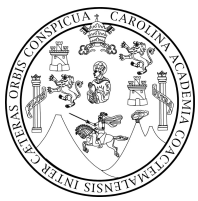


Universidad de San Carlos de Guatemala
Facultad de Ingeniería
Escuela de Ciencias

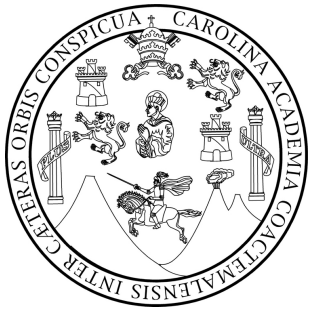
REPRESENTACIÓN DE NÚMEROS MEDIANTE FORMAS CUADRÁTICAS BINARIAS

José Carlos Alberto Bonilla Aldana

Asesorado por el M.Sc José Rodrigo Vásquez Bianchi

Guatemala, octubre de 2013

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA



FACULTAD DE INGENIERÍA

REPRESENTACIÓN DE NÚMEROS MEDIANTE FORMAS CUADRÁTICAS BINARIAS

TRABAJO DE GRADUACIÓN

PRESENTADO A LA JUNTA DIRECTIVA DE LA
FACULTAD DE INGENIERÍA
POR

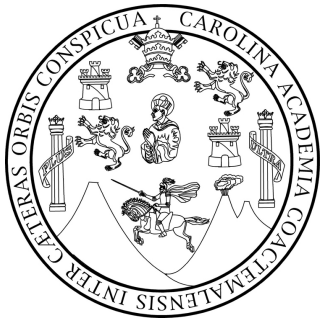
JOSÉ CARLOS ALBERTO BONILLA ALDANA
ASESORADO POR EL M.SC JOSÉ RODRIGO VÁSQUEZ BIANCHI

AL CONFERÍRSELE EL TÍTULO DE

LICENCIADO EN MATEMÁTICA APLICADA

GUATEMALA, OCTUBRE DE 2013

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
FACULTAD DE INGENIERÍA



NÓMINA DE JUNTA DIRECTIVA

DECANO	Ing. Murphy Olympo Paiz Recinos
VOCAL I	Ing. Alfredo Enrique Beber Aceituno
VOCAL II	Ing. Pedro Antonio Aguilar Polanco
VOCAL III	Inga. Elvia Miriam Ruballos Samayoa
VOCAL IV	Br. Walter Rafael Véliz Muñoz
VOCAL V	Br. Sergio Alejandro Donis Soto
SECRETARIO	Ing. Hugo Humberto Rivera Pérez

TRIBUNAL QUE PRACTICÓ EL EXAMEN GENERAL PRIVADO

DECANO	Ing. Murphy Olympo Paiz Recinos
EXAMINADORA	Dra. Mayra Virginia Castillo Montes
EXAMINADOR	Lic. Carlos Augusto Morales Santacruz
EXAMINADOR	Lic. Francisco Bernardo Raúl De La Rosa
SECRETARIO	Ing. Hugo Humberto Rivera Pérez

HONORABLE TRIBUNAL EXAMINADOR

En cumplimiento con los preceptos que establece la ley de la Universidad de San Carlos de Guatemala, presento a su consideración mi trabajo de graduación titulado:

REPRESENTACIÓN DE NÚMEROS MEDIANTE FORMAS CUADRÁTICAS BINARIAS

Tema que me fuera asignado por la Coordinación de la Licenciatura en Matemática Aplicada, el 29 de noviembre de 2011.

José Carlos Alberto Bonilla Aldana

Guatemala, 29 de agosto de 2013

Doctora Mayra Castillo Montes
Coordinadora de la Licenciatura en Matemáticas Aplicadas

Estimada doctora Castillo:

Buenos días. La presente es para informarle que he estudiado el trabajo de graduación del estudiante José Carlos Bonilla Aldana, número de carnet 2005-15870, titulado Representación de números mediante formas cuadráticas binarias y he encontrado que cumple con todos los requisitos correspondientes, por lo cual le doy mi aprobación.

Agradeciendo de antemano la fina atención que se sirva prestar a la presente, le reitero a usted las muestras de mi más distinguida consideración.

Rodrigo Vásquez Bianchi

MATEMATICO
RODRIGO VASQUEZ BIANCHI
Colegiado No. 1762

USAC
TRICENTENARIA
Universidad de San Carlos de Guatemala

FACULTAD DE INGENIERÍA

REF. LMA- 55-2013.
Guatemala, 17 de septiembre de 2013.

Ing. Edwin Adalberto Bracamonte Orozco.
Director de Escuela de Ciencias.
Facultad de Ingeniería.
Presente.

Ingeniero Bracamonte:

Al saludarle atentamente, le informo que he revisado el informe final del trabajo de graduación titulado *"Representación de números mediante formas cuadráticas binarias"* presentado por el estudiante de Licenciatura en Matemática Aplicada **José Carlos Alberto Bonilla Aldana**, quien se identifica con carné número 2005-15870. Dicho documento se recibió acompañado de carta del Lic. Rodrigo Vásquez en la que manifiesta su aprobación como asesor del trabajo presentado.

Al respecto del resultado de la revisión realizada, le manifiesto mi aprobación para el trabajo de graduación elaborado, agregando que los resultados obtenidos se consideran de mucha utilidad como material de apoyo en cursos que se imparten en la carrera.

Sin otro particular, me suscribo.

Atentamente,

"Id y Enseñad a Todos"

Facultad de Ingeniería USAC - Coordinacion - Licenciatura en Matemática Aplicada

Dra. Mayra Virginia Castro Montes
Coordinadora de Licenciatura en Matemática Aplicada

UNIVERSIDAD DE SAN CAROLOS
DE GUATEMALA

FACULTAD DE INGENIERÍA
ESCUELA DE CIENCIAS

El Director de la Escuela de Ciencias de la Facultad de Ingeniería de la Universidad de San Carlos de Guatemala, después de conocer el dictamen del asesor, con el visto bueno de la Coordinadora de la Carrera de Licenciatura en Matemática Aplicada al trabajo de graduación del estudiante ***José Carlos Alberto Bonilla Aldana,*** titulado "REPRESENTACIÓN DE NÚMEROS MEDIANTE FORMAS CUADRÁTICAS BINARIAS", procede a la autorización del mismo.

Ing. Edwin Adalberto Bracamonte Orozco
Director Escuela de Ciencias

Guatemala, 18 de octubre de 2013
EABOP/scvs

Universidad de San Carlos
de Guatemala

Facultad de Ingeniería
Decanato

Ref.DTG.722.2013

El Decano de la Facultad de Ingeniería de la Universidad de San Carlos de Guatemala, luego de conocer la aprobación por parte del Director de la Escuela de Ciencias, al trabajo de graduación titulado: **REPRESENTACIÓN DE NÚMEROS MEDIANTE FORMAS CUADRÁTICAS BINARIAS,** presentado por el estudiante universitario: **José Carlos Bonilla Aldana,** procede a la autorización para la impresión del mismo.

IMPRÍMASE.

Ing. Murphy Olympo Paiz Recinos
Decano

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
DECANO
FACULTAD DE INGENIERIA

Guatemala, octubre de 2013

/cc

ACTO QUE DEDICO A:

Mi familia — Tanto a aquellos que la componen actualmente, como a quienes algún día formarán parte de ella. Mi conocimiento es suyo.

Los curiosos — Los que, como yo, dedican su vida a la búsqueda de la verdad. Aquellos que encuentran respuestas pero, sobre todo, nuevas preguntas.

Los olímpicos — Aquellos que compartieron conmigo la verdadera Matemática y también los que la recibieron de mí. Mi abuela dijo que llevo en el interior una chispa propicia a provocar gran incendio. A mis alumnos les pido que extiendan la llama.

AGRADECIMIENTOS A:

Dios	Por concederme dones, y presentarme causas dignas para utilizarlos en su gloria. Y por tantas otras cosas que son demasiadas para listar.
Mis padres	Francisco Eduardo Bonilla Porras y Araceli Aldana Marín, por el amor con que me criaron, los valores que me inculcaron y el apoyo que me ofrecieron.
Mi iglesia	Castillo Fuerte, por permitirme escribir el trabajo de graduación en su computadora, entre otras cosas.
Mis catedráticos	Y en particular a Pedro Morales y a mi asesor, el Lic. Rodrigo Vásquez, por todo el conocimiento que compartieron libremente conmigo.
Mi novia	Glenda Gómez, por su apoyo durante las largas horas de investigación y esfuerzo mental.
Familiares y amigos	Que de una u otra forma influenciaron mi vida.

PREFACIO

En el 2005 me presentaron formalmente a la «Reina de las Matemáticas». Sucedió en los cursos de preparación para la Olimpiada Iberoamericana de ese año. Antes de ello, apenas había vislumbrado fugazmente su magnificencia, en un problema de la Olimpiada Internacional con el que me tropecé mientras leía un libro en el colegio: Hallar todas las parejas (a, b) de enteros positivos que cumplan la ecuación $a^{b^2} = b^a$. Pude hallarlas todas, pero no tenía la más mínima idea de como asegurar que no existían otras. En los cursos de olimpiadas aprendí aquello que me faltaba, y grande fue mi emoción al completar la prueba que me había eludido. Desde entonces quise ser un teórico de números.

Con el pasar del tiempo heredé, junto con otros, la responsabilidad de preparar a los jóvenes talentosos de Guatemala. En el 2010, Hugo García —otro de los catedráticos olímpicos— y yo nos encontrábamos fabricando el examen de selección para la Olimpiada Iberoamericana de ese año. Nuestro antiguo profesor, Pedro Morales, había propuesto el problema de hallar todas las soluciones enteras de la ecuación $x^2 - y^2 = 304$. Hugo y yo lo modificamos, sustituyendo 304 por n, y exigiendo que se determinara el conjunto de valores de n para los cuáles existiera una solución. A pesar de su apariencia inocente, me percaté de que el problema tenía el germen del trascendentalismo. Así nació mi interés por las formas algebraicas.

A menos que usted sea un experto en Teoría de Números, no es prudente que comience la lectura sin tener lápiz y papel a la mano. Los documentos científicos, y especialmente los de índole matemática, no pueden ser leídos como se lee una revista. Con la (poca) experiencia que he tenido en el mundo de las matemáticas, me he afianzado en el uso de dos tácticas que recomiendo combinar, para obtener mejores resultados. La primera es «el avance cauteloso», en el cual no se prosigue con la lectura de un párrafo sin asegurarse de entender a cabalidad los anteriores. La segunda,

«la comprensión retrospectiva», consiste en saltarse partes complicadas o engorrosas, intentar adquirir una perspectiva más amplia del tema, para luego regresar al pasaje oscuro viéndolo bajo una nueva luz. Por ejemplo, si su álgebra está oxidada, la sección 2.2 podría ofrecer cierta resistencia. Recomiendo leer las definiciones y los enunciados de las proposiciones, poner especial atención a la tabla VI y al ejemplo de la página 45, dejando de último la «lectura cautelosa» de las demostraciones y argumentos.

Habiendo hecho las advertencias pertinentes, como acostumbro en mis escritos, quisiera ahora discutir un punto particular de este documento. La distribución de las referencias bibliográficas en el texto es muy irregular, varias secciones no tienen ninguna. Esto no es aleatorio, sino que obedece a la forma en la que fueron redactadas las distintas partes del texto. Casi todo el material de los capítulos 2,3 y 4 es original, a excepción del argumento que se usa para probar el lema 7 en la página 71 —que es una amalgama parafraseada de las demostraciones de Euler y Legendre— junto con otros resultados debidamente citados, sin su demostración.

Por supuesto, no soy el primero en discutir estos problemas. Hice mi mejor esfuerzo por darle crédito a los autores originales, aunque esto no siempre fue posible. Después de descubrir las cerraduras de la sección 4.1, llevé a cabo la búsqueda rutinaria de precursores y pude determinar que una ha sido conocida por al menos 60 años, mas desconozco los detalles de su historia. Ésta y cualquier otra omisión, en lo que respecta a la autoría, fueron totalmente inintencionadas.

El primer capítulo juega el doble papel de introducción y recordatorio de los temas clave en la Teoría de Números elemental. Es recomendable investigar las demostraciones y aplicaciones de cualquier teorema que le resulte desconocido, de entre los incluidos en dicho capítulo. En el segundo, se introduce el tema principal comenzando por la terminología, que en parte es de elaboración propia, para desarrollar formalmente el tema en los capítulos 3, 4 y 5, que contienen el material más interesante. Quiero cerrar este (ya bastante largo) preámbulo deseándoles un viaje placentero en uno de los inexplorados parajes de la Teoría de Números, cuyos misterios hace apenas 4 siglos comenzaron a descifrar los más grandes matemáticos de la historia.

ÍNDICE GENERAL

ÍNDICE DE ILUSTRACIONES

FIGURAS

TABLAS

LISTA DE SÍMBOLOS

Símbolo	**Significado**
✠	Cambio ligero de tema dentro de una sección.
$[\mathfrak{q}]$	Clase de equivalencia de $\mathfrak{q}$ respecto de $\sim$.
$\boxed{c}$	Composición de representaciones empleando la cerradura $\mathcal{C}$.
$a \equiv b \pmod{m}$	Congruencia, se lee "a es congruente con b en el módulo m".
$\mathbb{C}$	Conjunto de los números complejos.
$\mathbb{Z}$	Conjunto de los números enteros.
$\mathbb{Z}^+$	Conjunto de los números enteros positivos.
$\mathbb{N}$	Conjunto de los números naturales (se incluye al cero).
$\mathbb{R}$	Conjunto de los números reales.
$\mathscr{D}(\mathfrak{q})$	Conjunto de los números representables por $\mathfrak{q}$.
$\varnothing$	Conjunto vacío.
$\forall$	Cuantificador universal, se lee *para todo*.
✓	Cumple las condiciones (utilizado en tablas de exhaustión).
$\det(M)$	Determinante de la matriz M.
$\setminus$	Diferencia de conjuntos.
$a \mid b$	Divisibilidad, se lee *a es divisor de b*.
$\sim$	Equivalencia de formas cuadráticas (representabilidad).
$\overset{+}{\sim}$	Equivalencia propia de formas cuadráticas.
$\square$	Fin de una demostración.
$\diamondsuit$	Fin de una solución o ejemplo.
$\langle\!\langle a, b, c \rangle\!\rangle$	Forma auto-composición de $ax^2 + bxy + cy^2$.
$\langle a, b, c \rangle$	Forma cuadrática binaria $ax^2 + bxy + cy^2$ (énfasis en coeficientes).
$\mathfrak{q}(x, y)$	Forma cuadrática binaria $ax^2 + bxy + cy^2$ (énfasis en variables).

$\mathfrak{D}\langle a_i\rangle$	Forma cuadrática diagonal con coeficientes (a_i).
$\mathfrak{q}_0$	Forma primitiva asociada a $\mathfrak{q}$.
$\mathfrak{q}^{op}$	Forma que se obtiene de $\mathfrak{q}$ al cambiar el signo del término cruzado.
$\mathfrak{C}_\Delta$	Grupo de clases de formas con discriminante Δ.
$\Longrightarrow$	Implicación.
∞	Infinito.
$D(a_i)$	Matriz diagonal con entradas (a_i) en la diagonal principal.
$\text{MCD}(m,n)$	Máximo común divisor de m y n.
máx S	Máximo elemento del conjunto numérico S.
$\text{MCM}(m,n)$	Mínimo común múltiplo de m y n.
mín S	Mínimo elemento del conjunto numérico S.
$\neg$	Negación proposicional.
$\cdot$	No cumple las condiciones (utilizado en tablas de exhaustión).
$\notin$	No pertenencia.
$\langle a,b,c\rangle\,\overline{\mathcal{R}}(n)$	Número de representaciones de n en la forma $\langle a,b,c\rangle$.
$\langle a,b,c\rangle\,\mathcal{R}(n)$	Número de representaciones independientes de n en la forma $\langle a,b,c\rangle$.
$\mathfrak{H}$	Plano hiperbólico (forma x^2-y^2).
$\in$	Pertenencia.
$\prod_C T$	Producto de los términos T que cumplen las condiciones C. Si los términos son a_i, siendo las condiciones $1 \leq i \leq k$, esto es, los términos de una sucesión finita, escribimos $\prod_{i=1}^{k} a_i$, o bien $\prod_{i=1}^{k} a_i$.
$a \boxdot b$	Residuo cuadrático, se lee *a es residuo módulo $\lvert b\rvert$*.
$\Longleftrightarrow$	Si, y sólo si.
$[a,b]_p$	Símbolo de Hilbert de $\mathfrak{D}\langle a,b,-1\rangle$ en p.
$\left(\frac{a}{p}\right)$	Símbolo de Legendre de a en p.

$\subseteq$	Subconjunto propio o igual.
$(a_i)_{1\leq i\leq n}$	Sucesión finita de los términos a_i, con i variando de 1 hasta n, es lo mismo que un vector o una n-ada ordenada.
$(a_i)_{i\in\mathbb{N}}$	Sucesión infinita de los términos a_i, con i variando en $\mathbb{N}$.
$\sum_{C} T$	Suma de los términos T que cumplen las condiciones C. Si los términos son a_i, siendo las condiciones $1 \leq i \leq k$, esto es, los términos de una sucesión finita, escribimos $\sum_{i=1}^{k} a_i$, o bien $\sum_{i=1}^{k} a_i$.
$\mapsto$	Sustitución, o mapeo de elementos bajo una función dada.
:	Tal que (para conjuntos en forma descriptiva).
$\overset{\mathcal{T}}{\longmapsto}$	Transformación $\mathcal{T}$ aplicada a un elemento específico.
$[\mathfrak{e}]$	Unidad en $\mathfrak{C}_{\Delta}$.
$\lvert\cdot\rvert$	Valor absoluto.
$\mathbf{x}$	Vector de variables $(x_1, \ldots, x_n)$.

RESUMEN

En este trabajo de graduación se estudian las formas cuadráticas binarias restringidas al anillo $\mathbb{Z}$ de los enteros, o bien al campo $\mathbb{Q}$ de los números racionales. Se demuestra que, para ciertos coeficientes, el conjunto de números que se obtienen al recorrer con las variables todo su dominio es cerrado bajo el producto. Más específicamente, se describen los conjuntos de números representables por algunas formas cuadráticas particulares en términos de los primos que los componen, haciendo uso de la relación de congruencia. Con esto, se abre paso al estudio de las distintas identidades de cerradura que poseen algunas formas. También se trata el problema de la cantidad de representaciones distintas que un número posee, bajo ciertas formas cuadráticas, poniendo énfasis en el caso de los números primos.

Se concluye el tema de las formas cuadráticas en los enteros con algunos elementos de la teoría general de las cerraduras, donde se generalizan ciertos conceptos estudiados en los capítulos anteriores. Específicamente, se determinan cerraduras semejantes a las de Brahmagupta, pero válidas para toda forma cuadrática mónica en una de sus variables. Después de esto, expandiendo el estudio a $\mathbb{Q}$, se describen los teoremas fundamentales de la teoría de formas racionales. También se pone de manifiesto la utilidad de dicha teoría para resolver problemas de representabilidad que tratan sobre enteros.

OBJETIVOS

General

Plantear y, siempre que sea posible, resolver problemas de carácter general, relativos a la representabilidad de números mediante formas cuadráticas binarias, poniendo énfasis en los que versen sobre las identidades de cerradura asociadas.

Específicos

1. Presentar las técnicas básicas empleadas para la resolución de problemas teórico-numéricos de la índole descrita en el objetivo general.

2. Determinar los conjuntos de números representables por formas cuadráticas específicas, como lo son $x^2 - y^2,\ x^2 + y^2,\ x^2 + xy + y^2$.

3. Encontrar funciones que describan la cantidad de representaciones que posee un número en las formas cuadráticas anteriores.

4. Plantear identidades de cerradura de la mayor generalidad posible, respecto a los coeficientes de las formas. De ser posible, obtener cerraduras válidas para todas las formas mónicas.

5. Identificar interrelaciones entre los problemas planteados, especialmente al variar la estructura algebraica subyacente o al colapsar los resultados generales en casos particulares.

6. Hallar nexos entre éstos y otros problemas conocidos de la Teoría de Números.

INTRODUCCIÓN

Una *forma cuadrática binaria* es un polinomio homogéneo de segundo grado en dos variables, esto es, una expresión del tipo: $ax^2 + bxy + cy^2$, donde a, b, c son los coeficientes, en tanto que x, y son las variables. Habiendo fijado los coeficientes, se dice que un número n es *representable* en la forma cuadrática anterior, si existen soluciones x, y dentro de alguna estructura algebraica de interés, para la ecuación $n = ax^2 + bxy + cy^2$. El estudio de las formas cuadráticas en el marco de la Teoría de Números ha suscitado numerosos descubrimientos en varios campos de las matemáticas, y de la ciencia en general.

Una *cerradura* es una identidad algebraica que permite verificar que el producto de dos números representables en una forma dada es también un número representable. No todas las formas cuadráticas poseen cerraduras, y este fenómeno es un indicador de la complejidad que tiene el problema de decidir cuándo una forma representa a un número dado. El interés primordial del documento será éste, el problema de la representación, y en segundo lugar la intrincada teoría de las cerraduras, buscando siempre conectar los resultados clásicos y conocidos con las investigaciones de vanguardia. La mayoría de las demostraciones son propias, aunque algunos de los problemas planteados sean conocidos.

1. MARCO TEÓRICO

1.1. Antecedentes

El problema de la representación de números mediante formas cuadráticas ha interesado a los matemáticos desde épocas muy remotas. Las identidades de cerradura para los números de la forma $x^2 + y^2$, conocidas como *identidades de Brahmagupta-Fibonacci*:

$$\begin{cases} (t^2+u^2)(v^2+w^2) = (tv-uw)^2 + (tw+uv)^2 \\ (t^2+u^2)(v^2+w^2) = (tv+uw)^2 + (tw-uv)^2 \end{cases} \tag{1.1}$$

aparecen por primera vez [11] en los escritos de Diofanto,[1] y son un caso especial ($n = 2$) de la identidad de Lagrange,[2] la cual se puede apreciar a continuación:

$$\begin{aligned} \left(\sum_{k=1}^{n} a_k^2\right)\left(\sum_{k=1}^{n} b_k^2\right) - \left(\sum_{k=1}^{n} a_k b_k\right)^2 &= \sum_{i=1}^{n-1}\sum_{j=i+1}^{n} (a_i b_j - a_j b_i)^2 \\ &= \frac{1}{2}\sum_{i=1}^{n}\sum_{j=1}^{n}(a_i b_j - a_j b_i)^2 \end{aligned}$$

Las identidades de Brahmagupta-Fibonacci indican que si dos números pueden ser escritos como suma de dos cuadrados, entonces el producto de ellos también. Dichas identidades son equivalentes a la propiedad de los números complejos que

[1] **Diofanto de Alejandría** (207? – 291?), algunas veces llamado «El Padre del Álgebra», fue un distinguido matemático griego de la Escuela de Alejandría, y autor de la serie de libros titulada "Aritmética". En el estudio de las ecuaciones con variable entera, su aporte fue tan significativo para su tiempo, que hoy en día a ese tipo de ecuaciones se les denomina ecuaciones diofantinas, y a su estudio, el Análisis Diofantino.

[2] **Joseph-Louis Lagrange** (1736 – 1813) fue un matemático y astrónomo nacido en Turin, quien vivió parte de su vida en Prusia y parte en Francia. Hizo invaluables contribuciones al Análisis, la Teoría de Números y la Mecánica Clásica, y fue uno de los fundadores del Cálculo Variacional. En Teoría de Números, Lagrange fue el primero en probar que las ecuaciones de Pell: $x^2 - ny^2 = 1$, poseen soluciones no triviales en enteros, para cada valor de n que no sea un cuadrado perfecto. Demostró además el teorema de Wilson, y el teorema que dice que todo natural es suma de cuatro cuadrados. Desarrolló una teoría general sobre las formas cuadráticas binarias.

indica que el producto de los módulos de dos complejos es igual al módulo de su producto. Lo anterior es evidencia del lugar preponderante que ocupan las identidades de cerradura en la teoría; asimismo, es una muestra de que las formas cuadráticas están interconectadas con numerosas ramas de la matemática.

En el estudio de la representatividad de números mediante formas cuadráticas es central el problema de cuáles primos se pueden escribir en la forma $x^2 + ny^2$. El mismo Brahmagupta[3] encontró identidades de cerradura generales:

$$\begin{cases} (t^2 + nu^2)(v^2 + nw^2) = (tv - nuw)^2 + n(tw + uv)^2 \\ (t^2 + nu^2)(v^2 + nw^2) = (tv + nuw)^2 + n(tw - uv)^2 \end{cases} \tag{1.2}$$

Este problema, y la Teoría de Formas Cuadráticas en la que desemboca, tuvieron su origen en ciertos teoremas de Fermat,[4] quien en 1654 mostró, entre otras cosas, que todo número primo de la forma $8n + 1$ es representable en la forma $x^2 + 2y^2$. Muchas de las demostraciones de Fermat se perdieron, si es que existieron realmente, y el notable matemático Leonhard Euler[5] se tomó la tarea de reconstruirlas. En 1749, Euler probó, no sin muchas dificultades, que un primo es representado por la forma $x^2 + y^2$ si, y sólo si, al dividir el primo entre 4 no deja residuo 3. La demostración de un teorema análogo para la forma $x^2 + 3y^2$ le tomó una buena parte de su tiempo productivo, en un período de 30 años, hasta que se sintió satisfecho con el argumento [9, 36]. Tales estudios lo llevaron a descubrir la *reciprocidad cuadrática*.

[3]**Bramagupta** (598 – 668) fue un matemático y astrónomo hindú, famoso por numerosos resultados algebraicos y geométricos. Fue el primer matemático en dejar por escrito reglas para utilizar el cero y números negativos. En su tratado *"Brahmasphutasiddhanta"*, propone soluciones a ecuaciones diofantinas lineales y cuadráticas, fórmulas para calcular $\sum_{k=1}^{n} k^2$ y $\sum_{k=1}^{n} k^3$ en términos de $\sum_{k=1}^{n} k$, e incluso algunas relaciones de recurrencia para generar soluciones a ecuaciones de Pell, mediante el algoritmo de Euclides o, como él le llamaba, el «pulverizador».

[4]**Pierre de Fermat** (1601? – 1665), jurista y matemático francés, fue uno de los principales matemáticos de la primera mitad del siglo XVII. Descubrió el Cálculo Diferencial antes que Newton y Leibniz, fue cofundador de la Teoría de Probabilidades junto con Blaise Pascal, y descubrió el principio fundamental de la Geometría Analítica, independientemente de Descartes. Sin embargo, es más conocido por sus aportaciones a la Teoría de Números, y en especial por el famoso «último teorema de Fermat».

[5]**Leonhard Euler** (1707 – 1783) fue un matemático y físico suizo conocido por sus aportes al Cálculo, el Análisis, la Mecánica Clásica, la Teoría de Números, la Óptica y la Astronomía. Euler es posiblemente el científico más prolífico de la historia, solamente equiparable a Gauss. Laplace inmortalizó el espíritu didáctico de Euler en la frase: «Leed a Euler, leed a Euler. Él es el maestro de todos nosotros».

Gauss[6] fue el primero en atacar de manera sistemática el problema general, muchas de sus definiciones siguen vigentes hoy en día. Su Teoría de Géneros resuelve el problema para un conjunto grande, pero ultimadamente finito, de formas cuadráticas. Las leyes de reciprocidad cúbica y bicuadrática expanden el conjunto pero siguen fallando en el caso general.

Poco después, la Teoría Analítica de Formas Cuadráticas comenzó a proveer resultados más interesantes, por ejemplo el teorema publicado por Jacobi[7] en 1834, transcrito a continuación.

Teorema de Jacobi. *El número de maneras de escribir un entero positivo k como suma de cuatro cuadrados está dado por*

$$8 \sum_{\substack{m \mid k \\ 4 \nmid m}} m$$

8 veces la suma de todos los números $m \in \mathbb{N}$, tales que m es divisor de k y 4 no divide a m.

Tal resultado se obtiene de estudiar los coeficientes de Fourier de ciertas funciones denominadas Theta, que se asocian a las formas cuadráticas. Este teorema es una muestra de la universalidad de los conceptos en la Matemática, de cómo no puede existir una rama totalmente independiente de las demás.

La Teoría de Cuerpos de Clases de Hilbert resuelve finalmente el problema [9]. Sin embargo, los métodos que se emplean para demostrar los teoremas de Hilbert están fuera del rango fijado para este trabajo de graduación. Empleando técnicas más elementales se estudiarán algunas partes del problema, buscando siempre que el material permanezca accesible al mayor número posible de personas.

[6] **Johann Carl Friedrich Gauss** (1777 – 1855) fue un matemático, astrónomo, y físico alemán que contribuyó significativamente en muchos campos, incluida la Teoría de Números, el Análisis, la Geometría Diferencial, la Estadística, el Álgebra, la Geodesia, la Teoría Electromagnética y la Óptica. Es, sin lugar a dudas, uno de los matemáticos más influyentes de todos los tiempos, al punto de ser considerado «El Príncipe de las Matemáticas».

[7] **Carl Gustav Jacob Jacobi** (1804 – 1851) fue un matemático alemán considerado por muchos como el más apasionado maestro de su tiempo, y uno de los más grandes científicos de su generación. Uno de sus mayores logros fue su teoría de las funciones elípticas. También es conocido por sus contribuciones a la Mecánica, las Ecuaciones Diferenciales, y a la Teoría de Números.

1.2. Fundamentos de la Teoría de Números

La divisibilidad es uno de los bloques de construcción básicos de la Teoría de Números antigua y moderna. Hoy en día se estudian sus generalizaciones a conjuntos numéricos más extensos que los naturales o enteros. Por ejemplo, se tiene a los enteros cuadráticos, de suma importancia en la Teoría de Números, y entre ellos a los enteros gaussianos. Se describirá aquí la relación de divisibilidad en su forma tradicional.

1.2.1. Divisibilidad elemental

Definición (divisibilidad)**.** Dados $a, b \in \mathbb{Z}$, se dice que a *divide* a b, y se escribe $a \mid b$, si existe $c \in \mathbb{Z}$ tal que $ac = b$. Si $a \mid b$, a es llamado *divisor* de b, y b es llamado *múltiplo* de a.

La relación de divisibilidad no debe confundirse con la operación de división. $a \mid b$ es una proposición que puede ser verdadera o falsa, en tanto que $\frac{a}{b}$ es una operación cuyo resultado es un número.

Definición (combinación lineal)**.** Dados $a, b \in \mathbb{Z}$, se dice que $c \in \mathbb{Z}$ es una *combinación lineal* de a y b si existen $m, n \in \mathbb{Z}$ tales que $c = an + bm$. En otras palabras, la suma de un múltiplo de a con un múltiplo de b es una combinación lineal de ellos.

Propiedades. Sean $a, b, c \in \mathbb{Z}$, la divisibilidad cumple:

- $a \mid 0$, y en particular $0 \mid 0$
- $0 \mid a \implies a = 0$
- $1 \mid a$
- $a \mid a$ (reflexividad)
- $a \mid b,\ \ b \mid c \implies a \mid c$ (transitividad)

- $a \mid b \implies ac \mid bc$
- $a \mid b \implies a \mid bc$ (caso especial de la transitividad)
- $ac \mid bc,\ c \neq 0 \implies a \mid b$ (simplificación)
- $a \mid b,\ a \mid c \implies a \mid bm + cn\ \forall m, n \in \mathbb{Z}$ (combinaciones lineales)
- $a \mid b,\ b \neq 0 \implies |a| \leq |b|$
- $a \mid b,\ b \mid a \implies |a| = |b|$ (antisimetría atenuada)

Ahora se prosigue con el estudio de los números primos, tomando la pista de Euclides[8] y su lema [12], con el propósito de enunciar el teorema de factorización única. Al igual que en el caso de la divisibilidad, la demostración de la factorización única puede ser llevada a cabo en estructuras algebraicas más generales: los *dominios de factorización única*, que son ampliamente estudiados en el Álgebra Abstracta.

Definición (divisor común y múltiplo común)**.** Dados $a, b \in \mathbb{Z}$, a un entero d' se le llama *divisor común* de a y b siempre que $d' \mid a$ y $d' \mid b$. Análogamente, a un entero m' se le llama *múltiplo común* de a y b si $a \mid m'$ y $b \mid m'$.

Definición (máximo común divisor)**.** Dados $a, b \in \mathbb{Z}$, no ambos cero, el máximo entero d del conjunto de divisores comunes es llamado *máximo común divisor*. Para denotar al máximo común divisor se emplean las siguientes notaciones:

$$d = (a, b) \qquad d = \text{MCD}(a, b)$$

Definición (mínimo común múltiplo)**.** Dados $a, b \in \mathbb{Z}$, ambos distintos de cero, el mínimo entero m del conjunto de múltiplos comunes positivos es llamado *mínimo común múltiplo*. Para denotar al mínimo común múltiplo se emplean las siguientes notaciones:

$$m = [a, b] \qquad m = \text{MCM}(a, b)$$

[8] **Euclides de Alejandría** (325? AC – 265? AC) fue un matemático griego conocido como «El Padre de la Geometría». Es el autor de "Los Elementos", libro que encapsula el conocimiento matemático de la antigua Grecia, y que por dos milenios sirvió de guía para la formación de nuevos matemáticos, tanto en conocimiento como en rigor. Muchos de sus resultados teórico-numéricos son precisamente aquellos que exponemos en la sección actual.

Propiedades. Sean $a, b, c, m \in \mathbb{Z}$. El máximo común divisor y el mínimo común múltiplo cumplen las siguientes propiedades:

- $\text{MCD}(a, a) = a$
  $\text{MCM}(a, a) = a$
- $\text{MCD}(a, b) = \text{MCD}(b, a)$
  $\text{MCM}(a, b) = \text{MCD}(b, a)$ (conmutatividad)
- $\text{MCD}(\text{MCD}(a, b), c) = \text{MCD}(a, \text{MCD}(b, c))$
  $\text{MCM}(\text{MCM}(a, b), c) = \text{MCM}(a, \text{MCM}(b, c))$ (asociatividad)
- $\text{MCD}(a, b) = \text{MCD}(|a|, |b|)$
- $\text{MCD}(ma, mb) = m\ \text{MCD}(a, b)$
  $\text{MCM}(ma, mb) = m\ \text{MCM}(a, b)$ (homogeneidad)
- $|ab| = \text{MCD}(a, b)\ \text{MCM}(a, b)$

Las propiedades justifican el uso de la notación $\text{MCD}(a, b, c)$ sin prestar atención al orden y, en general, para cualquier cantidad finita de números. Las definiciones originales de MCD y MCM también se pueden expandir a una cantidad infinita de números aunque, en el caso del MCM, podría no existir.

Teorema (algoritmo de la división)**.** *Dados $a, b \in \mathbb{Z}$ existen $q, r \in \mathbb{Z}$ únicos, llamados* cociente *y* residuo *respectivamente, tales que $a = qb + r$, donde $0 \leq r < b$.*

Corolario (iteración del algoritmo de Euclides)**.** *Si $a, b \in \mathbb{Z}$, r es el residuo dado por el algoritmo de la división, entonces*

$$\text{MCD}(a, b) = \text{MCD}(a - b, b) \qquad \text{MCD}(a, b) = \text{MCD}(r, b)$$

Definición (primo)**.** Se dice que un entero $p > 0$ es *primo* si tiene exactamente cuatro divisores en los enteros (dos positivos y dos negativos).

Definición (primos relativos)**.** A dos enteros a, b se les llama *primos relativos* si $\text{MCD}(a, b) = 1$.

Lema de Bézout. *Dados a, b primos relativos, existen $s, t \in \mathbb{Z}$ tales que $as+bt = 1$.*

Lema de Euclides. *Si p es primo y p divide al producto de dos números, entonces p debe dividir a alguno de ellos (o ambos).*

Lema (Euclides generalizado)**.** *El lema de Euclides permanece válido en el contexto más amplio de primos relativos, esto es, si* $\text{MCD}(c, a) = 1$ *y* $c \mid ab$*, entonces* $c \mid b$*.*

Teorema Fundamental de la Aritmética. *Si n es un entero mayor que uno, entonces existen $p_1, p_2, \ldots, p_k$ primos positivos distintos entre sí, únicos, con $p_1 < p_2 < \ldots < p_k$ y existen $\alpha_1, \alpha_2, \ldots, \alpha_k$ enteros positivos únicos, tales que*

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k} = \prod_{i=1}^{k} p_i^{\alpha_i}$$

es decir, n tiene una factorización única en primos positivos.

El teorema fundamental permite, entre otras cosas, demostrar que existen infinitos primos, tal y como lo hace el propio Euclides en la proposición 20, tomo IX, de "Los Elementos". También permite expresar los valores del MCD y MCM en términos de los primos que componen a los números en cuestión.

