}$. Repitiendo este proceso llegamos al final a que $\xi_0 = \xi_{k-j}$. Pongamos $l = k - j$. Demostramos por inducción que $\xi_t = \xi_{t+l}$ para todo $t \geq 0$.

▪ *Caso inicial:* $t = 0$. Ya probado.

▪ *Hipótesis de inducción.* Suponemos que la afirmación es cierta para t.

▪ *Paso de inducción.* Como $\xi_t = \xi_{t+l}$, tenemos que $a_t = \lfloor \xi_t \rfloor = \lfloor \xi_{t+l} \rfloor = a_{t+l}$. Entonces:

$$\xi_{t+1} = \frac{1}{\xi_t - a_t} = \frac{1}{\xi_{t+l} - a_{t+l}} = \xi_{t+l+1}.$$

Por tanto, $a_t = a_{t+l}$ para todo $t \geq 0$. Es decir, la EFCS de ξ es puramente periódica. ■

Acabamos este capítulo con el teorema de Lagrange, que descubre un vínculo entre la longitud del periodo de la EFCS de $\sqrt{d}$ y $\lfloor \sqrt{d} \rfloor$. También nos da una información útil sobre los valores de w_i en el cálculo de la EFCS de $\sqrt{d}$ mediante el algoritmo 2.19. Este resultado es la otra pieza fundamental, junto al teorema 2.18, en la resolución de la ecuación de Pell. Véanse la proposición 3.2 y el teorema 3.4.

Teorema 2.22 (Lagrange). *Sea $d \in \mathbb{N}$ que no es un cuadrado. La EFCS de $\sqrt{d}$ tiene la forma*

$$\sqrt{d} = [a_0; \overline{a_1, \ldots, a_{\ell-1}, 2a_0}],$$

donde $a_0 = \lfloor \sqrt{d} \rfloor$ y ℓ es la longitud del periodo. Además, en las ecuaciones 2.19 aplicadas a $\xi_0 = \sqrt{d}$ se cumple que:

(i) $w_i = 1$ *si y sólo si* $\ell \mid i$.

(ii) $w_i \neq -1$ *para todo* $i \geq 0$.

Demostración. Consideremos el número irracional $\lfloor\sqrt{d}\rfloor+\sqrt{d}$. Este número cumple las condiciones del teorema 2.21: $\lfloor\sqrt{d}\rfloor+\sqrt{d}>1$ y $-1<\lfloor\sqrt{d}\rfloor-\sqrt{d}<0$. Para la segunda condición nótese que $0<\sqrt{d}-\lfloor\sqrt{d}\rfloor<1$. En virtud de ese teorema, la EFCS de $\lfloor\sqrt{d}\rfloor+\sqrt{d}$ es puramente periódica. Pongamos

$$\lfloor\sqrt{d}\rfloor+\sqrt{d} \;=\; [\overline{c_0;c_1,\ldots,c_{\ell-1}}] \;=\; [c_0;\overline{c_1,\ldots,c_{\ell-1},c_0}], \tag{2.22}$$

donde ℓ es la longitud del periodo. Recuérdese que $c_0=\lfloor\lfloor\sqrt{d}\rfloor+\sqrt{d}\rfloor=2\lfloor\sqrt{d}\rfloor$. Ahora calculamos:

$$\begin{aligned}\sqrt{d} &= -\lfloor\sqrt{d}\rfloor+\left(\lfloor\sqrt{d}\rfloor+\sqrt{d}\right)\\ &= -\lfloor\sqrt{d}\rfloor+[2\lfloor\sqrt{d}\rfloor;\overline{c_1,\ldots,c_{\ell-1},c_0}]\\ &= [\lfloor\sqrt{d}\rfloor;\overline{c_1,\ldots,c_{\ell-1},c_0}].\end{aligned}$$

Escribiendo $a_0=\lfloor\sqrt{d}\rfloor$ y $a_i=c_i$ para $i=1,\ldots,\ell-1$, obtenemos:

$$\sqrt{d} \;=\; [a_0;\overline{a_1,\ldots,a_{\ell-1},2a_0}].$$

Esto establece la primera afirmación.

Joseph-Louis Lagrange
(1736-1813)

Para probar las otras dos retomamos la expresión 2.22. Para cada $i\geq 0$ ponemos:

$$\xi_i \;=\; [c_i;c_{i+1},c_{i+2},\ldots].$$

Nótese que ξ_i se define a partir de ξ_0 suprimiendo sus i primeros términos. Entonces, ξ_i es puramente periódica, ya que ξ_0 lo es, y $\xi_0=\xi_{n\ell}$ para todo $n\in\mathbb{N}$. Mostramos a continuación que, de hecho, al ser ℓ mínimo, se cumple que:

(†) $\xi_i=\xi_0$ si y sólo si $\ell\mid i$.

Sólo la condición necesaria requiere demostración. Dividimos i entre ℓ. Pongamos $i=\ell q+r$ con $q,r\in\mathbb{N}$ y $0\leq r<\ell$. Supongamos que $r\neq 0$. Entonces, para cada $n\in\mathbb{N}$ tendríamos $c_n=c_{n+i}=c_{n+\ell q+r}=c_{n+r}$, lo que nos dice que la longitud del periodo, ℓ, debe ser menor o igual que r, una contradicción. Luego, i es un múltiplo de ℓ.

Aplicamos el algoritmo 2.19 al número irracional $\lfloor\sqrt{d}\rfloor+\sqrt{d}$:

$$\begin{aligned}&\xi_0=\lfloor\sqrt{d}\rfloor+\sqrt{d}=\frac{m_0+\sqrt{d}}{w_0}, \qquad m_0=\lfloor\sqrt{d}\rfloor,\quad w_0=1,\quad w_0\mid d-m_0^2.\\ &a_i=\lfloor\xi_i\rfloor,\qquad \xi_i=\frac{m_i+\sqrt{d}}{w_i},\qquad m_{i+1}=a_iw_i-m_i,\qquad w_{i+1}=\frac{d-m_{i+1}^2}{w_i},\qquad i\geq 0,\end{aligned} \tag{2.23}$$

(i) Debemos mostrar que $w_i=1$ si y sólo si $\ell\mid i$. Supongamos que $w_i=1$. Entonces, $\xi_i=m_i+\sqrt{d}$. Como la EFCS de ξ_i es puramente periódica, según el teorema 2.21, debe cumplirse que $-1<\widehat{\xi_i}<0$. Esto es, $-1<m_i-\sqrt{d}<0$. Restando aquí m_i y multiplicando por -1 obtenemos $m_i<\sqrt{d}<m_i+1$. Luego, $m_i=\lfloor\sqrt{d}\rfloor$ y, por tanto, $\xi_i=\xi_0$. La afirmación (†) nos da que ℓ divide a i.

Recíprocamente, supongamos que $i=j\ell$. De (2.23) tenemos:

$$\frac{m_{j\ell}+\sqrt{d}}{w_{j\ell}} \;=\; \xi_{j\ell} \;=\; \xi_0 \;=\; \frac{m_0+\sqrt{d}}{w_0} \;=\; \lfloor\sqrt{d}\rfloor+\sqrt{d}.$$

Operando aquí llegamos a:

$$m_{j\ell} - w_{j\ell}\lfloor\sqrt{d}\rfloor = (w_{j\ell} - 1)\sqrt{d}.$$

El lado izquierdo de esta igualdad es racional y el derecho irracional. Luego, $w_{j\ell} - 1 = 0$, es decir, $w_{j\ell} = 1$. Con esto termina la demostración de (i).

(ii) Debemos mostrar que $w_i \neq -1$ para todo $i \geq 0$. Supongamos, razonando por reducción al absurdo, que $w_i = -1$. Entonces, por las ecuaciones 2.23, $\xi_i = -m_i - \sqrt{d}$. Como ξ_i es puramente periódico, el teorema 2.21 nos dice que $\xi_i > 1$ y $-1 < \widehat{\xi_i} < 0$. Por tanto, $-m_i - \sqrt{d} > 1$ y $-1 < -m_i + \sqrt{d} < 0$. Esto nos conduce a la contradicción $\sqrt{d} < m_i < -\sqrt{d} - 1$. Así que $w_i \neq -1$. ■

Observación 2.23. *Las EFCS de $\sqrt{d}$ y $\lfloor\sqrt{d}\rfloor + \sqrt{d}$ son las mismas excepto en los valores de a_0 y m_0. Si le aplicamos a cada uno las fórmulas 2.19, para $i = 0, 1$ obtenemos:*

ξ	a_0	m_0	w_0	m_1	w_1
$\sqrt{d}$	$\lfloor\sqrt{d}\rfloor$	0	1	$\lfloor\sqrt{d}\rfloor$	$d - \lfloor\sqrt{d}\rfloor^2$
$\sqrt{d} + \lfloor\sqrt{d}\rfloor$	$2\lfloor\sqrt{d}\rfloor$	$\lfloor\sqrt{d}\rfloor$	1	$\lfloor\sqrt{d}\rfloor$	$d - \lfloor\sqrt{d}\rfloor^2$

Como los valores iniciales w_0, m_1 y w_1 son los mismos para ambos números, las fórmulas de recurrencia 2.19 implican que los valores de a_i, m_i y w_i también lo son para todo $i \geq 1$. La ventaja de trabajar con $\lfloor\sqrt{d}\rfloor + \sqrt{d}$ es que su EFCS es puramente periódica.

Notas bibliográficas

En la preparación de este capítulo hemos seguido principalmente [15, Capítulo 7]. Por motivos de formación, hemos incluido demostraciones, ejercicios y detalles que se dejaban al lector, muchos de los cuales requerían inducción matemática. También han ayudado mucho a nuestra compresión de este apasionante tema los libros [10], [17], [6], [18] y [7]. A ellos referimos al lector para profundizar más. Para los aspectos históricos recomendamos [7]. La cita de Knuth está tomada de [13, Capítulo 5]. Para el cálculo de la EFCS de números trascendentes, como π o e, referimos a [6].

Nuestra discusión de la aproximación mediante fracciones continuas se ha limitado a aquellos aspectos necesarios para la resolución de la ecuación de Pell. Referimos al lector a [6, Sección 1.4] para un tratamiento más profuso. Es obligado resaltar aquí el teorema de aproximación de Dirichlet y el teorema de Hurwitz. El uso de las fracciones continuas para aproximar números racionales cobra sentido cuando se trata con fracciones enormemente grandes. Una situación así surgió en el diseño del planetario de Huygens en 1680 con la proporción entre las órbitas de los distintos planetas. Recomendamos para esto [18, Capítulo 4], [W7] y [W8].

Tampoco hemos entrado en los aspectos computacionales de los algoritmos. Cabe mencionar dos resultados en esta dirección. El teorema de Lamé, que afirma: sean $a, b \in \mathbb{N}$ con $a > b > 0$. El número de divisiones necesarias en el algoritmo de Euclides para calcular $\mathrm{mcd}(a, b)$ es menor que 5 veces el número de cifras decimales de b. El otro resultado afirma que el orden de complejidad del algoritmo 2.19 para calcular la EFCS de un número irracional cuadrático es $\sqrt{d}\log d$, véase [18, página 50].

Créditos fotográficos

El icono de ordenador usado para los apartados de programación fue descargado de https://www.flaticon.es/. La imagen de Joseph-Louis Lagrange de la página anterior está tomada de [W9].

3 Resolución de la ecuación de Pell y problema de Arquímedes

Cualquiera capaz de resolver $x^2 - 92y^2 = 1$
en el plazo de un año, es un matemático.

Brahmagupta (598-660),
matemático y astrónomo hindú.

Tras todo el esfuerzo realizado en el capítulo anterior, que ha requerido literalmente la mitad de este trabajo, ya estamos preparados en este capítulo para resolver completamente la ecuación de Pell. Nuestro conocimiento de la forma de las soluciones y el algoritmo para calcularlas mediante fracciones continuas nos permitirá resolver, con la ayuda del ordenador, el problema del ganado de Arquímedes.

3.1 Resolución completa de la ecuación de Pell

Sea $d \in \mathbb{N}$ que no es un cuadrado. Aplicamos el algoritmo 2.19 a $\sqrt{d}$ para calcular su EFCS. Consideremos los convergentes $\left\{\frac{p_n}{q_n}\right\}_{n\in\mathbb{N}}$ y los números $\{w_n\}_{n\in\mathbb{N}}$ que surgen de él. En los siguientes dos resultados ya se refleja claramente la relación entre estos convergentes y la solución de la ecuación de Pell.