Corolario. *Sean $a, b \in \mathbb{Z}$, con factorizaciones en primos dadas por*

$$a = \left(\prod_{i=1}^{k} p_i^{\alpha_i}\right)\left(\prod_{i=1}^{l} q_i^{\alpha_i}\right) \qquad b = \left(\prod_{i=1}^{k} p_i^{\beta_i}\right)\left(\prod_{i=1}^{m} r_i^{\beta_i}\right)$$

donde los primos p_i son comunes a ambos números, en tanto que los primos no comunes de a, b son los q_i, r_i respectivamente. Entonces se tiene que

$$\text{MCD}(a, b) = \prod_{i=1}^{k} p_i^{\text{mín}\{\alpha_i, \beta_i\}}$$

$$\text{MCM}(a, b) = \left(\prod_{i=1}^{k} p_i^{\text{máx}\{\alpha_i, \beta_i\}}\right)\left(\prod_{i=1}^{l} q_i^{\alpha_i}\right)\left(\prod_{i=1}^{m} r_i^{\beta_i}\right)$$

1.2.2. Congruencias

La notación de las congruencias es de mucha utilidad para describir los conjuntos de números representables por formas cuadráticas, motivo por el cual es importante estar familiarizado con ella. Tal vez sea la similitud entre manipular congruencias y resolver ecuaciones lo que facilita la solución de problemas de divisibilidad, cuando se utiliza esta notación. Fue nada menos que Gauss quien, en su obra magistral *"Disquisitiones Arithmeticae"*, introdujo las congruencias [15: Sec. 1], empleándolas en el engrandecimiento de la teoría que había sido edificada ya por Fermat, Euler, Lagrange y Legendre, entre otros. Cuando «El Príncipe» habla, los súbditos prestan atención.

Definición (congruencia)**.** Sean $a, b, m \in \mathbb{Z}$. Se dice que a es *congruente* con b en el módulo m, y se escribe $a \equiv b \pmod{m}$, si, y sólo si, $m \mid (a - b)$. Cuando se manejan varias congruencias del mismo módulo, usualmente se escribe (mód m) una única vez al final de la proposición o el sistema.

Definición (clase de equivalencia)**.** El conjunto $\{x : x \equiv a \pmod{m}\}$ es llamado *clase de equivalencia de* a, y es denotado con el símbolo $\overline{a}$. A manera de ejemplo, en el módulo 4, la clase de equivalencia del 3 es $\{..., -9, -5, -1, 3, 7, 11, 15, ...\} = \overline{3}$.

Propiedades. Si $a, b, c, d, m, n \in \mathbb{Z}$, entonces se tiene que:

- $a \equiv a \pmod{m}$ (reflexividad)
- $a \equiv b \implies b \equiv a \pmod{m}$ (simetría)
- $a \equiv b,\ b \equiv c \implies a \equiv c \pmod{m}$ (transitividad)
- $a \equiv b \implies a + n \equiv b + n \pmod{m}$
- $a \equiv b \implies na \equiv nb \pmod{m}$
- $a \equiv b,\ c \equiv d \implies ac \equiv bd \pmod{m}$ (multiplicatividad)
- $a \equiv b,\ c \equiv d \implies a + c \equiv b + d \pmod{m}$ (aditividad)

- $a \equiv b,\ n \geq 0 \implies a^n \equiv b^n \pmod{m}$
- $a \equiv b \pmod{m},\ a \equiv b \pmod{n} \iff a \equiv b \pmod{\text{MCM}(m,n)}$

Definición (sistema completo)**.** Al conjunto de enteros $\{a_1, a_2, \ldots, a_n\}$ se le llama *sistema completo de residuos* módulo n si para cada entero z existe un único índice j, entre los números del 1 al n, que cumpla

$$a_j \equiv z \pmod{n}$$

esto es, en el conjunto $\{a_1, a_2, \ldots, a_n\}$ existe exactamente un representante de cada clase de equivalencia módulo n.

Definición (inversos)**.** Dados $a, m \in \mathbb{Z}$, se dice que $b \in \mathbb{Z}$ es el *inverso* de a en el módulo m si $ab \equiv 1 \pmod{m}$. Extendiendo la terminología, se dice que $\overline{b}$ es el inverso de $\overline{a}$. Si a posee un inverso, se dice que a es *invertible* y frecuentemente se usa el símbolo a^{-1} para representarlo.

Corolario. *El número a es invertible en el módulo m si, y sólo si a, m son primos relativos. El conjunto de números invertibles es cerrado bajo el producto.*

Definición (sistema reducido)**.** Al conjunto $\{a_1, a_2, \ldots, a_r\}$ se le llama *sistema reducido de residuos* módulo n, si $\text{MCD}(a_i, n) = 1$ para cada índice i; además, para cada entero z tal que $\text{MCD}(z, n) = 1$, existe un único índice j, entre los números del 1 al r, que cumple

$$a_j \equiv z \pmod{n}$$

esto es, cada entero invertible en el módulo n es equivalente a uno y sólo uno de los elementos del conjunto.

Pequeño Teorema de Fermat. *Sean p un primo y a un entero cualquiera, entonces $a^p \equiv a \pmod{p}$. Si a, p son primos relativos, entonces $a^{p-1} \equiv 1 \pmod{p}$.*

Teorema de Wilson. *p es un número primo si, y sólo si, $(p-1)! \equiv p-1 \pmod{p}$.*

Definición (solución)**.** Si $m \in \mathbb{Z}$ y $P(x)$ es un polinomio con coeficientes enteros, no constante, en la variable x, a la expresión $P(x) \equiv 0 \pmod{m}$ se le llama *congruencia polinomial*. Si el grado de $P(x)$ es $1, 2, 3, 4, \ldots$, a la congruencia se le llama lineal, cuadrática, cúbica, cuártica, $\ldots$, respectivamente. Se dice que $a \in \mathbb{Z}$ es una *solución* de la congruencia polinomial si $P(a) \equiv 0 \pmod{m}$. En tal caso, también se dice que $\overline{a}$ es solución de la congruencia, y que la congruencia polinomial es *soluble*.

Nota. La congruencia polinomial es una proposición abierta y, por lo tanto, se le asocia un *conjunto solución*, que es el conjunto de valores que la hacen verdadera. Una congruencia lineal es soluble si el coeficiente de x es invertible.

1.3. Reciprocidad cuadrática

El teorema de reciprocidad cuadrática consta de dos proposiciones suplementarias y una ley principal. Algunos casos particulares del teorema pueden ser deducidos de los teoremas de Fermat. Guiado por estos teoremas, Euler fue capaz de demostrar uno de los suplementos y conjeturar la ley principal [26: p. 5], mas no logró demostrarla. Euler fue uno de los matemáticos más brillantes de la historia, pero si alguien merece el título de genio entre los genios, ese es Gauss. A los 21 años de edad y sin dar muestras de esfuerzo o dificultad, Gauss completó el rompecabezas que había mantenido entretenidos a los sabios de Europa por casi dos siglos.

1.3.1. Fermat y Euler

En este documento se tomará la misma ruta que fue trazada por los grandes de la Teoría de Números. La meta a la que se dirigían fue la de encontrar un mecanismo para verificar cuáles congruencias cuadráticas son solubles; el primer paso fue dado por Fermat con su «Pequeño Teorema». Éste indica que $a^{p-1} \equiv 1 \pmod{p}$, siempre que a sea primo relativo con p, esto es, cuando $a \not\equiv 0 \pmod{p}$. Si p es un primo impar, entonces $\frac{p-1}{2}$ es un entero. De ello se deduce que $a^{(p-1)/2}$ es una solución de la

congruencia cuadrática $x^2 \equiv 1 \pmod{p}$. Esto es señal de que deben considerarse las congruencias cuadráticas sin término lineal, en particular las de módulo primo.

Definición (residuo cuadrático)**.** Sean $r, m \in \mathbb{Z}$ tales que $m \neq 0, \text{MCD}(r, m) = 1$. Se dice que r es un *residuo cuadrático* en el módulo m, si la congruencia $x^2 \equiv r \pmod{m}$ tiene una solución para la variable x. De lo contrario se dice que r es un *residuo no cuadrático*. También se dice que la clase $\overline{r}$ es un residuo cuadrático (pues cada elemento lo es). Si $r \equiv 0$, se tiene que $x \equiv 0$ es solución, pero los elementos de $\bar{0}$ constituyen un caso trivial y generalmente no se consideran residuos cuadráticos.

Es bastante obvio que si a es una solución para la congruencia $x^2 \equiv r \pmod{m}$, entonces $-a$ también lo es, y si el módulo es un primo impar, entonces estas dos soluciones son incongruentes siempre que $r \not\equiv 0$. Aunque en un módulo compuesto no se puede asegurar nada, en módulos primos impares es posible demostrar que este tipo de congruencias tiene, o bien dos soluciones, o ninguna.

Lema. *Sea p un primo impar. Existen $\frac{p-1}{2}$ residuos cuadráticos, en el módulo p, dentro del sistema reducido de residuos $\{1, 2, \ldots, p-1\}$.*

Ya se hizo una excepción con las congruencias, se abandonará nuevamente el orden cronológico para introducir la notación de Legendre, que ayudará a aclarar las propiedades encontradas por Euler mientras estudiaba los problemas de Fermat.

Definición (símbolo de Legendre)**.** Sean p un primo impar, a un entero cualquiera. El *símbolo de Legendre* de a respecto de p está definido por

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{si } a \not\equiv 0, \text{ y } a \text{ es un residuo cuadrático } (\text{mód } p) \\ -1 & \text{si } a \text{ es un residuo no cuadrático } (\text{mód } p) \\ 0 & \text{si } a \equiv 0 \pmod{p} \end{cases}$$

Dos de las propiedades más importantes del símbolo de Legendre son precisamente los suplementos del teorema de reciprocidad, que se estudiarán en la siguiente sección. Por el momento, se enuncian otras proposiciones de interés teórico en las que p es un número primo.

Propiedades del símbolo de Legendre:

- $a \equiv b \pmod{p} \implies \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$
- $a, b \in \mathbb{Z} \implies \left(\frac{a \cdot b}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$ (multiplicatividad completa)
- $F_p \equiv \left(\frac{p}{5}\right) \pmod{p}$, donde F_p es el $p-$ésimo número de Fibonacci.[9]

La definición dada para el símbolo no es aquella que planteó el propio Legendre. Él lo hizo en términos de expresiones del tipo $a^{(p-1)/2}$, y la equivalencia de estas dos definiciones radica en el siguiente resultado.

Criterio de Euler. *Sean p un primo impar, $a \in \mathbb{Z}$ primo relativo con p. Entonces*

$$\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}$$

Como se había mencionado anteriormente, Euler llegó más allá, enunciando incluso la ley general, aunque admitió no haber sido capaz de demostrarla. Se debe recordar que Euler no disponía ni de la notación de congruencias, ni del símbolo de Legendre, motivo por el cual su variante es algo engorrosa [26: p. 3–5], pero, traduciéndola a la notación moderna, se obtiene la siguiente proposición, que es equivalente a las versiones de Legendre y Gauss.

Ley de Reciprocidad (enunciado de Euler)**.** *Sean p, q dos primos impares distintos.*

- *Si* $q \equiv 1 \pmod{4}$, *entonces* $\left(\frac{q}{p}\right) = 1 \iff \left(\frac{p}{q}\right) = 1$.
- *Si* $q \equiv 3 \pmod{4}$, *entonces* $\left(\frac{q}{p}\right) = 1 \iff$ $p \equiv \pm b^2 \pmod{4q}$, *donde b es un entero impar,* $\text{MCD}(b, q) = 1$.

[9] Esta propiedad del símbolo de Legendre es utilizada en tests de primalidad. Los números de Fibonacci, llamados así en honor al matemático Leonardo de Pisa, quien también era conocido como «Fibonacci», conforman una sucesión numérica definida recursivamente mediante la siguiente fórmula: $F_{n+2} = F_{n+1} + F_n$ para $n \in \mathbb{N}$, usando los valores iniciales $F_0 = 0, F_1 = 1$. Para la propiedad del símbolo de Legendre, interesan los de índice primo.

1.3.2. Legendre y Gauss

Al haber observado que $a^{(p-1)/2} \equiv \pm 1 \pmod{p}$, Legendre [26: p. 6–8] establece un listado de 8 teoremas, en los que emplea las letras a, A para representar primos congruentes con 1 en el módulo 4, y las letras b, B para primos congruentes con 3 en el mismo módulo, como se puede apreciar en la tabla I.

Tabla I. **Clasificación de residuos según Legendre**

Teorema	Hipótesis	Conclusión
I	$b^{(a-1)/2} \equiv +1 \pmod{a}$	$a^{(b-1)/2} \equiv +1 \pmod{b}$
II	$a^{(b-1)/2} \equiv -1 \pmod{b}$	$b^{(a-1)/2} \equiv -1 \pmod{a}$
III	$a^{(A-1)/2} \equiv +1 \pmod{A}$	$A^{(a-1)/2} \equiv +1 \pmod{a}$
IV	$a^{(A-1)/2} \equiv -1 \pmod{A}$	$A^{(a-1)/2} \equiv -1 \pmod{a}$
V	$a^{(b-1)/2} \equiv +1 \pmod{b}$	$b^{(a-1)/2} \equiv +1 \pmod{a}$
VI	$b^{(a-1)/2} \equiv -1 \pmod{a}$	$a^{(b-1)/2} \equiv -1 \pmod{b}$
VII	$b^{(B-1)/2} \equiv +1 \pmod{B}$	$B^{(b-1)/2} \equiv -1 \pmod{b}$
VIII	$b^{(B-1)/2} \equiv -1 \pmod{B}$	$B^{(b-1)/2} \equiv +1 \pmod{b}$

Fuente: LEMMERMEYER, Franz. *Reciprocity laws.* p. 6–8.

Habiendo enunciado las proposiciones que deseaba probar, intentó hacerlo basándose en un lema de su autoría que, lamentablemente, no permite demostrar todos los casos planteados.

Lema (Legendre)**.** *Si $a, b, c \in \mathbb{Z}$ son primos relativos a pares tales que no todos tienen el mismo signo, y si las congruencias $u^2 \equiv -bc \pmod{a}, v^2 \equiv -ca \pmod{b}, w^2 \equiv -ab \pmod{c}$ son solubles en las variables u, v, w respectivamente, entonces la ecuación $ax^2 + by^2 + cz^2 = 0$ tiene una solución no trivial[10] en enteros, para x, y, z.*

[10]En este caso, *no trivial* significa que no todas las variables se anulen en la solución.

Ajeno a los descubrimientos de Legendre, Gauss primero demostró las proposiciones suplementarias, luego estableció algunos casos específicos, a partir de los cuales conjeturó la ley general y, finalmente, la probó con todo rigor empleando inducción fuerte [15: Art. 108–144].

En *"Disquisitiones Arithmeticae"*, lo bautizó como teorema fundamental, pero al conversar con amigos lo llamaba «teorema áureo». En el mismo libro elaboró una tabla con los ocho casos de Legendre, pero le agregó seis generalizaciones a números compuestos. No satisfecho con esto, continuó estudiándolo a lo largo de su vida, desde otras perspectivas, y llevó a cabo ocho demostraciones distintas. En dos de ellas hizo uso de lo que llegó a ser conocido como el «lema de Gauss», que ahora constituye el fundamento de las demostraciones más simples.

Suplemento 1. *Si p es un primo impar, entonces se puede decidir si -1 es residuo cuadrático, en el módulo p, mediante la siguiente regla:* $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$

Suplemento 2. *Si p es un primo impar, entonces:* $\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}$

Lema de Gauss. *Sean p un primo impar, $a \in \mathbb{Z}$ primo relativo con p. Considere el conjunto de enteros $\left\{a, 2a, 3a, \ldots, \frac{p-1}{2}a\right\}$, y sus respectivos representantes dentro del sistema reducido de residuos $\{1, 2, \ldots, p-1\}$. Sea n el número de esos representantes que sean mayores a $\frac{p}{2}$, entonces $\left(\frac{a}{p}\right) = (-1)^n$.*

Ley de Reciprocidad (enunciado de Gauss)**.** *Sean p, q primos impares distintos. Se consideran dos casos:*

- $q \equiv 1 \pmod 4 \implies \left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$
- $q \equiv 3 \pmod 4 \implies \left(\frac{p}{q}\right) = \left(\frac{-q}{p}\right)$

Legendre notó que no es necesaria la división en casos, pues se puede expresar el teorema en una única ecuación. Hoy en día, el enunciado de Legendre es el más común en la literatura, y el mecanismo por medio del cual se lleva a cabo la demostración usualmente hace uso del lema de Gauss para establecer la igualdad.

Ley de Reciprocidad (enunciado de Legendre)**.** *Si p, q son primos impares distintos, entonces*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$$

Nota. Las fracciones en el exponente están multiplicadas, pero nunca se colocan entre paréntesis, para no confundirlas con símbolos de Legendre. Este convenio es aplicado de manera general cuando se trabaja el tema de la reciprocidad cuadrática en Teoría de Números.

1.3.3. Módulos compuestos y aplicación

Para obtener un criterio que permita decidir cuáles congruencias cuadráticas poseen soluciones se necesita, además de los resultados previos, un mecanismo que permita analizar módulos compuestos en términos de los primos que los dividen. El primer paso es sencillo y directo.

Proposición 1. *Sean $r \in \mathbb{Z}$, y n compuesto con factorización prima $n = \prod_{i=1}^{k} p_i^{\alpha_i}$. Entonces se cumple que la congruencia $x^2 \equiv r \pmod{n}$ tiene solución si, y sólo si, las congruencias $x^2 \equiv r \pmod{p_i^{\alpha_i}}$ tienen solución, para cada índice $i \in \{1, \ldots, k\}$.*

Aquí se ve la necesidad de considerar al primo 2, que había sido excluido desde el inicio de la sección. Las reglas para la solubilidad en módulos potencia de primos son las siguientes.

Proposición 2. *Todo número es residuo cuadrático en el módulo 2. En el módulo 4, los residuos cuadráticos son $\overline{0}, \overline{1}$. Si el módulo es 8, o cualquier otra potencia de 2, los residuos cuadráticos son los números de la forma $4^k(8t+1)$, y los miembros de $\overline{0}$.*

Proposición 3. *Sean p un primo impar, $k \in \mathbb{Z}^+$. Un número $a \in \mathbb{Z}$, primo relativo con p, es residuo cuadrático $\pmod{p^k}$ si, y sólo si, es residuo cuadrático $\pmod{p}$.*

Proposición 4. *Con las hipótesis de la proposición anterior, el número $p^i a$ (donde $i \in \mathbb{Z}^+$) es residuo cuadrático módulo p^k, si, y sólo si, se cumple alguna de las siguientes condiciones:*

- *$i \geq k$.*
- *i es par y el número a es un residuo cuadrático módulo p^k.*

Ahora, se pondrá en práctica todo el arsenal teórico de la sección, para decidir si algunas congruencias específicas poseen solución.

Ejemplo 1. Determine la solubilidad de la congruencia $x^2 \equiv 39 \pmod{600}$.

Solución. Puesto que $600 = 2^3 \cdot 3 \cdot 5^2$, en virtud de la proposición 1 se tiene que la congruencia será soluble si, y sólo si, cada una de las siguientes congruencias lo es:

$$\begin{cases} x^2 \equiv 39 & (\text{mód } 2^3) \\ x^2 \equiv 39 & (\text{mód } 3) \\ x^2 \equiv 39 & (\text{mód } 5^2) \end{cases}$$

Las soluciones no tienen por qué ser iguales entre sí, basta con que existan. Eligiendo representantes para 39 que sean menores a los módulos, se obtienen las siguientes congruencias:

$$\begin{cases} x^2 \equiv 7 & (\text{mód } 2^3) \\ x^2 \equiv 0 & (\text{mód } 3) \\ x^2 \equiv 14 & (\text{mód } 5^2) \end{cases}$$

La segunda congruencia es obviamente soluble pues 0 es residuo cuadrático en todo módulo. La tercera congruencia tiene módulo potencia de primo, y 14 es primo relativo con éste, así que es soluble sólo si 14 es residuo cuadrático módulo el primo base que es 5. Como $14 \equiv 4 \pmod{5}$, y 4 es residuo cuadrático en ese módulo, entonces la tercera congruencia es soluble. Sin embargo, el trabajo hecho en estas dos congruencias es inútil, pues la primera de ellas no es soluble por la proposición 2 y, por lo tanto, la del enunciado original tampoco. $\diamondsuit$

Ejemplo 2. Determine la solubilidad de la congruencia $x^2 + 3x \equiv 7 \pmod{23}$.

Solución. Esta congruencia es de un tipo distinto a las encontradas anteriormente, el coeficiente de su término lineal es no nulo. Se usará el método de la completación de cuadrados, con la salvedad de que no es la fracción $\frac{3}{2}$ la que se elevará al cuadrado para sumarla a ambos miembros, sino la expresión $3 \cdot 2^{-1}$. Esto puede hacerse ya que el módulo es impar, así que 2 sí posee inverso, que en este caso se puede tomar como 12 o cualquier otro elemento de su clase. Sumando $36^2 \equiv 13^2$ a ambos miembros de la congruencia se obtiene:

$$\begin{aligned}
x^2 + 3x \equiv 7 \pmod{23} \text{ es soluble} &\iff \\
x^2 + 3x + 13^2 \equiv 7 + 13^2 \pmod{23} \text{ es soluble} &\iff \\
(x + 13)^2 \equiv 7 + 169 \pmod{23} \text{ es soluble} &\iff \\
(x + 13)^2 \equiv 176 \pmod{23} \text{ es soluble} &\iff \\
(x + 13)^2 \equiv 15 \pmod{23} \text{ es soluble}
\end{aligned}$$

En algunos pasos se han sustituido números por equivalentes menores al módulo. Si ahora se toma $w = x + 13$, se tiene una congruencia atacable con reciprocidad cuadrática vía el símbolo de Legendre.

$$\left(\frac{15}{23}\right) = \left(\frac{3}{23}\right)\left(\frac{5}{23}\right)$$

Ahora, como $23 \equiv 3 \pmod{4}$, de la ley de reciprocidad (enunciado de Gauss) se puede deducir que

$$\left(\frac{3}{23}\right)\left(\frac{5}{23}\right) = \left(\frac{-23}{3}\right)\left(\frac{-23}{5}\right)$$

Buscando representantes positivos para -23 en los módulos 3 y 5 se obtienen

$$\left(\frac{-23}{3}\right)\left(\frac{-23}{5}\right) = \left(\frac{1}{3}\right)\left(\frac{2}{5}\right)$$

Y aquí es claro que 1 es residuo cuadrático módulo 3, pero 2 no lo es para el módulo 5, de donde

$$\left(\frac{1}{3}\right)\left(\frac{2}{5}\right) = (+1)(-1) = -1 \implies \left(\frac{15}{23}\right) = -1$$

Así que, una vez más, se tiene que la congruencia original no es soluble. En la tabla II se ha llevado a cabo un análisis exhaustivo, con el cual es posible verificar el resultado obtenido anteriormente. ♢

Tabla II. **Insolubilidad de $x^2 + 3x \equiv 7 \pmod{23}$**

x	$x^2 + 3x$	residuo (mód 23)
0	0	0
1	4	4
2	10	10
3	18	18
4	28	5
5	40	17
6	54	8
7	70	1
8	88	19
9	108	16
10	130	15
11	154	16
12	180	19
13	208	1
14	238	8
15	270	17
16	304	5
17	340	18
18	378	10
19	418	4
20	460	0
21	504	21
22	550	21

Fuente: elaboración propia.

Para cerrar la sección, en la tabla III se puede apreciar la reciprocidad cuadrática en todo su esplendor. Los cuadros claros corresponden al primer caso de la ley (enunciado de Gauss), y puede verse en ellos una simetría perfecta respecto de la diagonal principal. Los cuadros oscuros son el segundo caso, y muestran antisimetría. La leyenda explica el significado de los símbolos R y N, usados por Gauss.

Tabla III. **Carácter cuadrático de los primos menores que cien**

q \ p	3	5	7	11	13	17	19	23	29	31	37	41	43	47	53	59	61	67	71	73	79	83	89	97
3		N	R	N	R	N	R	N	N	R	R	N	R	N	N	N	R	R	N	R	R	N	N	R
5	N		N	R	N	N	R	N	R	R	N	R	N	N	N	R	R	N	R	N	R	N	R	N
7	N	N		R	N	N	N	R	R	N	R	N	R	N	R	N	N	R	R	N	R	N	N	N
11	R	R	N		N	N	N	R	N	R	R	N	N	R	R	R	N	R	R	N	N	N	R	R
13	R	N	N	N		R	N	R	R	N	N	N	R	N	R	N	R	N	N	N	R	N	N	N
17	N	N	N	N	R		R	N	N	N	N	N	R	R	R	R	N	R	N	N	N	R	R	N
19	N	R	R	R	N	R		R	N	N	N	N	R	R	N	N	R	N	N	R	N	R	N	N
23	R	N	N	N	R	N	N		R	R	N	R	N	R	N	R	N	N	R	R	N	N	N	N
29	N	R	R	N	R	N	N	R		N	N	N	N	N	R	R	N	R	R	N	N	R	N	N
31	N	R	R	N	N	N	R	N	N		N	R	N	R	N	R	N	R	R	N	N	N	N	R
37	R	N	R	R	N	N	N	N	N	N		R	N	R	R	N	N	R	R	R	N	R	N	N
41	N	R	N	N	N	N	N	R	N	R	R		R	N	N	R	R	N	N	R	N	R	N	N
43	N	N	N	R	R	R	N	R	N	R	N	R		R	R	R	N	R	N	N	R	R	N	R
47	R	N	R	N	N	R	N	N	N	N	R	N	N		R	R	R	N	R	N	R	R	R	R
53	N	N	R	R	R	R	N	N	R	N	R	N	R	R		R	N	N	N	N	N	N	R	R
59	R	R	R	N	N	R	R	N	R	N	N	R	N	N	R		N	N	R	N	R	N	N	N
61	R	R	N	N	R	N	R	N	N	N	N	R	N	R	N	N		N	N	R	N	R	N	R
67	N	N	N	N	N	R	R	R	R	N	R	N	N	R	N	R	N		R	R	N	R	R	N
71	R	R	N	N	N	N	R	N	R	N	R	N	R	N	N	N	N	N		R	R	R	R	N
73	R	N	N	N	N	N	R	R	N	N	R	R	N	N	N	N	R	R	R		R	N	R	R
79	N	R	N	R	R	N	R	R	N	R	N	N	N	N	N	N	N	R	N	R		R	R	R
83	R	N	R	R	N	R	N	R	R	R	R	R	N	N	N	R	R	N	N	N	N		N	N
89	N	R	N	R	N	R	N	N	N	N	N	N	N	R	R	N	N	R	R	R	R	N		R
97	R	N	N	R	N	N	N	N	N	R	N	N	R	R	R	N	R	N	N	R	R	N	R	

- **N:** p no es residuo cuadrático en el módulo q.
- **R:** p es residuo cuadrático en el módulo q.
- **Cuadros oscuros:** $p \equiv q \equiv 3 \pmod 4$.

Fuente: elaboración propia.

1.4. Análisis diofantino

Cualquier ecuación algebraica, ya sea que involucre una o más variables, es llamada ecuación diofantina o diofántica, si se restringe la búsqueda de soluciones a los números enteros, o bien a los naturales. Como se había mencionado en la sección de antecedentes, ellas deben su nombre a Diofanto de Alejandría, pero su estudio se remonta a la escuela pitagórica y aún más atrás.

Aunque en el presente documento interesan exclusivamente las ecuaciones diofantinas polinomiales, esto no implica que el tema de estudio sea simple. El matemático alemán David Hilbert, en el año 1900, presentó un listado de 10 problemas en la conferencia del Congreso Internacional de Matemáticos, celebrada en París. Poco después fue publicado un listado extendido con un total de 23 problemas, que fueron llamados «los problemas de Hilbert». La resolución de ellos se convirtió en la meta de los matemáticos del siglo XX. El décimo problema decía:

> Encontrar un algoritmo que sea capaz de determinar la existencia de soluciones para cualquier ecuación diofantina polinomial con coeficientes enteros.

El teorema de Matiyasevich,[11] en conjunción con el trabajo hecho por otros matemáticos, permite concluir que es imposible construir tal algoritmo [28]. Hilbert se hubiera sorprendido mucho si hubiera vivido lo suficiente como para enterarse de la solución; el propio Matiyasevich demostró posteriormente que la respuesta sigue siendo negativa aún si se restringe a ecuaciones con 9 variables. En referencia al *primer teorema de incompletitud* de Gödel,[12] en el cual las proposiciones verdaderas

[11] **Yuri Matiyasevich** (1947 – $\star$) es un matemático y científico computacional ruso. En 1964 ganó una medalla de oro en la Olimpiada Matemática Internacional (IMO) celebrada en Moscú. Desde 1995 ha sido profesor de la Universidad Estatal de San Petersburgo, y algunos años después comenzó a dirigir la olimpiada de matemáticas de la ciudad.

[12] **Kurt Friedrich Gödel** (1906 – 1978) fue un matemático, filósofo y logicista austriaco/americano. Es mejor conocido por sus dos *teoremas de incompletitud*, publicados en 1931. El primero y más famoso de ellos dice: "En todo sistema axiomático recursivo auto-consistente, suficientemente poderoso como para describir la aritmética de los naturales, existen proposiciones verdaderas que no pueden ser demostradas a partir de los axiomas." También demostró que la *hipótesis del continuo* y el *axioma de selección* son independientes de la Teoría de Conjuntos.

pero indemostrables no parecen del todo relevantes a la teoría, puede obtenerse una versión más fuerte de incompletitud a partir del trabajo de Matiyasevich:

> Correspondiendo a cualquier axiomatización consistente de la Teoría de Números, uno puede construir, de manera explícita, una ecuación diofantina polinomial sin soluciones, tal que su insolubilidad no pueda ser demostrada dentro de la axiomatización dada.

Este resultado trajo como consecuencia que los matemáticos modernos dirigieran sus esfuerzos a la búsqueda de métodos aplicables a ciertas familias de ecuaciones, en lugar de a todas ellas. Tal es el caso del *último teorema de Fermat*, que trata sobre una familia de ecuaciones polinomiales, o bien, una sola ecuación exponencial. A continuación se presenta una lista de ecuaciones diofantinas famosas. Las letras x, y, z son variables enteras, n, m variables naturales, y las otras letras son constantes dadas. Entre paréntesis está escrito el tipo de ecuación.

- $ax + by = c$ diofantina lineal general (lineal binaria)
- $x^2 + y^2 = z^2$ pitagórica (cuadrática ternaria)
- $2^n - 7 = x^2$ Ramanujan-Nagell (exponencial)
- $x^n + y^n = z^n$ último teorema de Fermat (exponencial)
- $x^n - y^m = 1$ Catalan-Mihăilescu (exponencial)
- $x^2 - ay^2 = \pm 1$ Pell-Fermat (cuadrática binaria)
- $\frac{4}{n} = \frac{1}{x} + \frac{1}{y} + \frac{1}{z}$ Erdős-Strauss (polinomial ternaria)

La ecuación de Erdős-Strauss es equivalente a $4xyz = n(xy + xz + yz)$, y es por esto que es clasificada como polinomial, aunque usualmente no se escribe de esta forma. Por tener términos con tres variables sin exponente, se trata de una ecuación cúbica (se suman los grados). Las palabras *binaria, ternaria, cuaternaria, 5-aria, 6-aria,* etc. corresponden al número de variables presentes en una ecuación polinomial.

Definición (solución)**.** Sea $P(x_1, x_2, \ldots, x_n) = 0$, una ecuación diofantina polinomial n-aria, con coeficientes enteros. A una n-ada de números enteros que satisface la

ecuación se le llama *solución individual*. La *solución completa* es el conjunto de todas las soluciones individuales. En ocaciones, algunas variables se restringen a valores naturales, debido a sus aplicaciones teóricas, y se exige la misma condición sobre sus soluciones.

Definición. Un *problema diofantino* es un sistema de ecuaciones diofánticas independientes, en el cual se tiene una cantidad de ecuaciones estrictamente menor a la cantidad de variables (sistema sub-determinado).

A manera de ejemplo, la ecuación $x^2 + y^2 = 25$ es, por sí sola, un problema diofántico, pues se trata de una ecuación con dos variables. Una solución individual es $(3, 4)$, que se puede sustituir en lugar de (x, y) para obtener la igualdad. La solución completa está dada por el conjunto

$$S = \Big\{(-5,0),(-4,-3),(-4,3),(-3,-4),(-3,4),\\ (0,-5),(0,5),(3,-4),(3,4),(4,-3),(4,3),(5,0)\Big\}$$

Las técnicas para resolver problemas diofánticos son, como seguramente se imaginará el lector, muy distintas a aquellas empleadas en la variable real, que se aprenden en la escuela. Además de que el sistema no esté determinado, tienen la complicación inherente a los problemas que versan sobre números primos. Hoy en día, hay dos métodos de aplicación más o menos general: el favorito de Fermat, *descenso infinito*; y una técnica basada en congruencias, el *análisis local*.

1.4.1. Ecuaciones elementales

El tipo de ecuación diofantina más básico que existe es la ecuación lineal general binaria. La primera solución completa, de la que se tenga conocimiento, fue propuesta por Brahmagupta. Dicha solución se obtiene mediante una técnica semejante a la utilizada para resolver ecuaciones diferenciales, la superposición de soluciones. Basta con hallar una solución individual, para generar de ella todas las demás. Y esa primera puede ser hallada mediante el *algoritmo extendido de Euclides*.

Teorema (algoritmo extendido de Euclides, método recursivo)**.** *Sean $a, b \in \mathbb{Z}$, y suponga que $a \geq b$. El máximo común divisor de ellos puede ser hallado mediante el siguiente procedimiento.*

- *defina $r_0 := a, r_1 := b$.*
- *aplique el algoritmo de la división a los números anteriores para hallar el cociente q_2 y el residuo $r_2 = r_0 - q_2 r_1$. Note que se ha expresado a r_2 como combinación lineal de los números r_0, r_1.*
- *(paso iterativo) aplicando el algoritmo de la división a r_{i-2}, r_{i-1}, obtenga el cociente q_i y el residuo $r_i = r_{i-2} - q_i r_{i-1}$. Exprese a r_i como combinación lineal de a, b, mediante sustituciones y simplificaciones. Repita este paso incrementando el valor de i hasta llegar a un índice n tal que $r_n = 0$.*
- *El máximo común divisor es r_{n-1}, y en el proceso ha sido expresado como combinación lineal de a, b.*

Nota. Este teorema permite demostrar el lema de Bézout, que fue mencionado al principio del capítulo. Además de hallar el máximo común divisor de dos números, este procedimiento permite hallar inversos de un número módulo el otro, siempre que sean primos relativos.

Teorema (solución de la ecuación lineal)**.** *La ecuación diofantina lineal $ax + by = c$ tiene solución si, y sólo si, $\text{MCD}(a, b) \mid c$. En tal caso, dividiendo cada término de la ecuación entre $\text{MCD}(a, b)$, se obtiene la ecuación equivalente: $a'x + b'y = c'$, en la cual $\text{MCD}(a', b') = 1$. El algoritmo de Euclides permite encontrar una solución individual (x_0, y_0), y la solución completa está dada por $S = \{(x_0 + b'k, y_0 - a'k) : k \in \mathbb{Z}\}$.*

Ejemplo. Resolver la ecuación $805x + 350y = 70$

Solución. Primero note que $\text{MCD}(805, 350) = 35$ es divisor de 70, por lo que la ecuación es soluble. Tómese la ecuación equivalente $\frac{805}{35}x + \frac{350}{35}y = \frac{70}{35}$, o bien, después de simplificar, $23x + 10y = 2$. Ahora se procederá mediante el algoritmo extendido de Euclides. Tomando $r_0 = 23, r_1 = 10$ se pueden comenzar las iteraciones, que están desplegadas en la tabla IV.

Tabla IV. **Solución de una ecuación diofantina lineal**

i	q_i	r_i	$r_i = r_{i-1} + (-q_i)r_{i-2}$
0	–	23	–
1	–	10	–
2	2	3	$3 = (1)23 + (-2)10$
3	3	1	$1 = (1)10 + (-3)3$
4	3	0	–

Fuente: elaboración propia.

Aquí debe notarse que, puesto que 1 fue escrito como combinación lineal de 3 y 10; y 3 es combinación lineal de 23 y 10; entonces 1 también puede escribirse como combinación lineal de 23 y 10, sustituyendo una de las ecuaciones en la otra:

$$1 = (1)10 + (-3)3 = (1)10 + (-3)[(1)23 + (-2)10] = (-3)23 + (7)10$$

en donde se ha operado algebraicamente como si el 23 y el 10 fueran variables. Esto muestra que $(-3, 7)$ es solución de la ecuación $23x+10y = 1$. Si se duplican los valores de la solución, se obtiene al par $(-6, 14)$, que es solución de la ecuación $23x+10y = 2$ y, por la equivalencia, también es solución de la original. Empleando estos valores:

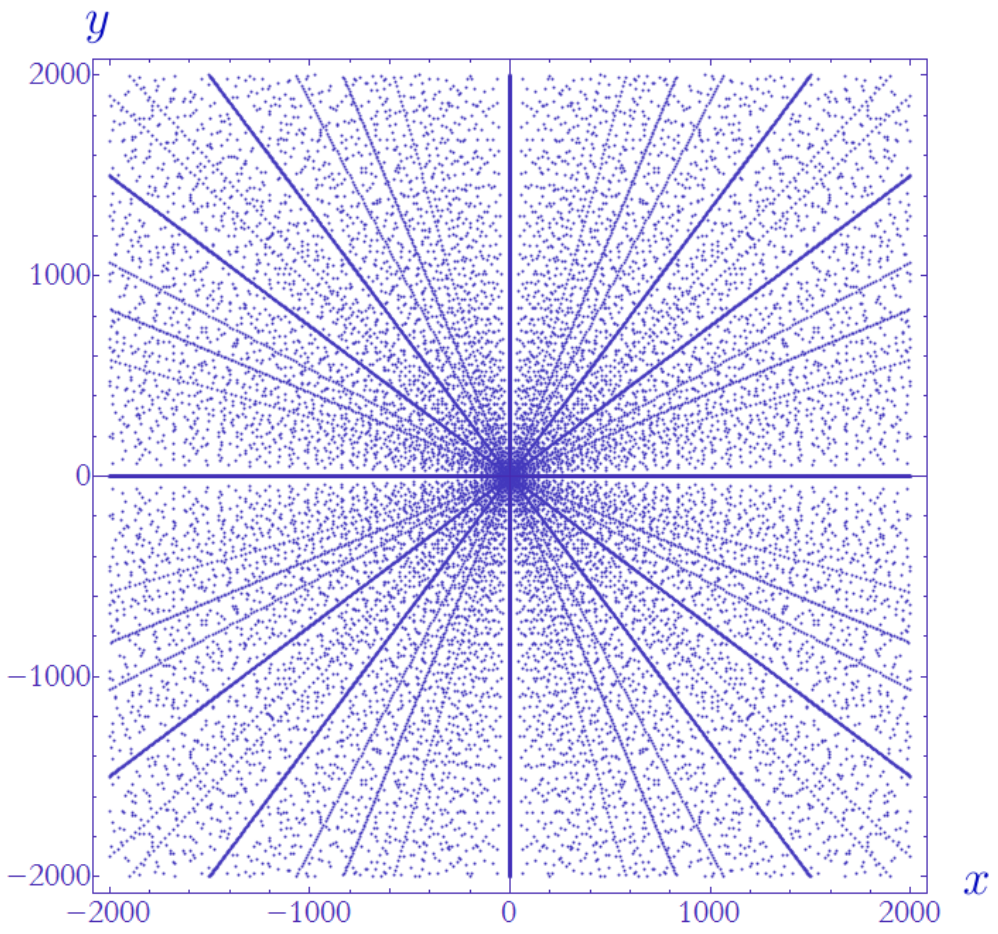
$$x_0 = -6 \qquad y_0 = 14$$
$$a' = 23 \qquad b' = 10$$

la solución completa de la ecuación $805x + 350y = 70$, de acuerdo al teorema previo, está dada por $S = \{(-6 + 10k, 14 - 23k) : k \in \mathbb{Z}\}$. $\diamondsuit$

Otra ecuación de suma importancia en la teoría, es la pitagórica: $x^2+y^2 = z^2$. A las soluciones individuales (a, b, c) se les llama *ternas pitagóricas*. Si $\text{MCD}(a, b, c) = 1$, se dice que la terna pitagórica es *primitiva*, en tanto que si una de las variables se anula, es llamada *trivial*. Cualquier terna puede ser obtenida de una primitiva mediante *escalamiento* (multiplicar cada coordenada por una cierta constante).

Hay infinitas ternas primitivas, y el escalamiento les asocia una familia de triángulos rectángulos semejantes. El conjunto T de todas las ternas pitagóricas puede describirse como la intersección del cono descrito por la ecuación de Pitágoras, con la *cubícula de enteros* $\mathbb{Z}^3$, dentro del espacio $\mathbb{R}^3$. La cubícula es el subconjunto del espacio conformado por todos los puntos de coordenadas enteras. Creando una proyección de T al plano xy (borrando la z de cada terna), se observa una asombrosa regularidad, y la presencia de curvas y rectas sobre las cuales la densidad es mayor, como puede apreciarse en la figura 1.

Figura 1. **Distribución de las ternas pitagóricas**



Fuente: elaboración propia, mediante Wolfram Mathematica 8.

Las rectas eran algo esperado, pues corresponden a las familas generadas por una misma primitiva. Las curvas (que resultan ser parábolas), por el contrario, constituyen una sorpresa grata e inexplicable, cosa común en la Teoría de Números. En cuanto a cómo hallar todas las soluciones, se cuenta con el siguiente teorema, fruto del esfuerzo de varios sabios griegos, inmortalizado en "Los Elementos".

Teorema (fórmula de Euclides)**.** *Dados $m, n \in \mathbb{Z}^+$ uno par y el otro impar, tales que $m > n, \text{MCD}(m, n) = 1$, se cumple que*

$$a = m^2 - n^2, \qquad b = 2mn, \qquad c = m^2 + n^2$$

conforman una terna pitagórica primitiva. Más aún, para cualquier terna pitagórica $(a, b, c) \in \mathbb{N}^3$ existen m, n únicos, tales que la terna es generada por ellos.

1.4.2. Descenso infinito y análisis local

El *descenso infinito* es un tipo particular de demostración por contradicción que se basa en dos propiedades de los naturales, el hecho de que $\mathbb{N}$ es un conjunto *bien ordenado*,[13] y que para cada elemento de $\mathbb{N}$ hay sólo una cantidad finita de naturales menores que él.

El descenso infinito es utilizado para demostrar que, para cada elemento n de un conjunto $A \subseteq \mathbb{N}$, no se cumple una propiedad $p(n)$ determinada, esto es, proposiciones del tipo $\forall n \in A, \neg p(n)$. Se supone la existencia de un elemento que cumple con la propiedad, y se utiliza para generar otro, estrictamente menor, que también la cumple. El principio de inducción matemática garantiza la existencia de una sucesión infinita y estrictamente decreciente de naturales que cumplen la propiedad, lo cual es absurdo. La conclusión es que ningún elemento de A puede cumplir la propiedad.

El método fue empleado sistemáticamente por Fermat para justificar la insolubilidad de muchas ecuaciones diofantinas, al menos si uno está dispuesto a confiar

[13] A un conjunto S se le dice *bien ordenado*, si posee un orden tal que cualquier subcojunto no vacío de S tiene un elemento mínimo.

en su palabra, pues la mayoría de sus demostraciones no llegaron a la actualidad. No importando cuál sea el caso, es innegable la utilidad del descenso infinito en la Teoría de Números; matemáticos renombrados del siglo pasado, como Mordell y Weil, lo utilizaron en algunos de sus resultados más famosos.

Ejemplo. Demuestre que la ecuación diofantina $w^2 + x^2 = 3(y^2 + z^2)$, no posee soluciones a excepción de la trivial $(0, 0, 0, 0)$.

Demostración. Supóngase entonces que una solución no trivial (a, b, c, d) existe, tal que ninguna coordenada es negativa. Esta condición no implica pérdida de la generalidad, pues todas las variables están elevadas al cuadrado, así que la ecuación es invariante a cambios de signo de las variables. El *tamaño* de la solución estará dado por la suma $a+b+c+d$. Ahora bien, $3 \mid 3(c^2+d^2)$, por lo que $3 \mid (a^2+b^2)$. Se puede revisar fácilmente mediante congruencias que esta condición implica $3 \mid a$ y $3 \mid b$. Esto quiere decir que existen $e, f \in \mathbb{Z}^+$, tales que $a = 3e, b = 3f$, con e, f menores que a, b, respectivamente.

Sustituyendo en la ecuación se obtiene $(3e)^2 + (3f)^2 = 3(c^2 + d^2)$, de donde $3(e^2 + f^2) = c^2 + d^2$. Es inmediatamente verificable que (c, d, e, f) es otra solución no trivial de la ecuación, de tamaño estrictamente menor, con coordenadas no negativas. Por inducción existirían infinitas soluciones, en sucesión decreciente, generadas por este procedimiento. Se concluye entonces que la solución inicial no puede existir. $\diamondsuit$

El descenso infinito era ya conocido por los matemáticos griegos. Hipaso, en el siglo V antes de Cristo, lo empleó para demostrar que $\sqrt{2}$ es un número irracional. Esto no debería ser una sorpresa, pues si $\sqrt{2}$ fuera un número racional, como $\frac{a}{b}$, entonces el par (a, b) sería una solución individual de la ecuación diofantina $x^2 = 2y^2$. El ejemplo que fue dado arriba es una generalización del teorema de Hipaso, por lo que sus demostraciones siguen las mismas pautas.

Note que este tipo de problemas admite una interpretación en geometría analítica. Teoremas como el de Hipaso indican que una cierta curva, superficie o, de manera

más general, una *variedad*[14] no pasa por ningún punto tal que todas sus coordenadas sean enteras, salvo el origen. Resolver problemas diofantinos es hallar la intersección de variedades en $\mathbb{R}^n$ con la retícula de los enteros $\mathbb{Z}^n$.

La otra técnica de amplio espectro es el *análisis local*. Consiste en estudiar una determinada ecuación en cada módulo primo, intentando identificar restricciones. Posteriormente se estudia en módulos potencia de primos y, finalmente, se intenta construir una solución al problema original, encajando las obtenidas en cada módulo.

Definición (local vs. global)**.** Dada una ecuación diofantina $P(x_1, \ldots, x_n) = 0$, donde P es un polinomio de coeficientes enteros, considérense las congruencias asociadas $P(x_1, \ldots, x_n) \equiv 0 \pmod{m}$ variando a m en el conjunto de los naturales. Una n-ada ordenada $(a_1, \ldots, a_n) \in \mathbb{Z}^n$, que satisfaga la congruencia para un m específico,será llamada *solución local individual en el módulo* m de la ecuación original. También se le dice así a la n-ada de las clases de equivalencia $(\overline{a_1}, \ldots, \overline{a_n})$, como es costumbre. El conjunto de todas las soluciones locales individuales en un módulo fijo m, será llamado *solución completa local en el módulo* m. En contraposición, las soluciones de la ecuación diofantina se consideran *globales*. Note que una solución global debe ser solución local en todo módulo, pero es muy frecuente que soluciones locales de módulos específicos no sean globales.

Ejemplo. Hallar la solución completa de la ecuación $12x + 5y^2 = 7$.

Solución. Se desea elegir primos que resulten relevantes en la construcción de soluciones. Usualmente es una buena idea comenzar el estudio con los primos que aparecen explícita o implícitamente mencionados en la ecuación, que en este ejemplo son: $2, 3, 5$ y 7. En el módulo 2, el término $12x$ se anula, y la ecuación se reduce a la congruencia $y^2 \equiv 1 \pmod{2}$, que implica que y debe ser impar. En el módulo 5, después de simplificar, resulta $x \equiv 1 \pmod{5}$, que ofrece otra restricción. Sin embargo, no es

[14]Una *variedad algebraica* es el conjunto de soluciones de una ecuación en un espacio definido, y está emparentado con la variedad topológica, que generaliza el concepto de curva (1-variedad) y superficie (2-variedad) a cualquier número de dimensiones y posiblemente espacios distintos a $\mathbb{R}^n$.

necesario continuar el estudio, pues en el módulo 3 se obtiene $y^2 \equiv 2 \pmod 3$, que es imposible ya que 2 no es residuo cuadrático en ese módulo. Al no existir una solución local en un módulo, tampoco puede haber solución global. En otras palabras, la solución completa (global) es $\varnothing$, el conjunto vacío. $\diamondsuit$

Para poder reunir las soluciones locales en una global, siempre que ésta exista y haya una cantidad finita de módulos útiles, se puede usar el «teorema chino del residuo». El enunciado de este teorema apareció en el libro *"Sun Zi suanjing"*, escrito por Sun Zi en el siglo III d. C. El matemático hindú Aryabhata fue el primero en describir lo que podría tomarse como una demostración de este resultado.

Teorema chino del residuo. *Suponga que $(n_i)_{1\leq i\leq k}$ es una sucesión de k números enteros, primos relativos a pares. Entonces, para cualquier sucesión de enteros $(a_i)_{1\leq i\leq k}$, existe $A \in \mathbb{Z}$, tal que A es solución del sistema congruencias*

$$\begin{cases} x \equiv a_1 \pmod{n_1} \\ x \equiv a_2 \pmod{n_2} \\ \qquad\vdots \\ x \equiv a_k \pmod{n_k} \end{cases}$$

Más aún, cualquier otra solución B es congruente con A en el módulo N, donde $N = \prod_{i=1}^{k} n_i$.

Los números racionales se completan en los números reales, rellenando los agujeros que quedan especificados por la *métrica euclidiana.*[15] Sin embargo, al utilizar distintos tipos de métrica es posible obtener "completaciones" esencialmente diferentes. Tal es el caso de los números p-ádicos, que están directamente emparentados con el análisis local, pues éstos fueron creados con el propósito de implementar las herramientas de las series de potencias en el ámbito de las congruencias.

[15]Una métrica es una función que define una distancia abstracta en cierto conjunto. La métrica más común en $\mathbb{R}^n$ es la euclidiana (o Pitagórica) que describe la noción usual de distancia.

El análisis local sólo devuelve condiciones necesarias para la existencia de soluciones, pero, en algunas ocasiones, la existencia de soluciones reales y p-ádicas para cada primo p, resulta ser condición suficiente. En esas circunstancias puede determinarse la solución completa a través de este método, y se dice que la ecuación satisface el *principio de Hasse*, el cual es de especial utilidad en el estudio de las formas cuadráticas en los racionales (capítulo 5).

1.4.3. La ecuación de Pell-Fermat

La ecuación $x^2 - ny^2 = 1$, donde $n \in \mathbb{Z}^+$ no es un cuadrado perfecto, es llamada ecuación de Pell-Fermat, o simplemente, ecuación de Pell. Leonhard Euler atribuyó equívocamente su solución a John Pell cuando, en realidad, sólo contribuyó a que se hiciera pública [33]. El primer europeo en resolverla completamente fue Lord Brouncker. Cambiando el signo de uno de los miembros: $x^2 - ny^2 = -1$, se obtiene la llamada *ecuación de Pell negativa*. De manera general, el conjunto de ecuaciones que se obtienen de fijar los valores de $a, b, c \in \mathbb{Z}$ en $ax^2 + by^2 = c$, es conocido como la *familia de ecuaciones tipo Pell*. Esta familia es de suma importancia en la Teoría de Números, y está emparentada con el tema central del documento. En lo que sigue se hará referencia exclusivamente a la ecuación original.

La ecuación de Pell-Fermat había sido estudiada extensivamente en India, varios siglos antes del nacimiento de Fermat, comenzando con Brahmagupta, quien encontró un método recursivo para generar la solución completa a partir de una fundamental. Bhaskara[16] fue probablemente la primera persona en resolver el problema general, mediante el método llamado *chakravala*, en el siglo XII [35: p. 72–76]. Hermann Hankel se refiere a este método como «el logro más grande en la Teoría de Números antes de Lagrange» [23: p. 337]. Soluciones individuales a problemas es-

[16] **Bhaskara II** (1114 – 1185) fue un matemático y astrónomo hindú. Entre sus contribuciones más importantes a la Matemática se cuentan: una demostración del teorema de Pitágoras; la solución de algunas ecuaciones cuadráticas, cúbicas y cuárticas en más de una variable, en enteros y en reales; conceptos primitivos de Cálculo Diferencial e Integral, como la noción de derivada, las derivadas de funciones trigonométricas y el teorema de Rolle; desarrolló también la Trigonometría Esférica; adelantándose en varios de estos temas a los matemáticos europeos por cinco o más siglos.

pecíficos eran conocidas ya por los pitagóricos de Grecia, y es posible que Arquímedes tuviera conocimientos más profundos del problema general [27].

Definición (solución fundamental)**.** La solución individual (x_1, y_1) de la ecuación de Pell $x^2 - ny^2 = 1$, que minimice el valor de x en el conjunto de las soluciones, es llamada *solución fundamental*.

Teorema (solución completa de la ecuación de Pell)**.** *Una vez hallada la solución fundamental, las demás soluciones* (x_k, y_k) *pueden ser halladas recursivamente mediante las siguientes fórmulas:*

$$x_{k+1} = x_1 x_k + n y_1 y_k, \qquad y_{k+1} = x_1 y_k + y_1 x_k$$

Así que todo lo que hace falta es un método para hallar la solución fundamental. Para lograr este propósito es necesario desarrollar algunas herramientas teóricas previamente.

Una representación como fracción continua para el número a, es aquella que se obtiene mediante el siguiente proceso iterativo: Se escribe $a = \lfloor a \rfloor + \frac{1}{x}$, donde $\lfloor a \rfloor$ es la *parte entera* de a (se obtiene al truncar todos los decimales), y x es el recíproco de la *parte fraccionaria* (lo que fue truncado). Luego, x se expresa como una suma semejante. El procedimiento se detiene si una parte fraccionaria se hace cero, de lo contrario sigue indefinidamente. Como ejemplo se muestra abajo la expansión de π.

$$\pi = 3 + \cfrac{1}{7 + \cfrac{1}{15 + \cfrac{1}{1 + \cfrac{1}{292 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{2 + \ldots}}}}}}}}$$

Si se detiene el procedimiento después de una cantidad finita k de pasos, y se hace caso omiso de la parte fraccionaria que corresponde, el número racional obtenido (al simplificar la expresión) es una buena aproximación del original, y es llamado *k-ésimo convergente*. De manera general, una fracción continua es una expresión del tipo

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cfrac{1}{a_4 + \dots}}}}$$

Donde la sucesión (a_i) puede ser finita o infinita. En cualquiera de los casos, a_0 es un entero cualquiera, en tanto que todos los demás términos son enteros positivos. El *k-ésimo convergente* se representa mediante la notación compacta $[a_0; a_1, a_2, \dots, a_k]$, y si la fracción continua fuera infinita, puede representarse con $[a_0; a_1, a_2, \dots]$.

Definición (irracional cuadrático)**.** Un número ξ es llamado *irracional cuadrático* si es irracional, y es solución de una ecuación cuadrática $ax^2+bx+c = 0$ con coeficientes a, b, c enteros y discriminante Δ positivo, donde $\Delta = b^2 - 4ac$.

Nota. Por la fórmula cuadrática, todo irracional cuadrático se puede escribir de la forma $\xi = \frac{P+\sqrt{\Delta}}{Q}$, donde $P, Q \in \mathbb{Z}$, y Δ no es cuadrado perfecto.

Euler demostró que si ξ tiene una fracción continua infinita periódica, entonces ξ es un irracional cuadrático [14]. Lagrange probó el converso [10], esto es, que todo irracional cuadrático tiene fracción continua infinita periódica, y que la expansión comienza a repetirse cuando uno de los a_i tome como valor el doble de a_0. Este fragmento de teoría es de utilidad en virtud del siguiente teorema.

Teorema. *En referencia a la ecuación de Pell $x^2 - ny^2 = 1$, la solución fundamental es un convergente de la fracción continua de $\sqrt{n} = [a_0; a_1, a_2, \dots]$. El k-ésimo convergente $\frac{g_k}{h_k}$ puede ser hallado recursivamente mediante las siguientes fórmulas:*

$$g_k = a_k g_{k-1} + g_{k-2} \qquad\qquad h_k = a_k h_{k-1} + h_{k-2}$$

haciendo uso de los valores iniciales:

$$\begin{aligned} g_0 &= a_0, & h_0 &= 1 \\ g_1 &= a_0 a_1 + 1, & h_1 &= a_1 \end{aligned}$$

Este procedimiento puede ser usado hasta que el convergente $\frac{g_k}{h_k}$ corresponda a una solución (g_k, h_k) de la ecuación de Pell, y esa será la solución fundamental.

Ejemplo. Describir la solución completa de la ecuación $x^2 - 7y^2 = 1$.

Solución. Los pares (a, b) que resuelven la ecuación son convergentes $\frac{a}{b}$ del número $\sqrt{7}$. Es necesario determinar la fracción continua de $\sqrt{7}$ para comenzar las recurrencias. Haciendo uso de una calculadora (o el método numérico que prefiera) se obtiene la aproximación $\sqrt{7} \approx 2,645751311065$. La parte entera es $a_0 = \lfloor\sqrt{7}\rfloor = 2$, en tanto que la parte fraccionaria restante es aproximadamente $0,645751311065$, con lo que su recíproco $\frac{1}{\sqrt{7}-\lfloor\sqrt{7}\rfloor}$ es cercano a $1,54858377035$. Luego $a_1 = \left\lfloor \frac{1}{\sqrt{7}-\lfloor\sqrt{7}\rfloor} \right\rfloor = 1$. Se procede de esta forma hasta que uno de los a_i valga 4 (el doble de a_0). No hace falta avanzar mucho, pues $a_4 = 4$, y la secuencia $1, 1, 1, 4$ se repite periódicamente, lo que se denota por

$$[2; \overline{1, 1, 1, 4}] = [2; 1, 1, 1, 4, 1, 1, 1, 4, 1, 1, 1, 4, \ldots]$$

que en formato amplio es:

$$\sqrt{7} = 2 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{4 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{4 + \ldots}}}}}}}}$$

Al hacer esto, es recomendable utilizar una gran cantidad de decimales, para evitar que el redondeo iterado cause algún error en el cálculo de los a_i. Ahora se determinan los valores iniciales correspondientes a los primeros dos convergentes, mediante las fórmulas dadas en el teorema anterior. Las demás iteraciones se presentan en la tabla V.

$$\text{valores iniciales} \quad \begin{cases} g_0 = a_0 = 2 & h_0 = 1 \\ g_1 = a_0 a_1 + 1 = 3 & h_1 = a_1 = 1 \end{cases}$$

Tabla V. **Convergentes de la fracción continua de $\sqrt{7}$**

k	a_k	g_k	h_k	$g_k^2 - 7h_k^2 = c_k$
0	2	2	1	-3
1	1	3	1	$+2$
2	1	5	2	-3
3	1	8	3	$+1$
4	4	37	14	-3
5	1	45	17	$+2$
6	1	82	31	-3
7	1	127	48	$+1$

Fuente: elaboración propia.

A los c_k se les llama *aproximaciones tipo Pell*, en referencia a la familia de ecuaciones. Se podría detener el proceso al obtener el primer $+1$ en esa columna, que corresponde a la solución fundamental $(x_1, y_1) = (8, 3)$, pero continuando algunos pasos más se evidencia el hecho de que todas las soluciones aparecen eventualmente en la tabla anterior. Ahora sólo se tiene que aplicar el teorema de la solución completa, que aparece en la página 31, para generar el resto. La primera de ellas resulta ser: $(x_2, y_2) = (x_1^2 + 7y_1^2, 2x_1y_1) = (127, 48)$, como era de esperarse al inspeccionar la fila de la tabla en la que $k = 7$. $\diamondsuit$

2. FORMAS CUADRÁTICAS: ESTUDIO PRELIMINAR

2.1. Definiciones iniciales

Definición (forma cuadrática)**.** Se le llamará *forma cuadrática* a cualquier polinomio homogéneo de grado 2 en cualquier número de variables. De acuerdo a la cantidad de variables que posea, se le agregará al nombre anterior la palabra *binaria, ternaria, cuaternaria, quinaria,* etc. y de manera general, se dirá que es n-aria si posee $n \in \mathbb{N}$ variables.

Nota. Vale la pena recalcar que, para que un polinomio sea considerado una forma cuadrática, debe ser homogéneo. Esto quiere decir que todos sus términos poseen, o bien, una variable al cuadrado, o bien, el producto de dos variables distintas. Así, por ejemplo, la expresión $x^2 + 3x + 2$ es un polinomio cuadrático, pero no una forma.

Definición. Se dice que una forma cuadrática es natural, entera, racional o real, si sus coeficientes pertenecen al conjunto $\mathbb{N}, \mathbb{Z}, \mathbb{Q}$ o $\mathbb{R}$, respectivamente, y el dominio de sus variables está restringido al mismo conjunto. En ocasiones no se especificará el conjunto numérico en cuestión, sino que simplemente será denotado por $\mathbb{S}$ (en este documento sólo se permitirá que $\mathbb{S}$ represente a alguno de esos cuatro conjuntos, poniendo especial atención a los casos $\mathbb{Z}$ y $\mathbb{Q}$). En tales circunstancias, a la forma cuadrática que cumple las condiciones de arriba con respecto al conjunto $\mathbb{S}$, será llamada $\mathbb{S}$-*forma cuadrática*, y $\mathbb{S}$ es su *conjunto subyacente*.

Definición (representabilidad)**.** Se dice que $s \in \mathbb{S}$ es representable por una $\mathbb{S}$-forma cuadrática si existen valores en $\mathbb{S}$ que puedan sustituirse por las variables de la $\mathbb{S}$-forma, de manera que ésta tome el valor s. Dado $A \subseteq \mathbb{S}$, se dice que la forma es *universal en* A si puede representar a todos los elementos de A. Si $A = \mathbb{S}$, en lugar de decir universal en $\mathbb{S}$, se le llama simplemente *universal*. Si representa a casi todos

los elementos de $\mathbb{S}$, a excepción de un conjunto finito D, se le llama *cuasi-universal*, y a D, su *conjunto de deficiencia.* Si la cardinalidad de D es d, se dice que la forma cuasi-universal es *de déficit d*.

Definición (forma diagonal)**.** Se dice que una forma cuadratica es *diagonal* si no posee términos cruzados, esto es, términos que tengan dos variables.

Nota. No hay $\mathbb{Z}$-formas cuadráticas unarias, binarias o ternarias que sean universales en $\mathbb{N}$. Lagrange demostró que la $\mathbb{N}$-forma $x^2 + y^2 + z^2 + w^2$ es universal, y a este resultado se le llegó a conocer como «el teorema de los cuatro cuadrados». Ramanujan encontró todas las $\mathbb{N}$-formas diagonales que sean universales, de las cuales hay 54 en total [8]. En el apéndice B, en la página 149, se encuentra el listado de Ramanujan y de todas las $\mathbb{N}$-formas diagonales cuasi-universales que tengan déficit 1 ó 2.

Ejemplos.

forma:	$3x^2$
tipo:	unaria
diagonal:	sí
posibles $\mathbb{S}$:	$\mathbb{N}, \mathbb{Z}, \mathbb{Q}$ o $\mathbb{R}$
un representable:	si $\mathbb{S} = \mathbb{N}$, 12 es representable ya que $12 = 3(2)^2$
universal:	no; en $\mathbb{N}, \mathbb{Z}$ y $\mathbb{Q}$ no representa al 2, y en $\mathbb{R}$, al -5

forma:	$2x^2 + \frac{1}{3}xy - y^2 + zw$
tipo:	cuaternaria
diagonal:	no
posibles $\mathbb{S}$:	$\mathbb{Q}$ o $\mathbb{R}$
un representable:	si $\mathbb{S} = \mathbb{Q}$, $-\frac{69}{2} = 2(\frac{1}{2})^2 + \frac{1}{3}(\frac{1}{2})(6) - (6)^2 + (0)(-\frac{5}{7})$
universal:	sí, se puede tomar $y = x = 0, w = 1, z \in \mathbb{S}$

forma:	$x^2 - y^2$
tipo:	binaria
diagonal:	sí
posibles $\mathbb{S}$:	$\mathbb{Z}, \mathbb{Q}$ o $\mathbb{R}$
un representable:	si $\mathbb{S} = \mathbb{Z}$, $9 = (-5)^2 - (4)^2$
universal:	en el caso $\mathbb{S} = \mathbb{Z}$ no representa al 6; si $\mathbb{S} = \mathbb{R}$, es fácil probar que es universal; en $\mathbb{Q}$ se verá más adelante

Las formas cuadráticas son de central importancia en numerosas ramas de la Matemática, como lo son la Teoría de Números, el Álgebra Lineal, la Teoría de Grupos, la Geometría Diferencial, la Topología Diferencial, y la Teoría de Lie, por mencionar algunas. En Álgebra Lineal, una forma cuadrática es una generalización del producto punto de vectores y, como tal, se le puede asociar una matriz, lo que explica la terminología de forma diagonal, cuya definición la hace corresponder a una matriz diagonal [25].

En lo que resta del documento se estudiarán las formas cuadráticas binarias, en tanto que los demás tipos jugarán un papel secundario. Enfatizando esa disposición, se harán ocasionalmente algunas definiciones que son exclusivas de las formas binarias. Si no se especifica el número de variables en el discurso, se asume que son dos. Un convenio semejante será aplicado con el conjunto subyacente, en los capítulos 3 y 4 será $\mathbb{Z}$, y en el 5, será $\mathbb{Q}$, a menos que se especifique lo contrario. La mayoría de los resultados de este capítulo aplican para cualquier $\mathbb{S}$.

Dada la matriz simétrica $M = \left(\begin{smallmatrix} a & b/2 \\ b/2 & c \end{smallmatrix}\right)$ con $a, b, c \in \mathbb{S}$, a M se le asocia biyectivamente una $\mathbb{S}$-forma cuadrática, denotada $\mathfrak{q}_M$, definida por

$$\mathfrak{q}_M(x, y) = (x, y) \begin{pmatrix} a & {}^{b}\!/_{2} \\ {}^{b}\!/_{2} & c \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = ax^2 + bxy + cy^2 \tag{2.1}$$

Gauss colocó b en lugar de ${}^{b}\!/_{2}$ en la matriz M, lo cual explica por qué para él las formas cuadráticas tenían que ser expresiones del tipo $ax^2 + 2bxy + cy^2$. En este documento se optará por un camino ligeramente más general, permitiendo que el coeficiente del segundo término también pueda ser impar (en el caso de números enteros o naturales). Esta diferencia desaparece cuando el conjunto subyacente es $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ o cualquier otro campo en que 2 posea inverso multiplicativo.

Si no resultan de interés las variables de la $\mathbb{S}$-forma cuadrática $ax^2 + bxy + cy^2$, sino solamente los coeficientes, se le representa con el símbolo $\langle a, b, c\rangle$. Por el contrario, si se quiere especificar las variables de dicha forma, se le denota por $\mathfrak{q}(x, y)$.

Definición (representación)**.** Si $s, \xi, \eta \in \mathbb{S}$, se dice que (ξ, η) es una *representación* de s en la $\mathbb{S}$-forma $\mathfrak{q}(x, y)$ si se cumple que $\mathfrak{q}(\xi, \eta) = s$.

Nota. Las variables x, y no pertenecen a $\mathbb{S}$, sólo cuando se valúa la forma cuadrática en números de $\mathbb{S}$ es que se generan elementos representables. Pueden existir muchas representaciones para un mismo número s, pero, si existe al menos una, entonces el número *es representable*. El número cero siempre tiene al menos una representación, a saber $(0, 0)$, a la que se le llama *la representación trivial*. Puede, sin embargo, tener otras, dependiendo de la forma en cuestión.

La manera de generalizar la definición anterior a $\mathbb{S}$-formas n-arias es bastante obvia: *una representación* es una solución de la ecuación que iguala la forma cuadrática n-aria con el número s. En el caso en que $\mathbb{S} = \mathbb{N}$ o $\mathbb{S} = \mathbb{Z}$, la ecuación anterior es diofantina, y lo aprendido en el marco teórico puede ser de utilidad.

2.2. Sobre la búsqueda de cerraduras

Definición (cerradura homogénea)**.** Sea $\mathfrak{q} = \langle a, b, c \rangle$ una $\mathbb{S}$-forma cuadrática. Por *identidad de cerradura homogénea* se entiende una igualdad algebraica del tipo

$$\mathfrak{q}(t, u) \cdot \mathfrak{q}(v, w) = \mathfrak{q}(X, Y) \tag{2.2}$$

donde X, Y son polinomios cuadráticos homogéneos en las variables t, u, v, w, cuyos coeficientes están en $\mathbb{S}$. Al miembro izquierdo de la igualdad, una vez expandido y expresado como polinomio homogéneo de grado 4, se le representa simbólicamente con $\langle\!\langle a, b, c \rangle\!\rangle$, o bien $\mathsf{Q}(t, u, v, w)$, y es llamado *forma auto-composición de* $\mathfrak{q}$.

Note que las identidades de cerradura aseguran que el producto de números representables es otro número representable en la forma dada. Muchas formas cuadráticas poseen cerraduras, mas no todas. También existen cerraduras que no son homogéneas, es decir, en las cuales X, Y no son polinomios cuadráticos homogéneos. En el capítulo 4 se ahondará en estos detalles.

Notación. Sea z un término de grado 4 en las variables t, u, v, w, con coeficiente 1. El coeficiente de z en el polinomio Q será denotado por Q_z, o bien $\langle\!\langle a, b, c \rangle\!\rangle_z$. En el caso de que z sea de grado 2, se escribirá X_z, Y_z para representar los coeficientes de z en los polinomios X, Y.

Nota. A partir de este capítulo se usarán de manera sistemática las variables t, u, v, w en referencia a identidades de cerradura homogéneas, por lo que la notación anterior será consistente. Asimismo, las letras a, b, c siempre representarán constantes.

Ejemplos. Las dos ecuaciones de Brahmagupta-Fibonacci (1.1) son cerraduras homogéneas para la forma $\langle 1, 0, 1\rangle$, en tanto que las identidades de Brahmagupta (1.2) son cerraduras para cualquier forma del tipo $\langle 1, 0, n\rangle$. Considérese ahora la forma $\langle 1, 3, 2\rangle$. Su forma auto-composición es el polinomio que se obtiene de expandir la expresión $(t^2 + 3tu + 2u^2)(v^2 + 3vw + 2w^2)$, y resulta ser

$$\mathsf{Q}(t, u, v, w) = t^2v^2 + 3t^2vw + 2t^2w^2 + 3tuv^2 + 9tuvw + 6tuw^2 + 2u^2v^2 + 6u^2vw + 4u^2w^2$$

Con base en ello se han calculado algunos de los Q_z posibles. De entrada se nota que no aparece ningún término que tenga variables al cubo o a la cuarta potencia, así que si se solicita el coeficiente de uno de esos términos, automáticamente vale cero.

- $\mathsf{Q}_{t^2w^2} = 2$
- $\mathsf{Q}_{u^2vw} = 6$
- $\mathsf{Q}_{t^3v} = 0$
- $\mathsf{Q}_{t^2u^2} = 0$
- $\mathsf{Q}_{tuvw} = 9$

Si se quiere encontrar una identidad de cerradura homogénea para una $\mathbb{S}$-forma determinada, entonces X, Y deben ser polinomios homogéneos cuadráticos en las variables t, u, v, w. Los polinomios más generales que cumplen los requisitos son

$$X = h_1t^2 + h_2u^2 + h_3v^2 + h_4w^2 + h_5tu + h_6tv + h_7tw + h_8uv + h_9uw + h_{10}vw$$
$$Y = k_1t^2 + k_2u^2 + k_3v^2 + k_4w^2 + k_5tu + k_6tv + k_7tw + k_8uv + k_9uw + k_{10}vw$$

donde los h_i, k_i son constantes del conjunto subyacente. Supóngase momentáneamente que $h_1 \neq 0, k_1 \neq 0$. Delimitando la atención al término t^2 se tiene

$$X = h_1 t^2 + \ldots (\text{otros términos sin } t^2), \qquad Y = k_1 t^2 + \ldots (\text{otros términos sin } t^2)$$

Al sustituir estos polinomios dentro de la $\mathbb{S}$-forma $\mathfrak{q}(x, y) = \langle a, b, c\rangle$, después de expandir la expresión se obtiene lo siguiente:

$$\begin{aligned}\mathfrak{q}(X, Y) &= a(h_1 t^2 + \ldots)^2 + b(h_1 t^2 + \ldots)(k_1 t^2 + \ldots) + c(k_1 t^2 + \ldots)^2 \\ &= a h_1^2 t^4 + b h_1 k_1 t^4 + c k_1^2 t^4 + \ldots (\text{otros términos sin } t^4) \\ &= (a h_1^2 + b h_1 k_1 + c k_1^2) t^4 + \ldots (\text{otros términos sin } t^4)\end{aligned}$$

Nótese aquí que ésos son los únicos términos en los que la variable t aparece elevada a la cuarta potencia y, puesto que t^4 no aparece en $\mathbb{Q}$, entonces su coeficiente debe anularse, pero eso es equivalente a exigir que (h_1, k_1) sea una representación no trivial del cero en la forma $\langle a, b, c\rangle$. Eso demuestra el siguiente criterio.