Proposición 3.1. *Sea $d \in \mathbb{N}$ que no es un cuadrado. Entonces,*

$$p_n^2 - dq_n^2 = (-1)^{n+1} w_{n+1}, \qquad \forall n \in \mathbb{N}.$$

Demostración. Aplicamos el algoritmo 2.19 a $\xi_0 = \sqrt{d}$. Conservamos la notación usada allí. Por la proposición 2.4, tenemos:

$$\sqrt{d} = [a_0; a_1, \ldots, a_n, \xi_{n+1}] = \frac{\xi_{n+1} p_n + p_{n-1}}{\xi_{n+1} q_n + q_{n-1}}.$$

Sustituyendo en esta igualdad ξ_{n+1} por su valor en (2.19), resulta:

$$\sqrt{d} = \frac{\left(m_{n+1} + \sqrt{d}\right) p_n + w_{n+1} p_{n-1}}{\left(m_{n+1} + \sqrt{d}\right) q_n + w_{n+1} q_{n-1}}.$$

Operamos aquí de modo que en un lado de la igualdad queden los términos multiplicados por $\sqrt{d}$ y en el otro un número racional. Obtenemos:

$$\left(m_{n+1} q_n + w_{n+1} q_{n-1} - p_n\right)\sqrt{d} = m_{n+1} p_n + w_{n+1} p_{n-1} - d q_n.$$

Ambas expresiones deben ser cero:

$$\begin{aligned} m_{n+1} q_n + w_{n+1} q_{n-1} - p_n &= 0, \\ m_{n+1} p_n + w_{n+1} p_{n-1} - d q_n &= 0. \end{aligned}$$

Multiplicamos la primera igualdad por p_n y la segunda por $-q_n$ y después sumamos. Resulta:

$$p_n^2 - dq_n^2 = (p_n q_{n-1} - p_{n-1} q_n) w_{n+1}.$$

La proposición 2.6(i) finalmente nos da:

$$p_n^2 - dq_n^2 = (p_n q_{n-1} - p_{n-1} q_n) w_{n+1} = (-1)^{n-1} w_{n+1} = (-1)^{n+1} w_{n+1}.$$

■

De la anterior proposición se deduce:

Proposición 3.2. *Sea ℓ la longitud del periodo de la EFCS de $\sqrt{d}$. Entonces,*

$$p_{n\ell-1}^2 - dq_{n\ell-1}^2 = (-1)^{n\ell}, \qquad \forall n \in \mathbb{N}.$$

Demostración. Sustituimos n por $n\ell - 1$ en la proposición anterior y usamos el teorema 2.22(i):

$$p_{n\ell-1}^2 - dq_{n\ell-1}^2 = (-1)^{n\ell-1+1} w_{n\ell-1+1} = (-1)^{n\ell} w_{n\ell} = (-1)^{n\ell}.$$

■

La igualdad precedente muestra nítidamente la relación entre los convergentes de la EFCS de $\sqrt{d}$ y la ecuación de Pell. Si ℓ es par, todo convergente proporciona una solución. Si ℓ es impar, los convergentes de índice par proporcionan soluciones. A continuación profundizamos más en esta relación.

Teorema 3.3. *Sea $d \in \mathbb{N}$ que no es un cuadrado. Sea $(u, v) \in \mathbb{Z}^+ \times \mathbb{Z}^+$ una solución de la ecuación*

$$x^2 - dy^2 = 1. \tag{3.1}$$

Entonces, $u = p_n$ y $v = q_n$ para algún convergente $\frac{p_n}{q_n}$ de la EFCS de $\sqrt{d}$.

Demostración. La estrategia consiste en mostrar que $\frac{u}{v}$ es un convergente de la EFCS de $\sqrt{d}$ aplicando el teorema 2.18. Tenemos:

$$1 = u^2 - dv^2 = \left(u - v\sqrt{d}\right)\left(u + v\sqrt{d}\right) = \left(\frac{u}{v} - \sqrt{d}\right) v \left(u + v\sqrt{d}\right).$$

Entonces,

$$\frac{u}{v} - \sqrt{d} = \frac{1}{v\left(u + v\sqrt{d}\right)}.$$

De aquí obtenemos:

$$0 < \frac{u}{v} - \sqrt{d} < \frac{\sqrt{d}}{v\left(u + v\sqrt{d}\right)} = \frac{1}{v^2\left(\frac{u}{v\sqrt{d}} + 1\right)}.$$

La primera desigualdad implica que $\frac{u}{v\sqrt{d}} > 1$. Así que el término entre paréntesis en el denominador de la fracción anterior es mayor que 2. Por tanto, concluimos que:

$$\left|\frac{u}{v} - \sqrt{d}\right| < \frac{1}{2v^2}.$$

El teorema 2.18 nos dice que $\frac{u}{v}$ es un convergente de la EFCS de $\sqrt{d}$. Pongamos $\frac{u}{v} = \frac{p_n}{q_n}$. Entonces, $uq_n = vp_n$. Como (u,v) es solución de (3.1), debe ser $\mathrm{mcd}(u,v) = 1$. Recordemos que $\mathrm{mcd}(p_n,q_n) = 1$. El teorema fundamental de la aritmética aplicado a $uq_n = vp_n$ nos da $u = p_n$ y $v = q_n$. ■

Llega el momento de recompensar todo el esfuerzo realizado. Ya estamos en condiciones de resolver completamente la ecuación de Pell. Recordemos que el análisis preliminar realizado en la sección 1.1 y el teorema 1.10 redujeron la tarea a encontrar la solución fundamental. No obstante, enunciaremos el resultado de forma exhaustiva:

Teorema 3.4. *Sea $d \in \mathbb{N}$ que no es un cuadrado. Consideremos la ecuación de Pell*

$$x^2 - dy^2 = 1. \tag{3.2}$$

Sean $\left\{\frac{p_n}{q_n}\right\}_{n\in\mathbb{N}}$ los convergentes de la EFCS de $\sqrt{d}$. Sea ℓ su periodo. Entonces:

(i) La solución fundamental de (3.2) es

$$(x_1,y_1) = \begin{cases} (p_{\ell-1},q_{\ell-1}) & \text{si } \ell \text{ es par,} \\ (p_{2\ell-1},q_{2\ell-1}) & \text{si } \ell \text{ es impar.} \end{cases}$$

(ii) Toda solución entera y positiva de (3.2) es de la forma (x_n,y_n), donde x_n e y_n están definidos por la siguiente fórmula en $\mathbb{Z}[\sqrt{d}]$:

$$x_n + y_n\sqrt{d} = \left(x_1 + y_1\sqrt{d}\right)^n, \quad n \in \mathbb{N}. \tag{3.3}$$

Esta expresión se puede describir recursivamente como:

$$\begin{cases} x_{n+1} = x_nx_1 + dy_ny_1, \\ y_{n+1} = x_ny_1 + y_nx_1, \quad n \in \mathbb{N}. \end{cases}$$

(iii) Se cumple que

$$(x_n,y_n) = \begin{cases} (p_{n\ell-1},q_{n\ell-1}) & \text{si } \ell \text{ es par,} \\ (p_{2n\ell-1},q_{2n\ell-1}) & \text{si } \ell \text{ es impar.} \end{cases}$$

Demostración. Sea $j \in \mathbb{N}$. La proposición 3.2 muestra que $(p_{j\ell-1},q_{j\ell-1})$ es solución de la ecuación de Pell cuando ℓ es par y $(p_{2j\ell-1},q_{2j\ell-1})$ lo es cuando ℓ es impar. Veamos que, recíprocamente, toda solución positiva (x,y) es de esa forma. Por el teorema 3.3 sabemos que $x = p_n$ e $y = q_n$ para algún convergente $\frac{p_n}{q_n}$ de la EFCS de $\sqrt{d}$. Juntándolo con la proposición 3.1, obtenemos $1 = x^2 - dy^2 = p_n^2 - dq_n^2 = (-1)^{n+1}w_{n+1}$. Así que $1 = (-1)^{n+1}w_{n+1}$. Ahora, $w_{n+1} \neq -1$ según el teorema 2.22(ii). Por tanto, esta igualdad es cierta si y sólo si $w_{n+1} = 1$ y $(-1)^{n+1} = 1$. También, según el teorema 2.22(i), $w_{n+1} = 1$ si y sólo si ℓ divide a $n+1$. Luego, $n = m\ell - 1$ para algún $m \in \mathbb{N}$. Queda $1 = (-1)^{n+1} = (-1)^{m\ell}$. Si ℓ es par, ponemos $m = j$. Si ℓ es impar, $(-1)^{m\ell} = 1$ si y sólo si m es par. Es decir, $m = 2j$ para algún $j \in \mathbb{N}$. Por tanto, $n = 2j\ell - 1$.

(i) Recordemos el orden definido en el conjunto de soluciones, véase el lema 1.8: $(x,y) \preceq (x',y')$ si y sólo si $x \leq x'$ e $y \leq y'$. Este orden es total. Por otro lado, las sucesiones $\{p_n\}_{n\in\mathbb{N}}$ y $\{q_n\}_{n\in\mathbb{N}}$ son crecientes. Dos soluciones (p_n,q_n) y $(p_{n'},q_{n'})$ cumplen pues

$(p_n, q_n) \preceq (p_{n'}, q_{n'})$ si y sólo si $n \leq n'$. Según el párrafo anterior, la solución mínima positiva (x_1, y_1) es $(p_{\ell-1}, q_{\ell-1})$ cuando ℓ es par y $(p_{2\ell-1}, q_{2\ell-1})$ cuando ℓ es impar.

(ii) Esto ya fue probado en el teorema 1.10.

(iii) Esta afirmación es consecuencia de que el conjunto de soluciones está totalmente ordenado. Para cada $n \in \mathbb{N}$ denotemos por (r_n, s_n) a la solución $(p_{n\ell-1}, q_{n\ell-1})$ si ℓ es par y $(p_{2n\ell-1}, q_{2n\ell-1})$ si ℓ es impar. Probamos la afirmación por inducción:

- *Caso inicial:* $n = 1$. Mostrado en (i).
- *Hipótesis de inducción.* Suponemos que $(x_n, y_n) = (r_n, s_n)$.
- *Paso de inducción.* Lo mostramos para $n+1$. Tomamos la solución (x_{n+1}, y_{n+1}) construida según (3.3). Por lo demostrado al principio, debe ser $(x_{n+1}, y_{n+1}) = (r_m, s_m)$ para algún $m \in \mathbb{N}$. Puesto que $s_m = y_{n+1} > y_n = s_n$, tenemos $m > n$. Entonces, $m \geq n+1$. Supongamos que $m > n+1$. Como $y_{n+1} = s_m > s_{n+1} > s_n = y_n$, tendríamos que (r_{n+1}, s_{n+1}) sería una solución entre (x_n, y_n) y (x_{n+1}, y_{n+1}), en contra de (ii). Por tanto, $m = n+1$. ■

Ilustramos el teorema anterior con varios ejemplos:

Ejemplos 3.5. *Consideremos la ecuación de Pell* $x^2 - 92y^2 = 1$. *Hallamos su solución fundamental calculando la EFCS de* $\sqrt{92}$ *mediante el algoritmo 2.19. Recordemos que, según el teorema 2.22, la longitud del periodo* ℓ *se detecta mediante la condición* $a_\ell = 2a_0$. *La siguiente tabla muestra nuestros cálculos:*

n	0	1	2	3	4	5	6	7	8
m_n	0	9	2	6	8	8	6	2	9
w_n	1	11	8	7	4	7	8	11	1
a_n	⑨	1	1	2	4	2	1	1	⑱
$\frac{p_n}{q_n}$	9	10	$\frac{19}{2}$	$\frac{48}{5}$	$\frac{211}{22}$	$\frac{470}{49}$	$\frac{681}{71}$	$\frac{1151}{120}$	$\frac{21399}{2231}$

La EFCS de $\sqrt{92}$ *es* $[9; \overline{1,1,2,4,2,1,1,18}]$. *El periodo es* 8 *(par). La solución fundamental viene dada por* $(p_{8-1}, q_{8-1}) = (p_7, q_7) = (1151, 120)$.

Consideremos ahora la ecuación de Pell $x^2 - 53y^2 = 1$. *La siguiente tabla muestra nuestros cálculos de la EFCS de* $\sqrt{53}$ *al aplicar el algoritmo 2.19:*

n	0	1	2	3	4	5	6	7	8	9
m_n	0	7	5	2	5	7	7	5	2	5
w_n	1	4	7	7	5	1	4	7	7	5
a_n	⑦	3	1	1	3	⑭	3	1	1	3
$\frac{p_n}{q_n}$	7	$\frac{22}{3}$	$\frac{29}{4}$	$\frac{51}{7}$	$\frac{182}{25}$	$\frac{2599}{357}$	$\frac{7979}{1096}$	$\frac{10578}{1453}$	$\frac{18557}{2549}$	$\frac{66249}{9100}$

La EFCS de $\sqrt{53}$ *es* $[7; \overline{3,1,1,3,14}]$. *El periodo es* 5 *(impar). La solución fundamental viene dada por* $(p_{2\cdot5-1}, q_{2\cdot5-1}) = (p_9, q_9) = (66249, 9100)$. *Obsérvese en la tabla la repetición de los valores de* m_n, w_n *y* a_n *para* $n = 6, 7, 8, 9$.

Programación. *En la sección A.6 del apéndice aparece nuestra implementación en* Mathematica *de un programa para calcular la solución fundamental de la ecuación de Pell. Con ese programa hemos elaborado la tabla de la página 54 que lista las soluciones fundamentales de la ecuación de Pell para $d < 100$. La misma sección contiene otro programa para calcular potencias de la solución fundamental.*

3.2 El problema del ganado de Arquímedes

Volvamos al enunciado del problema del ganado de Arquímedes de la página 2. Llamamos x, y, z, t al número de toros blancos, negros, moteados y amarillos respectivamente. Similarmente, llamamos x', y', z', t' al número de vacas de esos mismos colores. Las condiciones de la primera parte del problema se traducen en los dos sistemas de ecuaciones lineales siguientes:

$$\begin{cases} x = \left(\frac{1}{2}+\frac{1}{3}\right)y + t \\ y = \left(\frac{1}{4}+\frac{1}{5}\right)z + t \\ z = \left(\frac{1}{6}+\frac{1}{7}\right)x + t \end{cases} \qquad \begin{cases} x' = \left(\frac{1}{3}+\frac{1}{4}\right)(y+y') \\ y' = \left(\frac{1}{4}+\frac{1}{5}\right)(z+z') \\ z' = \left(\frac{1}{5}+\frac{1}{6}\right)(t+t') \\ t' = \left(\frac{1}{6}+\frac{1}{7}\right)(x+x') \end{cases} \tag{3.4}$$

Resolvemos los dos sistemas detalladamente con el fin de resaltar la magnitud de los números que surgen y la dificultad de operar con ellos en una época en la que no se disponía de la capacidad de cálculo actual. Llama poderosamente la atención que aparezcan números tan grandes habiendo utilizado en el enunciado los más pequeños posibles para formar fracciones: 2, 3, 4, 5, 6 y 7.

Resolvemos el primer sistema. Comenzamos restando a la primera ecuación la segunda y después la tercera. Obtenemos:

$$x - y = \frac{5}{6}y - \frac{9}{20}z \quad\Rightarrow\quad x = \frac{11}{6}y - \frac{9}{20}z.$$
$$x - z = \frac{5}{6}y - \frac{13}{42}x \quad\Rightarrow\quad \frac{55}{42}x = \frac{5}{6}y + z.$$

En estas dos ecuaciones, sumamos a la segunda la primera multiplicada por $\frac{20}{9}$. Queda:

$$\left(\frac{20}{9}+\frac{55}{42}\right)x = \left(\frac{110}{27}+\frac{5}{6}\right)y \quad\Rightarrow\quad \frac{445}{126}x = \frac{265}{54}y \quad\Rightarrow\quad \frac{5\cdot 89}{2\cdot 3^2\cdot 7}x = \frac{5\cdot 53}{2\cdot 3^3}y$$
$$\Rightarrow\quad x = \frac{7\cdot 53}{3\cdot 89}y = \frac{371}{267}y.$$

Sustituimos el valor de x obtenido en la primera ecuación del sistema:

$$\frac{371}{267}y = \frac{5}{6}y + t \quad\Rightarrow\quad t = \frac{371\cdot 2 - 5\cdot 89}{534}y = \frac{297}{534}y = \frac{3^3\cdot 11}{2\cdot 3\cdot 89}y = \frac{99}{178}y.$$

Sustituimos el valor de t obtenido en la segunda ecuación del sistema:

$$y = \frac{9}{20}z + \frac{99}{178}y \quad\Rightarrow\quad \frac{79}{178}y = \frac{9}{20}z \quad\Rightarrow\quad \frac{79}{89}y = \frac{9}{10}z \quad\Rightarrow\quad z = \frac{79\cdot 10}{89\cdot 9}y = \frac{790}{801}y.$$

La solución del primer sistema es pues:

$$x = \frac{371}{267}y, \qquad z = \frac{790}{801}y, \qquad t = \frac{99}{178}y.$$

Como x, z y t son números naturales, y debe ser divisible por el mínimo común múltiplo de $267, 801$ y 178. Tenemos $267 = 3 \cdot 89$, $801 = 3^2 \cdot 89$ y $178 = 2 \cdot 89$. Luego, $\mathrm{mcm}(267, 801, 178) = 2 \cdot 3^2 \cdot 89 = 1602$. Las soluciones enteras positivas del primer sistema de ecuaciones lineales son:

$$(x, y, z, t) = (2226, 1602, 1580, 891)\lambda, \qquad \lambda \in \mathbb{N}.$$

Resolvemos seguidamente el segundo sistema. Sustituimos x, y, z y t por los valores que acabamos de hallar. Obtenemos:

$$\begin{aligned}
x' &= \frac{7}{12}y + \frac{7}{12}y' = \frac{7 \cdot 1602}{12}\lambda + \frac{7}{12}y' = \frac{1869}{2}\lambda + \frac{7}{12}y', \\
y' &= \frac{9}{20}z + \frac{9}{20}z' = \frac{9 \cdot 1580}{20}\lambda + \frac{9}{20}z' = 711\lambda + \frac{9}{20}z', \\
z' &= \frac{11}{30}t + \frac{11}{30}t' = \frac{11 \cdot 891}{30}\lambda + \frac{11}{30}t' = \frac{3267}{10}\lambda + \frac{11}{30}t', \\
t' &= \frac{13}{42}x + \frac{13}{42}x' = \frac{13 \cdot 2226}{42}\lambda + \frac{13}{42}x' = 689\lambda + \frac{13}{42}x'.
\end{aligned} \tag{3.5}$$

Sumamos a la primera ecuación la segunda multiplicada por $\frac{7}{12}$. Queda:

$$x' = \left(\frac{1869}{2} + \frac{7 \cdot 711}{12}\right)\lambda + \frac{7 \cdot 9}{12 \cdot 20}z' = \frac{16191}{12}\lambda + \frac{21}{80}z' = \frac{5397}{4}\lambda + \frac{21}{80}z'.$$

Sumamos a la tercera ecuación la cuarta multiplicada por $\frac{11}{30}$. Queda:

$$z' = \left(\frac{3267}{10} + \frac{11 \cdot 689}{30}\right)\lambda + \frac{11 \cdot 13}{30 \cdot 42}x' = \frac{17380}{30}\lambda + \frac{143}{1260}x' = \frac{1738}{3}\lambda + \frac{143}{1260}x'.$$

En estas dos últimas ecuaciones, sumamos a la primera la segunda multiplicada por $\frac{21}{80}$. Queda:

$$x' = \left(\frac{5397}{4} + \frac{21 \cdot 1738}{80 \cdot 3}\right)\lambda + \frac{21 \cdot 143}{80 \cdot 1260}x' = \frac{360318}{240}\lambda + \frac{143}{4800}x' = \frac{60053}{40}\lambda + \frac{143}{4800}x'.$$

Operamos aquí:

$$\frac{60053}{40}\lambda = \left(1 - \frac{143}{4800}\right)x' = \frac{4657}{4800}x' \quad \Rightarrow \quad x' = \frac{60053 \cdot 120}{4657} = \frac{7206360}{4657}\lambda.$$

(Resulta que 4657 es primo. Un número primo curioso además: sus dígitos son cuatro números consecutivos de los usados en el enunciado.) Sustituimos el valor hallado de x' en la primera ecuación del sistema 3.5. Queda:

$$\begin{aligned}
\frac{7206360}{4657}\lambda = \frac{1869}{2}\lambda + \frac{7}{12}y' \quad \Rightarrow \quad \frac{7}{12}y' &= \left(\frac{7206360 \cdot 2 - 4657 \cdot 1869}{2 \cdot 4657}\right)\lambda \\
\Rightarrow \quad \frac{7}{12}y' = \frac{5708787}{2 \cdot 4657}\lambda \quad \Rightarrow \quad y' &= \frac{6 \cdot 5708787}{7 \cdot 4657}\lambda = \frac{4893246}{4657}\lambda.
\end{aligned}$$

Sustituimos el valor hallado de y' en la segunda ecuación del sistema 3.5. Queda:

$$\frac{4893246}{4657}\lambda = 711\lambda + \frac{9}{20}z' \Rightarrow \frac{9}{20}z' = \frac{4893246 - 4657\cdot 711}{4657}\lambda = \frac{1582119}{4657}\lambda$$
$$\Rightarrow z' = \frac{20\cdot 1582119}{9\cdot 4657} = \frac{3515820}{4657}\lambda.$$

Sustituimos el valor hallado de z' en la tercera ecuación del sistema 3.5. Queda:

$$\frac{3515820}{4657}\lambda = \frac{3267}{10}\lambda + \frac{11}{30}t' \Rightarrow \frac{11}{30}t' = \frac{3515820\cdot 10 - 4657\cdot 3267}{10\cdot 4657}\lambda$$
$$\Rightarrow \frac{11}{30}t' = \frac{19943781}{10\cdot 4657}\lambda \Rightarrow t' = \frac{3\cdot 19943781}{11\cdot 4657} = \frac{5439213}{4657}\lambda.$$

Puesto que x', y', z' y t' son números naturales, λ debe ser divisible por 4657. Pongamos $\lambda = 4657\mu$. Por tanto, las soluciones enteras positivas de los dos sistemas de ecuaciones lineales son:

$$\begin{aligned}(x', y', z', t') &= (7206360, 4893246, 3515820, 5439213)\mu,\\ (x, y, z, t) &= (10366482, 7460514, 7358060, 4149387)\mu, \qquad \mu \in \mathbb{N}.\end{aligned} \tag{3.6}$$

Solución de la primera parte del problema del ganado de Arquímedes. *Sumando estas cantidades obtenemos que el número de toros es* 29334443μ*, el de vacas es* 21054639μ *y el número total de reses en el rebaño del dios Helios es* 50389082μ*.*

Resolvemos a continuación la segunda parte. Aquí aparecen dos condiciones más: que $x+y$ sea un número cuadrado y que $z+t$ sea un número triangular. Analizamos ambas condiciones:

- El número $x+y$ es un cuadrado[1]. Calculamos $x+y$ usando las fórmulas 3.6:

$$x + y = (10366482 + 7460514)\mu = 17826996\mu = 2^2 \cdot \underbrace{3\cdot 11\cdot 29\cdot 4657\cdot \mu}.$$

Se pide que $x+y = c^2$ para algún $c \in \mathbb{N}$. Ponemos $k = 3\cdot 11\cdot 29\cdot 4657 = 4456749$. Por el teorema fundamental de la aritmética, $x+y$ es un cuadrado si y sólo si $k\mu$ lo es. Como los factores primos de k tienen exponente impar, $k\mu$ es un cuadrado si y sólo si

$$\mu = ks^2, \quad \text{con} \quad s \in \mathbb{N}. \tag{3.7}$$

- El número $z+t$ es triangular. Calculamos $z+t$ usando las fórmulas 3.6:

$$z + t = (7358060 + 4149387)\mu = 11507447\mu = 7\cdot 353\cdot 4657\cdot \mu. \tag{3.8}$$

Que sea triangular significa que $z+t = \frac{m(m+1)}{2}$ para algún $m \in \mathbb{N}$. Esto nos lleva a la ecuación $m^2 + m - 2(z+t) = 0$. Resolviéndola obtenemos:

$$m = \frac{-1 \pm \sqrt{8(z+t)+1}}{2}.$$

[1] Existe otra interpretación de esta condición que da lugar al llamado *problema de Wurm*. Aquí se entiende que los toros forman una figura cuadrada, un rectángulo, y que, por tanto, $x+y$ es el producto de dos números distintos. Este problema es más sencillo de resolver. Su resolución puede consultarse en [21, Sección 1.3]. Hay una solución que simula bastante bien un cuadrado: $x+y = 1409076\cdot 1485583$.

Como $m \in \mathbb{N}$, debe ocurrir que $8(z+t)+1$ sea un cuadrado. Esto es, $8(z+t)+1 = r^2$ para algún $r \in \mathbb{N}$. No hemos de preocuparnos por la fracción ya que $8(z+t)+1$ es impar, así que r también lo será y el numerador será par.

Juntándolo todo, tenemos pues:

$$r^2 \;=\; 8(z+t)+1 \overset{(3.8)}{=} 8\cdot(7\cdot 353\cdot 4657\cdot \mu)+1 \overset{(3.7)}{=} 8\cdot 7\cdot 353\cdot 4657\cdot(k\cdot s^2)+1.$$

Ponemos

$$\begin{aligned} d \;&=\; 8\cdot 7\cdot 353\cdot 4657\cdot k \;=\; 8\cdot 7\cdot 353\cdot 4657\cdot(3\cdot 11\cdot 29\cdot 4657) \\ &=\; 2\cdot 3\cdot 7\cdot 11\cdot 29\cdot 353\cdot(2\cdot 4657)^2 \;=\; 4729494\cdot 9314^2 \\ &=\; 410286423278424. \end{aligned} \tag{3.9}$$

Hemos llegado a la ecuación de Pell:

$$r^2 - ds^2 \;=\; 1, \qquad \text{con} \quad d = 410286423278424. \tag{3.10}$$

El valor de d es excesivamente grande para resolver esta ecuación con la capacidad de cálculo[2] de 1880. Amthor procedió en [1] del siguiente modo para reducir esta ecuación a una tratable con los medios de su época. Pongamos $D = 4729494$. Vemos en (3.9) que D es libre de cuadrados y que $d = D\cdot(2\cdot 4657)^2$. Nótese que si (u,v) es solución de la ecuación 3.10, entonces $(u, 2\cdot 4657\cdot v)$ es solución de esta otra ecuación de Pell:

$$x^2 - Dy^2 \;=\; 1, \qquad \text{con} \quad D = 4729494. \tag{3.11}$$

El valor con el que hemos de trabajar ahora es bastante más pequeño. En la sección A.7 del apéndice resolvemos esta ecuación utilizando los programas que hemos implementado anteriormente. La EFCS de $\sqrt{4729494}$ es:

$$\begin{aligned} [2174;\ &\overline{1,2,1,5,2,25,3,1,1,1,1,1,1,15,1,2,16,1,2,1,1,8,6,1,21,1,1,3,1,1,1,2,} \\ &\overline{2,6,1,1,5,1,17,1,1,47,3,1,1,6,1,1,3,47,1,1,17,1,5,1,1,6,2,2,1,1,1,3,} \\ &\overline{1,1,21,1,6,8,1,1,2,1,16,2,1,15,1,1,1,1,1,1,3,25,2,5,1,2,1,4348}]. \end{aligned}$$