Lema 1. *Si la $\mathbb{S}$-forma $\langle a, b, c\rangle$ no tiene representaciones no triviales de cero, entonces todas sus identidades de cerradura homogéneas (Ec. 2.2), si hubiera alguna, son tales que los polinomios X, Y cumplen $X_{t^2} = 0, Y_{t^2} = 0$, y lo mismo si se cambia t por cualquiera de las otras tres variables u, v, w.*

Toca el turno de investigar los términos del tipo t^3u, t^3v, t^3w, pero los cálculos podrían volverse engorrosos. Eso inspira el siguiente convenio notacional.

Notación. Al sustituir en la $\mathbb{S}$-forma $\mathfrak{q}(x, y)$ las letras x, y por dos polinomios cualesquiera X, Y que sean homogéneos cuadráticos en las variables t, u, v, w; y después de expandir y simplificar, se obtendrá un polinomio homogéneo de grado 4, que se representará con el símbolo $\mathcal{Q}$. Si z es un término de grado 4 en las mismas variables, entonces $\mathcal{Q}_z$ representará el coeficiente del término z en el polinomio $\mathcal{Q}$.

Advertencia. Si se quisiera considerar múltiples opciones para los polinomios que sustituyen a x, y, entonces la notación anterior es ambigua. Por ese motivo, a lo largo de todo el documento se estudiará una única sustitución a la vez.

Escolio 1. *Una sustitución de (x,y) por un par de polinomios (X,Y), en la* $\mathbb{S}$*-forma cuadrática* $\mathfrak{q}$*, da origen a una identidad de cerradura homogénea si, y sólo si,* $\mathcal{Q}_z = \mathsf{Q}_z$ *para cada término z de cuarto grado, en las variables* t, u, v, w*.*

Con la ayuda del conveniente símbolo $\mathcal{Q}$, se ampliará el estudio a todos los términos con la variable t. Las conclusiones a las que se lleguen serán válidas para otras variables por la simetría.

$$\text{Sustitución} \begin{cases} x \mapsto X = & h_1t^2 + h_5tu + h_6tv + h_7tw + \ldots \text{(otros términos sin } t) \\ y \mapsto Y = & k_1t^2 + k_5tu + k_6tv + k_7tw + \ldots \text{(otros términos sin } t) \end{cases}$$

$$\begin{aligned} \mathfrak{q}(X,Y) = \mathcal{Q} &= aX^2 + bXY + cY^2 \\ &= a(h_1t^2 + h_5tu + h_6tv + h_7tw + \ldots)^2 + \\ &\quad b(h_1t^2 + h_5tu + h_6tv + h_7tw + \ldots)(k_1t^2 + k_5tu + k_6tv + k_7tw + \ldots) + \\ &\quad c(k_1t^2 + k_5tu + k_6tv + k_7tw + \ldots)^2 \end{aligned}$$

Identificando las multiplicaciones apropiadas, se obtienen los coeficientes

$$\begin{aligned} \mathcal{Q}_{t^3u} &= 2ah_1h_5 + bh_1k_5 + bh_5k_1 + 2ck_1k_5 \\ \mathcal{Q}_{t^3v} &= 2ah_1h_6 + bh_1k_6 + bh_6k_1 + 2ck_1k_6 \\ \mathcal{Q}_{t^3w} &= 2ah_1h_7 + bh_1k_7 + bh_7k_1 + 2ck_1k_7 \end{aligned}$$

Ninguno de estos términos aparece en Q, así que sus coeficientes se anulan, por el escolio 1. Junto con la ecuación correspondiente para t^4, se tiene el siguiente sistema:

$$\begin{cases} ah_1^2 + bh_1k_1 + ck_1^2 = 0 \\ 2ah_1h_5 + bh_1k_5 + bh_5k_1 + 2ck_1k_5 = 0 \\ 2ah_1h_6 + bh_1k_6 + bh_6k_1 + 2ck_1k_6 = 0 \\ 2ah_1h_7 + bh_1k_7 + bh_7k_1 + 2ck_1k_7 = 0 \end{cases} \tag{2.3}$$

las últimas tres equivalen a exigir que los pares $(h_5, k_5), (h_6, k_6), (h_7, k_7)$ sean soluciones de la ecuación $(2ah_1 + bk_1)x + (bh_1 + 2ck_1)y = 0$, en las variables (x, y). Una vez más aparecen representaciones de cero en una forma, sólo que esta vez es lineal (se permite que sean triviales).

Se podría seguir derivando condiciones sobre los coeficientes de los polinomios X, Y, para que $X_{t^2} \neq 0, Y_{t^2} \neq 0$, o para alguna otra variable, mas ya se ha establecido que depende de la representabilidad de cero en distintas formas. Por otro lado, el autor de este documento ha sido capaz de encontrar identidades de cerradura que cumplan $X_{t^2} \neq 0$, pero sólo para ciertas formas cuadráticas triviales (capítulo 4). Esto sugiere restringir un poco más la definición de cerradura.

Definición (cerradura cruzada)**.** Una cerradura homogénea es *cruzada* si sus polinomios X, Y no poseen variables al cuadrado, sino únicamente términos cruzados. De manera explícita, se exige que X, Y sean polinomios del tipo

$$h_1tu + h_2tv + h_3tw + h_4uv + h_5uw + h_6vw$$

donde los h_i son elementos del conjunto subyacente de la forma cuadrática.

Definición (cerradura reducida)**.** Se dice que una cerradura homogénea es *reducida* si los polinomios X, Y son del tipo

$$h_1tv + h_2tw + h_3uv + h_4uw$$

En la práctica, siempre se usará la sucesión (h_i) para los coeficientes de X, y (k_i) para los de Y.

Ahora se estudiarán las cerraduras cruzadas, y se quiere analizar los posibles valores de los coeficientes de X, Y para que se generen los términos de Q. Esto se puede hacer comparando los polinomios Q y $\mathcal{Q}$, y por ese motivo lo primero que se necesita es expandir la expresión general de Q para una $\mathbb{S}$-forma $\langle a, b, c\rangle$.

$$\begin{aligned}\mathsf{Q} &= (at^2 + btu + cu^2)(av^2 + bvw + cw^2) \\ &= a^2t^2v^2 + abt^2vw + act^2w^2 + \\ &\quad abtuv^2 + b^2tuvw + bctuw^2 + \\ &\quad acu^2v^2 + bcu^2vw + c^2u^2w^2\end{aligned} \tag{2.4}$$

Finalmente se tienen los requisitos para enunciar el resultado principal de esta sección, el cual será de utilidad al estudiar las formas $\langle 1, 0, 1\rangle$ y $\langle 1, 1, 1\rangle$, en el siguiente

capítulo. En lo que resta del documento, cuando se diga *representación de cero*, se hace referencia de manera casi exclusiva a las no triviales.

Teorema 1. *Si cero no es representable (excepto trivialmente) en la* $\mathbb{S}$*-forma* $\mathfrak{q}$*, entonces toda cerradura homogénea de* $\mathfrak{q}$ *es reducida.*

Demostración. Note que el lema 1 de la página 40, con las definiciones más recientes, postula que si $\mathfrak{q}$ no representa a cero, entonces sus cerraduras homogéneas son cruzadas; hace falta demostrar que resultan ser reducidas. La prueba es sencilla, y sigue los mismos lineamientos que los de dicho lema. Suponga que X, Y son polinomios homogéneos cuadráticos que sólo poseen términos cruzados:

$$X = h_1tu + h_2tv + h_3tw + h_4uv + h_5uw + h_6vw$$
$$Y = k_1tu + k_2tv + k_3tw + k_4uv + k_5uw + k_6vw$$

Céntrese la atención en los términos que poseen a la variable t en X, Y; esto porque se desea calcular los coeficientes de términos de $\mathcal{Q}$, que tengan a t^2 con otras letras. Al sustituir $(x, y) \mapsto (X, Y)$ en $\mathfrak{q} = \langle a, b, c\rangle$ se obtiene

$$\begin{aligned}\mathcal{Q} = {} & a(h_1tu + h_2tv + h_3tw + \ldots)^2 + \\ & b(h_1tu + h_2tv + h_3tw + \ldots)(k_1tu + k_2tv + k_3tw + \ldots) + \\ & c(k_1tu + k_2tv + k_3tw + \ldots)^2\end{aligned}$$

El término t^2u^2 se puede generar en X^2 al multiplicar h_1tu por sí mismo; en el producto cruzado XY, se genera al multiplicar h_1tu con k_1tu; en tanto que en Y^2, se produce al multiplicar k_1tu consigo mismo. De lo anterior se puede deducir

$$\mathcal{Q}_{t^2u^2} = ah_1^2 + bh_1k_1 + ck_1^2$$

De manera análoga, al fijarse solamente en los términos de X, Y que posean a la letra v, puede calcularse el coeficiente de v^2w^2, que resulta ser $\mathcal{Q}_{v^2w^2} = ah_6^2 + bh_6k_6 + ck_6^2$. Esto fue hecho porque los dos términos que se deben anular en X, Y para que la cerradura sea reducida son tu y vw. De acuerdo a la ecuación (2.4), los respectivos coeficientes en Q son cero, pues no aparecen. Esto quiere decir que los dos calculados también deben ser cero. Lo anterior se traduce en que $(h_1, k_1), (h_6, k_6)$

sean representaciones de cero. Pero la forma $\mathfrak{q}$, de acuerdo al enunciado, no posee representaciones de cero, así que la única opción es la trivial. De ello se deduce que $h_1 = k_1 = 0$, y también $h_6 = k_6 = 0$, y esto es precisamente lo que se necesitaba para que la cerradura fuera reducida. □

Para futura referencia, la tabla VI muestra una comparación de los coeficientes de los polinomios Q y $\mathcal{Q}$, cuando se consideran las sustituciones de la cerradura reducida, esto es, cuando X, Y son

$$X = h_1tv + h_2tw + h_3uv + h_4uw$$
$$Y = k_1tv + k_2tw + k_3uv + k_4uw$$

Tabla VI. **Q_z versus $\mathcal{Q}_z$ para cerraduras reducidas de $\langle a, b, c\rangle$**

z	Q_z	$\mathcal{Q}_z$
t^2v^2	a^2	$ah_1^2 + bh_1k_1 + ck_1^2$
t^2vw	ab	$2ah_1h_2 + b(h_1k_2 + h_2k_1) + 2ck_1k_2$
t^2w^2	ac	$ah_2^2 + bh_2k_2 + ck_2^2$
tuv^2	ab	$2ah_1h_3 + b(h_1k_3 + h_3k_1) + 2ck_1k_3$
$tuvw$	b^2	$2a(h_1h_4 + h_2h_3) + b(h_1k_4 + h_4k_1 + ...$ $... h_2k_3 + h_3k_2) + 2c(k_1k_4 + k_2k_3)$
tuw^2	bc	$2ah_2h_4 + b(h_2k_4 + h_4k_2) + 2ck_2k_4$
u^2v^2	ac	$ah_3^2 + bh_3k_3 + ck_3^2$
u^2vw	bc	$2ah_3h_4 + b(h_3k_4 + h_4k_3) + 2ck_3k_4$
u^2w^2	c^2	$ah_4^2 + bh_4k_4 + ck_4^2$

Fuente: elaboración propia.

Las dos líneas marcadas con puntos suspensivos deben interpretarse como una única expresión algebraica. La tabla será de utilidad pues muchas de las formas de interés no representan al cero y, en consecuencia del teorema anterior, todas sus

cerraduras homogéneas serán reducidas. Aún cuando el cero sea representable en la forma, todas sus cerraduras que sí sean reducidas se regirán por la tabla VI.

Ejemplo. Hallar todas las cerraduras homogéneas de la $\mathbb{Z}$-forma $\mathfrak{q} = \langle 1, 0, 2\rangle$.

Solución. Primero note que en el polinomio $x^2 + 2y^2$, ninguno de sus términos puede tener valor negativo. Lo mínimo que pueden valer individualmente es cero, y sólo se logra si cada variable toma el valor 0. En consecuencia, la única representación del cero es la trivial, para cualquier $\mathbb{S}$. Esto quiere decir que el teorema 1 aplica y, por lo tanto, las únicas cerraduras homogéneas que puede poseer son las reducidas. Valuando $a = 1, b = 0, c = 2$ en las igualdades $\mathsf{Q}_z = \mathcal{Q}_z$, cuyos miembros están dados en la tabla anterior, resulta el siguiente sistema de ecuaciones.

$$\begin{cases} 1 = h_1^2 + 2k_1^2 & (\text{R-1}) \\ 0 = 2h_1h_2 + 4k_1k_2 & (\text{R-2}) \\ 2 = h_2^2 + 2k_2^2 & (\text{R-3}) \\ 0 = 2h_1h_3 + 4k_1k_3 & (\text{R-4}) \\ 0 = 2(h_1h_4 + h_2h_3) + 4(k_1k_4 + k_2k_3) & (\text{R-5}) \\ 0 = 2h_2h_4 + 4k_2k_4 & (\text{R-6}) \\ 2 = h_3^2 + 2k_3^2 & (\text{R-7}) \\ 0 = 2h_3h_4 + 4k_3k_4 & (\text{R-8}) \\ 4 = h_4^2 + 2k_4^2 & (\text{R-9}) \end{cases}$$

Un sistema de ecuaciones que se origine mediante este método será llamado *sistema de ecuaciones de las cerraduras reducidas*, lo cual explica el R que aparece en la etiqueta de las ecuaciones. En el caso en que $\mathbb{S} = \mathbb{Z}$, las primeras tres ecuaciones conforman un problema diofantino, al igual que el último bloque de tres. Cada solución $(h_1, h_2, h_3, h_4; k_1, k_2, k_3, k_4)$ del sistema completo corresponde a una identidad de cerradura reducida.

La ecuación R-1 exige que (h_1, k_1) sea una representación del número 1 en la forma $\mathfrak{q}$. Si k_1 fuera distinto de cero, entonces el miembro derecho sería mayor que 1, puesto que el conjunto subyacente es $\mathbb{Z}$. Entonces, las únicas *representaciones de la unidad* en la forma $\mathfrak{q}$ son $(1, 0)$ y $(-1, 0)$. Eso implica $h_1 = \pm 1, k_1 = 0$. De

razonamientos semejantes en las ecuaciones R-3, R-7 y R-9 se obtienen valores para las otras incógnitas: $h_2 = 0, k_2 = \pm 1, h_3 = 0, k_3 = \pm 1, h_4 = \pm 2, k_4 = 0$. Se procederá a sustituir dentro del sistema anterior a aquellas que valgan cero, y simplificar lo que resulte, para aclarar el panorama. Algunas de las ecuaciones se trivializan, así que se omitirán en el nuevo sistema.

$$\begin{cases} 1 = h_1^2 & \text{(S-1)} \\ 1 = k_2^2 & \text{(S-2)} \\ 0 = h_1 h_4 + 2k_2 k_3 & \text{(S-3)} \\ 1 = k_3^2 & \text{(S-4)} \\ 4 = h_4^2 & \text{(S-5)} \end{cases}$$

Las ecuaciones S-1, S-2, S-4, S-5 permiten las mismas opciones que descritas previamente, en tanto que la ecuación S-3 es el criterio que permite diferenciar cuáles de esas opciones son válidas (La S en las etiquetas es por tratarse de una simplificación del sistema anterior). Note que, para los valores obtenidos antes, se cumple que $|h_1 h_4| = |2k_2 k_3|$, así que lo único que se necesita es que esos dos términos tengan signo distinto para que se anulen y cumplan el criterio S-3.

Si se clasifican las cuatro incógnitas en dos conjuntos $\{h_1, h_4\}$ y $\{k_2, k_3\}$, lo que se necesita es que la cantidad de números negativos que haya en el primer conjunto tenga una paridad distinta a la cantidad de negativos del segundo conjunto. También se puede hacer una tabla con las $2^4 = 16$ maneras de elegir los valores de estas cuatro incógnitas, y valuar esas opciones en el criterio, descartando las que no den cero. De cualquier forma, se obtienen las siguientes ocho soluciones del sistema R.

$$\begin{array}{ll} (+1,0,0,+2;0,+1,-1,0) & (+1,0,0,+2;0,-1,+1,0) \\ (+1,0,0,-2;0,+1,+1,0) & (-1,0,0,+2;0,+1,+1,0) \\ (+1,0,0,-2;0,-1,-1,0) & (-1,0,0,+2;0,-1,-1,0) \\ (-1,0,0,-2;0,+1,-1,0) & (-1,0,0,-2;0,-1,+1,0) \end{array}$$

Hay que recordar que esas soluciones indican los coeficientes de los polinomios X, Y para las cerraduras $\mathsf{Q} = \mathcal{Q}$. Es precisamente por eso que se divide cada solución

con un punto y coma central, los primeros cuatro coeficientes son de X, y los restantes, de Y. Las ocho cerraduras que se forman con esas soluciones son:

- $(t^2+2u^2)(v^2+2w^2) = (tv+2uw)^2 + 2(tw-uv)^2$
- $(t^2+2u^2)(v^2+2w^2) = (tv+2uw)^2 + 2(-tw+uv)^2$
- $(t^2+2u^2)(v^2+2w^2) = (tv-2uw)^2 + 2(tw+uv)^2$
- $(t^2+2u^2)(v^2+2w^2) = (-tv+2uw)^2 + 2(tw+uv)^2$
- $(t^2+2u^2)(v^2+2w^2) = (tv-2uw)^2 + 2(-tw-uv)^2$
- $(t^2+2u^2)(v^2+2w^2) = (-tv+2uw)^2 + 2(-tw-uv)^2$
- $(t^2+2u^2)(v^2+2w^2) = (-tv-2uw)^2 + 2(tw-uv)^2$
- $(t^2+2u^2)(v^2+2w^2) = (-tv-2uw)^2 + 2(-tw+uv)^2$

Éstas son las únicas cerraduras homogéneas que posee la forma $\langle 1,0,2\rangle$. Note que entre ellas están las dos que se obtienen de la identidad de Brahmagupta cuando se toma $n=2$. $\diamondsuit$

El caso $\mathbb{S} = \mathbb{N}$ merece especial consideración ya que, al estudiar las cerraduras de alguna $\mathbb{N}$-forma cuadrática particular para ciertos valores de las variables t,u,v,w, puede suceder que alguno de los polinomios X,Y tome un valor negativo. En algunas ocasiones es posible elegir distintas cerraduras para distintos valores de las variables, asegurando que los polinomios siempre tomen valores positivos.

Siempre que una forma posea cerraduras, existirán en el listado completo algunas que se pueden deducir trivialmente de otras. En el ejemplo anterior se podría sustituir el polinomio X por su negativo, y así deducir la penúltima cerradura a partir de la primera. Éste es precisamente el tema que se estudiará a continuación, con el cual comienzan a establecerse relaciones entre las cerraduras y las distintas representaciones que posee un mismo número.

2.3. Transformaciones y simetrías

En el contexto actual, una *transformación* es un mapeo que sustituye algunas variables por otras, o bien por una expresión que depende de otras variables. Previamente se hizo la sustitución de las variables x, y por los polinomios X, Y, que dependían de t, u, v, w; eso constituye un ejemplo de transformación. Si se representa con el símbolo $\mathcal{T}$,se puede escribir $\mathcal{T}(x, y) = (X, Y)$. Si el objeto matemático[1] $\mathcal{O}_1$ se convierte en $\mathcal{O}_2$ al sustituir todas las instancias de x por X, y las de y por Y, se usa la notación $\mathcal{O}_1 \overset{\mathcal{T}}{\longmapsto} \mathcal{O}_2$, que se lee: " $\mathcal{O}_1$ se transforma en $\mathcal{O}_2$, bajo la acción de $\mathcal{T}$". En particular se tiene que $\mathfrak{q} \overset{\mathcal{T}}{\longmapsto} \mathcal{Q}$. Se usará la misma notación con cualquier otro tipo de transformación. Para hacer más concisas las definiciones, se emplearán solamente las variables x, y para escribir todas las formas cuadráticas binarias.

Definición. Una *transformación simétrica* es cualquiera de las ocho transformaciones que aparecen en el siguiente listado.

- $\mathcal{T}_1(x, y) = (x, y)$ (identidad)
- $\mathcal{T}_2(x, y) = (-x, y)$ (reflexión de x)
- $\mathcal{T}_3(x, y) = (x, -y)$ (reflexión de y)
- $\mathcal{T}_4(x, y) = (-x, -y)$ (reflexión doble)
- $\mathcal{T}_5(x, y) = (y, x)$ (intercambio)
- $\mathcal{T}_6(x, y) = (y, -x)$
- $\mathcal{T}_7(x, y) = (-y, x)$
- $\mathcal{T}_8(x, y) = (-y, -x)$

Nota. A partir de $\mathcal{T}_2$ y $\mathcal{T}_5$ se pueden obtener las demás mediante la composición, cuyo símbolo es $\circ$. En el apéndice C se incluye una tabla con todas las composiciones.

[1]El término *objeto matemático* engloba varios conceptos. En este documento se limitará a: expresiones algebraicas, vectores cuyas coordenadas son expresiones, matrices cuyos registros (entradas) son expresiones, y a igualdadades entre objetos de la lista previa.

Definición (simetrías)**.** Para $i \in \{1, 2, \ldots, 8\}$, se dice que la forma cuadrática $\mathfrak{q}(x, y)$ es *simétrica respecto a* $\mathcal{T}_i$, si $\mathfrak{q} \overset{\mathcal{T}_i}{\longmapsto} \mathfrak{q}$. El *conjunto de simetrías* de $\mathfrak{q}$, denotado $\mathcal{S}_\mathfrak{q}$, es el que incluye todas las $\mathcal{T}_i$ con respecto a los cuales la forma $\mathfrak{q}$ sea simétrica. El *número de simetrías* de $\mathfrak{q}$ es la cardinalidad de este conjunto.

Volviendo a emplear el ejemplo de la sección anterior, la forma $\mathfrak{q}(x, y) = x^2+2y^2$ es simétrica respecto a $\mathcal{T}_1, \mathcal{T}_2, \mathcal{T}_3, \mathcal{T}_4$. Por ende, su número de simetrías es 4. Para tener variaciones de lenguaje, también se dice que $\mathfrak{q}$ posee 4 simetrías. Así, las formas $x^2+2xy+y^2, x^2+y^2, 3x^2+2xy+5y^2$ poseen $4, 8$ y 2 simetrías, respectivamente. Es fácil probar que el número de simetrías sólo puede tomar estos tres valores, considerando las relaciones de las $\mathcal{T}_i$ mediante composiciones.

También se puede hablar de transformaciones simétricas aplicadas a las identidades de cerradura. En tal caso, se hace aplicando las reglas de transformación al par (X, Y), en lugar de a (x, y).

Definición (equivalencia de cerraduras)**.** Se dice que dos identidades de cerradura de la $\mathbb{S}$-forma $\mathfrak{q}$ son equivalentes, si una se convierte en la otra mediante alguna transformación simétrica que pertenezca a $\mathcal{S}_\mathfrak{q}$. Si dos identidades no son equivalentes, también se dice que son *independientes*.

La relación anterior es simétrica, reflexiva y transitiva, por lo que su nombre es merecido. Al tratarse de una relación de equivalencia,[2] induce una partición en el conjunto de las identidades de cerradura de una forma dada. De cada clase de equivalencia puede tomarse un representante arbitrario, y con ellos se tendrá el máximo número de identidades independientes entre sí que pueden seleccionarse. Retornando nuevamente al ejemplo, para $x^2 + 2y^2$ se pueden tomar por representantes a las dos identidades de Brahmagupta, y ese es el máximo número posible de identidades independientes. Recuerde que el número 1 tenía también sólo dos representaciones distintas (note que aquí sí se cuentan las transformaciones simétricas por separado). Esto no es una mera coincidencia, como se verá en los capítulos posteriores.

[2]Para una exposición del concepto de relación en Teoría de Conjuntos, consultar [17].

Si se desea aumentar la complejidad de las transformaciones, el siguiente paso lógico son las lineales. Una *transformación lineal binaria* es aquella que sustituye a las variables x, y por formas lineales binarias, es decir, polinomios homogéneos lineales en dos variables. Con frecuencia, después de aplicar la transformación, se sustituyen las nuevas variables por las mismas x, y, para cumplir el convenio que se hizo de usar sólo estas variables al escribir formas.

La transformación lineal $\mathcal{T}(x, y) = (2x, x - y)$ convierte a las $\mathbb{Z}$-formas $x^2 + y^2, 2x^2 + 3xy, 5x^2 - xy + y^2$ en $5x^2 - 2xy + y^2, 14x^2 - 6xy, 19x^2 + y^2$, respectivamente. La clase más general de transformación que convierta formas cuadráticas en formas cuadráticas es ésta, la de las transformaciones lineales.

2.4. Matrices, discriminantes y determinantes

Como había sido dicho, una forma cuadrática posee una representación matricial. Las transformaciones lineales también pueden ser identificadas con matrices, de manera que al multiplicar dicha matriz con un vector de variables se obtenga el vector resultado de la transformación, y también se puede operar de cierta forma la matriz de la transformación con la matriz de una forma cuadrática, para obtener la de la forma en la cual se convierte. Si $\mathcal{T}$ es una transformación tal que $\mathcal{T}(x, y) = (\alpha x + \beta y, \gamma x + \delta y)$, donde $\alpha, \beta, \gamma, \delta \in \mathbb{S}$, entonces $\mathcal{T}$ se identifica con la matriz $M_{\mathcal{T}} = \left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right)$, ya que el producto de dicha matriz con el vector de variables transpuesto $\left(\begin{smallmatrix} x \\ y \end{smallmatrix}\right)$, es igual a la trasposición del resultado que se obtiene al aplicar $\mathcal{T}$ al vector de variables.

$$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} \alpha x + \beta y \\ \gamma x + \delta y \end{pmatrix} \xleftrightarrow{\text{trasposición}} (\alpha x + \beta y, \gamma x + \delta y) \tag{2.5}$$

El problema que experimentado al trabajar con matrices es que las inversas no siempre están restringidas al mismo $\mathbb{S}$ sobre el cual se definió la transformación lineal. Por ejemplo, una matriz con registros enteros puede tener una inversa en términos de números racionales. En lo que sigue, no se considerará el caso $\mathbb{S} = \mathbb{N}$, y de los otros tres sólo $\mathbb{Z}$ presenta este problema. Esto conduce a hacer la siguiente definición.

Definición (unimodular)**.** Se dice que una matriz cuadrada cuyas entradas están en $\mathbb{Z}$ es *unimodular* si es invertible, y su inversa también tiene entradas enteras. A las transformaciones lineales asociadas también se les llama unimodulares.

Lema 2. *Una matriz cuadrada M con entradas enteras es unimodular si, y sólo si, su determinante*[3] $\det(M)$ *es igual a +1 o -1.*

Demostración. Note que, empleando la expansión en cofactores, se puede deducir que el determinante de una matriz con entradas enteras es un entero. Supóngase primero que la matriz M es unimodular, luego su determinante es un entero distinto de cero (por ser invertible) y su inversa también tiene determinante entero, pues sus entradas pertenecen a $\mathbb{Z}$. Recordando ahora que, si A, B son matrices, entonces $\det(A)\det(B) = \det(AB)$, se deduce que $\det(M)\det(M^{-1}) = \det(MM^{-1}) = \det(I) = 1$, donde I es la matriz identidad cuyo tamaño es el de M. Como el producto de los enteros $\det(M), \det(M^{-1})$ da 1, entonces cada uno de ellos es un divisor de 1 y, por ende, cada uno debe ser igual a 1 o -1.

Ahora, por el contrario, supóngase que $\det(M) = \pm 1$. Calcúlese la inversa mediante la matriz de cofactores C, haciendo uso de la expresión $M^{-1} = \frac{1}{\det(M)}C$. Los cofactores son iguales en valor absoluto a determinantes de matrices menores que tienen entradas enteras y, por lo tanto, cada cofactor es un entero. Si cada entrada es dividida entre ± 1 seguirá siendo entera, así que la inversa tiene entradas enteras, como se quería. $\square$

En particular, para matrices de 2×2, se puede escribir la inversa en términos de los cofactores y el determinante así:

$$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}^{-1} = \frac{1}{\alpha\delta - \beta\gamma} \begin{pmatrix} \delta & -\beta \\ -\gamma & \alpha \end{pmatrix} \tag{2.6}$$

Teorema 2. *Si se aplica una transformación unimodular a una $\mathbb{Z}$-forma cuadrática $\mathfrak{q}_1 = \langle a_1, b_1, c_1 \rangle$ y se obtiene la forma $\mathfrak{q}_2 = \langle a_2, b_2, c_2 \rangle$, entonces los discriminantes de ambas formas son iguales, esto es, $b_1^2 - 4a_1c_1 = b_2^2 - 4a_2c_2$.*

[3]Para refrescar los conceptos del Álgebra Lineal, se recomienda [25].

Demostración. Recuerde que, si $\mathfrak{q} = \langle a, b, c\rangle$ es una forma cuadrática, entonces su matriz asociada es $M_{\mathfrak{q}} = \left(\begin{smallmatrix} a & b/2 \\ b/2 & c \end{smallmatrix}\right)$, según la ecuación (2.1). Note que

$$-4\det(M_{\mathfrak{q}}) = -4\begin{vmatrix} a & b/2 \\ b/2 & c \end{vmatrix} = -4\left(ac - \frac{b^2}{4}\right) = b^2 - 4ac$$

Así que el discriminante de una forma es múltiplo del determinante de su matriz. Se probará que el determinante se conserva bajo transformaciones unimodulares. Considérese la transformación $\mathcal{T}(x, y) = (\alpha x + \beta y, \gamma x + \delta y)$, donde $|\alpha\delta - \beta\gamma| = 1$, o bien, $(\det(M_{\mathcal{T}}))^2 = 1$. Se desea expresar $M_{\mathfrak{q}_2}$ en términos de $M_{\mathfrak{q}_1}$ y $M_{\mathcal{T}}$. Trasponiendo el primer miembro de la identidad (2.5) se obtiene

$$(x, y)\begin{pmatrix} \alpha & \gamma \\ \beta & \delta \end{pmatrix} = (\alpha x + \beta y, \gamma x + \delta y)$$

Esto, en conjunción con la propia (2.5), indica que

$$\begin{aligned}(x, y)\begin{pmatrix} \alpha & \gamma \\ \beta & \delta \end{pmatrix}\begin{pmatrix} a_1 & b_1/2 \\ b_1/2 & c_1 \end{pmatrix}\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix} &= \\ (\alpha x + \beta y, \gamma x + \delta y)\begin{pmatrix} a_1 & b_1/2 \\ b_1/2 & c_1 \end{pmatrix}\begin{pmatrix} \alpha x + \beta y \\ \gamma x + \delta y \end{pmatrix} &= \\ (x, y)\begin{pmatrix} a_2 & b_2/2 \\ b_2/2 & c_2 \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix}&\end{aligned}$$

La última igualdad se da precisamente por la definición de $\mathfrak{q}_2$. Comparando el primer y último miembros de la cadena de igualdades, y sabiendo que cada forma cuadrática está asociada con una única matriz, se deduce que $M'_{\mathcal{T}} M_{\mathfrak{q}_1} M_{\mathcal{T}} = M_{\mathfrak{q}_2}$, donde $M'_{\mathcal{T}}$ es la traspuesta de $M_{\mathcal{T}}$.

Aplicando la función $\det(\cdot)$ a ambos lados de la última ecuación se obtiene

$$\begin{aligned}
\det(M'_{\mathcal{T}} M_{\mathfrak{q}_1} M_{\mathcal{T}}) = \det(M_{\mathfrak{q}_2}) &\implies \\
\det(M'_{\mathcal{T}}) \det(M_{\mathfrak{q}_1}) \det(M_{\mathcal{T}}) = \det(M_{\mathfrak{q}_2}) &\implies \\
\det(M_{\mathcal{T}}) \det(M_{\mathfrak{q}_1}) \det(M_{\mathcal{T}}) = \det(M_{\mathfrak{q}_2}) &\implies \\
\det(M_{\mathcal{T}})^2 \det(M_{\mathfrak{q}_1}) = \det(M_{\mathfrak{q}_2}) &\implies \\
(1) \det(M_{\mathfrak{q}_1}) = \det(M_{\mathfrak{q}_2}) &\implies \\
\det(M_{\mathfrak{q}_1}) = \det(M_{\mathfrak{q}_2})
\end{aligned}$$

Que era lo que se quería probar. Ahora, basta multiplicar por -4 cada miembro para obtener la igualdad de los discriminantes. $\square$

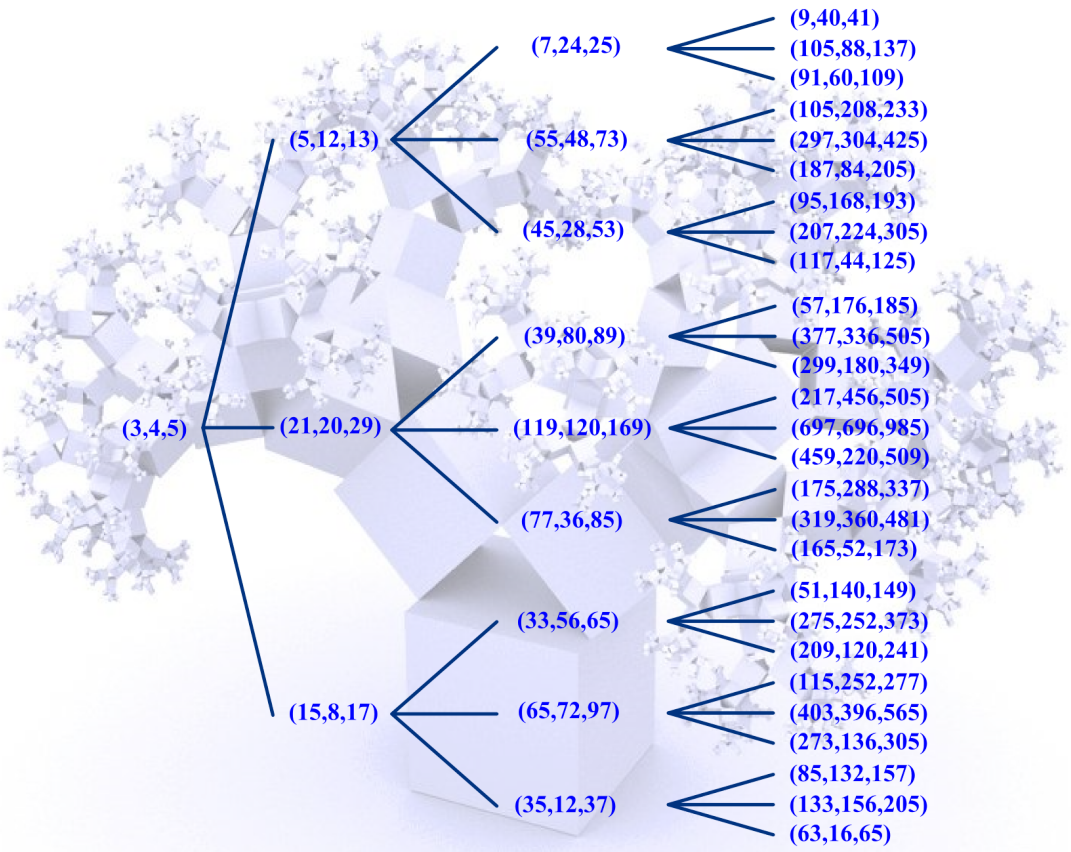
Las matrices unimodulares no solamente son útiles en la transformación de formas cuadráticas, también se pueden usar para generar representaciones para ciertos números. Como ejemplo de ello se tienen las siguientes tres matrices unimodulares.

$$\begin{pmatrix} 1 & -2 & 2 \\ 2 & -1 & 2 \\ 2 & -2 & 3 \end{pmatrix} \quad \begin{pmatrix} 1 & 2 & 2 \\ 2 & 1 & 2 \\ 2 & 2 & 3 \end{pmatrix} \quad \begin{pmatrix} -1 & 2 & 2 \\ -2 & 1 & 2 \\ -2 & 2 & 3 \end{pmatrix}$$

En 1963, F. J. Barning demostró que el conjunto de todas las ternas pitagóricas primitivas se puede organizar en forma de un árbol [5]. Comenzando con la terna fundamental $(3, 4, 5)$, de cada terna se pueden obtener otras tres diferentes, como resultado de multiplicar por cada una de las tres matrices de arriba, tal como puede apreciarse en la figura 2. Todas las ternas aparecen en el árbol exactamente una vez (Véanse los problemas 9 al 12 en el apéndice D).