La longitud del periodo es 92 (par). La solución fundamental viene dada por el convergente de índice 91. Nuestros cálculos allí dan:

$$\begin{aligned} x_1 \;&=\; 1099319867328297349798662328214335543901088049, \qquad \text{(45 dígitos)} \\ y_1 \;&=\; 505494852343150330744778197355404089863 40. \qquad \text{(41 dígitos)} \end{aligned}$$

Podemos escribir esta solución de modo más compacto en $\mathbb{Z}\big[\sqrt{4729494}\big]$ usando la identidad:

$$x + y\sqrt{D} \;=\; \left(\sqrt{\frac{x+1}{2}} + \sqrt{\frac{x-1}{2}}\right)^2.$$

Pongamos:

[2] Los medios actuales sí permiten resolver esta ecuación. En la sección A.7 del apéndice mostramos que la longitud del periodo de la EFCS de $\sqrt{d}$ es 203254 (par) y calculamos su solución fundamental. No obstante, la estrategia seguida por Amthor supone un ahorro considerable de cálculo.

$$w = \sqrt{\frac{x_1+1}{2}} + \sqrt{\frac{x_1-1}{2}}$$
$$= 300426607914281713365\sqrt{609} + 841295076778583932 58\sqrt{7766}.$$

(Cálculos realizados en la sección A.7.) Entonces:

$$x_1 + y_1\sqrt{4729494} = w^2.$$

Sabemos, por el teorema 3.4, que toda solución de la ecuación 3.11 es de la forma:

$$x_n + y_n\sqrt{4729494} = \left(x_1 + y_1\sqrt{4729494}\right)^n = w^{2n}, \quad n \in \mathbb{N}.$$

Para encontrar la solución $(u, 2 \cdot 4657 \cdot v)$ de (3.11), se debe hallar el menor n tal que y_n es divisible por $2 \cdot 4657$. Amthor averiguó, ayudándose de argumentos teóricos[3], que $n = 2329$. A partir de aquí mostró que el número total de dígitos en la solución más pequeña al problema es 206545 y dio como sus primeros cuatro dígitos 7766. El cuarto dígito resultó ser incorrecto: debe ser 0.

En la sección A.7 hemos realizado un programa que calcula n directamente. En este cálculo hemos experimentado la ventaja computacional de reducir modularmente primero y después efectuar potencias y no al revés. La solución fundamental (r_1, s_1) de (3.11) viene dada por $(x_{2329}, \frac{y_{2329}}{9314})$. Según (3.7), el valor de μ es $\mu = ks_1^2$. Sustituimos este valor en las fórmulas 3.6 y obtenemos la solución mínima a la segunda parte.

Solución mínima de la segunda parte del problema del ganado de Arquímedes. *La solución mínima viene dada por la siguiente tabla:*

Solución mínima	*Valor*	*No. dígitos*
Toros blancos (x)	159651 341800	206545
Toros negros (y)	114897 178600	206545
Toros moteados (z)	113319 894000	206545
Toros amarillos (t)	639034 026300	206544
Total toros	451770 440700	206545
Vacas blancas (x')	110982 564000	206545
Vacas negras (y')	753594 645400	206544
Vacas moteadas (z')	541460 318000	206544
Vacas amarillas (t')	837676 113700	206544
Total vacas	324256 641100	206545
Total de reses	776027 081800	206545

Comenta Amthor a propósito de la solución:

> *«Fácil es comprobar que una esfera que tuviera el diámetro de la Vía Láctea, que la luz tarda diez mil años en atravesar, podría contener tan solo una parte de este enorme número de animales, aunque cada uno de ellos tuviera el tamaño de la menor bacteria... Imprimir los ocho números de la solución, a 2500 cifras por página, requeriría un volumen de en torno a 660 páginas».*

[3] En [21, Sección 2.3] se da un argumento teórico, debido a Lenstra, que simplifica considerablemente la búsqueda. Usa reducción modular y teoría de cuerpos finitos. La idea es trabajar modularmente en el cuerpo finito $GF(4657^2) = \frac{\mathbb{Z}_{4657}[x]}{(x^2-4729494)}$, que es una extensión de grado 2 de $\mathbb{Z}_{4657}$. Un punto clave del argumento es que el grupo de Galois de esta extensión está generado por el automorfismo de Frobenius.

Terminaremos dando la solución completa a esta segunda parte del problema. Las soluciones (x_j, y_j) de (3.11) tal que y_j es divisible por 9314 vienen dadas por:

$$x_j + y_j\sqrt{4729494} \;=\; \left(x_1 + y_1\sqrt{4729494}\right)^{2329j} \;=\; w^{4658j}.$$

Usando el conjugado y la forma del inverso en $\mathbb{Z}\left[\sqrt{4729494}\right]$ podemos escribir:

$$2y_j\sqrt{4729494} \;=\; w^{4658j} - w^{-4658j}.$$

Entonces:

$$y_j^2 \;=\; \frac{1}{4\cdot 4729494}\left(w^{4658j} - w^{-4658j}\right)^2.$$

Sea (r_j, s_j) la j-ésima solución de la ecuación de Pell 3.10. Sabemos que $(r_j, s_j) = \left(x_j, \frac{y_j}{9314}\right)$. Recordemos de (3.7) que:

$$\mu_j \;=\; ks_j^2 \;=\; \frac{k}{9314^2}y_j^2 \;=\; \frac{4456749}{9314^2\cdot 4\cdot 4729494}y_j^2 \;=\; \frac{1}{368238304}\left(w^{4658j} - w^{-4658j}\right)^2.$$

Solución completa de la segunda parte del problema del ganado de Arquímedes. *La solución completa viene dada por:*

$$w \;=\; 300426607914281713365\sqrt{609} + 84129507677858393258\sqrt{7766}$$
$$\mu_j \;=\; \frac{1}{368238304}\left(w^{4658j} - w^{-4658j}\right)^2, \qquad j = 1, 2, 3, \ldots$$

j-ésima solución	*Toros*	*Vacas*	*Total*
Reses blancas	$10366482\mu_j$	$7206360\mu_j$	$17572842\mu_j$
Reses negras	$7460514\mu_j$	$4893246\mu_j$	$12353760\mu_j$
Reses moteadas	$7358060\mu_j$	$3515820\mu_j$	$10873880\mu_j$
Reses amarillas	$4149387\mu_j$	$5439213\mu_j$	$9588600\mu_j$
Todos los colores	$29334443\mu_j$	$21054639\mu_j$	$50389082\mu_j$

A la vista del tamaño de la solución surge inevitablemente la pregunta: ¿llegó realmente Arquímedes a resolver este problema? Parece poco probable que la capacidad de cálculo del siglo III a.C. lo permitiese. No obstante, hay que recordar que en su obra, *El contador de arena*, Arquímedes muestra su interés por los números grandes al preguntarse cuántos granos de arena harían falta para llenar el universo. En su discusión llega a manejar el número $10^{8\cdot 10^{16}}$.

La pregunta que sí nos deja con una duda razonable es: ¿sabía Arquímedes que el problema del ganado tenía solución? El conocimiento de las fracciones continuas de los antiguos griegos y el hecho de que en el propio trabajo de Arquímedes aparezcan dos convergentes de $\sqrt{3}$, uno de los cuales es solución de $x^2 - 3y^2 = 1$, sugiere que quizá Arquímedes sabía que la ecuación de Pell siempre admitía una solución no trivial, aunque quizá no poseyese una demostración formal de ello.

Notas bibliográficas

Para la primera sección de este capítulo hemos usado principalmente [15], con algunas contribuciones puntuales de [13]. Para la segunda sección hemos seguido la exposición de [12], añadiendo elementos tomados de [9, Sección 2.1], [21] y [W4]. Recomendamos al lector visitar la magnífica página temática de Arquímedes [W4].

4 Conclusiones

Las matemáticas puras son, a su manera,
la poesía de las ideas lógicas.

Albert Einstein (1879-1955),
físico alemán.

Desde el comienzo, el objetivo de este trabajo fue claro y concreto: la resolución de la ecuación de Pell. Esto me llevaría a realizar un recorrido por la historia de la matemática, desde la Grecia clásica hasta nuestros días, a introducirme en la teoría de fracciones continuas y a estudiar distintas aplicaciones de esta teoría y esta ecuación. Necesitaría conocimientos de las asignaturas de álgebra del grado, conocimientos de análisis matemático, específicamente sobre sucesiones y convergencia, y conocimientos y habilidades de programación. El carácter multidisciplinar de este proyecto fue una de las razones por las que lo escogí. Más tarde descubriría que el trabajo también me llevaría a saltar de ciencias a letras sumergiéndome en *La Odisea* de Homero e intentando descifrar un epigrama en griego clásico.

En mi experiencia trabajando en este proyecto, he observado cómo el álgebra y el análisis matemático han cooperado para resolver la ecuación de Pell, dejándose entrever ocasionalmente el análisis numérico. En el grado, sólo en casos muy puntuales han aparecido entrelazadas áreas diferentes de la matemática. Además, he podido comprobar la utilidad y el poder de la computación para las matemáticas. El problema del ganado es un ejemplo de problema matemático irresoluble en la práctica sin el uso del ordenador. He tenido la oportunidad de ver cómo se combinan los conocimientos y herramientas de distintas disciplinas para afrontar y resolver un problema.

He aprendido a valorar más la importancia de estudiar de manera crítica, cuestionándonos cada frase leída, fijándonos en los detalles, en cómo se usa cada hipótesis o resultado, relacionando las distintas partes o elementos, analizando cómo encajan, preguntándonos que fallaría si quitásemos una hipótesis o la cambiásemos por otra, etc. He de agradecer en esto la ayuda de mi tutor, que cada vez que yo afirmaba haber estudiado y comprendido parte de los contenidos, empezaba a hacerme preguntas, a revelarme detalles y relaciones, a veces incluso errores, que yo había pasado por alto y que al final evidenciaban que mi comprensión no era tan buena como yo creía. Esta habilidad ha mejorado mucho con respecto a mi formación antes de abordar este proyecto.

También he podido apreciar mejor los beneficios de escribir de manera clara, precisa y rigurosa. Parte de mis dificultades a la hora de entender algo en este tema han provenido de erratas, argumentos implícitos que no veía, cosas obvias que no lo eran para mí, demostraciones o ejercicios sencillos dejados al lector que no me lo parecieron, etc. Por eso he redactado este trabajo con la intención de que la lectura sea fácil. He cuidado mucho la redacción y las cadenas de razonamientos; las referencias a resultados y ecuaciones; no he dado nada por obvio, trivial o claro y he intentado que la información sea siempre explícita. Espero haberlo conseguido. De nuevo en esto he de agradecer la ayuda, los consejos y las exhaustivas revisiones de mi tutor.

Debido a la limitación de 50 páginas, no he podido incluir todo el material que he estudiado. En realidad, he aprendido también a resolver la ecuación diofántica $x^2 - dy^2 = -1$ y, más generalmente, $x^2 - dy^2 = N$ con $0 < |N| < \sqrt{d}$, véase [15, Teorema 7.25]. He implementado algoritmos para resolver ambas. Las ecuaciones $x^2 - dy^2 = \pm 1$

describen el grupo de elementos inversibles (unidades) de $\mathbb{Z}[\sqrt{d}]$. Su resolución nos dice que este grupo es finitamente generado, lo cual es un caso particular del llamado teorema de las unidades de Dirichlet. Me hubieran hecho falta tan sólo unas cinco páginas más para haber incluido eso. Las partes más afectada por esta limitación han sido la sección sobre aproximación diofántica y la introducción histórica a la ecuación de Pell. Había redactado el teorema de aproximación de Dirichlet, el teorema de Hurwitz y descrito el método de la Chakravala. Entre las aplicaciones que redacté y no incluí están la descripción de los números triangulares que son cuadrados (véase [4, Capítulo 2]) y el uso de las fracciones continuas en el planetario de Huygens (véase [18, Capítulo 4], [W7] y [W8]). Otras aplicaciones que he visto, aunque no las he estudiado en detalle, son: la descripción de los números piramidales que son cuadrados (véase [2]), el uso de las fracciones continuas para la factorización (véase [13, Sección 5.4]) y un criptosistema basado en la ecuación de Pell (véase [9, Sección 14.2]). En [9] y [12] he podido comprobar que la ecuación de Pell es, todavía hoy en día, un tema de investigación.

He sacrificado parte del material debido a esta limitación, pero he preferido exponer la resolución completa de la ecuación de Pell y el problema de Arquímedes antes que presentar resultados incompletos o aplicaciones explicadas de manera inadecuada. Me queda la duda de si, entre todas la formas que había de presentar los contenidos estudiados, he elegido la mejor o más adecuada. He de decir, no obstante, que he encontrado algo positivo en la limitación de espacio. Me ha hecho reflexionar sobre qué era lo verdaderamente importante y qué lo accesorio, qué debía incluir y qué no. Me ha hecho pensar sobre las frases que había escrito, revisarlas varias veces y ver si había formas más breves de decir lo mismo. De esta limitación también he aprendido.

He mejorado mi vocabulario en inglés puesto que todos los recursos utilizados (libros, artículos y páginas web) estaban en este idioma. Sobre informática, este proyecto me ha hecho poner en práctica mis conocimientos de programación. El lenguaje que hemos usado, *Mathematica*, era distinto al que nos explicaron en la asignatura de Programación de computadores. Sin embargo, las competencias adquiridas allí me han ayudado a adaptarme perfectamente. Gracias a este trabajo también han aumentado considerablemente mis conocimientos y habilidades con LaTeX.

Me ha impresionado el enorme conocimiento sobre matemáticas que existía en la antigüedad. Me parece sorprendente que sólo haya llegado hasta nuestros días una mínima parte y no comprendo cómo se pudo perder todo ese legado. He tenido la oportunidad de conocer a varios matemáticos hindúes y sus aportaciones. Este trabajo ha despertado mi interés por saber más sobre historia de las matemáticas.

Para terminar, este proyecto ha hecho replantearme el papel de las humanidades en nuestra formación: literatura, historia, filosofía, griego, latín, etc. Me hubiese gustado saber griego para haber leído el problema del ganado directamente del manuscrito. No esperaba el beneficio que este trabajo ha supuesto para mí en varios aspectos, a priori, poco relacionados con las matemáticas. He empezado a apreciar asignaturas de secundaria que en su momento me parecieron poco atractivas. Es extraño que cuando me hablaron en el instituto de *La Ilíada* y *La Odisea* me parecieron aburridas. Ahora me resultan muy interesantes. Me gustaría aprender más sobre mitología griega. He comprado *La Odisea* para mi biblioteca personal y la leeré con calma este verano.

Aquí acaba este episodio de mi particular viaje a la Ítaca matemática. Si tuviese que ponerle un título a este canto, sería: *El problema del ganado de Arquímedes: un punto de encuentro entre historia, literatura, matemáticas y computación.*

Bibliografía

[1] A. Amthor, *"Das Problema bovinum des Archimedes"*. Zeitschrift fur Math. u. Physik. (Hist.-litt.Abtheilung) Vol. **XXV** (1880), 153-171.

[2] W. S. Anglin, *The square pyramid puzzle*. Amer. Math. Monthly **97** (1990), no. 2, 120-124.

[3] A. H. Bell, *The "Cattle Problem." By Archimedes 251 B.C.* Amer. Math. Monthly **2** (1895), no. 5, 140-141.

[4] E. J. Barbeau, Pell's equation. Problem Books in Mathematics. Springer-Verlag, Nueva York, 2003.

[5] S. Barbero, U. Cerruti y N. Murru, *Solving the Pell equation via Rédei rational functions.* Fibonacci Quart. **48** (2010), no. 4, 348-357.

[6] J. Borwein, A. J. van der Poorten, J. Shallit y W. Zudilin, Neverending fractions. An introduction to continued fractions. Australian Mathematical Society Lecture Series 23. Cambridge University Press, Cambridge, 2014.

[7] C. Brezinski, History of continued fractions and Padé approximants. Springer Series in Computational Mathematics 12. Springer-Verlag, Berlín, 1991.

[8] H. Dörrie, 100 great problems of elementary mathematics. Their history and solution. Dover Publications, Inc., Nueva York, 1982.

[9] M. J. Jacobson y H. C. Williams, Solving the Pell equation. CMS Books in Mathematics/Ouvrages de Mathématiques de la SMC. Springer, Nueva York, 2009.

[10] A. Ya. Khinchin, Continued fractions. Dover Publications, Inc., Mineola, NY, 1997.

[11] S. Lang, Introduction to Diophantine approximations. Segunda edición. Springer-Verlag, Nueva York, 1995.

[12] H. W. Lenstra, Jr., *Solving the Pell equation*. Notices Amer. Math. Soc. **49** (2002), no. 2, 182-192.

[13] R. A. Mollin, Fundamental number theory with applications. Segunda edición. Discrete Mathematics and its Applications. Chapman & Hall/CRC, Boca Ratón, FL, 2008.

[14] H. L. Nelson, *A solution to Archimedes' Cattle Problem*. J. Recreational Math. **13** (1981), 162-176.

[15] I. Niven, H. S. Zuckerman y H. L. Montgomery, An introduction to the theory of numbers. Quinta edición. John Wiley & Sons, Inc., Nueva York, 1991.

[16] A. Nygrén, *A simple solution to Archimedes' cattle problem.* Acta Univ. Oulu. Ser. A Sci. Rerum Natur. No. 358 (2001), 45 pp.

[17] C. D. Olds, Continued fractions. Random House, Nueva York, 1963.

[18] A. M. Rockett y P. Szüsz, Continued fractions. World Scientific Publishing Co., Inc., River Edge, NJ, 1992.

[19] I. Stewart y D. Tall, Algebraic number theory and Fermat's last theorem. Cuarta edición. CRC Press, Boca Ratón, FL, 2016.

[20] I. Thomas, Greek Mathematical Works. Loeb Classical Library, Vol. 335 y 362. Harvard University Press, Cambridge, MA, 1980.

[21] I. Vardi, *Archimedes' cattle problem.* Amer. Math. Monthly **105** (1998), no. 4, 305-319.

[22] A. Weil, Number theory. An approach through history from Hammurapi to Legendre. Modern Birkhäuser Classics. Birkhäuser Boston, Inc., Boston, MA, 2007.

[23] H. C. Williams, R. A. German y C. R. Zarnke, *Solution of the Cattle Problem of Archimedes*. Math. Comp. **19** (1965), 671-674.

[24] N. J. Wildberger, *Pell's equation without irrational numbers.* J. Integer Seq. **13** (2010), no. 4, artículo 10.4.3, 11 pp.

Webgrafía

[W1] Página web del museo *Boijmans Van Beuningen* de Róterdam (Países Bajos):
https://www.boijmans.nl/en

[W2] Artículo en línea: S. Shirali, *The Chakravala method*. At right angles **3** (2014), no. 3, 13-18:
http://publications.azimpremjifoundation.org/1630/1/3_The%20Chakravala%20Method.pdf

[W3] *La Odisea* en línea (traducción de 1910 de Luis Segalá y Estalalella):
https://es.wikisource.org/wiki/La_Odisea_(Luis_Segal%C3%A1_y_Estalella)

[W4] Página web sobre Arquímedes:
https://www.math.nyu.edu/~crorres/Archimedes/contents.html

[W5] Archivo de historia de la matemática de la Universidad de St. Andrews (Reino Unido):
http://mathshistory.st-andrews.ac.uk/

[W6] *Los elementos* de Euclides en línea:
https://es.wikisource.org/wiki/Los_Elementos

[W7] Página web sobre el planetario de Huygens:
https://adcs.home.xs4all.nl/Huygens/21/plan.html

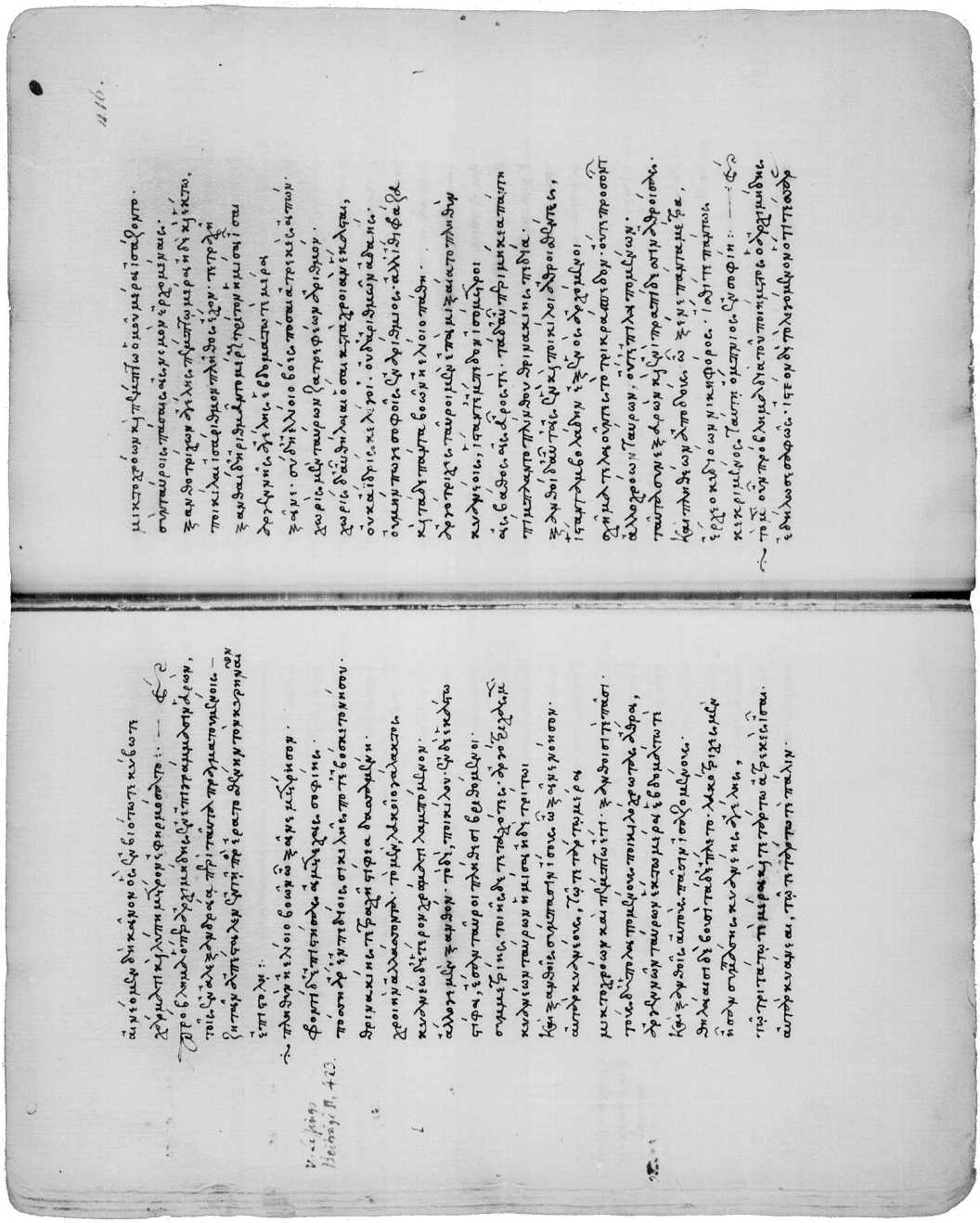
[W8] Obras completas de Huygens en línea:
https://archive.org/stream/oeuvrescompltesd21huyg#page/146/mode/1up

[W9] M. Ruiza, T. Fernández y E. Tamaro, *Biografía de Joseph-Louis de Lagrange*. En Biografías y vidas. La enciclopedia biográfica en línea. Barcelona (España):
https://www.biografiasyvidas.com/biografia/l/lagrange.htm

Apéndice

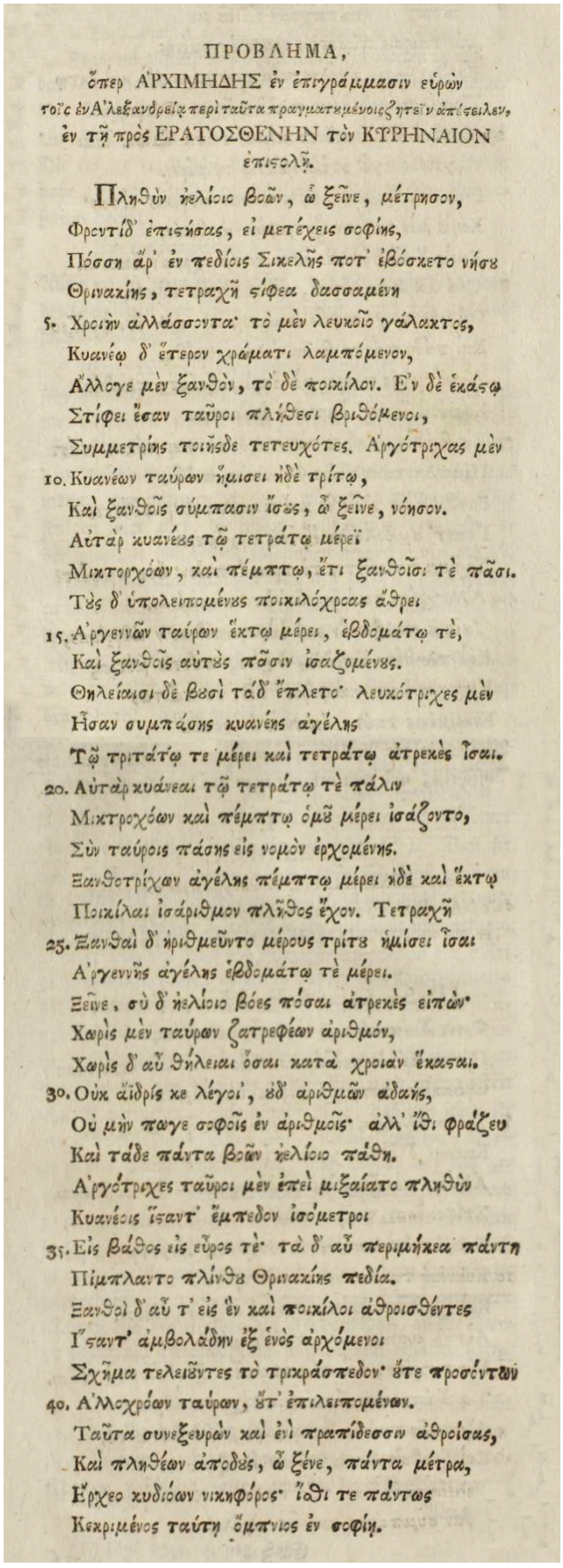
A

A.1 Manuscrito de Wolfenbüttel y transcripción de Lessing



Manuscrito de Wolfenbüttel

Fuente: https://www.math.nyu.edu/~crorres/Archimedes/Cattle/Statement_greek.html



ΠΡΟΒΛΗΜΑ,

ὅπερ ΑΡΧΙΜΗΔΗΣ ἐν ἐπιγράμμασιν εὑρὼν
τοῖς ἐνΑλεξανδρείᾳ περὶ ταῦτα πραγματευμένοις ζητεῖν ἀπέστειλεν,
ἐν τῇ πρὸς ΕΡΑΤΟΣΘΕΝΗΝ τὸν ΚΥΡΗΝΑΙΟΝ
ἐπιστολῇ.