H. Lee Price encontró un trío de matrices alternativo que logra el mismo trabajo, aunque los árboles generados organizan las ternas siguiendo un esquema distinto [32]. Note que cada terna pitagórica es una representación de cero en la forma cuadrática ternaria $x^2 + y^2 - z^2$, así que las matrices unimodulares están íntimamente ligadas con el problema de la representabilidad, en más de una manera.

Figura 2. **Árbol ternario pitagórico**



En la teoría de grafos, un *árbol ternario* es aquél en el que cada rama se subdivide en tres. Las soluciones se generan a partir de la fundamental $(3, 4, 5)$, aplicando en cada paso las matrices de transformación de Barning. Se le invita a buscar patrones en los números conforme se recorre un camino específico. Como fondo se tiene un fractal que, por casualidad, también es llamado *árbol pitagórico*.

Fuente: elaboración propia.

Definición. A una $\mathbb{S}$-forma cuadrática n-aria es llamada *definida positiva* si todo número representable por ella es no negativo, y si el cero sólo tiene la representación trivial. Análogamente se definen las formas *definidas negativas*. Una forma es *definida* si cae en alguna de las dos clasificaciones anteriores. Si existen otras representaciones para cero, entonces se reemplaza la palabra *definida* por *semidefinida*.

Considérese una forma cuadrática $\mathfrak{q} = \langle a, b, c\rangle$ cuyo discriminante Δ es negativo. Multiplicando la forma por $4a$ se obtiene:

$$\begin{aligned} 4a\mathfrak{q}(x,y) &= 4a^2x^2 + 4abxy + 4acy^2 \\ &= 4a^2x^2 + 4abxy + b^2y^2 + 4acy^2 - b^2y^2 \\ &= (2ax + by)^2 - (b^2 - 4ac)y^2 \\ &= (2ax + by)^2 - \Delta y^2 \\ &= (2ax + by)^2 + |\Delta|y^2 \implies \\ 4a\mathfrak{q}(x,y) &= (2ax + by)^2 + |\Delta|y^2 \end{aligned}$$

Note que el miembro derecho es no negativo, y sólo puede ser cero si $(x, y) = (0, 0)$. El miembro izquierdo debe cumplir lo mismo. En base a ello se concluye que, si a es positivo, entonces $\mathfrak{q}$ no puede ser negativa, en tanto que si a es negativa, entonces $\mathfrak{q}$ no puede ser positiva. Esto prueba el siguiente resultado.

Teorema 3. *Sea $\mathfrak{q} = \langle a, b, c\rangle$ una $\mathbb{S}$-forma cuadrática con discriminante $\Delta < 0$. Si $a > 0$, entonces $\mathfrak{q}$ es definida positiva. Si $a < 0$, entonces $\mathfrak{q}$ es definida negativa.*

Nota. $a = 0$ no puede darse mientras $\Delta < 0$.

Escolio 3. *Si $\mathfrak{q}$ es una $\mathbb{S}$-forma cuadrática con discriminante negativo, entonces todas sus cerraduras homogéneas son reducidas.*

Para verificar la validez del escolio, se debe tener en cuenta el importante teorema 1, de la página 43. Se suspenderá por ahora el desarrollo teórico para analizar algunas formas representativas, las cuales ejemplificarán varios conceptos fundamentales. Se destinará todo el capítulo 3 a esta tarea. Después de recibir iluminación a través de ese estudio intuitivo, en el capítulo 4 se ahondará en el tema de las cerraduras.

3. $\mathbb{Z}$-FORMAS: ENFOQUE INTUITIVO

Para cada una de las $\mathbb{Z}$-formas que se estudiarán a lo largo de este capítulo, se intentará responder a tres preguntas fundamentales: ¿Cuántas cerraduras independientes tiene? ¿Qué números son representables? ¿Qué puede decirse acerca de la cantidad de representaciones distintas que posee un número dado?

La búsqueda es de patrones o similitudes. También se quiere identificar diferencias y los motivos por los cuales se presentan. La información a recabar sobre las cerraduras ahora será de utilidad en el capítulo 4, donde se dará una clausura provisional al problema de la existencia de cerraduras.

3.1. La forma $x^2 - y^2$

La forma $\mathfrak{q}(x, y) = x^2 - y^2$ tiene discriminante $\Delta = 4$, así que el teorema 3 no es aplicable. De hecho, la forma tiene infinitas representaciones de cero, del tipo (ξ, ξ). También puede representar números positivos y negativos. Es, por tanto, una de las formas que comúnmente son conocidas como *indefinidas*. Tampoco se dispone del teorema 1 de la página 43. Se tienen limitaciones en cuanto a herramientas pero, afortunadamente, es una de las formas con discriminante positivo más simples.

3.1.1. Cerraduras

La forma auto-composición $\langle\!\langle 1, 0, -1 \rangle\!\rangle$, también simbolizada por Q, es el polinomio que se obtiene al expandir el producto:

$$\mathsf{Q} = (t^2 - u^2)(v^2 - w^2) = t^2v^2 - t^2w^2 - u^2v^2 + u^2w^2 \tag{3.1}$$

Considérense los polinomios cuadráticos homogéneos en las variables t, u, v, w, de la mayor generalidad posible, que puedan ocupar el papel de X, Y en las cerraduras. Es necesario hacerlo, pues podría haber cerraduras homogéneas no reducidas. Aún así, el objetivo es demostrar que no existen.

$$X = h_1t^2 + h_2u^2 + h_3v^2 + h_4w^2 + h_5tu + h_6tv + h_7tw + h_8uv + h_9uw + h_{10}vw$$

$$Y = k_1t^2 + k_2u^2 + k_3v^2 + k_4w^2 + k_5tu + k_6tv + k_7tw + k_8uv + k_9uw + k_{10}vw$$

Se aparejarán las variables de la siguiente forma: t con v, u con w. Suponga que existe una cerradura que no es cruzada. Por el argumento usado para demostrar el lema 1 de la página 40, para esa cerradura alguno de los pares $(h_1, k_1), (h_2, k_2), (h_3, k_3)$ y (h_4, k_4) es una representación no trivial de cero. Cada uno de esos pares corresponde a uno de los coeficientes $\mathcal{Q}_{t^4}, \mathcal{Q}_{u^4}, \mathcal{Q}_{v^4}, \mathcal{Q}_{w^4}$, de manera respectiva. Si (h_1, k_1) es una representación no trivial de cero, entonces se estudiará a la variable t y a aquella con la que fue aparejada, v. Los demás casos son análogos.

Se procederá de manera semejante a la usada para derivar el sistema de ecuaciones (2.3), de la página 41, aunque aquí importan solamente los términos que tengan de manera exclusiva a las variables t, v.

$$X = h_1t^2 + h_3v^2 + h_6tv + \ldots \text{(otros términos sin } t \text{ o sin } v)$$

$$Y = k_1t^2 + k_3v^2 + k_6tv + \ldots \text{(otros términos sin } t \text{ o sin } v)$$

Sustituyánse en la forma $\langle 1, 0, -1\rangle$ para formar $\mathcal{Q}$. Luego de ello, se deben calcular los coeficientes de los términos $t^4, t^3v, t^2v^2, tv^3, v^4$, y compararlos con (3.1)

$$\mathfrak{q}(X, Y) = \mathcal{Q} = (h_1t^2 + h_3v^2 + h_6tv + \ldots)^2 - (k_1t^2 + k_3v^2 + k_6tv + \ldots)^2$$

$$\left.\begin{array}{r} \mathcal{Q}_{t^4} = \mathsf{Q}_{t^4} \\ \mathcal{Q}_{t^3v} = \mathsf{Q}_{t^3v} \\ \mathcal{Q}_{t^2v^2} = \mathsf{Q}_{t^2v^2} \\ \mathcal{Q}_{tv^3} = \mathsf{Q}_{tv^3} \\ \mathcal{Q}_{v^4} = \mathsf{Q}_{v^4} \end{array}\right\} \implies \left\{\begin{array}{r} h_1^2 - k_1^2 = 0 \\ h_1h_6 - k_1k_6 = 0 \\ 2h_1h_3 + h_6^2 - 2k_1k_3 - k_6^2 = 1 \\ h_3h_6 - k_3k_6 = 0 \\ h_3^2 - k_3^2 = 0 \end{array}\right.$$

Teniendo en cuenta que $\forall r \in \mathbb{Z}$, $r^2 \equiv r$ (mód 2), considérese el sistema localmente en ese módulo.

$$\left.\begin{array}{rcl} h_1 & \equiv & k_1 \\ h_1h_6 & \equiv & k_1k_6 \\ h_6 & \equiv & 1+k_6 \\ h_3h_6 & \equiv & k_3k_6 \\ h_3 & \equiv & k_3 \end{array}\right\} \text{ (mód 2)}$$

Han sido eliminados los términos que tenían coeficiente 2, que es equivalente a 0 en este módulo. La tercera congruencia indica que los números h_6, k_6 son de distinta paridad. Sólo será necesario lo anterior, aunque se puede obtener un poco más de información usando este módulo, por ejemplo, empleando todas las congruencias se puede concluir que los números h_1, h_3, k_1, k_3 deben ser pares.

Ahora, olvidando el análisis local y regresando otra vez a las ecuaciones, se desea inspeccionar la existencia de soluciones globales. La primera ecuación implica $|h_1| = |k_1|$, y como (h_1, k_1) es una representación no trivial de cero, entonces puede dividirse entre k_1 la segunda ecuación, con lo que resulta $|h_6| = |k_6|$, lo que contradice el hecho de que sean de distinta paridad.

La contradicción se origina en la suposición de que (h_1, k_1) es una representación no trivial de 0. Otras contradicciones semejantes se deducen para los pares $(h_2, k_2), (h_3, k_3)$ y (h_4, k_4). Esto prueba el siguiente resultado.

Lema 4. *Todas las cerraduras homogéneas de* $\langle 1, 0, -1\rangle$ *son cruzadas.*

Se pretende fortalecer el lema, mostrando que no sólo son cruzadas, sino reducidas. Para tal propósito, considérense los polinomios cruzados X, Y generales, con el objetivo de demostrar que h_1, h_6, k_1, k_6 se anulan.

$$\text{sustitución } \left\{\begin{array}{ll} x \mapsto & X = h_1tu + h_2tv + h_3tw + h_4uv + h_5uw + h_6vw \\ y \mapsto & Y = k_1tu + k_2tv + k_3tw + k_4uv + k_5uw + k_6vw \end{array}\right.$$

$$\begin{aligned}\mathcal{Q} &= X^2 - Y^2 \\ &= (h_1tu + h_2tv + h_3tw + h_4uv + h_5uw + h_6vw)^2 - \\ &\quad (k_1tu + k_2tv + k_3tw + k_4uv + k_5uw + k_6vw)^2\end{aligned}$$

Los coeficientes de t^2u^2, t^2uv, t^2v^2 deben equivaler a los de (3.1).

$$\left.\begin{array}{c}\mathcal{Q}_{t^2u^2} = \mathsf{Q}_{t^2u^2} \\ \mathcal{Q}_{t^2uv} = \mathsf{Q}_{t^2uv} \\ \mathcal{Q}_{t^2v^2} = \mathsf{Q}_{t^2v^2}\end{array}\right\} \Longrightarrow \left\{\begin{array}{r} h_1^2 - k_1^2 = 0 \\ h_1h_2 - k_1k_2 = 0 \\ h_2^2 - k_2^2 = 1\end{array}\right.$$

La tercera ecuación indica que (h_2, k_2) es una representación de la unidad en la forma $\langle 1, 0, -1\rangle$. Si se factoriza $(h_2 - k_2)(h_2 + k_2) = 1$, es evidente que hay dos posibles opciones: que ambos paréntesis valgan 1, o bien, que ambos valgan -1. Cada opción devuelve una solución, así que las únicas dos representaciones de la unidad son $(1, 0)$ y $(-1, 0)$. En ambos casos se tiene $k_2 = 0$, y si se sustituye este valor en la segunda ecuación se revela que h_1 tiene que anularse, ya que $h_2 = \pm 1$. La primera ecuación implica que k_1 se anula en tal caso. La prueba de que h_6, k_6 también se anulan es análoga. La conclusión a la que se llega es el:

Teorema 4. *Todas las cerraduras homogéneas de $\langle 1, 0, -1\rangle$ son reducidas.*

En vista de lo anterior, se puede hacer uso de la tabla VI para generar el sistema de ecuaciones de las cerraduras reducidas, sustituyendo los valores de los coeficientes $a = 1, b = 0, c = -1$.

$$\left\{\begin{array}{rcll} 1 &=& h_1^2 - k_1^2 & (\text{R-1}) \\ 0 &=& 2h_1h_2 - 2k_1k_2 & (\text{R-2}) \\ -1 &=& h_2^2 - k_2^2 & (\text{R-3}) \\ 0 &=& 2h_1h_3 - 2k_1k_3 & (\text{R-4}) \\ 0 &=& 2(h_1h_4 + h_2h_3) - 2(k_1k_4 + k_2k_3) & (\text{R-5}) \\ 0 &=& 2h_2h_4 - 2k_2k_4 & (\text{R-6}) \\ -1 &=& h_3^2 - k_3^2 & (\text{R-7}) \\ 0 &=& 2h_3h_4 - 2k_3k_4 & (\text{R-8}) \\ 1 &=& h_4^2 - k_4^2 & (\text{R-9}) \end{array}\right.$$

Las ecuaciones R-1, R-9 implican que $(h_1, k_1), (h_4, k_4)$ son representaciones de la unidad, lo que implica que $k_1 = 0, k_4 = 0$. Cambiándoles de signo, R-3, R-7 dicen lo mismo de $(k_2, h_2), (k_3, h_3)$, y así, h_2, h_3 se anulan también. Sustituyendo las 4 incógnitas que se anulan en el sistema, y descartando las ecuaciones que se trivializan se obtiene

$$\begin{cases} 1 = h_1^2 & \text{(S-1)} \\ 1 = k_2^2 & \text{(S-2)} \\ 0 = h_1h_4 - k_2k_3 & \text{(S-3)} \\ 1 = k_3^2 & \text{(S-4)} \\ 1 = h_4^2 & \text{(S-5)} \end{cases}$$

Se tiene que $|h_1h_4| = |k_2k_3|$, y así, para que S-3 se cumpla, en el conjunto $\{h_1, h_4\}$, la cantidad de negativos tiene que tener la misma paridad que en $\{k_2, k_3\}$. Hay 8 opciones en total.

$$\begin{array}{ll} (+1,0,0,+1;0,+1,+1,0) & (+1,0,0,-1;0,+1,-1,0) \\ (-1,0,0,-1;0,+1,+1,0) & (+1,0,0,-1;0,-1,+1,0) \\ (+1,0,0,+1;0,-1,-1,0) & (-1,0,0,+1;0,+1,-1,0) \\ (-1,0,0,-1;0,-1,-1,0) & (-1,0,0,+1;0,-1,+1,0) \end{array}$$

La forma $x^2 - y^2$ tiene cuatro simetrías $(\mathcal{T}_1, \mathcal{T}_2, \mathcal{T}_3, \mathcal{T}_4)$, así que hay dos clases de equivalencia de cuatro elementos. Cada columna de arriba es una clase de equivalencia, y puede tomarse la primera solución de cada una como representante. Recuerde que esta forma posee dos representaciones distintas de la unidad, y ahora resulta que tiene exactamente dos cerraduras independientes.[1]

- $(t^2 - u^2)(v^2 - w^2) = (tv + uw)^2 - (tw + uv)^2$
- $(t^2 - u^2)(v^2 - w^2) = (tv - uw)^2 - (tw - uv)^2$

3.1.2. Representabilidad

Se resolverá el problema de la representabilidad en la forma $x^2 - y^2$ mediante dos métodos totalmente diferentes, cada uno con sus ventajas y desventajas.

[1] Cada clase de equivalencia de cerraduras es interpretada como «una cerradura independiente».

Teorema 5. *La $\mathbb{Z}$-forma $\langle 1, 0, -1\rangle$ representa a todos los impares y a todos los múltiplos de 4. No son representables los números congruentes con 2 en el módulo 4.*

Primera demostración. Se quieren los valores de n para los cuales existan soluciones de la ecuación diofantina $x^2 - y^2 = n$. El camino que se seguirá ahora es el que resulta más natural, factorizar e intentar derivar condiciones sobre n.

$$(x - y)(x + y) = n$$

Lo primero que se observa es que $2y \equiv 0 \pmod 2 \implies x + 2y \equiv x \pmod 2 \implies x+y \equiv x-y \pmod 2$, así que los dos factores poseen la misma paridad. Si ambos son impares, entonces n será impar; por el contrario, si ambos son pares, n será múltiplo de 4, aunque no es seguro que represente a todos. Como no es posible que los factores tengan distinta paridad, entonces $n \not\equiv 2 \pmod 4$. Falta demostrar que sí representa a todos los demás números. Considérense los dos casos:

I. (n *es impar*). En este caso, los números $n+1$, $n-1$ son pares. Como n se puede factorizar trivialmente como $1 \cdot n$, se puede exigir:

$$\begin{cases} x - y = 1 \\ x + y = n \end{cases}$$

y esperar que, con un poco de suerte, una idea tan simple pueda funcionar. Resolviendo el sistema para las variables x, y resultan las soluciones

$$x = \frac{n+1}{2}, \qquad y = \frac{n-1}{2}$$

y son enteras pues, como había sido dicho, los numeradores son pares. En consecuencia, $\left(\frac{n+1}{2}, \frac{n-1}{2}\right)$ es una representación de n en la forma $\langle 1, 0, -1\rangle$, siempre que n sea impar. Normalmente existen varias otras representaciones, pues la elección de cómo factorizar a n fue arbitraria.

II. (n *es múltiplo de* 4). Ahora, n es de la forma $4m$ para algún $m \in \mathbb{Z}$. Se quiere usar la misma idea, pero ahora se exige que:

$$\begin{cases} x - y = 2 \\ x + y = 2m \end{cases}$$

Las soluciones del sistema son

$$x = m + 1, \qquad y = m - 1$$

que obviamente son enteras también. Como $m = \frac{n}{4}$, se cumple que el par ordenado $\left(\frac{n}{4} + 1, \frac{n}{4} - 1\right)$ es una representación de n en la forma $\langle 1, 0, -1\rangle$, siempre que n sea múltiplo de 4. □

Segunda demostración. Ahora el enfoque estará centrado en los bloques de construcción del número n, sus factores primos. Gracias a que existen identidades de cerradura, si se mostrase que el número 4, el 8, y cualquier primo impar son representables en la forma $\langle 1, 0, -1\rangle$, entonces cualquier número que se pueda formar como producto de ellos también lo será, y el conjunto de números constructibles mediante estas multiplicaciones corresponde al del enunciado del teorema: los impares y los múltiplos de 4. El 8 es necesario para aquellos múltiplos de 4 cuya factorización en primos posea al 2 elevado a una potencia impar (que debe ser mayor que 1).

La diferencia entre esta demostración y la anterior es más sutil de lo que parece, pues se pueden usar las mismas representaciones halladas previamente. Para los primos p impares, se tiene que $\left(\frac{p+1}{2}, \frac{p-1}{2}\right)$ es una representación. La representación del 4 es $(2, 0)$ y la del 8 es $(3, 1)$. □

3.1.3. Cantidad de representaciones

Interesa ahora estudiar el número de representaciones distintas que un entero dado posee en la forma $\langle 1, 0, -1\rangle$. Se puede verificar fácilmente que el número 9, por ejemplo, tiene 6 representaciones, a saber: $(3, 0), (-3, 0), (5, 4), (-5, 4), (5, -4)$ y $(-5, -4)$. Tendría 8 representaciones si el cero pudiera tener ambos signos, y las transformaciones simétricas las agruparían en 2 clases de 4 representaciones cada una. Si se limita exclusivamente a las representaciones que no se obtengan de otras mediante transformaciones simétricas, se tienen únicamente dos «independientes», en el sentido en el que fue tomada esa palabra para las cerraduras, que son: $(3, 0)$ y $(5, 4)$.

Definición. La función que cuenta la cantidad de representaciones del número n en la $\mathbb{Z}$-forma cuadrática $\mathfrak{q}(x, y) = \langle a, b, c\rangle$ será simbolizada por $\langle a, b, c\rangle\, \overline{\mathcal{R}}(n)$. Si se desea la cantidad de *representaciones independientes*, esto es, eligiendo una de cada clase simétrica, se escribirá $\langle a, b, c\rangle\, \mathcal{R}(n)$. Si se sobreentiende de cuál forma cuadrática se habla, se escribirá solamente $\overline{\mathcal{R}}(n)$ y $\mathcal{R}(n)$.

Ya fueron especificadas todas las representaciones de 9 en la forma $x^2 - y^2$, con la nueva notación se puede escribir:

$$\overline{\mathcal{R}}(9) = 6 \qquad\qquad \mathcal{R}(9) = 2$$

Sería interesante hallar fórmulas generales para cualquier n. Las irregularidades que se manifiestan con el primo 2 para esta forma cuadrática hacen necesario que se examinen por separado los mismos casos considerados anteriormente.

I. (n *es impar*). Considérese un n positivo, pues la otra posibilidad es análoga. Suponiendo que $n = \prod_{i=1}^{k} p_i^{\alpha_i}$ es la factorización en primos de n, donde los p_i son primos impares, y los α_i son las potencias positivas respectivas, se buscan todas las soluciones de la ecuación diofantina

$$(x - y)(x + y) = n \tag{3.2}$$

Definiendo $X = x - y, Y = x + y$, la ecuación se convierte en

$$XY = n \tag{3.3}$$

Note que, despejando las variables x, y, sus valores quedan determinados por

$$x = \frac{Y + X}{2}, \qquad y = \frac{Y - X}{2}$$

Se tiene que x es el promedio de los números X, Y, mientras que y es una medida de la separación entre ellos. Esto hace evidente que, si al par (X, Y) se le asocia el par (x, y), el mapeo definido por esta asociación es biyectivo, pero se debe exigir que X, Y tengan la misma paridad, para que los valores de x, y sean enteros. Esta condición ya se había manifestado en la sección anterior, y fue el

motivo por el cual se tuvo que usar una prueba diferente para el segundo caso de la primera demostración dada. Lo que esta propiedad significa aquí es que la cantidad de soluciones (x, y) de la ecuación (3.2) es la misma que la cantidad de soluciones (X, Y) de (3.3), tales que los números X, Y tengan la misma paridad.

Ahora bien, la ecuación (3.3) es simplemente una factorización de n en dos factores. Una vez se elijan los primos y potencias respectivas que conformen al número X, los que sobren de la factorización en primos de n determinarán el valor de Y. En otras palabras, el número de soluciones de (3.3) es igual a la cantidad de divisores (positivos o negativos) de n que puedan reemplazar a X. El número Y será el *divisor complementario*, es decir, aquél que multiplicado por X devuelva n. En el caso que se está considerando no se presentan problemas con la paridad, pues todo divisor de n tiene que ser forzosamente impar. Esto será problemático en el caso de los múltiplos de 4.

De la Teoría de Números elemental se sabe que el número de divisores positivos de $n = \prod_{i=1}^{k} p_i^{\alpha_i}$, está dado por $\prod_{i=1}^{k} (\alpha_i + 1)$, esto es, el producto de todos los exponentes aumentados en una unidad.[2] Por ejemplo, el número $360 = 2^3 \cdot 3^2 \cdot 5$ tiene $(3+1)(2+1)(1+1) = 24$ divisores positivos. Como en este contexto interesan también los divisores negativos, se debe multiplicar por 2, y así se llega a la conclusión de que el número de soluciones de (3.2) es

$$\langle 1, 0, -1 \rangle \, \overline{\mathcal{R}}(n) = 2 \prod_{i=1}^{k} (\alpha_i + 1)$$

II. (n *es múltiplo de* 4). En este caso, la factorización en primos del número n será $2^{\beta+2} \cdot \prod_{i=1}^{k} p_i^{\alpha_i}$, donde los p_i son primos impares, los α_i son sus respectivos exponentes positivos, y el exponente de 2 es $\beta + 2$, donde β es no negativo. Se le suma 2 para asegurar que 4 sea divisor de n. La prueba es idéntica al caso anterior, excepto que de las $\beta+2$ veces que aparece el primo 2 en la factorización de n, es obligatorio asignarle al menos 1 a cada factor del producto XY, pues

[2] La expresión «se sabe», se refiere a las fórmulas de las funciones aritméticas, específicamente a σ_0, también conocida como d, o como τ. Se puede consultar el libro de Andrews [3], página 82, para una demostración.

deben tener la misma paridad. Los β restantes se pueden asignar libremente, como puede hacerse con las α_i copias del primo p_i. Se tiene entonces que

$$\langle 1, 0, -1\rangle\, \overline{\mathcal{R}}(n) = 2(\beta + 1) \cdot \prod_{i=1}^{k} (\alpha_i + 1)$$

Se considerarán ahora las representaciones independientes. Se verifica que la forma $\langle 1, 0, -1\rangle$ tiene 4 simetrías, así que las representaciones se agrupan en cuartetos. Las únicas excepciones son aquellas en que una variable se anule, como sucedió con el 9 en el ejemplo inicial, lo cual sólo sucede con los cuadrados perfectos, o bien, con los negativos de cuadrados perfectos, según sea x o y la que se anule. Esto indica que, si n es positivo, se deben dividir entre cuatro las fórmulas anteriores, excepto cuando es cuadrado perfecto, en cuyo caso se le debe sumar 2 (para completar ficticiamente el cuarteto que se volvió pareja) y luego dividir entre 4. También se debe ejercer el mismo cuidado con los números n que sean el negativo de un cuadrado perfecto.

Lo único que falta agregar, es que el cero posee infinitas representaciones del tipo (ξ, ξ), donde ξ es cualquier entero. Todos los argumentos anteriores quedan resumidos en el siguiente teorema.

Teorema 6. *Sea n un entero distinto de cero. Si n es impar, suponga que la factorización en primos de su valor absoluto es $\prod_{i=1}^{k} p_i^{\alpha_i}$. Si n es múltiplo de 4, divídalo entre 4, y suponga que la factorización en primos de $\left|\frac{n}{4}\right|$ es $\prod_{i=1}^{k} p_i^{\alpha_i}$. Entonces el número total de representaciones y el número de representaciones independientes de n en la forma $x^2 - y^2$ están dados por las fórmulas siguientes.*

$$\overline{\mathcal{R}}(n) = 2 \prod_{i=1}^{k} (\alpha_i + 1)$$

$$\mathcal{R}(n) = \begin{cases} \dfrac{1}{2}\left(1 + \displaystyle\prod_{i=1}^{k} (\alpha_i + 1)\right) & \textit{si } \pm n \textit{ es cuadrado perfecto} \\ \dfrac{1}{2} \displaystyle\prod_{i=1}^{k} (\alpha_i + 1) & \textit{en cualquier otro caso} \end{cases}$$

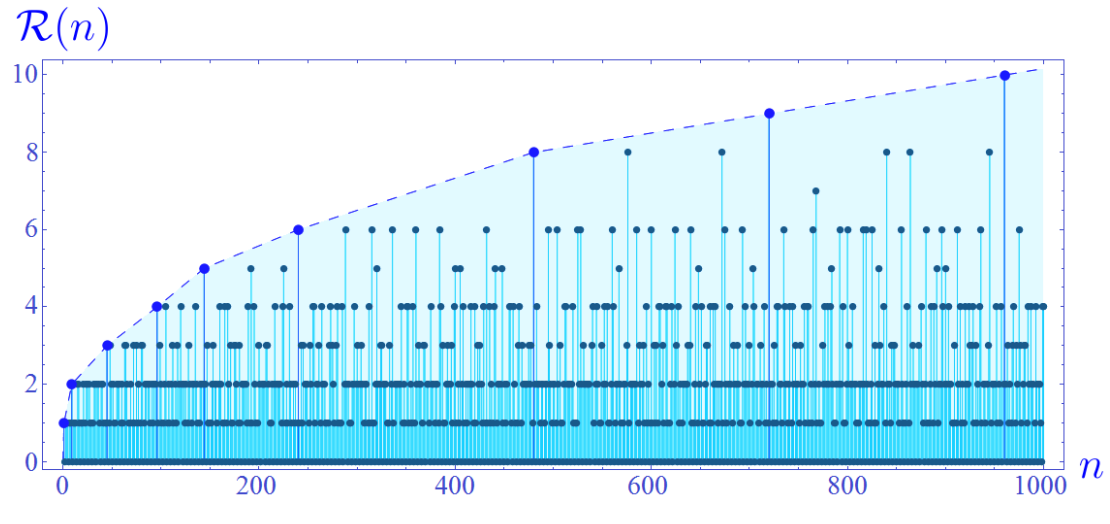
En particular, de la última fórmula se desprende que todo primo impar posee una única representación independiente. No existe ninguna representación para los números n que sean congruentes con 2 en el módulo 4. El caso faltante es:

$$\overline{\mathcal{R}}(0) = \infty \qquad\qquad \mathcal{R}(0) = \infty$$

Nota. En los casos $\pm 1, \pm 4$, hay que considerar la factorización en primos de 1, que no posee ningún factor. En consecuencia, el número k de primos presentes es cero. En tal circunstancia, los productos $\prod_{i=1}^{0}(\alpha_i + 1)$ correspondientes deben siempre tomarse como el neutro de la multiplicación, que es 1.

Las representaciones independientes son tratadas con menor frecuencia en la literatura. Para visualizar su comportamiento se presenta la gráfica de $\mathcal{R}(n)$, para los primeros 1000 enteros positivos, en la figura 3. La *envoltura poligonal* de la gráfica ha sido coloreada en el fondo, para apreciar mejor la curva de incrementos (línea punteada), que quizás es de orden logarítmico o incluso menor. La densidad de las capas horizontales decrece conforme $\mathcal{R}$ se incrementa, con ligeros aumentos en los valores pares de $\mathcal{R}$.

Figura 3. **Gráfica de $\langle 1, 0, -1\rangle\, \mathcal{R}(n)$**



Fuente: elaboración propia, mediante *Wolfram Mathematica 8*.

3.2. La forma $x^2 + y^2$

Para la forma $\langle 1, 0, 1\rangle$, la búsqueda de cerraduras se simplifica, pues su discriminante $\Delta = 0^2 - 4(1)(1) = -4$ es negativo, y así, el escolio 3 de la página 55 puede ser aplicado. Como consecuencia de ello, todas sus cerraduras homogéneas cumplen con el sistema de ecuaciones tipo $\mathsf{Q}_z = \mathcal{Q}_z$, que se genera a partir de la tabla VI.

3.2.1. Cerraduras

Se seguirá una ruta diferente a la de los sistemas con los que se había lidiado anteriormente, ya que no hay ecuaciones que se trivialicen. Se dividirá el sistema en tres bloques separados, de esta manera:

$$\text{sistema} \begin{cases} \text{bloque } t^2 \begin{cases} 1 = h_1^2 + k_1^2 & \text{(R-1)} \\ 0 = 2h_1h_2 + 2k_1k_2 & \text{(R-2)} \\ 1 = h_2^2 + k_2^2 & \text{(R-3)} \end{cases} \\ \text{bloque } tu \begin{cases} 0 = 2h_1h_3 + 2k_1k_3 & \text{(R-4)} \\ 0 = 2(h_1h_4 + h_2h_3) + 2(k_1k_4 + k_2k_3) & \text{(R-5)} \\ 0 = 2h_2h_4 + 2k_2k_4 & \text{(R-6)} \end{cases} \\ \text{bloque } u^2 \begin{cases} 1 = h_3^2 + k_3^2 & \text{(R-7)} \\ 0 = 2h_3h_4 + 2k_3k_4 & \text{(R-8)} \\ 1 = h_4^2 + k_4^2 & \text{(R-9)} \end{cases} \end{cases}$$

Los bloques t^2 y u^2 son independientes, ya que no comparten variables. Además de esto, son análogos, es decir, si se conocen las soluciones de uno, se sabrán las soluciones de ambos. El bloque tu es el que le da cohesión al sistema.

Problema. Hallar todas las soluciones enteras del bloque t^2.

Solución. Las ecuaciones R-1 y R-3 aseveran que (h_1, k_1) y (h_2, k_2) son representaciones de la unidad en la forma $x^2 + y^2$. Es fácil probar que sólo existen 4 de ellas: $(1, 0), (-1, 0), (0, 1), (0, -1)$. Ahora sólo se debe verificar cuáles parejas de representaciones cumplen con la ecuación R-2.

En la tabla VII se han desglosado todos los casos. Se le llama *exhaustión menor* porque ésta verifica solamente el bloque t^2. Se usarán las soluciones que se obtengan para llevar a cabo una segunda revisión que abarque los tres bloques y, generalmente, esta segunda exhaustión es más larga.

Tabla VII. **Exhaustión menor de las cerraduras de $\langle 1, 0, 1\rangle$**

(h_1, k_1)	(h_2, k_2)	$h_1h_2 + k_1k_2$	solución
$(+1, 0)$	$(+1, 0)$	$+1$	·
$(+1, 0)$	$(-1, 0)$	-1	·
$(+1, 0)$	$(0, +1)$	0	✓
$(+1, 0)$	$(0, -1)$	0	✓
$(-1, 0)$	$(+1, 0)$	-1	·
$(-1, 0)$	$(-1, 0)$	$+1$	·
$(-1, 0)$	$(0, +1)$	0	✓
$(-1, 0)$	$(0, -1)$	0	✓
$(0, +1)$	$(+1, 0)$	0	✓
$(0, +1)$	$(-1, 0)$	0	✓
$(0, +1)$	$(0, +1)$	$+1$	·
$(0, +1)$	$(0, -1)$	-1	·
$(0, -1)$	$(+1, 0)$	0	✓
$(0, -1)$	$(-1, 0)$	0	✓
$(0, -1)$	$(0, +1)$	-1	·
$(0, -1)$	$(0, -1)$	$+1$	·

Fuente: elaboración propia.

Se pudo haber razonado de esta forma: puesto que cada representación de la unidad tiene exactamente una coordenada cero, y ya que la ecuación R-2 básicamente indica que el producto escalar de las dos representaciones es cero, se deben elegir aquellos pares de representaciones que tengan al cero en posiciones alternas, y éstos son los ocho que han sido marcado en la tabla anterior. La exhaustión fue elaborada, sin embargo, para introducir el método que será necesario en la siguiente sección, cuando se analice la forma $\langle 1, 1, 1\rangle$. ♢

La exhaustión mayor consiste en tomar esas ocho soluciones (h_1, h_2, k_1, k_2) del bloque t^2 y, recordando que también son soluciones (h_3, h_4, k_3, k_4) para el bloque u^2, formar las 64 parejas posibles y revisar cuáles de ellas cumplen con el bloque tu. Este procedimiento es demasiado largo para llevarlo a cabo en el cuerpo del documento, pero puede ser hallado en el apéndice A.1, en la página 143. La forma $\langle 1, 0, 1\rangle$ posee las ocho simetrías posibles, así que las soluciones halladas con este procedimiento se deben agrupar en clases de equivalencia de ocho elementos cada una. Hay dos clases, que corresponden a las dos columnas siguientes, y de cada una de ellas se puede tomar por representante la primera solución.

$(+1, 0, 0, -1; 0, +1, +1, 0)$	$(+1, 0, 0, +1; 0, +1, -1, 0)$
$(+1, 0, 0, -1; 0, -1, -1, 0)$	$(+1, 0, 0, +1; 0, -1, +1, 0)$
$(-1, 0, 0, +1; 0, +1, +1, 0)$	$(-1, 0, 0, -1; 0, +1, -1, 0)$
$(-1, 0, 0, +1; 0, -1, -1, 0)$	$(-1, 0, 0, -1; 0, -1, +1, 0)$
$(0, +1, +1, 0; +1, 0, 0, -1)$	$(0, +1, -1, 0; +1, 0, 0, +1)$
$(0, +1, +1, 0; -1, 0, 0, +1)$	$(0, +1, -1, 0; -1, 0, 0, -1)$
$(0, -1, -1, 0; +1, 0, 0, -1)$	$(0, -1, +1, 0; +1, 0, 0, +1)$
$(0, -1, -1, 0; -1, 0, 0, +1)$	$(0, -1, +1, 0; -1, 0, 0, -1)$

Las cerraduras independientes vuelven a coincidir con aquellas provistas por Diofanto hace casi dos milenios. Es posible, sin embargo, agregar algo a lo dicho por él: la exhaustión prueba que no existe otra cerradura para la forma $\langle 1, 0, 1\rangle$.