Πληθὺν ἠελίοιο βοῶν, ὦ ξεῖνε, μέτρησον,
Φρυτίδ' ἐπιστήσας, εἰ μετέχεις σοφίης,
Πόσση ἄρ' ἐν πεδίοις Σικελῆς ποτ' ἐβόσκετο νήσῳ
Θρινακίης, τετραχῇ σίφεα δασσαμένη
Χροιὴν ἀλλάσσοντα· τὸ μὲν λευκοῖο γάλακτος,
Κυανέῳ δ' ἕτερον χράματι λαμπόμενον,
Ἄλλογε μὲν ξανθὸν, τὸ δὲ ποικίλον. Ἐν δὲ ἑκάστῳ
Στίφει ἦσαν ταῦροι πλήθεσι βριθόμενοι,
Συμμετρίης τοιῇσδε τετευχότες. Ἀργότριχας μὲν
Κυανέων ταύρων ἥμισει ἠδὲ τρίτῳ,
Καὶ ξανθοῖς σύμπασιν ἴσως, ὦ ξεῖνε, νόησον.
Αὖταρ κυανέας τῷ τετράτῳ μέρεϊ
Μικτορχόων, καὶ πέμπτῳ, ἔτι ξανθοῖσι τε πᾶσι.
Τὰς δ' ὑπολειπομένας ποικιλόχρους ἄθρει
Ἀργεννῶν ταύρων ἕκτῳ μέρει, ἑβδομάτῳ τε,
Καὶ ξανθοῖς αὖτὰς πᾶσιν ἰσαζομένας.
Θηλείαισι δὲ βουσὶ τάδ' ἔπλετο· λευκότριχες μὲν
Ἦσαν συμπάσης κυανέης ἀγέλης
Τῷ τριτάτῳ τε μέρει καὶ τετράτῳ ἀτρεκὲς ἶσαι.
Αὖταρ κυάνεαι τῷ τετράτῳ τὲ πάλιν
Μικτροχόων καὶ πέμπτῳ ὁμῶ μέρει ἰσάζοντο,
Σὺν ταύροις πάσης εἰς νομὸν ἐρχομένης.
Ξανθοτρίχων ἀγέλης πέμπτῳ μέρει ἠδὲ καὶ ἕκτῳ
Ποικίλαι ἰσάριθμον πλῆθος ἔχον. Τετραχῇ
Ξανθαὶ δ' ἠριθμεῦντο μέρους τρίτῳ ἡμίσει ἶσαι
Ἀργεννῆς ἀγέλης ἑβδομάτῳ τὲ μέρει.
Ξεῖνε, σὺ δ' ἠελίοιο βόες πόσαι ἀτρεκὲς εἰπών·
Χωρὶς μὲν ταύρων ζατρεφέων ἀριθμόν,
Χωρὶς δ' αὖ θήλειαι ὅσαι κατὰ χροιὰν ἔκασαι.
Οὐκ ἄϊδρίς κε λέγοι, οὐδ' ἀριθμῶν ἀδαής,
Οὐ μὴν πωγε σοφοῖς ἐν ἀριθμοῖς· ἀλλ' ἴθι φράζευ
Καὶ τάδε πάντα βοῶν ἠελίοιο πάθη.
Ἀργότριχες ταῦροι μὲν ἐπεὶ μιξαίατο πληθὺν
Κυανέοις ἴσαντ' ἔμπεδον ἰσόμετροι
Εἰς βάθος εἰς εὖρος τὲ· τὰ δ' αὖ περιμήκεα πάντη
Πίμπλαντο πλίνθῳ Θρινακίης πεδία.
Ξανθοὶ δ' αὖ τ' εἰς ἓν καὶ ποικίλοι ἀθροισθέντες
Ἴσαντ' ἀμβολάδην ἐξ ἑνὸς ἀρχόμενοι
Σχῆμα τελειοῦντες τὸ τριχράσπεδον· ἄτε προσέντων
Ἀλλοχρόων ταύρων, ἄτ' ἐπιλειπομένων.
Ταῦτα συνεξευρὼν καὶ ἐνὶ πραπίδεσσιν ἀθροίσας,
Καὶ πληθέων ἀποδὰς, ὦ ξένε, πάντα μέτρα,
Ἔρχεο κυδιόων νικηφόρος· ἴθι τε πάντως
Κεκριμένος ταύτῃ ὄμπνιος ἐν σοφίῃ.

Transcripción de Gotthold E. Lessing

Fuente: https://www.math.nyu.edu/~crorres/Archimedes/Cattle/Statement_Lessing_graphic.html

A.2 Soluciones fundamentales de la ecuación de Pell para $d < 100$

d	(x,y)	d	(x,y)
2	(3,2)	53	(66249,9100)
3	(2,1)	54	(485,66)
5	(9,4)	55	(89,12)
6	(5,2)	56	(15,2)
7	(8,3)	57	(151,20)
8	(3,1)	58	(19603,2574)
10	(19,6)	59	(530,69)
11	(10,3)	60	(31,4)
12	(7,2)	61	(1766319049,226153980)
13	(649,180)	62	(63,8)
14	(15,4)	63	(8,1)
15	(4,1)	65	(129,16)
17	(33,8)	66	(65,8)
18	(17,4)	67	(48842,5967)
19	(170,39)	68	(33,4)
20	(9,2)	69	(7775,936)
21	(55,12)	70	(251,30)
22	(197,42)	71	(3480,413)
23	(24,5)	72	(17,2)
24	(5,1)	73	(2281249,267000)
26	(51,10)	74	(3699,430)
27	(26,5)	75	(26,3)
28	(127,24)	76	(57799,6630)
29	(9801,1820)	77	(351,40)
30	(11,2)	78	(53,6)
31	(1520,273)	79	(80,9)
32	(17,3)	80	(9,1)
33	(23,4)	82	(163,18)
34	(35,6)	83	(82,9)
35	(6,1)	84	(55,6)
37	(73,12)	85	(285769,30996)
38	(37,6)	86	(10405,1122)
39	(25,4)	87	(28,3)
40	(19,3)	88	(197,21)
41	(2049,320)	89	(500001,53000)
42	(13,2)	90	(19,2)
43	(3482,531)	91	(1574,165)
44	(199,30)	92	(1151,120)
45	(161,24)	93	(12151,1260)
46	(24335,3588)	94	(2143295,221064)
47	(48,7)	95	(39,4)
48	(7,1)	96	(49,5)
50	(99,14)	97	(62809633,6377352)
51	(50,7)	98	(99,10)
52	(649,90)	99	(10,1)

A.3 Cálculo de la expansión en fracciones continuas simples de un número racional

Este programa calcula la expansión en fracciones continuas simples de un número racional. Se introducen el numerador y el denominador de la fracción. Por ejemplo, si queremos calcular dicha expansión para la fracción $\frac{4481}{1514}$ escribiremos FCR[4481,1514]. La salida debe ser {2, 1, 23, 1, 4, 1, 1, 5}.

```
In[1]:= FCR[X_, Y_] := Module[{x, y, q, r, a, b, c, d, a0, b0, Lq},
                          módulo
  x = X;
  y = Y;
  a = 1; b = 0; c = 0; d = 1;
  q = Quotient[x, y];
      cociente
  Lq = {q};
  r = Mod[x, y];
      operación módulo
  While[r ≠ 0,
  mientras
   x = y; y = r; a0 = a; b0 = b; c = a0 - q * d;
   q = Quotient[x, y];
       cociente
   r = Mod[x, y];
       operación módulo
   AppendTo[Lq, q];
   añade al final
  ];
  Return[Lq];
  retorna
 ]

In[2]:= FCR[4481, 1514]
Out[2]= {2, 1, 23, 1, 4, 1, 1, 5}
```

Mathematica dispone del comando *ContinuedFraction* para calcular la expansión en fracciones continuas simples de un número. Comparamos el resultado de nuestro programa con el que obtendríamos con *ContinuedFraction*.

```
In[3]:= ContinuedFraction[4481 / 1514]
        fracción continua
Out[3]= {2, 1, 23, 1, 4, 1, 1, 5}
```

A.4 Cálculo de la expansión en fracciones continuas simples de un número irracional cuadrático

Este programa calcula la expansión en fracciones continuas simples de un número irracional cuadrático, es decir, un número de la forma $x = \frac{m+\sqrt{d}}{w}$, donde d,m y w son números enteros, d es positivo y no cuadrado, w es no nulo y w divide a $d - m^2$. Se basa en el algoritmo explicado en la sección 2.6 del trabajo. Se introducen los valores m, w y d correspondientes a x . Por ejemplo, si $x = \sqrt{73}$, escribimos FC[0,1,73]. La salida debe ser {8 , {1, 1, 5, 5, 1, 1, 16}}. La lista {1, 1, 5 ,5, 1, 1, 16} es el periodo de la expansión en fracciones continuas.

```
In[7]:= FC[M_, W_, D_] := Module[{m, w, d, x, a, L1, L2, L3},
                                 módulo
  m = M;
  w = W;
  d = D;
      deriva
 x = (m + Sqrt[d]) / w;
          raíz cuadrada
  a = IntegerPart[x];
      parte entera
  L1 := {};
  L2 := {};
  L3 := {};
  m = a * w - m;
  w = (d - m^2) / w;
  x = (m + Sqrt[d]) / w;
          raíz cuadrada
  AppendTo[L1, a];
  añade al final
  AppendTo[L2, x];
  añade al final
  While[Length[L2] < 2, a = IntegerPart[x];
  mient··· longitud                  parte entera
   m = a * w - m;
   w = (d - m^2) / w;
   x = (m + Sqrt[d]) / w;
           raíz cuadrada
   AppendTo[L3, a];
   añade al final
   If[x == L2[[1]], AppendTo[L2, x]];
   si                 añade al final
  AppendTo[L1, L3];
  añade al final
  Return[L1];
  retorna
 ]

In[8]:= FC[0, 1, 73]

Out[8]= {8, {1, 1, 5, 5, 1, 1, 16}}
```

Comparamos el resultado obtenido con el que obtendríamos utilizando el comando *ContinuedFraction* de *Mathematica*.

```
In[9]:= ContinuedFraction[Sqrt[73]]
        fracción continua    raíz cuadrada
Out[9]= {8, {1, 1, 5, 5, 1, 1, 16}}
```

A.5 Cálculo de convergentes de un número irracional cuadrático

Este programa calcula los n primeros convergentes de un número irracional cuadrático. Se basa en las fórmulas para las sucesiones p y q descritas en la sección 2.3 del trabajo. Necesita los términos a_i de la expansión en fracciones continuas. Por eso, el programa FC anterior debe haber sido ejectuado para que funcione. Sigamos con el ejemplo $x=\sqrt{73}$. Para calcular sus 10 primeros convergentes escribimos CNG[0,1,73,10]. La salida debe ser $\{8, 9, \frac{17}{2}, \frac{94}{11}, \frac{487}{57}, \frac{581}{68}, \frac{1068}{125}, \frac{17669}{2068}, \frac{18737}{2193}, \frac{36406}{4261}\}$.

```
In[4]:= CNG[M_, W_, D_, n_] := Module[{x, p, q, pm1, qm1, pm2, qm2, La, Lc},
                                 módulo
  x = (M + Sqrt[D]) / W;
          raíz ··· deriva
  pm2 = 1;
  qm2 = 0;
  pm1 = IntegerPart[x];
        parte entera
  qm1 = 1;
  La := FC[M, W, D][[2]];
                  deriva
  Lc := {IntegerPart[x]};
          parte entera
  For[i = 1, i ≤ n - 1, i++,
  para cada
   If[Mod[i, Length[La]] == 0, j = Length[La], j = Mod[i, Length[La]]];
   si  operac··· longitud          longitud          operac··· longitud
   p = La[[j]] * pm1 + pm2;
   pm2 = pm1; pm1 = p;
   q = La[[j]] * qm1 + qm2;
   qm2 = qm1; qm1 = q;
   AppendTo[Lc, p / q];
   añade al final
  ];
  Return[Lc]]
  retorna

In[5]:= CNG[0, 1, 73, 10]

Out[5]= {8, 9, 17/2, 94/11, 487/57, 581/68, 1068/125, 17669/2068, 18737/2193, 36406/4261}
```

Mathematica dispone del comando *Convergents* para realizar esta misma tarea. Comparamos el resultado de nuestro programa con el obtenido mediante este comando.

```
In[6]:= Convergents[Sqrt[73], 10]
        convergentes  raíz cuadrada

Out[6]= {8, 9, 17/2, 94/11, 487/57, 581/68, 1068/125, 17669/2068, 18737/2193, 36406/4261}
```