- $(t^2 + u^2)(v^2 + w^2) = (tv - uw)^2 + (tw + uv)^2$
- $(t^2 + u^2)(v^2 + w^2) = (tv + uw)^2 + (tw - uv)^2$

Basándose en los resultados previos podría creerse que todas las formas poseerán sólo dos cerraduras independientes, pero esta pista es falsa y será desmentida por el análisis de la forma $x^2 + xy + y^2$, en la próxima sección. El esquema que sí se rompió en este punto es que anteriormente se habían encontrado el mismo número de representaciones de la unidad que de cerraduras independientes, pero la forma $x^2 + y^2$ representa al uno de cuatro maneras diferentes, que es el doble del número de cerraduras. La mejor conjetura, por el momento, es que eso se debe a que también posee el doble de simetrías. Y estos análisis sólo aplican a las formas que puedan representar a la unidad.

3.2.2. Representabilidad

Lema 7. *La forma cuadrática $x^2 + y^2$ representa al primo p si, y sólo si, p no es congruente con 3 en el módulo 4.*

Fermat declaró tener una demostración mediante descenso infinito en una carta escrita al padre Mersenne, fechada el 25 de diciembre de 1640, por lo cual es llamado ocasionalmente «el teorema navideño de Fermat». Leonhard Euler escuchó hablar de éste y otros resultados de Fermat vía su correspondencia con Goldbach. En 1730, Euler le escribe diciendo que el «teorema de los cuatro cuadrados de Fermat» (el mismo que fue mencionado al hablar de formas universales) le parece sumamente elegante. Él se sentía atraído por la belleza intrínseca de este tipo de proposiciones, pero más aún, por la ausencia de pruebas. La suerte estaba echada, Euler decidió no cejar hasta obtener las demostraciones que Fermat dejó sólo en promesas.

La parte de *sólo si* es muy fácil de argumentar, basta notar que los residuos cuadráticos en el módulo 4 son 0 y 1, y ninguna de las cuatro posibles sumas de ellos es congruente con 3. Para $p = 2$ se tiene $2 = 1^2 + 1^2$. El verdadero reto es demostrar que todos los primos congruentes con 1 poseen representaciones. Se puede probar que existen inifitos primos congruentes con 1, y también infinitos primos congruentes con 3, en el módulo 4 (Véanse los problemas 21 al 24 del apéndice D). Lo anterior indica que elaborar una larga lista de representaciones no será de mucho beneficio, salvo por la posibilidad de obtener inspiración de ella. No, se necesita un método general que permita construir la representación para cualquiera de ellos.

Euler descompone su demostración en dos partes: *descenso* y *reciprocidad*. La primera parte consiste en probar que si un primo impar p divide a un número n cualquiera, que sea representable en la forma $x^2 + y^2$, entonces p también es representable. Euler envió este resultado por correo a Goldbach en 1747. La carta también incluía una descripción incompleta de lo que faltaba demostrar. Dos años después completó la segunda parte, que dice: si p es congruente con 1 en el módulo 4, entonces divide a algún entero n que es representable en la forma $x^2 + y^2$. Para el presente

texto, se seguirán de cerca las ideas de Euler, pero empleando un enfoque moderno. Se dividirá la prueba en cinco pasos, con el propósito de facilitar su lectura.

Paso 1. *El conjunto S de los números representables por la forma x^2+y^2 es cerrado bajo el producto.*

Demostración. Las identidades de Brahmagupta-Fibonacci prueban que el producto de dos elementos de S es también un elemento de S. □

Paso 2. *Si n es un entero representable, y p es un primo, divisor de n, que también es representable, entonces el cociente $\frac{n}{p}$ también será representable.*

Demostración. Suponga que $n = a^2 + b^2, p = c^2 + d^2$; se quiere hallar una representación como suma de dos cuadrados para el número $\frac{a^2+b^2}{c^2+d^2}$ (que es un entero, porque p es divisor de n). Note que $c^2n - a^2p$ debe ser múltiplo de p, al ser una combinación lineal de múltiplos, y puede ser factorizado así:

$$c^2n - a^2p = c^2(a^2 + b^2) - a^2(c^2 + d^2) = b^2c^2 - a^2d^2 = (bc - ad)(bc + ad) \tag{3.4}$$

Luego, puesto que $p \mid (bc - ad)(bc + ad)$, por el lema de Euclides debe dividir a alguno de los factores. Supóngase primero que divide a $(bc - ad)$. Empleando la segunda identidad de Brahmagupta-Fibonacci, se puede escribir

$$(a^2 + b^2)(c^2 + d^2) = (ac + bd)^2 + (bc - ad)^2$$

Cada factor del miembro izquierdo es divisible entre p, entonces el producto es divisible entre p^2. También $(bc-ad)^2$ es divisible entre p^2. Otra vez, por la propiedad de las combinaciones lineales, p^2 debe dividir a $(ac + bd)^2$. Esto quiere decir que la ecuación anterior puede ser dividida entre p^2 y los términos resultantes serían enteros. Como $p^2 = (c^2 + d^2)^2$, al dividir se obtiene

$$\frac{a^2 + b^2}{c^2 + d^2} = \left(\frac{ac + bd}{c^2 + d^2}\right)^2 + \left(\frac{bc - ad}{c^2 + d^2}\right)^2 \tag{3.5}$$

que es la representación buscada, pues cada fracción es un entero. Si p dividiera al otro factor, es decir, a $(bc + ad)$, se puede elaborar un argumento similar, empleando la otra identidad de Brahmagupta-Fibonacci. □

Paso 3. *Si un número representable n es divisible entre un entero m que no puede ser escrito como suma de cuadrados, entonces el cociente $\frac{n}{m}$ posee algún factor que tampoco es representable.*

Demostración. Suponga que la factorización en primos de $\frac{n}{m}$ es $\prod_{i=1}^{k} p_i^{\alpha_i}$, entonces $n = m\prod_{i=1}^{k} p_i^{\alpha_i}$. Si cada p_i es representable en la forma $\langle 1, 0, 1\rangle$, entonces se podría dividir de manera sucesiva la expresión anterior entre cada uno de ellos (repitiendo α_i veces a cada p_i) y, por el paso 2, los cocientes obtenidos serían todos representables, hasta llegar al propio m, que también debería serlo. Esto contradice la hipótesis hecha sobre m, por lo que resulta ineludible que al menos uno de los p_i no puede ser escrito como suma de dos cuadrados. □

Paso 4. *Si a, b son primos relativos, entonces todos los factores de $n = a^2 + b^2$ son representables en la forma $\langle 1, 0, 1\rangle$.*

Demostración. Aquí es donde se necesita el descenso infinito. En este paso se considera un m que sea factor de n. Mediante el algoritmo de la división (empleando un cociente ligeramente mayor al usual, de ser necesario) se puede escribir

$$a = q_1 m \pm c \qquad\qquad b = q_2 m \pm d \tag{3.6}$$

donde c, d son enteros no negativos tales que ninguno de ellos es mayor a $\frac{m}{2}$. Sustituyendo estas expresiones en la definición de n se obtiene

$$n = (q_1 m \pm c)^2 + (q_2 m \pm d)^2 = q_1^2 m^2 \pm 2q_1 mc + c^2 + q_2^2 m^2 \pm 2q_2 md + d^2 = Am + c^2 + d^2$$

Aquí, A es el número que queda después de extraer el factor común m a todos los términos que lo poseen explícitamente en la fórmula anterior. Puesto que $c^2 + d^2 = (n - Am)$ es una combinación lineal de múltiplos de m, se concluye que $m \mid c^2 + d^2$. Sea r tal que

$$c^2 + d^2 = rm \tag{3.7}$$

Si c, d no fueran primos relativos, entonces $\text{MCD}(c, d)$ no puede dividir a m, de lo contrario, por (3.6), $\text{MCD}(c, d)$ dividiría simultáneamente a los números a, b, que según el enunciado son primos relativos. Como $(\text{MCD}(c, d))^2 \mid c^2 + d^2$, forzosamente $(\text{MCD}(c, d))^2 \mid r$. Esto quiere decir que cada término de la ecuación (3.7) puede ser

dividido entre $(\text{MCD}(c,d))^2$, y seguirían siendo enteros. Haciendo tal división se obtiene una expresión del tipo $e^2 + f^2 = sm$, donde e, f son primos relativos, y s está acotado por la siguiente desigualdad.

$$sm = e^2 + f^2 \leq c^2 + d^2 \leq \left(\tfrac{m}{2}\right)^2 + \left(\tfrac{m}{2}\right)^2 = \tfrac{1}{2}m^2 \implies s \leq \tfrac{1}{2}m$$

Si c, d fueran desde un principio primos relativos, entonces pueden ser usados directamente, en lugar de obtener los números e, f. Ahora bien, si m no pudiera ser escrito como la suma de dos cuadrados, entonces, por el paso 3, existe un factor de s que tampoco es representable, llámesele m_2. Note que $m_2 \leq s \leq \frac{1}{2}m$. Un argumento análogo puede ser fabricado en el cual se reemplazan todas las instancias de m por m_2, originando un m_3. Este mecanismo, iterado indefinidamente, genera un descenso infinito, pues cada m_i es menor en tamaño que el anterior, pero todos ellos son positivos. Claramente esto es imposible, así que m tiene que tener una representación como suma de dos cuadrados. □

Paso 5. *Todo primo de la forma $4k + 1$ es suma de dos cuadrados.*

Ser de la forma $4k + 1$ significa lo mismo que ser congruente con 1 en el módulo 4, así que éste es el paso final. Antes de llevar a cabo la demostración, es menester familiarizarse con un teorema de Lagrange.

Teorema (máximo número de raíces)**.** *El número de soluciones de una congruencia polinomial de grado g en el módulo p primo, elegidas de entre el sistema completo de residuos $\{0, 1, 2, \ldots, p-1\}$, es a lo sumo g.*

Este teorema se sigue del hecho de que los enteros en un módulo primo conforman un campo, y un polinomio de grado g definido sobre un campo tiene a lo sumo g raíces. Es el análogo en congruencias del teorema fundamental del Álgebra para los reales. Se puede consultar casi cualquier libro de Álgebra Moderna, por ejemplo, Hernstein [19], para investigar la teoría subyacente de este teorema.

Demostración del paso 5. Por el pequeño teorema de Fermat se sabe que $z^{4k} \equiv 1$ (mód p), para cada $z \in \mathbb{Z}$ que sea primo relativo con p. Restando 1 de ambos lados y

factorizando la diferencia de cuadrados que resulta, se tiene la congruencia polinomial (3.8) en la variable z, que posee $4k$ raíces distintas (soluciones en el sistema completo de residuos), pues la clase del cero es la única que no anula al polinomio.

$$(z^{2k}+1)(z^{2k}-1) \equiv 0 \pmod{p} \tag{3.8}$$

Como la congruencia $z^{2k}-1 \equiv 0 \pmod{p}$ tiene a lo sumo $2k$ raíces, debe haber residuos dentro del sistema completo que no anulen al factor $(z^{2k}-1)$. Sea r uno de ellos, entonces p no divide a $(r^{2k}-1)$, y como $0 < r < p$, se deduce que r, p son primos relativos. Pero r sí es raíz de (3.8), así que p debe dividir al otro factor, a $(r^{2k}+1)$. Como este factor es una suma de cuadrados, el paso 4 aplica y se concluye que p es representable en la forma x^2+y^2. $\square$

Teorema 7 (representabilidad)**.** *Un número n es representable en la forma $\langle 1,0,1\rangle$ si, y sólo si, ningún primo congruente con 3 en el módulo 4 aparece elevado a una potencia impar en la factorización en primos de n.*

Demostración. Supóngase primero que n es representable, y sea $n = a^2+b^2$ su representación. Note que $(\text{MCD}(a,b))^2$ es divisor de n, así que es posible dividir cada término de la ecuación entre ese factor, para obtener una expresión del tipo $m = c^2+d^2$, donde c, d son primos relativos. La división entre $(\text{MCD}(a,b))^2$, que transforma n en m, conserva la paridad de los exponentes de la factorización en primos de n, con la posibilidad de que algunos de ellos se hayan convertido en cero, pero sólo si eran en un principio pares. Todos los primos con exponente impar siguen estando presentes en m. Por el paso 4, todos estos primos deben ser representables, y ya se ha probado que ningún primo congruente con 3 en el módulo 4 lo es, así que ninguno de ellos podía tener originalmente un exponente impar.

Ahora supóngase que todos los primos congruentes con 3 en el módulo 4, que aparezcan en la factorización en primos de n, lo hacen con exponente par. Sea r el máximo cuadrado perfecto que sea divisor de n. Se tiene que r posee una representación trivial en la forma $\langle 1,0,1\rangle$ (anulando una de las variables). Además, por el paso 5, todos los primos congruentes con 1 en el módulo 4 son representables. Sean

$p_1, p_2, \ldots, p_k$ los primos que tienen exponente impar en la factorización de n (todos ellos son congruentes con 1). Usando las representaciones de r y los p_i se puede construir una para n, ya que $n = rp_1p_2 \ldots p_k$. Tal construcción se lleva a cabo mediante alguna de las identidades de Brahmagupta-Fibonacci (o ambas). $\square$

3.2.3. Cantidad de representaciones

Sea $\mathcal{C}$ una identidad de cerradura para la forma $\mathfrak{q} = \langle a, b, c\rangle$. Si los números f, g tienen las representaciones $(f_1, f_2), (g_1, g_2)$, respectivamente, al proceso de construir una representación (n_1, n_2) para el número $n = fg$, a través de la cerradura $\mathcal{C}$ aplicada a $(f_1, f_2), (g_1, g_2)$, se le llamará *composición de representaciones*, y se denotará por

$$(f_1, f_2)\ \boxed{\mathcal{C}}\ (g_1, g_2) = (n_1, n_2)$$

Por ejemplo, para la forma $\langle 1, 0, 1\rangle$, si $\mathcal{C}_1$ representa la primera de las identidades de Brahmagupta-Fibonacci, se puede escribir:

$$(2, 5)\ \boxed{\mathcal{C}_1}\ (11, 3) = (22 - 15, 6 + 55) = (7, 61)$$

Es importante tener presente que las transformaciones simétricas pueden ser aplicadas tanto a representaciones como a cerraduras. Se evitarán los paréntesis al transformar cerraduras, esto es, se escribirá $\boxed{\mathcal{T}_i\,\mathcal{C}}$, en lugar de $\boxed{\mathcal{T}_i(\mathcal{C})}$. La interrelación de las transformaciones simétricas con la composición de representaciones es intrincada, tal como lo muestra la siguiente identidad, que puede ser probada mediante un sencillo cálculo.

$$\mathcal{T}_2(f_1, f_2)\ \boxed{\mathcal{C}_1}\ (g_1, g_2) = (f_1, f_2)\ \boxed{\mathcal{T}_8\,\mathcal{C}_1}\ \mathcal{T}_5(g_1, g_2)$$

Es razonable suponer que las representaciones de un número compuesto n en la forma $\langle 1, 0, 1\rangle$ se pueden obtener mediante la composición de las representaciones de sus factores. Se verá que, al menos para algunos factores, es verdadero. Identidades como la anterior hacen pensar que probablemente no sea necesario usar las ocho cerraduras, sino que basta con una sola, o tal vez una de cada clase, por ejemplo

las de Brahmagupta-Fibonacci. Al menos, mediante el paso 2, se puede asegurar que si el número posee divisores congruentes con 1 en el módulo 4, entonces todas sus representaciones se pueden obtener de ciertos números menores que lo dividen. En el listado generado por todas las composiciones habrá repeticiones, pero al menos ofrece un método para encontrarlas a todas.

Lo que falta es determinar el número de representaciones que poseen los bloques de construcción básicos: un bloque por cada primo de la forma $4k+1$, y un sólo bloque conformado por el resto de la factorización. El primer paso es hallar el número de representaciones que tienen los primos. El 2 tiene 4 representaciones que pertenecen a la misma clase, es decir, $\overline{\mathcal{R}}(2) = 4, \mathcal{R}(2) = 1$. Los teoremas que se enuncian a continuación se encargan del resto.

Teorema 8 (unicidad de representación)**.** *Si p es un primo tal que $p \equiv 1 \pmod 4$, entonces $\overline{\mathcal{R}}(p) = 8, \mathcal{R}(p) = 1$. En otras palabras, p tiene una única representación, salvo transformaciones simétricas.*

Demostración. La igualdad $\overline{\mathcal{R}}(p) = 8$ se sigue inmediatamente de $\mathcal{R}(p) = 1$, así que sólo se mostrará la segunda. Supóngase que $(a, b), (c, d)$ son dos representaciones del primo p, tales que a, b, c, d son enteros positivos que cumplen $a < b, d < c$ (este orden es conveniente para la demostración). Como p es divisor de sí mismo, es posible argumentar que p divide a $(bc - ad)(bc + ad)$, ya que puede tomarse $n = p$ en (3.4). Debido al orden elegido, cada uno de estos factores es un entero positivo y, como p es primo, debe dividir a alguno de ellos. Note que

$$\begin{gathered} p \mid bc \pm ad \implies \\ p \leq bc \pm ad \implies \\ a^2 + b^2 \leq bc \pm ad, \qquad c^2 + d^2 \leq bc \pm ad \end{gathered}$$

Sumando las dos desigualdades anteriores, y pasando todos los términos al miembro izquierdo resulta

$$\begin{gathered} a^2 \mp 2ad + d^2 + b^2 \mp 2bc + c^2 \leq 0 \implies \\ (a \mp d)^2 + (b \mp c)^2 \leq 0 \end{gathered}$$

Y la última desigualdad sólo puede darse si cada cuadrado se anula. Como los números a, b, c, d son todos positivos, el signo $\mp$ debe ser negativo, y entonces, el hecho de que se anulen los cuadrados implica que las representaciones son equivalentes. $\square$

Lema 9. *Si el número representable m es compuesto y tal que todos sus factores primos son congruentes con 3 en el módulo 4, entonces m posee una única representación independiente, y cuatro en total.*

Demostración. Cada uno de los factores primos de m debe estar elevado a una potencia par, así que m es un cuadrado perfecto, tómese $m = \zeta^2$, y una de sus representaciones es $(\zeta, 0)$. Sea (ξ, η) una representación cualquiera de m en la forma $\langle 1, 0, 1\rangle$, luego $\xi^2 + \eta^2 = \zeta^2$, de donde (ξ, η, ζ) es una terna pitagórica. Dicha terna no puede ser primitiva, de lo contrario ξ, η serían primos relativos, y por el paso 4 de la página 73, los factores primos de m deberían ser representables, lo cual constituye un absurdo.

Divídase la terna entre $\text{MCD}(\xi, \eta)$, para obtener la terna primitiva correspondiente (ξ_0, η_0, ζ_0). Note que (ξ_0, η_0) es una representación para el número m_0 definido por $\frac{m}{(\text{MCD}(\xi,\eta))^2}$. Si hubiera un primo que fuera divisor de m_0, ese primo sería divisor de m y, por lo tanto, sería congruente con 3 en el módulo 4. Como $\text{MCD}(\xi_0, \eta_0) = 1$, el mismo paso 4 aplicado a m_0 implica que éste no puede tener divisores primos. Por la definición de m_0 se deduce que la terna original era trivial, esto quiere decir que en la representación (ξ, η), una de las componentes se anula, y todas las representaciones de ese tipo son transformaciones simétricas de $(\zeta, 0)$. $\square$

Teorema 9. *Si $n = 2^\alpha \cdot m$, donde m es como en el lema anterior y $\alpha \in \mathbb{Z}^+$, entonces n posee una representación independiente y cuatro en total.*

Demostración. Sea (ξ, η) una representación de n como suma de dos cuadrados, tal que $\xi, \eta \in \mathbb{N}$ y ordénense de forma que $\xi \geq \eta$. Es necesario que ξ, η tengan la misma paridad, para que $\xi^2 + \eta^2 = n$ sea par, como en el enunciado. Lo anterior justifica la existencia de $a, b \in \mathbb{N}$ tales que $(\xi, \eta) = (a + b, a - b)$. Como $\eta \in \mathbb{N}$, se tiene $a \geq b$. Se propone que (a, b) es una representación para el número $\frac{n}{2}$, una que cumple los

mismos criterios de orden: $a \geq b$, y signos: $a, b \in \mathbb{N}$, que cumplía (ξ, η). La prueba de esta propuesta radica en la siguiente fórmula, en la que $(a^2 + b^2)$ ocupa el papel de $\frac{n}{2}$, y que puede ser verificada por simple expansión.

$$2(a^2 + b^2) = (a + b)^2 + (a - b)^2$$

La elección inicial de orden y signos para (ξ, η) se hace con el propósito de precisar un único elemento de cada clase de representaciones. El procedimiento anterior puede iterarse, y con cada repetición el número n pierde otro factor 2, hasta que queda solamente el número m. Según el lema anterior, m solamente posee la representación independiente $(\sqrt{m}, 0)$, y esta unicidad se transmite paso a paso en las iteraciones, hasta alcanzar al número n. $\square$

Los teoremas 8 y 9 son esos bloques de construcción que fueron mencionados al principio, y a partir de ellos se pueden fabricar todas las representaciones de un número compuesto, mediante la composición. Cabe señalar que se puede obtener una demostración alternativa para el último teorema si se aplican las iteraciones de dos en dos, forma en la cual resultan más naturales:

$$4(a^2 + b^2) = 2[(a + b)^2 + (a - b)^2] = (a + b + a - b)^2 + (a + b - a + b)^2 = (2a)^2 + (2b)^2$$

Para llevar a cabo la primera iteración doble, el número n debe ser tal que α sea mayor o igual a 2, ya que cada iteración divide a n entre 4. Estudiando la ecuación $2^\alpha m = \xi^2 + \eta^2$ localmente en el módulo 4, se concluye que ξ, η son pares en este caso, y así pueden tomarse $(\xi, \eta) = (2a, 2b)$, donde (a, b) es una representación para $\frac{n}{4}$.

Este procedimiento se debe subdividir en casos, según la paridad de α. Uno de ellos requiere como paso final el lema 9. El otro exige una representación de $2m$. Como m es un cuadrado perfecto, eso sugiere estudiar la ecuación diofantina

$$2y^2 = x^2 + z^2$$

Note que las soluciones son ternas (x, y, z) tales que sus cuadrados están en progresión aritmética, pues al despejar y^2 se tiene que este cuadrado es el promedio de los

otros dos. En el capítulo 5, en la sección sobre la forma $x^2 + y^2$, se investigará cómo generar todas las soluciones de dicha ecuación. Ese conocimiento puede ser utilizado para completar este esquema de demostración, verificando que $2m$ tiene una única representación independiente. Como dato curioso, se puede probar que las sucesiones aritméticas de cuadrados más largas son precisamente las de tres términos.

En otro orden de ideas, si lo que resulta de interés es el número de representaciones, aunque no se especifique cuáles son, Jacobi encontró una fórmula muy interesante para calcularlo, mediante el estudio de una función elíptica que él propuso. Aquí se enuncia su teorema sin demostración, pues las técnicas requeridas escapan del marco propuesto inicialmente.

Teorema de Jacobi. *Si $d_i(n)$ representa la cantidad de divisores de n que sean congruentes con i en el módulo 4, entonces*

$$\langle 1, 0, 1\rangle\, \overline{\mathcal{R}}(n) = 4[d_1(n) - d_3(n)]$$

Una manera alternativa de escribir este resultado es la siguiente. Si n tiene una factorización en primos como la siguiente

$$n = 2^{\alpha_0} \prod_{i=1}^{k} p_i^{\alpha_i} \prod_{i=1}^{\ell} q_i^{2\beta_i}$$

donde los p_i son primos congruentes con 1 en el módulo 4, en tanto que los q_i son congruentes con 3; entonces la cantidad de representaciones de n como suma de dos cuadrados está dada por

$$\langle 1, 0, 1\rangle\, \overline{\mathcal{R}}(n) = 4 \prod_{i=1}^{k} (\alpha_i + 1)$$

Por ejemplo, si n se factoriza como $2^7 \cdot 3^4 \cdot 5^9 \cdot 7^2 \cdot 13^3$, primero se revisa que los primos de la forma $4k + 3$ tengan exponente par, y luego se usan los exponentes de los de la forma $4k+1$ para hallar el número de representaciones: $\overline{\mathcal{R}}(n) = 4(9+1)(3+1) = 160$.

También resulta sumamente interesante estudiar el comportamiento global de $\overline{\mathcal{R}}(n)$ en términos de su valor promedio. Cuando un conjunto de números es infinito, existen varias formas de definir un promedio aritmético, la más natural de ellas es la suma de Cesáro.

Definición (suma de Cesáro)**.** Sea $(a_i)_{i\in\mathbb{Z}^+}$ una sucesión de números reales. La *n-ésima suma parcial de Cesáro* s_n está definida por $s_n = \frac{1}{n}\sum_{i=1}^{n} a_i$, es decir, s_n es el promedio de los primeros n términos de la sucesión. Se puede considerar una nueva sucesión conformada por las sumas parciales de Cesáro $(s_n)_{n\in\mathbb{Z}^+}$. Si ésta es convergente, entonces su límite $\mathcal{S}$ es llamado *suma de Cesáro* de la sucesión original. En símbolos, se tiene que $\mathcal{S} = \lim\limits_{n\to\infty}\left[\frac{1}{n}\sum_{i=1}^{n} a_i\right]$, siempre que el límite exista.

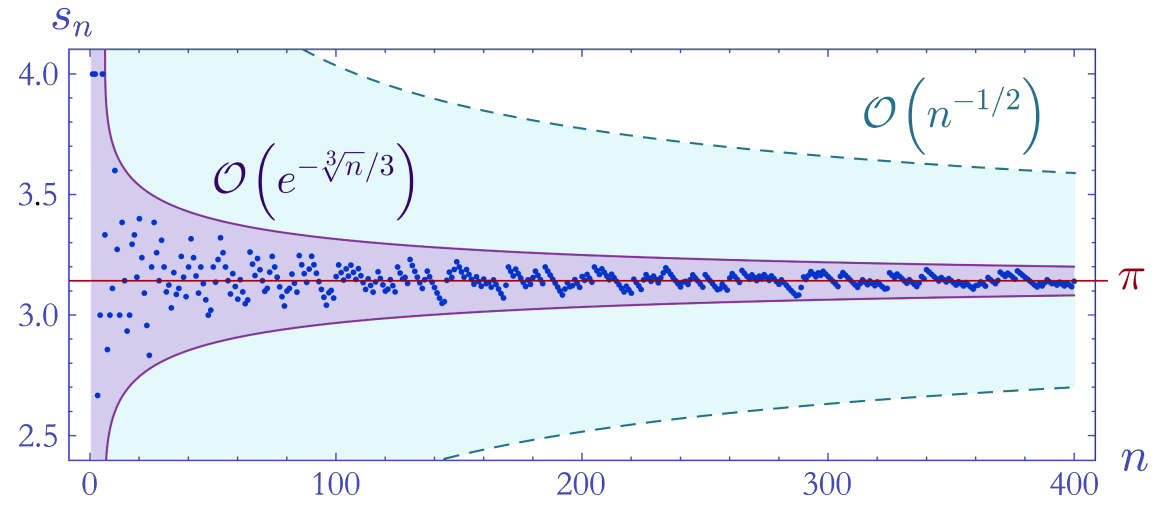
Gauss demostró que la suma de Cesáro de la sucesión $\left(\overline{\mathcal{R}}(i)\right)_{i\in\mathbb{Z}^+}$ existe, y vale π. Este resultado se hace un poco menos sorprendente si se considera que la ecuación diofantina $x^2 + y^2 = n$ describe a los puntos de coordenadas enteras en una circunferencia centrada en el origen, que tiene radio $\sqrt{n}$. En la prueba, sin embargo, se requiere más rigurosidad. Básicamente, se debe probar que $\sum_{i=1}^{n}\overline{\mathcal{R}}(i)$ es una aproximación al área del círculo de radio $\sqrt{n}$, que mejora relativamente conforme n crece. Dicha suma calcula el número de puntos reticulares, es decir, puntos con coordenadas enteras, que hay en el interior o borde de la circunferencia mencionada.

El problema de determinar, en términos de n, una fórmula para el número de puntos reticulares en el círculo llegó a conocerse como «el problema del círculo de Gauss». Él demostró que el error al aproximar el área del círculo de radio $\sqrt{n}$, mediante la suma $\sum_{i=1}^{n}\overline{\mathcal{R}}(i)$, es menor o igual a $2\pi\sqrt{2n} + 2\pi$, en valor absoluto (véase el problema 25 en el apéndice D). En otras palabras, Gauss encontró una cota de error del orden de $n^{1/2}$ para esa aproximación. Dividiendo entre n se puede inferir que la n-ésima suma de Cesáro de la sucesión $\left(\overline{\mathcal{R}}(i)\right)_{i\in\mathbb{Z}^+}$ se aproxima al límite π, al menos a una rapidez del orden de $n^{-1/2}$, explícitamente dada por

$$\left|\pi - \frac{1}{n}\sum_{i=1}^{n}\overline{\mathcal{R}}(i)\right| \leq \frac{2\pi\sqrt{2}}{\sqrt{n}} + \frac{2\pi}{n} \tag{3.9}$$

Según las fuentes consultadas, la mejor cota de error conocida es del orden de $n^{-131/416}$, y fue propuesta por Huxley [21] en el 2003. En la figura 4 se ha marcado marcado con líneas punteadas la cota que se deriva del trabajo de Gauss, en tanto que las curvas continuas representan una tentativa cota del orden de $e^{-\sqrt[3]{n}/3}$ para la rapidez con que la sucesión de sumas parciales de Cesáro se aproxima al límite π.

Figura 4. **Sumas parciales de Cesáro de $\langle 1, 0, 1\rangle\, \overline{\mathcal{R}}(n)$**



Fuente: elaboración propia, mediante *Wolfram Mathematica 8, Inkscape* y *Geogebra 4*.

3.3. La forma $x^2 + xy + y^2$

Para usar el método de las exhaustiones, el paso inicial es determinar todas las representaciones de la unidad. En esto hay notar que la forma es simétrica respecto a $\mathcal{T}_1, \mathcal{T}_4, \mathcal{T}_5$ y $\mathcal{T}_8$. Considérese entonces la ecuación diofantina $x^2 + xy + y^2 = 1$. Los casos en que x vale 0 o 1 devuelven de manera trivial las representaciones $(0, 1), (0, -1), (1, 0), (1, -1)$, y aplicándoles las transformaciones simétricas resultan dos nuevas: $(-1, 0), (-1, 1)$. Se demostrará que estas seis representaciones son las únicas, para ello suponga que ninguna de las variables vale 0 o 1. Las variables deben tener signo distinto, de lo contrario la expresión $x^2 + xy + y^2$ sería mayor

que 1. Sin pérdida de la generalidad, asuma $|x| \geq |y| > 1$. En tales circunstancias, $x^2 + xy + y^2 \geq x^2 - x^2 + y^2 = y^2 > 1$, así que no hay otras soluciones.

3.3.1. Cerraduras

Como la forma $\langle 1, 1, 1\rangle$ tiene discriminante negativo, todas sus cerraduras son reducidas. Una vez más se recurre a la tabla VI para generar el sistema de las cerraduras, desglosado en los bloques t^2, tu y u^2. Inmediatamente después se lleva a cabo la exhaustión menor del bloque t^2, en la tabla VIII.

$$
\text{sistema}\left\{\begin{array}{ll}
\text{bloque } t^2 & \left\{\begin{array}{rcll} 1 &=& h_1^2 + h_1k_1 + k_1^2 & (\text{R-}1)\\ 1 &=& 2h_1h_2 + h_1k_2 + h_2k_1 + 2k_1k_2 & (\text{R-}2)\\ 1 &=& h_2^2 + h_2k_2 + k_2^2 & (\text{R-}3)\end{array}\right.\\
\text{bloque } tu & \left\{\begin{array}{rcll} 1 &=& 2h_1h_3 + h_1k_3 + h_3k_1 + 2k_1k_3 & (\text{R-}4)\\ 1 &=& 2(h_1h_4 + h_2h_3) + h_1k_4 + h_4k_1 + & \\ & & h_2k_3 + h_3k_2 + 2(k_1k_4 + k_2k_3) & (\text{R-}5)\\ 1 &=& 2h_2h_4 + h_2k_4 + h_4k_2 + 2k_2k_4 & (\text{R-}6)\end{array}\right.\\
\text{bloque } u^2 & \left\{\begin{array}{rcll} 1 &=& h_3^2 + h_3k_3 + k_3^2 & (\text{R-}7)\\ 1 &=& 2h_3h_4 + h_3k_4 + h_4k_3 + 2k_3k_4 & (\text{R-}8)\\ 1 &=& h_4^2 + h_4k_4 + k_4^2 & (\text{R-}9)\end{array}\right.
\end{array}\right.
$$

Tabla VIII. **Exhaustión menor de las cerraduras de $\langle 1, 1, 1\rangle$**

(h_1, k_1)	(h_2, k_2)	$2h_1h_2 + h_1k_2 + h_2k_1 + 2k_1k_2$	solución
$(+1, -1)$	$(+1, -1)$	$+2$	·
$(+1, -1)$	$(+1,\ 0\ )$	$+1$	✓
$(+1, -1)$	$(-1,\ 0\ )$	-1	·
$(+1, -1)$	$(-1, +1)$	-2	·
$(+1, -1)$	$(\ 0\ , +1)$	-1	·
$(+1, -1)$	$(\ 0\ , -1)$	$+1$	✓

continúa

(h_1, k_1)	(h_2, k_2)	$2h_1h_2 + h_1k_2 + h_2k_1 + 2k_1k_2$	solución
$(+1,\ 0\ )$	$(+1, -1)$	$+1$	✓
$(+1,\ 0\ )$	$(+1,\ 0\ )$	$+2$	·
$(+1,\ 0\ )$	$(-1,\ 0\ )$	-2	·
$(+1,\ 0\ )$	$(-1, +1)$	-1	·
$(+1,\ 0\ )$	$(\ 0\ , +1)$	$+1$	✓
$(+1,\ 0\ )$	$(\ 0\ , -1)$	-1	·
$(-1,\ 0\ )$	$(+1, -1)$	-1	·
$(-1,\ 0\ )$	$(+1,\ 0\ )$	-2	·
$(-1,\ 0\ )$	$(-1,\ 0\ )$	$+2$	·
$(-1,\ 0\ )$	$(-1, +1)$	$+1$	✓
$(-1,\ 0\ )$	$(\ 0\ , +1)$	-1	·
$(-1,\ 0\ )$	$(\ 0\ , -1)$	$+1$	✓
$(-1, +1)$	$(+1, -1)$	-2	·
$(-1, +1)$	$(+1,\ 0\ )$	-1	·
$(-1, +1)$	$(-1,\ 0\ )$	$+1$	✓
$(-1, +1)$	$(-1, +1)$	$+2$	·
$(-1, +1)$	$(\ 0\ , +1)$	$+1$	✓
$(-1, +1)$	$(\ 0\ , -1)$	-1	·
$(\ 0\ , +1)$	$(+1, -1)$	-1	·
$(\ 0\ , +1)$	$(+1,\ 0\ )$	$+1$	✓
$(\ 0\ , +1)$	$(-1,\ 0\ )$	-1	·
$(\ 0\ , +1)$	$(-1, +1)$	$+1$	✓
$(\ 0\ , +1)$	$(\ 0\ , +1)$	$+2$	·
$(\ 0\ , +1)$	$(\ 0\ , -1)$	-2	·
$(\ 0\ , -1)$	$(+1, -1)$	$+1$	✓
$(\ 0\ , -1)$	$(+1,\ 0\ )$	-1	·
$(\ 0\ , -1)$	$(-1,\ 0\ )$	$+1$	✓
$(\ 0\ , -1)$	$(-1, +1)$	-1	·
$(\ 0\ , -1)$	$(\ 0\ , +1)$	-2	·
$(\ 0\ , -1)$	$(\ 0\ , -1)$	$+2$	·

Fuente: elaboración propia.