A.6 Cálculo de soluciones de la ecuación de Pell

Este programa calcula la solución fundamental de la ecuación de Pell $x^2 - d\,y^2 = 1$. Necesita de los programas FC y CNG anteriores para que funcione, así que estos deben haber sido ejecutados previamente. Si queremos calcular la solución fundamental de esta ecuación para d=73, escribimos SF[73]. La salida debe ser {2281249, 267000}.

```
In[54]:= SF[D_] := Module[{La, l, f},
                   módulo
           La := FC[0, 1, D][[2]];
                         deriva
           If[Mod[Length[La], 2] == 0, l = Length[La], l = 2 * Length[La]];
           si  op···  longitud                longitud              longitud
           f = CNG[0, 1, D, l][[l]];
                        deriva
           {Numerator[f], Denominator[f]}]
            numerador      denominador

In[55]:= SF[73]

Out[55]= {2 281 249, 267 000}
```

Comprobamos que el resultado obtenido es efectivamente una solución:

```
In[56]:= 2 281 249^2 - 73 * 267 000^2

Out[56]= 1
```

Calculamos las soluciones fundamentales para los valores de d menor que 100.

```
In[57]:= V = {2, 3, 5, 6, 7, 8, 10, 11, 12, 13, 14, 15, 17, 18, 19, 20, 21, 22,
             23, 24, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 37, 38, 39, 40, 41, 42,
             43, 44, 45, 46, 47, 48, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61,
             62, 63, 65, 66, 67, 68, 69, 70, 71, 72, 73, 74, 75, 76, 77, 78, 79, 80,
             82, 83, 84, 85, 86, 87, 88, 89, 90, 91, 92, 93, 94, 95, 96, 97, 98, 99}

Out[57]= {2, 3, 5, 6, 7, 8, 10, 11, 12, 13, 14, 15, 17, 18, 19, 20, 21, 22, 23, 24, 26, 27, 28, 29,
          30, 31, 32, 33, 34, 35, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 50, 51, 52, 53,
          54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 65, 66, 67, 68, 69, 70, 71, 72, 73, 74, 75, 76,
          77, 78, 79, 80, 82, 83, 84, 85, 86, 87, 88, 89, 90, 91, 92, 93, 94, 95, 96, 97, 98, 99}
```

```
In[58]:= Table[{V[[i]], SF[V[[i]]]}, {i, 1, Length[V]}]
         tabla                                longitud
```

```
Out[58]= {{2, {3, 2}}, {3, {2, 1}}, {5, {9, 4}}, {6, {5, 2}}, {7, {8, 3}}, {8, {3, 1}},
  {10, {19, 6}}, {11, {10, 3}}, {12, {7, 2}}, {13, {649, 180}}, {14, {15, 4}},
  {15, {4, 1}}, {17, {33, 8}}, {18, {17, 4}}, {19, {170, 39}}, {20, {9, 2}},
  {21, {55, 12}}, {22, {197, 42}}, {23, {24, 5}}, {24, {5, 1}}, {26, {51, 10}},
  {27, {26, 5}}, {28, {127, 24}}, {29, {9801, 1820}}, {30, {11, 2}},
  {31, {1520, 273}}, {32, {17, 3}}, {33, {23, 4}}, {34, {35, 6}}, {35, {6, 1}},
  {37, {73, 12}}, {38, {37, 6}}, {39, {25, 4}}, {40, {19, 3}}, {41, {2049, 320}},
  {42, {13, 2}}, {43, {3482, 531}}, {44, {199, 30}}, {45, {161, 24}},
  {46, {24 335, 3588}}, {47, {48, 7}}, {48, {7, 1}}, {50, {99, 14}}, {51, {50, 7}},
  {52, {649, 90}}, {53, {66 249, 9100}}, {54, {485, 66}}, {55, {89, 12}},
  {56, {15, 2}}, {57, {151, 20}}, {58, {19 603, 2574}}, {59, {530, 69}}, {60, {31, 4}},
  {61, {1 766 319 049, 226 153 980}}, {62, {63, 8}}, {63, {8, 1}}, {65, {129, 16}},
  {66, {65, 8}}, {67, {48 842, 5967}}, {68, {33, 4}}, {69, {7775, 936}},
  {70, {251, 30}}, {71, {3480, 413}}, {72, {17, 2}}, {73, {2 281 249, 267 000}},
  {74, {3699, 430}}, {75, {26, 3}}, {76, {57 799, 6630}}, {77, {351, 40}},
  {78, {53, 6}}, {79, {80, 9}}, {80, {9, 1}}, {82, {163, 18}}, {83, {82, 9}},
  {84, {55, 6}}, {85, {285 769, 30 996}}, {86, {10 405, 1122}}, {87, {28, 3}},
  {88, {197, 21}}, {89, {500 001, 53 000}}, {90, {19, 2}}, {91, {1574, 165}},
  {92, {1151, 120}}, {93, {12 151, 1260}}, {94, {2 143 295, 221 064}}, {95, {39, 4}},
  {96, {49, 5}}, {97, {62 809 633, 6 377 352}}, {98, {99, 10}}, {99, {10, 1}}}
```

El siguiente programa calcula las n primeras soluciones positivas de la ecuación de Pell mediante potencias de la solución fundamental. Es necesario que el programa SF anterior esté ejecutado para que funcione. Se introduce el valor de d y el número de soluciones n a calcular. Por ejemplo, si queremos hallar las 4 primeras soluciones positivas de $x^2 - 73\,y^2 = 1$, escribimos SOLN[73,4]. La salida debe ser la lista {{2281249, 267000}, {10408194000001, 1218186966000}, {47487364308614281249, 5557975596000801000}, {216661004683313632776000001, 25358252540801244373932000}}.

```
In[59]:= SOLN[D_, n_] := Module[{x, y, x1, y1},
                         módulo
  x1 = SF[D][[1]];
       deriva
  y1 = SF[D][[2]];
       deriva
  x[1] = x1; y[1] = y1;
  x[m_] := x[m - 1] * x[1] + D * y[m - 1] * y[1];
                             deriva
  y[m_] := x[m - 1] * y1 + y[m - 1] * x1;
  Table[{x[i], y[i]}, {i, 1, n}]]
  tabla
```

```
In[60]:= SOLN[73, 4]
```

```
Out[60]= {{2 281 249, 267 000}, {10 408 194 000 001, 1 218 186 966 000},
  {47 487 364 308 614 281 249, 5 557 975 596 000 801 000},
  {216 661 004 683 313 632 776 000 001, 25 358 252 540 801 244 373 932 000}}
```

Comprobamos que son soluciones:

```
In[61]:= 10 408 194 000 001^2 - 73 * 1 218 186 966 000^2
Out[61]= 1

In[62]:= 47 487 364 308 614 281 249^2 - 73 * 5 557 975 596 000 801 000^2
Out[62]= 1

In[63]:= 216 661 004 683 313 632 776 000 001^2 - 73 * 25 358 252 540 801 244 373 932 000^2
Out[63]= 1
```

A.7 Cálculos para la resolución del problema de Arquímedes

Resolución del sistema de ecuaciones lineales

La matriz de coeficientes del sistema es:

```
In[5]:= M = {{1, -5/6, 0, -1, 0, 0, 0, 0}, {0, 1, -9/20, -1, 0, 0, 0, 0},
    {-13/42, 0, 1, -1, 0, 0, 0, 0}, {0, -7/12, 0, 0, 1, -7/12, 0, 0},
    {0, 0, -9/20, 0, 0, 1, -9/20, 0}, {0, 0, 0, -11/30, 0, 0, 1, -11/30},
    {-13/42, 0, 0, 0, -13/42, 0, 0, 1}, {0, 0, 0, 0, 0, 0, 0, 0}}
```

$$\text{Out[5]}= \left\{\left\{1, -\frac{5}{6}, 0, -1, 0, 0, 0, 0\right\}, \left\{0, 1, -\frac{9}{20}, -1, 0, 0, 0, 0\right\}, \left\{-\frac{13}{42}, 0, 1, -1, 0, 0, 0, 0\right\}, \left\{0, -\frac{7}{12}, 0, 0, 1, -\frac{7}{12}, 0, 0\right\}, \left\{0, 0, -\frac{9}{20}, 0, 0, 1, -\frac{9}{20}, 0\right\}, \left\{0, 0, 0, -\frac{11}{30}, 0, 0, 1, -\frac{11}{30}\right\}, \left\{-\frac{13}{42}, 0, 0, 0, -\frac{13}{42}, 0, 0, 1\right\}, \{0, 0, 0, 0, 0, 0, 0, 0\}\right\}$$

Como el sistema es homogéneo y sabemos que es compatible indeterminado, su solución, en los números reales, es:

```
In[6]:= S = NullSpace[M]
        espacio nulo
```

$$\text{Out[6]}= \left\{\left\{\frac{3\,455\,494}{1\,813\,071}, \frac{828\,946}{604\,357}, \frac{7\,358\,060}{5\,439\,213}, \frac{461\,043}{604\,357}, \frac{2\,402\,120}{1\,813\,071}, \frac{543\,694}{604\,357}, \frac{1\,171\,940}{1\,813\,071}, 1\right\}\right\}$$

Su solución mínima en los números naturales vendrá dada por:

```
In[7]:= l = LCM[1 813 071, 604 357, 5 439 213]
        mímino común múltiplo
```

```
Out[7]= 5 439 213
```

```
In[8]:= S * l
```

```
Out[8]= {{10 366 482, 7 460 514, 7 358 060, 4 149 387, 7 206 360, 4 893 246, 3 515 820, 5 439 213}}
```

Resolución de la ecuación $r^2 - 410286423278424s^2 = 1$

Queremos resolver la ecuación de Pell $r^2 - 410\,286\,423\,278\,424\,s^2=1$. Calculamos la longitud de la EFCS de $\sqrt{410\,286\,423\,278\,424}$ con nuestro programa FC. El cálculo se realiza en 2 minutos y 18 segundos.

In[20]:=
```
V = FC[0, 1, 410 286 423 278 424]
```

Out[20]=
```
{20 255 528, {4, 1, 1, 1, 4, 1, 2, 3, 4, 1, 3, 1, 1, 50, 1, 3, 2, 1, 16, 34,
  6, 3, 4, 2, 1, 6, 1, 2, 33, 1, 2, 2, 1, 8, 9, 1, 1, 3, 6, 2, 1, 2, 21, 22,
  1, 6, 1, 1, 1, 1, 20, 7, 2, 3, 1, 2, 1, 2, 2, 1, 15, 1, 1, 13, 4, 2, 3, 1,
  1, 1, 2, 1, 1, 6, 1, 1, 2, 3, 1, 1, 1, 1, 6, 7, 1, 1, 1, 1, 4, 1, 1, 1, 3,
  1, 1, 1, 3, 9, 1, 4, 2, 1, 2, 2, 5, 2, 5, 1, 2, 3, 4, 1, 1, 1, 4, 1, 9, 5,
  1, 5, 5, 5, 1, 12, 1, 2, 1, 6, ··· 202 998 ···, 1, 2, 1, 12, 1, 5, 5, 5, 1,
  5, 9, 1, 4, 1, 1, 1, 4, 3, 2, 1, 5, 2, 5, 2, 2, 1, 2, 4, 1, 9, 3, 1, 1, 1,
  3, 1, 1, 1, 4, 1, 1, 1, 1, 7, 6, 1, 1, 1, 1, 3, 2, 1, 1, 6, 1, 1, 2, 1, 1,
  1, 3, 2, 4, 13, 1, 1, 15, 1, 2, 2, 1, 2, 1, 3, 2, 7, 20, 1, 1, 1, 1, 6, 1,
  22, 21, 2, 1, 2, 6, 3, 1, 1, 9, 8, 1, 2, 2, 1, 33, 2, 1, 6, 1, 2, 4, 3, 6,
  34, 16, 1, 2, 3, 1, 50, 1, 1, 3, 1, 4, 3, 2, 1, 4, 1, 1, 1, 4, 40 511 056}}
```

salida grande | **Mostrar menos** | **Mostrar más** | **Mostrar salida completa** | **Establecer límite de tamaño**

La longitud del periodo es 203254 (par).