Las doce soluciones marcadas en la exhaustión anterior, también pueden ser utilizadas en el bloque u^2, por lo que hay 144 maneras de elegir soluciones para ambos bloques. La exhaustión mayor (Apéndice A.2), revisa cuáles de esas opciones son soluciones $(h_1, h_2, h_3, h_4; k_1, k_2, k_3, k_4)$ para el sistema global. Sobreviven éstas 24, que pueden ser agrupadas en seis clases:

$$\begin{array}{ll}
(+1,+1,+1,\ 0;-1,\ 0,\ 0,+1) & (+1,+1,\ 0,+1;-1,\ 0,-1,-1)\\
(-1,-1,-1,\ 0;+1,\ 0,\ 0,-1) & (-1,-1,\ 0,-1;+1,\ 0,+1,+1)\\
(-1,\ 0,\ 0,+1;+1,+1,+1,\ 0) & (-1,\ 0,-1,-1;+1,+1,\ 0,+1)\\
(+1,\ 0,\ 0,-1;-1,-1,-1,\ 0) & (+1,\ 0,+1,+1;-1,-1,\ 0,-1)
\end{array}$$

$$\begin{array}{ll}
(+1,+1,\ 0,+1;\ 0,-1,+1,\ 0) & (+1,+1,+1,\ 0;\ 0,-1,-1,-1)\\
(-1,-1,\ 0,-1;\ 0,+1,-1,\ 0) & (-1,-1,-1,\ 0;\ 0,+1,+1,+1)\\
(\ 0,-1,+1,\ 0;+1,+1,\ 0,+1) & (\ 0,-1,-1,-1;+1,+1,+1,\ 0)\\
(\ 0,+1,-1,\ 0;-1,-1,\ 0,-1) & (\ 0,+1,+1,+1;-1,-1,-1,\ 0)
\end{array}$$

$$\begin{array}{ll}
(+1,\ 0,+1,+1;\ 0,+1,-1,\ 0) & (\ 0,+1,+1,+1;+1,\ 0,\ 0,-1)\\
(-1,\ 0,-1,-1;\ 0,-1,+1,\ 0) & (\ 0,-1,-1,-1;-1,\ 0,\ 0,+1)\\
(\ 0,+1,-1,\ 0;+1,\ 0,+1,+1) & (+1,\ 0,\ 0,-1;\ 0,+1,+1,+1)\\
(\ 0,-1,+1,\ 0;-1,\ 0,-1,-1) & (-1,\ 0,\ 0,+1;\ 0,-1,-1,-1)
\end{array}$$

Tomando la primera solución de cada clase como representante, se tienen las siguientes seis cerraduras independientes:

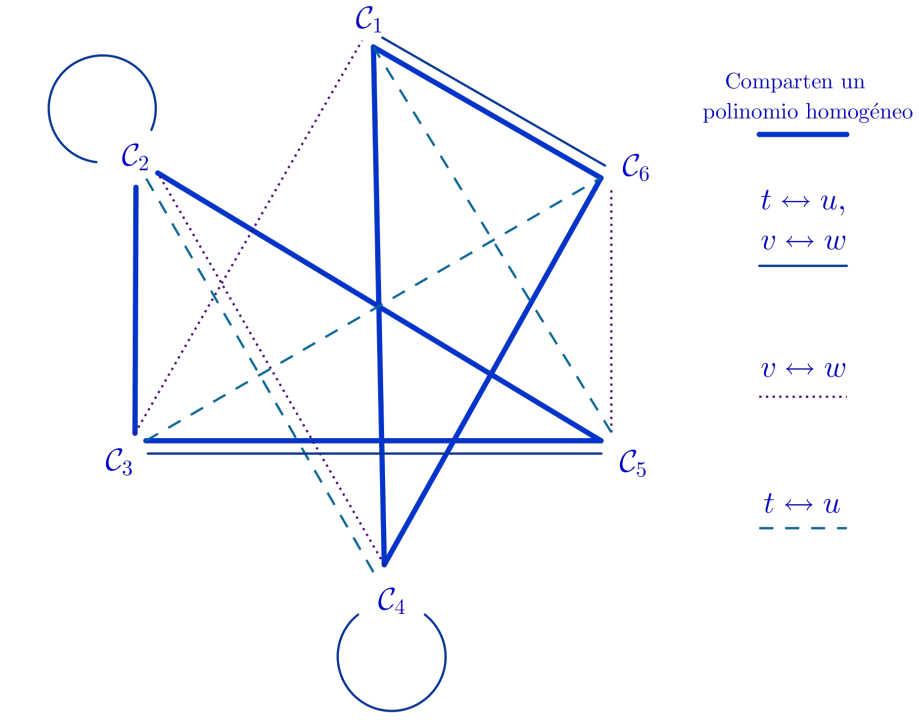
$$(t^2+tu+u^2)(v^2+vw+w^2) =$$

- $(tv+tw+uv)^2+(tv+tw+uv)(-tv+uw)+(-tv+uw)^2$ $(\mathcal{C}_1)$
- $(tv+tw+uw)^2+(tv+tw+uw)(-tv-uv-uw)+(-tv-uv-uw)^2$ $(\mathcal{C}_2)$
- $(tv+tw+uw)^2+(tv+tw+uw)(-tw+uv)+(-tw+uv)^2$ $(\mathcal{C}_3)$
- $(tv+tw+uv)^2+(tv+tw+uv)(-tw-uv-uw)+(-tw-uv-uw)^2$ $(\mathcal{C}_4)$
- $(tv+uv+uw)^2+(tv+uv+uw)(tw-uv)+(tw-uv)^2$ $(\mathcal{C}_5)$
- $(tw+uv+uw)^2+(tw+uv+uw)(tv-uw)+(tv-uw)^2$ $(\mathcal{C}_6)$

Aquí se observa nuevamente que la cantidad de cerraduras independientes es la misma que el número de representaciones de la unidad. Es una agradable sorpresa el encontrarse con seis cerraduras, pues pone de manifiesto propiedades interesantes. Algunos pares de cerraduras comparten totalmente un polinomio homogéneo, tal es el caso de $(\mathcal{C}_2)$ y $(\mathcal{C}_5)$, que comparten al polinomio $(tv+uv+uw)$, mientras se identifique a éste con su negativo.

Si se dibuja un grafo con los nombres de las cerraduras como vértices, uniendo dos de ellos con una arista cuando compartan un polinomio homogéneo, se obtienen dos triángulos separados. Además de esto, las cerraduras se transforman en otras haciendo intercambios de variables. Por ejemplo, $(\mathcal{C}_1)$ se convierte en $(\mathcal{C}_5)$ al hacer el intercambio $t \leftrightarrow u$. La figura 5 resume todas las relaciones halladas al analizarlo.

Figura 5. **Multigrafo de las cerraduras de $\langle 1, 1, 1\rangle$**



Fuente: elaboración propia, mediante *Geogebra 4*.

3.3.2. Representabilidad

Lema 10. *Si un número n puede ser escrito en la forma x^2+3y^2, entonces también puede ser escrito en la forma x^2+xy+y^2. Si n es múltiplo de 4, entonces el recíproco también es válido, esto es, si n se puede escribir en la segunda forma, entonces también en la primera.*

Demostración. Sea $\mathcal{T}$ la transformación definida mediante

$$(x,y) \mapsto (X,Y)$$
$$X = 2y$$
$$Y = x - y$$

La identidad $x^2+3y^2 = (2y)^2+(2y)(x-y)+(x-y)^2 = X^2+XY+Y^2$ muestra que la transformación $\mathcal{T}$ convierte representaciones (x,y) de la forma $\langle 1,0,3\rangle$, en representaciones (X,Y), correspondientes a la forma $\langle 1,1,1\rangle$.

Para la segunda parte, mediante un análisis en el módulo 4 se concluye que x, y deben ser pares, para que x^2+xy+y^2 sea múltiplo de 4. La identidad $4(x^2+xy+y^2) = (2x)^2+(2x)(2y)+(2y)^2 = (2x+y)^2+3y^2$, es todo lo que se necesita para inspirar la definición de una transformación análoga. □

Como se ha dicho anteriormente, Euler extendió los métodos para sumas de dos cuadrados, logrando abarcar la representación de primos en la forma x^2+3y^2. Su esfuerzo queda resumido en el siguiente resultado.

Teorema de Euler (primos de la forma x^2+3y^2)**.** *Un primo p es representable en $\langle 1,0,3\rangle$ si, y sólo si, p no es congruente con 2 en el módulo 3.*

La técnica es la misma que la usada en la sección anterior, pero ponerla en práctica en este nuevo contexto conlleva nuevas dificultades, hay que tomar en cuenta que a Euler le tomó varios años completar la prueba. También es un poco más larga,

así que sólo se señalará el camino que se debe seguir para llevarla a cabo, por motivos de espacio y también porque no aporta nada radicalmente nuevo al arsenal de métodos. Se recorrerán con Euler los pasos clave, y luego se retornará al tema principal, que es la forma $x^2 + xy + y^2$. Antes de ello, una definición más se hace necesaria por el frecuente uso.

Definición (representación propia)**.** Si (a, b) es una representación del número n en una forma cuadrática $\mathfrak{q}$, tal que $\text{MCD}(a, b) = 1$, se dice que (a, b) es una *representación propia* de n en esa forma.

Bosquejo de la demostración. La prueba se desglosa nuevamente en dos proposiciones principales, *descenso* y *reciprocidad*, que se demuestran siguiendo los mismos pasos empleados para la forma $x^2 + y^2$. En lo que sigue, p es un primo impar arbitrario.

Descenso: Si p divide a un número n que posee una representación propia en la forma $x^2 + 3y^2$, entonces p también es (propiamente) representable.

Reciprocidad: Si $p \equiv 1 \pmod 3$, entonces p es divisor de algún n que es propiamente representable en la forma $x^2 + 3y^2$.

Los pasos 1 al 4 de la demostración de Euler para $\langle 1, 0, 1\rangle$ servirán de guía para fabricar una prueba del *descenso*. Deben emplearse ahora las identidades de Brahmagupta correspondientes, y utilizar el módulo 3 en lugar del 4, estas diferencias son fáciles de notar. Lo que puede constituir una complicación más sutil, es que el primo 2 no es representable, y por ello se exige que p sea un primo impar. Esto es problemático en el paso 3, en el que se debe considerar un m impar, y se tiene que generar un factor de $\frac{n}{m}$, también impar, que no sea representable.

En el paso 5 se necesita ingenio para lograr la modificación. Suponiendo que $p = 3k + 1$, donde $k \in \mathbb{N}$, el siguiente polinomio es jugará el papel de aquél que fue empleado en la congruencia (3.8) de la página 75.

$$4(x^{3k} - 1) = (x^k - 1)((2x^k + 1)^2 + 3 \cdot 1^2) \tag{3.10}$$

Se emplea una vez más el pequeño teorema de Fermat, y el teorema de Lagrange sobre la cantidad de raíces de una congruencia polinomial, para deducir que existen números que anulan al segundo factor en el módulo p. Pero este factor es la representación propia de algún número en la forma $\langle 1, 0, 3\rangle$, así que puede concluirse vía el paso 4, al igual que antes. $\square$

Teorema 10. *Un primo p es representable en la forma $x^2 + xy + y^2$ si, y sólo si, p no es congruente con 2 en el módulo 3.*

Demostración. Primero nótese que $3 = 1^2 + 1 \cdot 1 + 1^2$. En virtud del lema 10 y el teorema de Euler, lo único que falta probar es que los primos congruentes con 2 en el módulo 3 no son representables. Basta una inspección local de todos los casos en dicho módulo para concluir que la congruencia $x^2 + xy + y^2 \equiv 2 \pmod 3$ no tiene soluciones y, por lo tanto, estos primos no tienen representación. $\square$

Los argumentos de la sección anterior pueden ser modificados y resulta que, para que un número compuesto sea representable en la forma $\langle 1, 1, 1\rangle$, no debe aparecer en su factorización en primos uno que sea congruente con 2 en el módulo 3, elevado a una potencia impar. La cantidad de representaciones es algo que también puede ser estudiado siguiendo los lineamientos que ya se han presentado. Se omitirán estos detalles para pasar a otros temas que resulten más atractivos, puesto que tratan sobre conceptos que aún no han sido tocados.

Para cerrar el capítulo cabe decir que los métodos expuestos pueden ser usados en el estudio de una familia pequeña pero importante de formas cuadráticas. Entre los resultados adicionales que pueden obtenerse, vale la pena mencionar el caso de las formas de Pell $\langle 1, 0, -d\rangle$, donde d es un número natural que no es cuadrado perfecto. Puesto que estas formas poseen infinitas representaciones de la unidad, según lo expuesto en el marco teórico, entonces tienen también infinitas cerraduras independientes. Las exhaustiones se convierten en un método sin fin, que continúa generando cerraduras conforme se emplean nuevas representaciones. Varios patrones interesantes pueden ser señalados en la frecuencia y distribución de las soluciones del sistema de las cerraduras reducidas (Véase el problema 26, apéndice D).

4. $\mathbb{Z}$-FORMAS: CERRADURAS MÁS GENERALES

Se ha empleado en numerosas ocasiones el método de exhaustión en la generación de cerraduras para formas cuadráticas específicas. La pregunta de si todas las formas cuadráticas poseen al menos una cerradura se responde negativamente, ofreciendo un contraejemplo. La forma $2x^2 + 3y^2$ puede representar al número 2, pero es incapaz de representar al 4, y en consecuencia no posee ninguna cerradura (homogénea o de otro tipo). De inmediato se observa que es una forma cuadrática en la que la unidad no posee representaciones.

Podría entonces atribuirse la inexistencia de cerraduras a la mencionada ausencia de representaciones para la unidad, pero otro contraejemplo viene a desmoronar la hipótesis que se había manejado de que el número de cerraduras tiene que estar ligado con la cantidad de representaciones del 1. La forma $2x^2 + 3xy + 4y^2$ es incapaz de representarlo, pero posee una cerradura independiente, que es

$$(2t^2 + 3tu + 4u^2)(2v^2 + 3vw + 4w^2) =$$
$$2(2tw + 2uv + 3uw)^2 + 3(2tw + 2uv + 3uw)(tv - 2uw) + 4(tv - 2uw)^2$$

No se debe tomar tan a pecho lo anterior. Es perfectamente posible que, para las formas que sí representen a la unidad, exista alguna relación algebraica entre la cantidad de cerraduras independientes, la cantidad de simetrías que posea la forma, y el número de representaciones que posee la unidad (véase la última sección del capítulo, y el problema 50, apéndice D). Por otro lado, se demostrará más adelante que todas las formas que representan a la unidad poseen al menos una cerradura.

Independientemente de ello, un buen punto de partida para la búsqueda de cerraduras generales de una familia de formas cuadráticas, es exigir que todos los miembros de la familia representen a la unidad. La identidad de Brahmagupta es un ejemplo de lo que se busca, correspondiente a la familia $\{ \langle 1, 0, n\rangle : n \in \mathbb{N} \}$, pero se pretende mayor generalidad.

4.1. Formas mónicas en una de las variables

Las formas del tipo $\langle 1, b, c\rangle$ o, equivalentemente, $\langle a, b, 1\rangle$, son llamadas *formas mónicas*, pues esa palabra se usa para designar polinomios cuyo coeficiente principal, respecto a alguna de sus variables, es 1. Sin pérdida de la generalidad, considérese únicamente el tipo $\langle 1, b, c\rangle$. Todas las formas mónicas tienen, por lo menos, dos representaciones de la unidad: $(1, 0)$ y $(-1, 0)$. En lo que sigue se modificará el método de exhaustión para que opere en expresiones algebraicas que dependen de b y c, en lugar de números fijos. Deliberadamente se menguará su alcance para obtener una cantidad finita de evaluaciones por realizar, pues no es preciso encontrar todas las cerraduras generales para las formas mónicas, sino por lo menos una.

La primera suposición es que la cerradura general —si ésta existe— es reducida, lo cual es razonable pues todas las encontradas anteriormente son de esta clase. Ahora bien, el plan es considerar expresiones del tipo $\mu_1 a + \mu_2 b + \mu_3 c = \mu_1 + \mu_2 b + \mu_3 c$ para que ocupen el lugar de cada coeficiente h_i, k_i en las exhaustiones. Un polinomio homogéneo lineal es lo más simple que se puede probar, además de esto, las cerraduras de Brahmagupta cumplen con el criterio, cosa que da esperanza. Para fijar ideas, se usará el símbolo μ^i cuando se trate de un coeficiente h_i, haciendo coincidir el superíndice con el subíndice. Para los coeficientes k_i se usará ν^i, esto es

$$\begin{aligned} h_i &= \mu_1^i + \mu_2^i b + \mu_3^i c \\ k_i &= \nu_1^i + \nu_2^i b + \nu_3^i c \end{aligned}$$

Parece poco probable que los coeficientes μ, ν tengan valores distintos a $1, 0, -1$, pues las cerraduras generales deben colapsar en las de Brahmagupta cuando se tome $b = 0$. También, si se exige $b = c = 1$, deberían convertirse en algunas de las 24 cerraduras de la forma cuadrática $\langle 1, 1, 1\rangle$, que no involucran coeficientes mayores que 1, o menores que -1. Esta última condición logra limitar la búsqueda a una cantidad finita de evaluaciones: ¡solamente son 3^{24}!

Afortunadamente, las ecuaciones R-1, R-3, R-7, R-9 (ver abajo) del sistema de cerraduras reducidas sólo involucran dos coeficientes cada una, y son independientes

de las otras, así que puede aplicarse la exhaustión a cada una de ellas por separado. Aún así, se trata de la considerable cantidad de 729 evaluaciones por cada ecuación. Sin embargo, es posible hacer una suposición adicional que simplifique el trabajo.

Se asumirá que para cada h_i, al menos dos de las tres μ_j^i se anulan, y lo mismo para los k_i. La evidencia a favor la constituyen nuevamente las cerraduras que han sido halladas previamente. De lo contrario, algunos de los coeficientes h_i, k_i podrían tomar valores mayores en valor absoluto que 1 en las formas $\langle 1,0,-1\rangle, \langle 1,0,1\rangle, \langle 1,1,1\rangle$, a menos que se den condiciones especiales en los signos de los μ, ν, que son engorrosas de traducir a un algoritmo para que una computadora lleve a cabo los cálculos. Así que se trabajará con la última suposición, y si esto fallara, debe retornarse a las exhaustiones más largas. ¡Se ha reducido el trabajo a 49 opciones por ecuación! con la esperanza de que sean suficientes. Para contextualizar, el sistema de ecuaciones de las cerraduras reducidas para una forma mónica es

$$
\text{sistema}\begin{cases}
\text{bloque } t^2 \begin{cases}
1 &= h_1^2 + bh_1k_1 + ck_1^2 & \text{(R-1)}\\
b &= 2h_1h_2 + b(h_1k_2 + h_2k_1) + 2ck_1k_2 & \text{(R-2)}\\
c &= h_2^2 + bh_2k_2 + ck_2^2 & \text{(R-3)}
\end{cases}\\
\text{bloque } tu \begin{cases}
b &= 2h_1h_3 + b(h_1k_3 + h_3k_1) + 2ck_1k_3 & \text{(R-4)}\\
b^2 &= 2(h_1h_4 + h_2h_3) + b(h_1k_4 + h_4k_1 + & \\
 & \quad h_2k_3 + h_3k_2) + 2c(k_1k_4 + k_2k_3) & \text{(R-5)}\\
bc &= 2h_2h_4 + b(h_2k_4 + h_4k_2) + 2ck_2k_4 & \text{(R-6)}
\end{cases}\\
\text{bloque } u^2 \begin{cases}
c &= h_3^2 + bh_3k_3 + ck_3^2 & \text{(R-7)}\\
bc &= 2h_3h_4 + b(h_3k_4 + h_4k_3) + 2ck_3k_4 & \text{(R-8)}\\
c^2 &= h_4^2 + bh_4k_4 + ck_4^2 & \text{(R-9)}
\end{cases}
\end{cases}
$$

En la tabla IX se llevan a cabo las 49 evaluaciones, en las que se han omitido los subíndices de los h_i, k_i, para poder emplear la misma evaluación en las cuatro ecuaciones R-1, R-3, R-7 y R-9. Así por ejemplo, el par (h,k) que resuelva a R-3 se deberá interpretar como (h_2, k_2). Posteriormente se evalúa cuáles combinaciones resuelven R-2 y R-8, completando la exhaustión que fue apodada «menor» anteriormente, y por último se realiza la exhaustión «mayor», esto es, la del bloque tu.

Tabla IX. **Primera exhaustión algebraica para $\langle 1, b, c\rangle$**

h	k	$h^2+bhk+ck^2$	R-1	R-3	R-7	R-9
0	0	0	·	·	·	·
0	1	c	·	✓	✓	·
0	−1	c	·	✓	✓	·
0	b	b^2c	·	·	·	·
0	$-b$	b^2c	·	·	·	·
0	c	c^3	·	·	·	·
0	$-c$	c^3	·	·	·	·
1	0	1	✓	·	·	·
1	1	$1+b+c$	·	·	·	·
1	−1	$1-b+c$	·	·	·	·
1	b	$1+b^2+b^2c$	·	·	·	·
1	$-b$	$1-b^2+b^2c$	·	·	·	·
1	c	$1+bc+c^3$	·	·	·	·
1	$-c$	$1-bc+c^3$	·	·	·	·
−1	0	1	✓	·	·	·
−1	1	$1-b+c$	·	·	·	·
−1	−1	$1+b+c$	·	·	·	·
−1	b	$1-b^2+b^2c$	·	·	·	·
−1	$-b$	$1+b^2+b^2c$	·	·	·	·
−1	c	$1-bc+c^3$	·	·	·	·
−1	$-c$	$1+bc+c^3$	·	·	·	·
b	0	b^2	·	·	·	·
b	1	$2b^2+c$	·	·	·	·
b	−1	c	·	✓	✓	·
b	b	$b^2+b^3+b^2c$	·	·	·	·
b	$-b$	$b^2-b^3+b^2c$	·	·	·	·
b	c	$b^2+b^2c+c^3$	·	·	·	·
b	$-c$	$b^2-b^2c+c^3$	·	·	·	·

continúa

h	k	$h^2+bhk+ck^2$	R-1	R-3	R-7	R-9
$-b$	0	b^2	·	·	·	·
$-b$	1	c	·	✓	✓	·
$-b$	-1	$2b^2+c$	·	·	·	·
$-b$	b	$b^2-b^3+b^2c$	·	·	·	·
$-b$	$-b$	$b^2+b^3+b^2c$	·	·	·	·
$-b$	c	$b^2-b^2c+c^3$	·	·	·	·
$-b$	$-c$	$b^2+b^2c+c^3$	·	·	·	·
c	0	c^2	·	·	·	✓
c	1	$c+bc+c^2$	·	·	·	·
c	-1	$c-bc+c^2$	·	·	·	·
c	b	$2b^2c+c^2$	·	·	·	·
c	$-b$	c^2	·	·	·	✓
c	c	$c^2+bc^2+c^3$	·	·	·	·
c	$-c$	$c^2-bc^2+c^3$	·	·	·	·
$-c$	0	c^2	·	·	·	✓
$-c$	1	$c-bc+c^2$	·	·	·	·
$-c$	-1	$c+bc+c^2$	·	·	·	·
$-c$	b	c^2	·	·	·	✓
$-c$	$-b$	$2b^2c+c^2$	·	·	·	·
$-c$	c	$c^2-bc^2+c^3$	·	·	·	·
$-c$	$-c$	$c^2+bc^2+c^3$	·	·	·	·

Fuente: elaboración propia mediante Wolfram Mathematica 8.

La tabla anterior se interpreta de la siguiente manera. Si el par (h,k) toma, por ejemplo, los valores $(b,-1)$, entonces el cheque en la columna R-7 indica que las expresiones siguientes son candidatas para (h_3,k_3).

$$h_3=\mu_1^3+\mu_2^3b+\mu_3^3c=(0)+(1)b+(0)c$$
$$k_3=\nu_1^3+\nu_2^3b+\nu_3^3c=(-1)+(0)b+(0)c$$

Ahora, en la tabla X, se verificará cuáles parejas de soluciones de R-1 y R-3 cumplen con R-2, y justo después se llevará a cabo una revisión análoga para R-8.

Tabla X. **Segunda exhaustión algebraica para $\langle 1, b, c\rangle$**

h_1	k_1	h_2	k_2	$2h_1h_2 + b(h_1k_2 + h_2k_1) + 2ck_1k_2$	R-2
1	0	0	1	b	✓
1	0	0	-1	$-b$	·
1	0	b	-1	b	✓
1	0	$-b$	1	$-b$	·
-1	0	0	1	$-b$	·
-1	0	0	-1	b	✓
-1	0	b	-1	$-b$	·
-1	0	$-b$	1	b	✓
h_3	k_3	h_4	k_4	$2h_3h_4 + b(h_3k_4 + h_4k_3) + 2ck_3k_4$	R-8
0	1	c	0	bc	✓
0	1	c	$-b$	$-bc$	·
0	1	$-c$	0	$-bc$	·
0	1	$-c$	b	bc	✓
0	-1	c	0	$-bc$	·
0	-1	c	$-b$	bc	✓
0	-1	$-c$	0	bc	✓
0	-1	$-c$	b	$-bc$	·
b	-1	c	0	bc	✓
b	-1	c	$-b$	$-b^3 + 3bc$	·
b	-1	$-c$	0	$-bc$	·
b	-1	$-c$	b	$b^3 - 3bc$	·
$-b$	1	c	0	$-bc$	·
$-b$	1	c	$-b$	$b^3 - 3bc$	·
$-b$	1	$-c$	0	bc	✓
$-b$	1	$-c$	b	$-b^3 + 3bc$	·

Fuente: elaboración propia mediante Wolfram Mathematica 8.

Hasta el momento no ha fracasado el método, pues la tabla anterior muestra cuatro soluciones (h_1, k_1, h_2, k_2) para el bloque t^2, y seis soluciones (h_3, k_3, h_4, k_4) para el bloque u^2. Se dispone entonces de 24 candidatos $(h_1, k_1, h_2, k_2, h_3, k_3, h_4, k_4)$ para soluciones globales, y falta revisar si alguno de ellos cumple con el bloque tu. Dicha revisión es llevada a cabo en la tabla XI. Nótese que si existiera en la tabla alguna solución al sistema, se deben reordenar las variables, colocando las h_i al principio del octeto y dejando las k_i al final, para tenerlas en el formato que se ha manejado hasta ahora, y que se traduce inmediatamente en las cerraduras.

Tabla XI. **Exhaustión algebraica final para $\langle 1, b, c\rangle$**

h_1	k_1	h_2	k_2	h_3	k_3	h_4	k_4	R-4	R-5	R-6	✓
1	0	0	1	0	1	c	0	b	$4c$	bc	·
1	0	0	1	0	1	$-c$	b	b	b^2	bc	✓
1	0	0	1	0	-1	c	$-b$	$-b$	$-b^2$	$-bc$	·
1	0	0	1	0	-1	$-c$	0	$-b$	$-4c$	$-bc$	·
1	0	0	1	b	-1	c	0	b	b^2	bc	✓
1	0	0	1	$-b$	1	$-c$	0	$-b$	$-b^2$	$-bc$	·
1	0	b	-1	0	1	c	0	b	b^2	bc	✓
1	0	b	-1	0	1	$-c$	b	b	$2b^2 - 4c$	$b^3 - 3bc$	·
1	0	b	-1	0	-1	c	$-b$	$-b$	$-2b^2 + 4c$	$-b^3 + 3bc$	·
1	0	b	-1	0	-1	$-c$	0	$-b$	$-b^2$	$-bc$	·
1	0	b	-1	b	-1	c	0	b	$4c$	bc	·
1	0	b	-1	$-b$	1	$-c$	0	$-b$	$-4c$	$-bc$	·
-1	0	0	-1	0	1	c	0	$-b$	$-4c$	$-bc$	·
-1	0	0	-1	0	1	$-c$	b	$-b$	$-b^2$	$-bc$	·
-1	0	0	-1	0	-1	c	$-b$	b	b^2	bc	✓
-1	0	0	-1	0	-1	$-c$	0	b	$4c$	bc	·
-1	0	0	-1	b	-1	c	0	$-b$	$-b^2$	$-bc$	·
-1	0	0	-1	$-b$	1	$-c$	0	b	b^2	bc	✓

continúa

h_1	k_1	h_2	k_2	h_3	k_3	h_4	k_4	R-4	R-5	R-6	✓
-1	0	$-b$	1	0	1	c	0	$-b$	$-b^2$	$-bc$	·
-1	0	$-b$	1	0	1	$-c$	b	$-b$	$-2b^2+4c$	$-b^3+3bc$	·
-1	0	$-b$	1	0	-1	c	$-b$	b	$2b^2-4c$	b^3-3bc	·
-1	0	$-b$	1	0	-1	$-c$	0	b	b^2	bc	✓
-1	0	$-b$	1	b	-1	c	0	$-b$	$-4c$	$-bc$	·
-1	0	$-b$	1	$-b$	1	$-c$	0	b	$4c$	bc	·

Fuente: elaboración propia mediante Wolfram Mathematica 8.

¡Se han producido soluciones! No será necesario realizar una exhaustión más completa. Como todas las formas $\langle 1, b, c\rangle$ poseen en común dos simetrías, se pueden aparejar las soluciones de la siguiente manera.

$$\begin{array}{l}(\ 1,\ 0,\ 0,-c\,;\ 0,\ 1,\ 1,\ b\,)\\(-1,\ 0,\ 0,\ c\,;\ 0,-1,-1,-b\,)\end{array}$$

$$\begin{array}{l}(\ 1,\ 0,\ b,\ c\,;\ 0,\ 1,-1,\ 0\,)\\(-1,\ 0,-b,-c\,;\ 0,-1,\ 1,\ 0\,)\end{array}$$

$$\begin{array}{l}(\ 1,\ b,\ 0,\ c\,;\ 0,-1,\ 1,\ 0\,)\\(-1,-b,\ 0,-c\,;\ 0,\ 1,-1,\ 0\,)\end{array}$$

Podrían existir otras cerraduras generales para las formas mónicas, pero éstas son las únicas tales que los coeficientes de sus polinomios homogéneos en las variables t, u, v, w son monomios en las constantes a, b, c de la forma, de coeficiente ± 1. Las cerraduras independientes son:

$$(t^2+btu+cu^2)(v^2+bvw+cw^2) =$$

- $(tv-cuw)^2+b(tv-cuw)(tw+uv+buw)+c(tw+uv+buw)^2$ $(\mathcal{M}_1)$
- $(tv+buv+cuw)^2+b(tv+buv+cuw)(tw-uv)+c(tw-uv)^2$ $(\mathcal{M}_2)$
- $(tv+btw+cuw)^2+b(tv+btw+cuw)(-tw+uv)+c(-tw+uv)^2$ $(\mathcal{M}_3)$

Parece extraño encontrar tres cerraduras independientes para todas las formas mónicas, cuando las formas del tipo $\langle 1, 0, n\rangle$, que son mónicas, poseen solamente dos. La razón de ello es que la palabra «independientes» cambia de significado conforme se reduce la cantidad de formas cuadráticas consideradas. Así, las cerraduras $\mathcal{M}_2$ y $\mathcal{M}_3$ colapsan en una sola cuando se toma $b = 0$.

Anteriormente se había observado que las cerraduras de la forma $\langle 1, 1, 1\rangle$ se organizaban en tríos en más de una manera (Figura 5). Con la familia mónica, una vez más, el número tres juega un papel importante, sin embargo, no es el caso que la ternaridad de la familia sea la responsable de las relaciones expuestas en el grafo. Las cerraduras $\mathcal{M}_1, \mathcal{M}_2, \mathcal{M}_3$ se convierten respectivamente en $\mathcal{C}_6, \mathcal{C}_5, \mathcal{C}_3$, al tomar $b = c = 1$. Aquí no se visualiza ningún patrón obvio. Las formas mónicas en la otra variable, $\langle a, b, 1\rangle$, poseen también tres cerraduras, pero éstas no se transforman en las $\mathcal{C}_i$ restantes al tomar $a = b = 1$, sino que corresponden a las cerraduras $\mathcal{C}_1, \mathcal{C}_3, \mathcal{C}_5$, aumentando el misterio.

4.2. Otras cerraduras

La tricerradura de Arnol'd-Aicardi, que se discutirá más adelante, revelará al menos una parte del enigma. Aún así, el esquema general que organiza la intrincada estructura de las cerraduras permanece oculto en su propia complejidad.

4.2.1. Formas de discriminante nulo

Este tema se incluye en el documento no tanto por su importancia, como por motivos de completitud. El propósito es poner de manifiesto un extraño tipo de cerraduras posiblemente exclusivo de la familia de formas con discriminante nulo.

Definición (forma cuadrado perfecto)**.** Se le llamará ℤ-*forma cuadrado perfecto* a cualquier miembro de la familia $\{\, \langle a^2, 2ab, b^2\rangle \,:\, a, b \in \mathbb{Z}\}$.

Se puede demostrar fácilmente que una $\mathbb{Z}$-forma cuadrática binaria es una $\mathbb{Z}$-forma cuadrado perfecto si, y sólo si, su discriminante vale cero (la necesidad es casi inmediata, la suficiencia requiere un argumento simple). Muchos autores descartan las formas cuadrado perfecto por motivo de su trivialidad. Aquí se rescindirá de tal convenio porque dichas formas poseen cerraduras no homogéneas, y esto es algo que merece ser examinado con más detalle.

Sean a, b enteros dados. Como su nombre lo indica, una forma cuadrado perfecto se puede factorizar de la siguiente manera: $a^2x^2 + 2abxy + b^2y^2 = (ax + by)^2$. Todas ellas son cerradas bajo el producto. En virtud de la ecuación (2.2) de la página 38, sus cerraduras homogéneas son expresiones del tipo

$$(at + bu)^2(av + bw)^2 = (aX + bY)^2$$

en la cual X, Y son polinomios cuadráticos homogéneos en las variables t, u, v, w. Si se multiplican bajo el cuadrado los factores del miembro izquierdo de la ecuación, se pueden fabricar fácilmente cerraduras homogéneas, factorizando los coeficientes comunes a, b. Esto se puede hacer de varias maneras, una de ellas es

$$[(at+bu)(av+bw)]^2 = [a^2tv+abtw+abuv+b^2uw]^2 = [a(atv+btw)+b(auv+buw)]^2$$

donde $X = atv + btw$, $Y = auv + buw$. Ahora, recordando la forma en la que se generan todas las soluciones de una ecuación diofantina lineal, es válido sumarle a X y Y expresiones que se cancelen mutuamente al expandir. Sea $F = F(t, u, v, w)$ cualquier función (no tiene que ser un polinomio), entonces la siguiente también es una identidad de cerradura:

$$(at + bu)^2(av + bw)^2 = [a(atv + btw + bF) + b(auv + buw - aF)]^2$$

La expresión anterior engloba cerraduras homogéneas no reducidas, e incluso cerraduras no homogéneas. En referencia al escolio 3 de la página 55, la cerradura anterior es evidencia de que no existe un teorema general que asegure lo mismo para todas las formas cuadráticas. Aún si se descartan aquellas que son cuadrado perfecto, la prueba podría resultar muy elusiva debido a irregularidades como la anterior. Es un problema abierto el de determinar la existencia de cerraduras no reducidas para formas cuyo discriminante sea no nulo (véase el problema 51, apéndice D).

4.2.2. La tricerradura de Arnol'd-Aicardi

Según se vio anteriormente, no todas las formas cuadráticas son cerradas bajo el producto. De hecho, la evidencia numérica señala que la mayoría de las formas, en el sentido de la densidad, poseen esta insatisfactoria característica. En sus escritos, Vladimir Arnol'd[1] llamó *formas perfectas* a aquellas que sí poseyeran la propiedad de cerradura, aunque el término fue utilizado por Voronoi a principios del siglo XX, con un significado distinto [1]. Después de realizar unos cuantos miles de ejemplos numéricos, Arnol'd conjeturó que todas las formas poseen una característica asombrosa que él bautizó «la propiedad del trigrupo». Él observó que todas las formas parecían cumplir que el producto de tres números representables también es representable.

Una *tricerradura de una forma cuadrática* $\mathfrak{q}(x,y) = \langle a,b,c\rangle$ es una identidad algebraica del tipo

$$\mathfrak{q}(r,s)\cdot\mathfrak{q}(t,u)\cdot\mathfrak{q}(v,w) = \mathfrak{q}(X,Y) \tag{4.1}$$

donde X, Y son polinomios cúbicos homogéneos en las variables r, s, t, u, v, w. Todas las tricerraduras no triviales conocidas hasta ahora son tales que el vector (X,Y) depende trilinealmente de los vectores $(r,s),(t,u),(v,w)$. Al igual que con las cerraduras ordinarias, el nombre se aplicará también a conjuntos de identidades correspondientes a familias de formas. La matemática Francesca Aicardi encontró una tricerradura asociada a la familia más general posible, la compuesta por todas las formas cuadráticas, con lo cual demostró la conjetura de Arnol'd. Ya conociendo la identidad hallada por Aicardi, ésta puede ser demostrada por una simple expansión, al igual que las cerraduras encontradas previamente para las formas mónicas.

[1] **Vladimir Igorevich Arnol'd** (1937 – 2010), nacido en la Rusia soviética, fue uno de los matemáticos más prolíficos de nuestros tiempos. A la edad de 19 años, mientras era estudiante de Andrey Kolmogorov en la Universidad Estatal de Moscú, Arnol'd demostró que cualquier función continua de varias variables puede ser construida con un número finito de funciones de dos variables, resolviendo de manera parcial el *décimo tercer problema de Hilbert*. Es considerado el fundador de la Topología Simplética y en el 2006 se reportó que poseía el índice de citación más alto de Rusia. También es recordado por su sentido del humor. Por ejemplo, al inicio del año en su seminario, cuando acostumbraba formular nuevos problemas, dijo en una ocasión: «Hay un principio general que dice que un hombre estúpido puede hacer preguntas tales que ni siquiera cien sabios serían capaces de contestar. En conformidad con este principio, permítanme formular algunos problemas».