In[21]:=
```
Length[V[[2]]]
```
longitud

Out[21]= 203 254

Modificamos el programa CNG para que en lugar de darnos todos los convergentes hasta 203253 nos dé sólo este último:

```
In[22]:= f := Module[{x, p, q, pm1, qm1, pm2, qm2, La},
            módulo
          x = Sqrt[410 286 423 278 424];
              raíz cuadrada
          pm2 = 1;
          qm2 = 0;
          pm1 = IntegerPart[x];
                parte entera
          qm1 = 1;
          La := V[[2]];
          For[i = 1, i ≤ 203 253, i++,
          para cada
           If[Mod[i, Length[La]] == 0, j = Length[La], j = Mod[i, Length[La]]];
           si  operac···  longitud          longitud          operac···  longitud
           p = La[[j]] * pm1 + pm2;
           pm2 = pm1; pm1 = p;
           q = La[[j]] * qm1 + qm2;
           qm2 = qm1; qm1 = q;
          ];
          p / q]

In[23]:= fnum := Numerator[f]; fden := Denominator[f]
                 numerador          denominador
```

Comprobamos que los valores obtenidos son soluciones de la ecuación:

```
In[24]:= fnum^2 - 410 286 423 278 424 * fden^2 == 1
Out[24]= True
```

El valor de μ sería:

```
In[25]:= mu := 4 456 749 * fden^2
```

Resolución de la ecuación $x^2 - 4729494y^2 = 1$

Queremos resolver la ecuación de Pell $x^2 - 4\,729\,494\,y^2=1$. Calculamos la longitud de la EFCS de $\sqrt{4\,729\,494}$ con nuestro programa FC.

```
In[26]:= T = FC[0, 1, 4 729 494]
Out[26]= {2174, {1, 2, 1, 5, 2, 25, 3, 1, 1, 1, 1, 1, 1, 15, 1, 2, 16, 1, 2, 1, 1,
    8, 6, 1, 21, 1, 1, 3, 1, 1, 1, 2, 2, 6, 1, 1, 5, 1, 17, 1, 1, 47, 3, 1, 1,
    6, 1, 1, 3, 47, 1, 1, 17, 1, 5, 1, 1, 6, 2, 2, 1, 1, 1, 3, 1, 1, 21, 1, 6,
    8, 1, 1, 2, 1, 16, 2, 1, 15, 1, 1, 1, 1, 1, 1, 3, 25, 2, 5, 1, 2, 1, 4348}}
```

La longitud del periodo es 92 (par).

```
In[27]:= Length[T[[2]]]
         longitud
Out[27]= 92
```

La solución fundamental (x_1,y_1) vendrá dada por el convergente de índice 92-1=91. Calculamos la solución fundamantal con nuestro programa SF.

```
In[28]:= S = SF[4 729 494]
Out[28]= {109 931 986 732 829 734 979 866 232 821 433 543 901 088 049,
     50 549 485 234 315 033 074 477 819 735 540 408 986 340}
```

Comprobamos que es solución:

```
In[29]:= S[[1]]^2 - 4 729 494 * S[[2]]^2 == 1
Out[29]= True
```

El valor de x_1 tiene 45 dígitos.

```
In[30]:= IntegerLength[S[[1]]]
         longitud de entero
Out[30]= 45
```

El valor de y_1 tiene 41 dígitos.

```
In[31]:= IntegerLength[S[[2]]]
         longitud de entero
Out[31]= 41
```

Escribimos la solución $x_1 + y_1\sqrt{D}$ de manera más compacta como $\left(\sqrt{\frac{x_1+1}{2}} + \sqrt{\frac{x_1-1}{2}}\right)^2$:

```
In[32]:= g = (S[[1]] + 1) / 2
Out[32]= 54 965 993 366 414 867 489 933 116 410 716 771 950 544 025

In[33]:= Sqrt[g]
         raíz cuadrada
Out[33]= 300 426 607 914 281 713 365 √609

In[34]:= h = (S[[1]] - 1) / 2
Out[34]= 54 965 993 366 414 867 489 933 116 410 716 771 950 544 024
```

```
In[35]:= Sqrt[h]
         raíz cuadrada
Out[35]= 84 129 507 677 858 393 258 √7766
```

Calculamos el menor n tal que y_n es divisible por 9314 con el siguiente código:

```
In[36]:= a = 109 931 986 732 829 734 979 866 232 821 433 543 901 088 049;
         b = 50 549 485 234 315 033 074 477 819 735 540 408 986 340; Module[{xm = a, ym = b, n = 1},
                                                                     módulo
          While[Mod[ym, 9314] ≠ 0, {xm, ym} = {xm * a + 4 729 494 * ym * b, xm * b + ym * a};
          mient··· operación módulo
           n++];
          n]
Out[36]= 2329
```

Es n=2329. Calculamos la solución (x_{2329}, y_{2329}) con el siguiente código:

```
In[37]:= F[n_] := Module[{xm = a, ym = b, i = 1},
                  módulo
           While[i++ < n, {xm, ym} = {xm * a + 4 729 494 * ym * b, xm * b + ym * a}];
           mientras
           {xm, ym}]
```

La solución (x_{2329}, y_{2329}) es F[2329]. Entonces (r_1,s_1)=(x_{2329}, $\frac{y_{2329}}{9314}$) es la solución fundamental de la ecuaciónn de Pell inicial $r^2 - 410\,286\,423\,278\,424\,s^2=1$.

```
In[38]:= r1 := F[2329][[1]]; s1 := F[2329][[2]] / 9314
```

Comprobamos que es solución:

```
In[39]:= r1^2 - 410 286 423 278 424 s1^2 == 1
Out[39]= True
```

Comprobamos que esta solución coincide con la que calculamos en el apartado anterior:

```
In[40]:= r1 == fnum
Out[40]= True

In[41]:= s1 == fden
Out[41]= True
```

Solución mínima al problema del ganado de Arquímedes

El valor de mu que buscamos es:

```
In[42]:= μ := 4 456 749 * (s1)^2
```

Número de toros blancos: 159651...341800. Tiene 206545 dígitos.

```
In[43]:= x := 10 366 482 * μ

In[44]:= RealDigits[x, 10, 6]
         dígitos de un real
Out[44]= {{1, 5, 9, 6, 5, 1}, 206 545}

In[45]:= Mod[x, 10^6]
         operación módulo
Out[45]= 341 800
```

Número de toros negros: 114897...178600. Tiene 206545 dígitos.

```
In[46]:= y := 7 460 514 * μ

In[47]:= RealDigits[y, 10, 6]
         dígitos de un real
Out[47]= {{1, 1, 4, 8, 9, 7}, 206 545}

In[48]:= Mod[y, 10^6]
         operación módulo
Out[48]= 178 600
```

Número de toros moteados: 113319...894000. Tiene 206545 dígitos.

```
In[49]:= z = 7 358 060 * μ;

In[50]:= RealDigits[z, 10, 6]
         dígitos de un real
Out[50]= {{1, 1, 3, 3, 1, 9}, 206 545}

In[51]:= Mod[z, 10^6]
         operación módulo
Out[51]= 894 000
```

Número de toros amarillos: 639034...026300. Tiene 206544 dígitos.

```
In[52]:= t := 4 149 387 * μ;

In[53]:= RealDigits[t, 10, 6]
         dígitos de un real
Out[53]= {{6, 3, 9, 0, 3, 4}, 206 544}

In[54]:= Mod[t, 10^6]
         operación módulo
Out[54]= 26 300
```

Número total de toros del rebaño: 451770...440700. Tiene 206545 dígitos.

```
In[55]:= ttoros := x + y + z + t
```

```
In[56]:= RealDigits[ttoros, 10, 6]
         dígitos de un real
Out[56]= {{4, 5, 1, 7, 7, 0}, 206545}

In[57]:= Mod[ttoros, 10^6]
         operación módulo
Out[57]= 440700
```

Número de vacas blancas: 110982...564000. Tiene 206545 dígitos.

```
In[58]:= x' := 7206360 * μ

In[59]:= RealDigits[x', 10, 6]
         dígitos de un real
Out[59]= {{1, 1, 0, 9, 8, 2}, 206545}

In[60]:= Mod[x', 10^6]
         operación módulo
Out[60]= 564000
```

Número de vacas negras: 753594...645400. Tiene 206544 dígitos.

```
In[61]:= y' := 4893246 * μ

In[62]:= RealDigits[y', 10, 6]
         dígitos de un real
Out[62]= {{7, 5, 3, 5, 9, 4}, 206544}

In[63]:= Mod[y', 10^6]
         operación módulo
Out[63]= 645400
```

Número de vacas moteadas: 541460...318000. Tiene 206544 dígitos.

```
In[64]:= z' := 3515820 * μ

In[65]:= RealDigits[z', 10, 6]
         dígitos de un real
Out[65]= {{5, 4, 1, 4, 6, 0}, 206544}

In[66]:= Mod[z', 10^6]
         operación módulo
Out[66]= 318000
```

Número de vacas amarillas: 837676...113700. Tiene 206544 dígitos.

```
In[67]:= t' := 5439213 * μ

In[68]:= RealDigits[t', 10, 6]
         dígitos de un real
Out[68]= {{8, 3, 7, 6, 7, 6}, 206544}

In[69]:= Mod[t', 10^6]
         operación módulo
Out[69]= 113700
```

Número total de vacas del rebaño: 324256...641100. Tiene 206545 dígitos.

```
In[70]:= tvacas := x' + y' + z' + t'

In[71]:= RealDigits[tvacas, 10, 6]
         dígitos de un real
Out[71]= {{3, 2, 4, 2, 5, 6}, 206545}

In[72]:= Mod[tvacas, 10^6]
         operación módulo
Out[72]= 641100
```

Número total de reses del rebaño del dios Helios: 776027...081800. Tiene 206545 dígitos.

```
In[73]:= total := ttoros + tvacas

In[74]:= RealDigits[total, 10, 6]
         dígitos de un real
Out[74]= {{7, 7, 6, 0, 2, 7}, 206545}

In[75]:= Mod[total, 10^6]
         operación módulo
Out[75]= 81800
```

A.8 Artículo de Bell

140

THE "CATTLE PROBLEM." BY ARCHIMEDIES 251 B. C.

By A. H. BELL, Hillsboro, Illinois.

Compute, O stranger! the number of of cattle of Helios, which once grazed on the plains of Sicily, divided according to their color, to wit:

$$\text{1st White Bulls} = \frac{\text{Black Bulls}}{2} + \frac{\text{Black Bulls}}{3} + \text{Yellow Bulls.}$$

2nd Black Bulls=$\frac{1}{4}$ and $\frac{1}{5}$ of the Dappled Bulls+the Yellow.
3rd Dappled Bulls=$\frac{1}{6}$ and $\frac{1}{7}$ of the White Bulls+the Yellow Bulls.
4th The White cows=$\frac{1}{3}$ and $\frac{1}{4}$ of the Black Herd,Bulls and Cows=Herd.
5th The Black cows=$\frac{1}{4}$ and $\frac{1}{5}$ of the Dappled Herd.
6th The Dappled cows=$\frac{1}{5}$ and $\frac{1}{6}$ of the Yellow Herd.
7th The Yellow cows=$\frac{1}{6}$ and $\frac{1}{7}$ of the White Herd.

He who can answer the above is no novice in numbers. Nevertheless he is not yet skilled in wise calculations! but come consider also all the following numerical relations between the Oxen of the Sun.

8th If the White Bulls were combined in one total, with the Black Bulls they would be in a figure equal in depth and breadth and the far stretching plains of Thrinacia would be covered by the figure (square) formed by them.

9th Should the Yellow and Dappled Bulls be collected in one place, they would stand, if they ranged themselves one after another completing the form of an equilateral triangle. If thou discover the solution of this at the same time; if thou grasp it with thy brain; and give correctly all the numbers; O Stranger! go and exult as conqueror; be assured that thou art by all means proved to have abundant of knowledge in this science.—This is translated by T. L. Heath, author of Diophantos, Cambridge, England, 1889.

The first known answer to the Celebrated Cattle Problem by Archimedes 251 B. C. was computed by the Hillsboro, Illinois, Mathematical Club, 1889 to 1893. Edmund Fish, Geo. H. Richards, and A. H. Bell.

The numbers satisfying all of the 9 conditions as given are the very smallest that will meet the requirements and critical tests that are also given. Mathematicians have heretofore obtained the 8th condition which requires the White and Black Bulls to equal a square number, and is 79 450 446 596 004 = □ number; the 9th condition that the Dappled and Yellow Bulls should equal a triangular number is not fullfilled by the corresponding number, 51, 285 802 909 803, which is designated by B. We seek a square multiplier which call x^2 let $Bx^2 = \frac{n(n+1)}{2}$ = the expression for a triangular number which gives $8Bx^2+1=(2n+1)^2=y^2$ and we at once get $\sqrt{8B}=\frac{\sqrt{(y^2-1)}}{x}$. The square root of $8B$ by continued fractions will give x, and then we have

$x^2 =$ 34 555 906 354 559 370 506 303 802 963 617 + 68 829 periods of 3's + 252 058 980 100.

White Bulls 1 596 510 804 671 144 531 435 526 194 370 + 68 834 periods of 3's + 385 150 341 800.

Black Bulls 1 148 971 387 728 289 999 712 359 821 824 + 68 834 periods of 3's + 899 825 178 600

Dappled Bulls 1 133 192 754 438 638 077 119 555 879 202 + 68 834 periods of 3's + 921175 894 000

Yellow Bulls 639 034 648 230 902 865 008 559 676 183 + 68 834 periods of 3's + 635 296 026 300

White Cows 1 109 829 892 373 319 039 723 960 215 824 + 68 834 periods of 3's + 914 059 564 000

Black Cows 753 594 142 054 542 639 814 429 119 589 + 68 834 periods of 3's + 238 562 645 400

Dappled Cows 541 460 894 571 456 678 023 619 942 106 + 68 834 periods of 3's + 608 963 318 000

Yellow Cows 837 676 882 418 524 438 692 221 984 107 + 68 834 periods of 3's + 116 422 113 700

Total 7 760 271 406 486 818 269 530 232 833 209 + 68 834 periods of 3's + 719 455 081 800

W. and B. Bulls 2 745 482 192 399 434 531 147 886 016 194 + 68 834 periods of 3's + 284 975 520 400

Root of above 1 656 949 665 133 506 668 + 34 414 periods of 3's + 357 460 163 020

D. & Y. $= \triangle =$ 1 772 227 402 669 540 942 128 115 555 385 + 68 834 periods of 3's + 556 471 920 300

Root of $8\triangle + 1$ 3 765 344 502 347 205 884 + 34 414 periods of 3's + 363 134 961 201

These enormous numbers using 206545 figures will make numbers one-half mile long. In the computations to this problem difficulties are encountered at every step, wonderfull discoveries in the properties of vast numbers are disclosed at every turn. A new summation of continued fractions with many novel ways used to obtain the exact figures shown can be had of A. H. Bell, Hillsboro, Illinois.