Teorema 11 (trigrupo)**.** *Toda $\mathbb{Z}$-forma cuadrática binaria posee la propiedad del trigrupo, esto es, el conjunto de números representables es cerrado bajo el producto de tríos de ellos.*

Demostración. Sea $\langle a, b, c\rangle$ una $\mathbb{Z}$-forma arbitraria. En referencia a la identidad (4.1), se pueden definir los polinomios X, Y mediante:

$$X = artv - csuv + cstw + cruw + brtw$$
$$Y = aruv + astv + bsuv + csuw - artw$$

Ahora bien, sustituyendo estos polinomios en (4.1) y expandiendo ambos miembros se obtienen dos expresiones de 52 términos cada una, entre las cuales se puede verificar la identidad. □

Si se deseara encontrar polinomios X, Y correspondientes a una cerradura para las formas mónicas, sin fraccionar ingeniosamente el sistema mostrado en la página 93 para llevar a cabo exhaustiones más pequeñas, sino que se intentara resolver simultáneamente las nueve ecuaciones, los cálculos tomarían aproximadamente una hora y media, haciendo uso de una computadora de dos núcleos tal como la empleada para escribir este documento.

Para lograr lo mismo con la tricerradura, la exhaustión se llevaría a cabo en más de 500 años,[2] asumiendo que no se agotara la memoria, cosa que puede ser evitada con un código cuidadoso. Si se dispusiera de 1000 computadoras de 24 núcleos, el mismo cálculo se podría llevar a cabo en días. En vista de ello, el método es aplicable, aunque no es del todo práctico en términos del poder computacional actual. Por supuesto, haciendo uso del ingenio, los cálculos son mucho más accesibles, al igual que en el caso de las formas mónicas, cuyo tiempo de ejecución se reduce a menos de un segundo.

Arnol'd indica que la tricerradura puede ser empleada para demostrar algunas proposiciones interesantes relativas a la existencia de cerraduras para familias de formas [4]. Por ejemplo, si una forma $\mathfrak{q}$ representa al número 1, entonces se puede tomar

[2] Cálculo hecho con base en los resultados del comando `Timing[]` de *Mathematica 8*, aplicado a un pequeño fragmento de la exhaustión. Procesador: Intel Core 2 Duo @ 2,93GHz.

(r, s) como una representación de la unidad, y la tricerradura (4.1) se transforma en una cerradura convencional. Esto demuestra la siguiente proposición.

Corolario 11. *Toda forma cuadrática que represente a la unidad es perfecta, esto es, la multiplicación de dos números representables en dicha forma también es representable.*

Aicardi también encontró una forma matricial de representar a las fórmulas para X, Y propuestas en la demostración del teorema 11. Según la descripción dada en la página 37, a cada forma cuadrática $\mathfrak{q} = \langle a, b, c\rangle$ se le asocia biyectivamente una matriz $\mathbf{M}_{\mathfrak{q}} = \left(\begin{smallmatrix} a & b/2 \\ b/2 & c \end{smallmatrix}\right)$. Esta matriz puede ser empleada para describir a la forma cuadrática $\mathfrak{q}$, como fue planteado en (2.1). Si se emplean dos vectores distintos en el producto, en lugar de una forma cuadrática se obtiene una forma bilineal simétrica $\mathfrak{B}_{\mathfrak{q}}$. Para fijar ideas, dados dos vectores variables $\mathbf{x} = (x_1, x_2),\ \mathbf{y} = (y_1, y_2)$, la forma bilineal simétrica asociada a la forma cuadrática $\mathfrak{q}$ actúa sobre ellos así:

$$\begin{aligned}\mathfrak{B}_{\mathfrak{q}}(\mathbf{x}, \mathbf{y}) = \mathbf{x}\ \mathbf{M}_{\mathfrak{q}}\ \mathbf{y}' &= (x_1, x_2) \begin{pmatrix} a & {}^{b}/_{2} \\ {}^{b}/_{2} & c \end{pmatrix} \begin{pmatrix} y_1 \\ y_2 \end{pmatrix} \\ &= ax_1y_1 + \tfrac{b}{2}(x_1y_2 + x_2y_1) + cx_2y_2\end{aligned}$$

Ahora bien, bautizando $\mathbf{r}, \mathbf{t}, \mathbf{v}, \mathbf{X}$ a los vectores $(r, s), (t, u), (v, w), (X, Y)$ respectivamente, entonces la tricerradura se puede escribir como: $\mathfrak{q}(\mathbf{r}) \cdot \mathfrak{q}(\mathbf{t}) \cdot \mathfrak{q}(\mathbf{v}) = \mathfrak{q}(\mathbf{X})$, y la fórmula matricial hallada por Aicardi es:

$$\mathbf{X} = \mathfrak{B}_{\mathfrak{q}}(\mathbf{r}, \mathbf{t})\mathbf{v} + \mathfrak{B}_{\mathfrak{q}}(\mathbf{t}, \mathbf{v})\mathbf{r} - \mathfrak{B}_{\mathfrak{q}}(\mathbf{v}, \mathbf{r})\mathbf{t} \tag{4.2}$$

Esta fórmula es sumamente interesante debido a la antisimetría originada por el último signo negativo. Si se intercambian cíclicamente los vectores $\mathbf{r}, \mathbf{t}, \mathbf{v}$ se producen tres tricerraduras distintas. Este hecho, y la propia estructura ternaria de la tricerradura, son causas de las agrupaciones en tríos que fueron observadas previamente en las cerraduras de las formas mónicas. Aún así, quedan varios problemas sin resolver, quizá el más grande de ellos sea el de determinar si existen otras tricerraduras.

4.3. Otros resultados clásicos e investigaciones modernas

Esta sección se fundamenta en el documento escrito por A.G. Earnest y Robert W. Fitzgerald, que se intitula *Multiplicative Properties of Integral Binary Quadratic Forms* [13], publicado en el 2009, y el ensayo no publicado *Composition and Bhargava's Cubes*, escrito por Florian Bouyer del Instituto Matemático de Warwick, en el 2012. Se incluyen estos temas con el propósito de ofrecer una vista panorámica del trabajo que se ha hecho en la teoría de cerraduras, durante los últimos años.

Para obtener una mejor apreciación de estos avances, se debe introducir un concepto cuya mención ya ha sido postergada demasiado: la *composición Gaussiana*. A lo largo de la sección, con el término *forma* se hara referencia exclusiva a $\mathbb{Z}$-formas binarias cuadráticas no degeneradas, esto es, aquellas tales que su discriminante es no nulo, aunque algunos aspectos aplican también a formas degeneradas. Se enunciarán varios resultados sin ofrecer demostración, algunos de los cuales pueden ser hallados como problemas en el apéndice D.

Notación. Si $\mathfrak{q}$ es una forma, $\mathscr{D}(\mathfrak{q})$ denotará el conjunto de números enteros representables mediante $\mathfrak{q}$. A la forma $\langle a, b, c\rangle$ se le llama *primitiva* si $\text{MCD}(a, b, c) = 1$.

4.3.1. Composición de formas

Muchos opinan que la composición gaussiana es un verdadero *tour de force*, un logro difícilmente igualable para la humanidad, incluso tal vez para el propio Gauss. Si se quisiera hablar apropiadamente de ella se necesitaría un libro completo, así que se limitará el discurso para abarcar algunas generalidades. Una definición fundamental para el tema es la del concepto de *equivalencia propia*.

Definición (tipos de equivalencia)**.** Se dice que dos formas $\mathfrak{f}, \mathfrak{g}$ son *equivalentes*, denotado $\mathfrak{f} \sim \mathfrak{g}$, si existe una transformación unimodular $\mathcal{T}$ (ver sección 2.4) que convierta una en la otra; o, en la notación de la sección 2.3, tal que $\mathfrak{f} \overset{\mathcal{T}}{\longmapsto} \mathfrak{g}$. Si la

matriz asociada a $\mathcal{T}$ tiene determinante 1, entonces se dice que la equivalencia es *propia*, y es denotada por $\overset{+}{\sim}$ en tanto que si fuera -1, se dice que es *impropia*.

Es fácil probar que $\sim$ y $\overset{+}{\sim}$ son relaciones de equivalencia. La clase de equivalencia (propia) de $\mathfrak{f}$ bajo $\overset{+}{\sim}$ será denotada por $[\,\mathfrak{f}\,]$. La definición de cerraduras reducidas dada en la sección 2.2 puede ser escrita en términos de aplicaciones bilineales: Una *cerradura reducida* para la $\mathbb{S}$-forma $\mathfrak{q}$ es una expresión del tipo

$$\mathfrak{q}(\mathbf{t}) \cdot \mathfrak{q}(\mathbf{v}) = \mathfrak{q}\big(\sigma(\mathbf{t}, \mathbf{v})\big)$$

donde $\sigma : \mathbb{S}^2 \times \mathbb{S}^2 \to \mathbb{S}^2$ es un operador bilineal fijo, y la igualdad se cumple para cualquier par $\mathbf{t}, \mathbf{v}$ de vectores en $\mathbb{S}^2$. La imagen de $(\mathbf{t}, \mathbf{v})$ bajo σ, al considerar las componentes de los vectores $\mathbf{t}, \mathbf{v}$ como variables, es el par (X, Y) de polinomios homogéneos que ya son familiares.

La brillante idea de Gauss[3] fue la de considerar expresiones como la anterior, pero que relacionen a varias formas cuadráticas simultáneamente, en lugar de una sola. Es decir, identidades como la siguiente, en la cual $\mathfrak{f}, \mathfrak{g}, \mathfrak{h}$ pueden ser formas iguales o distintas:

$$\mathfrak{f}(\mathbf{t}) \cdot \mathfrak{g}(\mathbf{v}) = \mathfrak{h}\big(\sigma(\mathbf{t}, \mathbf{v})\big)$$

Alrededor de esta expresión nació una teoría intrincada cuyos resultados tienen de profundidad lo que carecen de fama, al menos en este país. Hablando burdamente, la composición gaussiana consiste en la búsqueda de una forma que represente a todos los números que se obtienen de multiplicar números representables por otras dos formas. La definición exacta es la siguiente.

Definición (composición gaussiana)**.** Dadas dos formas $\mathfrak{f}$ y $\mathfrak{g}$, se dice que la forma $\mathfrak{h}$ es una *composición gaussiana* de $\mathfrak{f}$ y $\mathfrak{g}$ si existen formas bilineales X, Y tales que:

$$\begin{cases} \mathfrak{f}(t,u) \cdot \mathfrak{g}(v,w) = \mathfrak{h}\big(X(t,u;v,w), Y(t,u;v,w)\big) \quad \forall t,u,v,w \in \mathbb{Z} \\ h_1k_2 - k_1h_2 = \mathfrak{f}(1,0) \\ h_1k_3 - k_1h_3 = \mathfrak{g}(1,0) \end{cases}$$

[3]Otros matemáticos, notablemente Lagrange, dejaron implícito en sus estudios algunos aspectos de la composición, pero Gauss fue el primero en entender su profundidad y estudiar sus interconexiones con la representabilidad.

Las últimas dos condiciones hacen referencia a los coeficientes de las formas bilineales, al expresarlas como polinomios homogéneos: $X(t,u;v,w) = h_1tv + h_2tw + h_3uv + h_4uw$, $\quad Y(t,u;v,w) = k_1tv + k_2tw + k_3uv + k_4uw$.

Nota. En formato vectorial, $\sigma(\mathbf{t},\mathbf{v}) = \big(X(\mathbf{t},\mathbf{v}), Y(\mathbf{t},\mathbf{v})\big)$ es el operador bilineal del que se hablaba antes, donde $\mathbf{t} = (t,u)$, $\quad \mathbf{v} = (v,w)$. El cambio de notación consiste en un isomorfismo entre $\mathbb{Z}^4$ y $\mathbb{Z}^2 \times \mathbb{Z}^2$.

La definición dada por Gauss no es fácil de utilizar, pues no provee una forma de computar las composiciones. Dirichlet[4] propone una alternativa, con la ventaja de que ofrece una fórmula explícita para $\mathfrak{h}$, pero su método requiere que las formas a componer cumplan ciertas condiciones. Afortunadamente, el método de Dirichlet puede ser modificado para operar sobre cualquier par de formas que posean el mismo discriminante. Antes de enunciar la fórmula modificada, se presenta un lema que resulta de utilidad al momento de aplicarla.

Lema 12. *Sean* $\mathfrak{f} = \langle a_1, b_1, c_1\rangle$, $\mathfrak{g} = \langle a_2, b_2, c_2\rangle$ *dos formas cuadráticas de discriminante* Δ*, y suponga que* $\text{MCD}(a_1, a_2, \frac{b_1+b_2}{2}) = e$ *(Note que* b_1, b_2 *deben tener la misma paridad para que las formas posean el mismo discriminante). Entonces existe un entero* B *único* $(\text{mód } \frac{2a_1a_2}{e^2})$ *tal que:*

$$\begin{cases} B \equiv b_1 \pmod{\frac{2a_1}{e}} \\ B \equiv b_2 \pmod{\frac{2a_2}{e}} \\ B^2 \equiv \Delta \pmod{\frac{4a_1a_2}{e^2}} \end{cases}$$

Definición (Composición de Dirichlet)**.** Sean $\mathfrak{f}, \mathfrak{g}, B$ como en el lema anterior, entonces la *composición de Dirichlet* de $\mathfrak{f}$ y $\mathfrak{g}$, denotada $\mathfrak{f} \circ \mathfrak{g}$, es la forma:

$$\mathfrak{h} = \left\langle \frac{a_1a_2}{e^2}\ ,\ B\ ,\ \frac{e^2(B^2-\Delta)}{4a_1a_2} \right\rangle$$

[4]**Johann Peter Gustav Lejeune Dirichlet** (1805 – 1859) fue un matemático alemán que ofreció contribuciones notables a la Teoría de Números y la teoría de las series de Fourier. A él se le atribuye la definición formal moderna de función. Tras graduarse, fue profesor en las universidades de Breslau, Berlín y Gotinga, en donde ocupó la cátedra dejada por Gauss tras su muerte. Su primera publicación comprendió un fragmento de la demostración para el caso $n = 5$ del «último teorema de Fermat», que fue completada por Legendre, quien era uno de sus revisores. Después de completar su propia prueba, logró resolver también el caso $n = 14$.

Nota. B también se puede calcular mediante la fórmula $B = n_1\frac{a_1b_2}{e} + n_2\frac{a_2b_1}{e} + n_3\frac{b_1b_2+\Delta}{2e}$, donde los números n_1, n_2, n_3 se eligen como una solución particular de la ecuación diofantina $n_1a_1 + n_2a_2 + n_3\frac{b_1+b_2}{2} = e$.

Se puede mostrar que si $\mathfrak{f}, \mathfrak{f}', \mathfrak{g}, \mathfrak{g}'$ son formas cuadráticas con el mismo discriminante Δ, todas definidas positivas o todas indefinidas, tales que $\mathfrak{f} \overset{+}{\sim} \mathfrak{f}'$ y $\mathfrak{g} \overset{+}{\sim} \mathfrak{g}'$, entonces $\mathfrak{f} \circ \mathfrak{g} \overset{+}{\sim} \mathfrak{f}' \circ \mathfrak{g}'$, por lo que no es ambiguo escribir $[\mathfrak{f}] \circ [\mathfrak{g}] = [\mathfrak{h}]$, en ese caso. Ahora bien, restringiendo la atención a formas primitivas, es posible obtener el siguiente resultado.

Teorema 12. *Si $\mathfrak{f}, \mathfrak{g}$ son formas primitivas de discriminante Δ, entonces existen formas $\hat{\mathfrak{f}}, \hat{\mathfrak{g}}$, también primitivas y con el mismo discriminante, tales que $\mathfrak{f} \overset{+}{\sim} \hat{\mathfrak{f}}$, $\mathfrak{g} \overset{+}{\sim} \hat{\mathfrak{g}}$, y que la composición de Dirichlet $\mathfrak{f} \circ \mathfrak{g}$ equivale propiamente a una composición gaussiana de $\hat{\mathfrak{f}}$ con $\hat{\mathfrak{g}}$.*

En virtud del teorema anterior, usualmente no es necesario especificar de cuál tipo de composición se habla. El hecho de que la composición de dos formas primitivas es también una forma primitiva (cerradura del producto, problema 38 del apéndice D) fundamenta la consideración de los otros axiomas de grupo. Al menos, cuando $\Delta < 0$, el conjunto de las clases de equivalencia (propia) de formas primitivas de un discriminante fijo Δ, es un grupo abeliano finito denotado por $\mathfrak{C}_\Delta$, cuyo elemento unitario $[\mathfrak{e}]$ es la clase de las formas que representan al número 1 (problemas 39 al 42). Finalmente, el elemento inverso de $[\langle a, b, c\rangle]$ es $[\langle a, -b, c\rangle]$. Lo que es realmente sorprendente es que Gauss llegara tan lejos en sus estudios antes de que existiera la noción formal de grupo algebraico.

Recordando que las matrices, arreglos cuadrados de números, están ligadas a las formas cuadráticas en más de una manera, no parece extraño plantearse si existen arreglos cúbicos que también guarden alguna relación con ellas. Barghava[5] se inspiró en esta pregunta para replantear la composición de formas empleando los ahora

[5]**Manjul Bhargava** (1974 – $\star$) es un matemático canadiense de ascendencia hindú, conocido principalmente por sus contribuciones a la Teoría de Números. Asesorado por Andrew Wiles, recibió su doctorado de Princeton en el 2001, por su trabajo en las leyes de composición. También es famoso por su demostración simple del *teorema* 15, que dice que una $\mathbb{Z}$-forma cuadrática n-aria tal

llamados *cubos de Bhargava*, y sus estudios lo han llevado a encontrar 14 nuevas reglas de composición hasta la fecha. Como se verá más adelante, sus ideas permiten demostrar algunos conceptos clave en la teoría de cerraduras.

4.3.2. Resultados recientes en la teoría de cerraduras

Haciendo uso de la composición, Earnest y Fitzgerald llevan a cabo una demostración muy simple de la propiedad de trigrupo, aunque ésta no ofrece ninguna tricerradura. Parte del hecho siguiente, que se deduce del teorema 12 con facilidad: si $\mathfrak{f}, \mathfrak{g}$ son dos formas primitivas, entonces

$$\mathscr{D}(\mathfrak{f})\mathscr{D}(\mathfrak{g}) := \left\{ fg : f \in \mathscr{D}(\mathfrak{f}), g \in \mathscr{D}(\mathfrak{g}) \right\} \subseteq \mathscr{D}(\mathfrak{h})$$

donde $\mathfrak{h}$ es cualquier forma en la clase $[\mathfrak{f}] \circ [\mathfrak{g}]$. Como la elección de $\mathfrak{h}$ es irrelevante, se puede denotar por $\mathscr{D}([\mathfrak{f}] \circ [\mathfrak{g}])$ al conjunto de la derecha.

Si $\mathfrak{q} = \langle a, b, c \rangle$, la forma $\langle a, -b, c \rangle$ es representada con el símbolo $\mathfrak{q}^{op}$ y, puesto que $\mathfrak{q}(x, -y) = \mathfrak{q}^{op}(x, y)$, es claro que $\mathscr{D}(\mathfrak{q}) = \mathscr{D}(\mathfrak{q}^{op})$. Luego

$$\begin{aligned} \mathscr{D}(\mathfrak{q})\mathscr{D}(\mathfrak{q})\mathscr{D}(\mathfrak{q}) &= \mathscr{D}(\mathfrak{q})\mathscr{D}(\mathfrak{q}^{op})\mathscr{D}(\mathfrak{q}) \\ &= \mathscr{D}([\mathfrak{q}])\mathscr{D}([\mathfrak{q}^{op}])\mathscr{D}([\mathfrak{q}]) \\ &\subseteq \mathscr{D}([\mathfrak{q}] \circ [\mathfrak{q}^{op}] \circ [\mathfrak{q}]) \\ &= \mathscr{D}([\mathfrak{q}]) = \mathscr{D}(\mathfrak{q}) \end{aligned}$$

que no es otra cosa que la propiedad del trigrupo, observando el primer y último miembros. La demostración se extiende fácilmente a formas $\mathfrak{q} = \langle a, b, c \rangle$ no primitivas, si se aplica la propiedad anterior a $\mathfrak{q}_0$, tomando $\mathfrak{q} = q\mathfrak{q}_0$, donde $\mathfrak{q}_0$ es primitiva y $q = \text{MCD}(a, b, c)$.

Como había sido dicho anteriormente, el estudio sistemático de las formas perfectas, es decir aquellas que poseen cerraduras, fue iniciado por Arnol'd. Poco después,

que su matriz asociada tiene todas sus entradas enteras, es universal si, y sólo si, representa a los números del 1 al 15. La complicada demostración original se debe a Conway, entre otros.

Aicardi y Timorin investigaron varias condiciones vinculadas a las formas perfectas. Hicieron varias conjeturas que ellos y otros matemáticos demostraron o refutaron posteriormente. El resultado principal para formas primitivas es el siguiente.

Teorema 13. *Sea* $\mathfrak{q}$ *una* $\mathbb{Z}$*-forma cuadrática primitiva de discriminante* Δ*. Las siguientes condiciones son equivalentes:*

a) $\mathscr{D}(\mathfrak{q})$ *es cerrada bajo el producto.*

b) $[\mathfrak{q}]^3 := [\mathfrak{q}] \circ [\mathfrak{q}] \circ [\mathfrak{q}] = [\mathfrak{e}]$.

c) *Existen* $\alpha, \beta, \gamma, \delta \in \mathbb{Z}$ *tales que* $\mathfrak{q} = \langle \alpha^2 - \gamma\delta, \alpha\gamma - \beta\delta, \gamma^2 - \alpha\beta \rangle$.

d) *Existe un operador bilineal* $\sigma : \mathbb{Z}^2 \times \mathbb{Z}^2 \to \mathbb{Z}^2$ *tal que:*

$$\mathfrak{q}(\mathbf{t}) \cdot \mathfrak{q}(\mathbf{v}) = \mathfrak{q}\big(\sigma(\mathbf{t}, \mathbf{v})\big) \qquad \forall \mathbf{t}, \mathbf{v} \in \mathbb{Z}^2$$

Contribuciones a la demostración. (b) $\Rightarrow$ (c) puede ser demostrado haciendo uso de una caracterización de la composición dada por Bhargava en el 2004. Aicardi conjeturó que (a) implica (c) en ese mismo año. La equivalencia de (a) con (b) fue demostrada por Earnest y Fitzgerald en el 2007, y en esa misma publicación demuestran (b) $\Rightarrow$ (c) y (c) $\Rightarrow$ (d). Esta última implicación se sigue del mapeo $\sigma(t, u; v, w) = (X, Y)$ dado por las formas bilineales $X(t, u; v, w) = \alpha tv + \gamma tw + \gamma uv + \beta uw$, $Y(t, u; v, w) = -\delta tv - \alpha tw - \alpha uv - \gamma uw$. Finalmente, (d) $\Rightarrow$ (a) es ulteriormente trivial. $\diamondsuit$

Aicardi y Timorin dicen que $\mathfrak{q}$ *admite un pareo normado entero* si cumple (d). Según la terminología del segundo capítulo, esto es la existencia de una cerradura homogénea reducida. En palabras de Earnest, $\mathfrak{q}$ es *multiplicativa*, *parametrizable* o *normada* si cumple (a), (c) o (d) respectivamente. Puesto que la prueba de que (c) implica (d) no depende del hecho de que $\mathfrak{q}$ sea primitiva, se concluye que las siguientes implicaciones permanecen válidas en el caso general:

$$\mathfrak{q} \text{ parametrizable} \implies \mathfrak{q} \text{ normada} \implies \mathfrak{q} \text{ multiplicativa}$$

Las conjeturas de Aicardi y Timorin estaban enunciadas para el caso general, es decir, para formas no necesariamente primitivas. Las principales son:

Conjetura 1. (Aicardi, 2004) $\mathfrak{q}$ *multiplicativa* $\implies$ $\mathfrak{q}$ *parametrizable.*

Conjetura 2. (Aicardi y Timorin, 2007) $\mathfrak{q}$ *multiplicativa* $\Longrightarrow$ $\mathfrak{q}$ *normada.*

Una vez más, Earnest y Fitzgerald resuelven los problemas. Ellos comentan que la forma $\langle 4, -2, 12\rangle$ es multiplicativa pero no es parametrizable (problema 43). En cuanto a la segunda conjetura, ésta resulta verdadera. Para verificarlo, ellos suponen que $\mathfrak{q} = q\mathfrak{q}_0$ como antes, y prueban que ambas condiciones son equivalentes a una tercera, que consta de una disyunción:

$$q \in \mathscr{D}(\mathfrak{q}_0) \quad \vee \quad q \in \mathscr{D}([\mathfrak{q}_0]^3)$$

Además de estos resultados, numerosas generalizaciones se han efectuado, para incluir formas n-arias, e incluso para formas cúbicas, cuárticas o de grados mayores. Sin embargo, vale aclarar que ninguna teoría es tan rica como la de las formas cuadráticas. Según se ha investigado para este documento, no se conocen generalizaciones de las tricerraduras, pero sí se han hecho progresos en generalizar la propiedad del trigrupo.

5. $\mathbb{Q}$-FORMAS: TEOREMAS SELECTOS

5.1. Generalidades

Así como sucedió con el Análisis Diofantino, el estudio de las formas cuadráticas comenzó en los enteros, pero, a finales del siglo XIX, se observó que al permitir que las variables tomen valores racionales se obtiene una teoría mucho más satisfactoria. De hecho, empleando campos como conjuntos subyacentes, en lugar de anillos como $\mathbb{Z}$, se consiguen resultados semejantes. Mucho del trabajo reciente se ha concentrado en éstas y otras generalizaciones.

Las definiciones iniciales se plantearán en el contexto general de las formas cuadráticas n-arias pues, como se verá más adelante, lo aprendido sobre ellas permitirá explicar más fácilmente algunas propiedades de las formas binarias. Se usará siempre $\mathbf{x} = (x_1, \ldots, x_n)$ como el vector de las variables usadas por las formas; $\mathbf{x} = (x, y)$ para las binarias y (x, y, z) para las ternarias. No importando cuál sea el conjunto subyacente, se distinguen dos tipos básicos de problemas.

Problema homogéneo o isotrópico: Determinar si existen $\xi_1, \ldots, \xi_n \in \mathbb{S}$, no todos ellos cero, tales que $\mathfrak{q}(\xi_1, \ldots, \xi_n) = 0$. Una forma cuadrática $\mathfrak{q}$ tal que la ecuación $\mathfrak{q}(\mathbf{x}) = 0$ tenga una solución no trivial será llamada *isotrópica*. Si sólo posee la solución trivial, la forma será llamada *anisotrópica*.

Ejemplo: Las formas sumas de cuadrados $x_1^2 + \ldots x_n^2$ son todas anisotrópicas en cualquier subcampo o subanillo de los reales. Obviamente, este no es el caso si $\mathbb{S} = \mathbb{C}$. Por otro lado, la $\mathbb{Z}$-forma $x^2 - ny^2$ es isotrópica si, y sólo si, n es un cuadrado perfecto.

Problema inhomogéneo: Dado un entero n, determinar si la ecuación $\mathfrak{q}(\mathbf{x}) = n$ posee una solución en $\mathbb{S}$. Éste es el que anteriormente había sido conocido como

problema de representación. Usualmente este problema se extiende a hallar el conjunto $\mathscr{D}(\mathfrak{q})$ de los números representables.

En general, y especialmente en los enteros, los problemas inhomogéneos son considerablemente más difíciles que los homogéneos. Uno de los motivos es que, aunque inicialmente se plantee un problema homogéneo en $\mathbb{Z}$, éste puede ser resuelto en $\mathbb{Q}$ gracias al *principio de equivalencia* que se enuncia a continuación.

Principio de equivalencia homogénea. Sea $\mathfrak{q}(\mathbf{x})$ una forma de grado k. Entonces la ecuación $\mathfrak{q}(\mathbf{x}) = 0$ tiene una solución no trivial en $\mathbb{Z}$ si, y sólo si, tiene una solución no trivial en $\mathbb{Q}$.

Demostración. La prueba es sencilla. Por supuesto, toda solución en $\mathbb{Z}$ es también una solución en $\mathbb{Q}$, así que lo único que se debe probar es la necesidad. Supóngase entonces que existen $\frac{a_1}{b_1}, \ldots, \frac{a_n}{b_n} \in \mathbb{Q}$, no todos cero, tales que $\mathfrak{q}\big(\frac{a_1}{b_1}, \ldots, \frac{a_n}{b_n}\big) = 0$. Tomando $M = \text{MCM}(b_1, \ldots b_n)$, y recordando que las formas son polinomios homogéneos, se puede multiplicar ambos lados de la ecuación por M^k para obtener:

$$\begin{aligned} M^k \mathfrak{q}\big(\tfrac{a_1}{b_1}, \ldots, \tfrac{a_n}{b_n}\big) = 0 \qquad &\Longrightarrow \\ \mathfrak{q}\big(M\tfrac{a_1}{b_1}, \ldots, M\tfrac{a_n}{b_n}\big) = 0 & \end{aligned}$$

y ésta última, es una solución en enteros. $\square$

Las formas $\mathfrak{q}$ no tienen que ser cuadráticas para que los problemas definidos anteriormente tengan sentido, pero tienden a ser extremadamente difíciles cuando el grado es mayor que 2, aún en los racionales. Por ejemplo, en el siglo XIX, Sylvester[1] y otros matemáticos conjeturaron que un primo p es representable en la forma $x^3 + y^3$, para un par (x, y) de números racionales, si $p \equiv 4, 7, 8 \pmod 9$. Una prueba para las primeras dos opciones fue anunciada por Noam Elkies en 1994, pero nunca la publicó.

[1] **James Joseph Sylvester** (1814 – 1897) fue un matemático inglés, famoso por sus contribuciones a la Teoría de Números y la Combinatoria, y por ser uno de los fundadores de la Teoría de Invariantes. Acuñó varios términos actualmente en uso, como *grafo, totiente, perpetuante* y *discriminante*. La Real Sociedad de Londres le otorgó la medalla Copley y la medalla De Morgan, sus más importantes reconocimientos en el ámbito científico.

Posteriormente, en el 2009, Dasgupta y Voight publicaron un resultado más débil: p es representable si $p \equiv 4, 7 \pmod 9$ y 3 no es un residuo cúbico en el módulo p. Retornando a la discusión sobre los problemas, conforme el grado aumenta arriba del 3, todavía menos es sabido sobre el caso inhomogéneo [7].

5.1.1. La representación matricial y la diagonalización

Se ampliará el enfoque momentáneamente para incluir formas cuadráticas n-arias con $n > 2$. De esta manera se pueden establecer algunos resultados más generales. Lo que sea dicho aquí no sólo es válido cuando el conjunto subyacente sea $\mathbb{Q}$, sino también para cualquier otro campo que no tenga característica 2. En este contexto, conviene bautizar los coeficientes de las formas n-arias según el siguiente esquema:

$$\mathfrak{q}(x_1, \ldots, x_n) = \sum_{1 \leq i \leq j \leq n} a_{ij} x_i x_j$$

A cada forma cuadrática se le puede asociar una única matriz simétrica $M_{\mathfrak{q}}$, tal que $\mathfrak{q}(\mathbf{x}) = \mathbf{x} M_{\mathfrak{q}} \mathbf{x}'$, donde la prima denota trasposición. Con la notación de arriba para $\mathfrak{q}$, los coeficientes m_{ij} de la matriz asociada están dados por:

$$\begin{cases} m_{ij} = a_{ij}, & \text{si } i = j \\ m_{ij} = \frac{a_{ij}}{2}, & \text{si } i \neq j \end{cases}$$

Para las $\mathbb{Z}$-formas, resulta problemático que las entradas no siempre son todas enteras, pero esto no es ningún problema en $\mathbb{Q}$. En el contexto matricial, la equivalencia $\sim$ que fue definida anteriormente se puede reformular de la siguiente manera: Dos formas $\mathfrak{q}_1, \mathfrak{q}_2$ son equivalentes si existe una matriz invertible $M_{\mathcal{T}}$ tal que $M_{\mathfrak{q}_1} = M_{\mathcal{T}} M_{\mathfrak{q}_2} M_{\mathcal{T}}'$. También se dice que las matrices $M_{\mathfrak{q}_1}, M_{\mathfrak{q}_2}$ son *equivalentes*. La matriz $M_{\mathcal{T}}$ debe tener entradas en $\mathbb{Q}$, y corresponde a una transformación lineal $\mathcal{T}$ de las variables, que posee coeficientes racionales.

Como se había visto, la condición para que una matriz sea invertible en $\mathbb{Z}$ es que su determinante valga ± 1 (matrices unimodulares). En $\mathbb{Q}$ no se tiene esta restricción,

basta con que el determinante no se anule. Naturalmente, esto implica que las clases de equivalencia son más amplias. Esta consideración es muy significativa, pues se pueden encontrar representantes muy simples para las clases de formas. Según el Álgebra Lineal, toda matriz simétrica puede ser diagonalizada mediante un cambio apropiado de coordenadas, como puede apreciarse en el teorema 14, cuya demostración puede encontrarse en cualquier libro de esta materia.

Notación. El símbolo $\mathfrak{D}\langle a_1, \ldots, a_n\rangle$ representará a la forma cuadrática diagonal $a_1x_1^2 + \ldots + a_nx_n^2$. El nombre es apropiado porque la matriz asociada también es diagonal, y será denotada por $D(a_1, \ldots, a_n)$. Cuando no haya necesidad de especificar el valor de n, se puede escribir simplemente $\mathfrak{D}\langle a_i\rangle$ y $D(a_i)$.

Teorema 14. *Toda matriz simétrica es equivalente a una matriz diagonal, vía una matriz de transformación $M_\mathcal{T}$ ortogonal, es decir, tal que $M_\mathcal{T}^{-1} = M'_\mathcal{T}$.*

Lamentablemente, este tipo de resultados se plantean usualmente en los libros considerando transformaciones lineales con coeficientes *reales*, y aquí se necesitan coeficientes *racionales*. Sin embargo, hay una manera de lograr la diagonalización sin invocar campos que sean extensiones de aquél que funge como conjunto subyacente, y la clave radica en uno de los conceptos más básicos: la completación de cuadrados. El procedimiento puede ser explicado más fácilmente mediante un ejemplo.

Ejemplo. Diagonalice la $\mathbb{Q}$-forma cuadrática: $2x^2 - 5y^2 + 3z^2 + \frac{7}{2}xy - 6xz + 2yz$.

Solución. Se quiere diagonalizar primero la variable x, para ello es útil tomar el coeficiente de x^2 como factor común, con lo cual se obtiene

$$2(x^2 - \tfrac{5}{2}y^2 + \tfrac{3}{2}z^2 + \tfrac{7}{4}xy - 3xz + yz)$$

Si x^2 no apareciera en la forma, se puede hacer un cambio de variable como $y \mapsto (x + y - 2z)$ para que aparezca. Sólo se debe elegir un término cruzado[2] que contenga a x, y sustituir la otra variable por una expresión que dependa de x.

[2]Aquellos términos que poseen dos variables.

Ahora hay que completar el cuadrado simultáneamente para todos los términos cruzados que involucren a x. En este ejemplo, tales términos son $\frac{7}{4}xy, -3xz$. Si se dividen sus coeficientes entre 2, y luego se elevan al cuadrado, los resultados son $\frac{49}{64}, \frac{9}{4}$, por lo que se deben sumar y restar a la expresión los términos $\frac{49}{64}y^2, \frac{9}{4}z^2$. Además de esto, deben ajustarse los términos cruzados que no incluyan a x, en este caso solamente el término yz. Nuestro propósito es poder factorizar todos los términos que involucren a x para expresarlo como un trinomio al cuadrado. Los pasos algebraicos son, entonces:

$$\begin{aligned}
2(x^2 - \tfrac{5}{2}y^2 + \tfrac{3}{2}z^2 + \tfrac{7}{4}xy - 3xz + yz) &= \\
2(x^2 - \tfrac{5}{2}y^2 + \tfrac{3}{2}z^2 + \tfrac{7}{4}xy - 3xz + yz + \tfrac{49}{64}y^2 - \tfrac{49}{64}y^2 + \tfrac{9}{4}z^2 - \tfrac{9}{4}z^2) &= \\
2[(x^2 + \tfrac{7}{4}xy - 3xz + \tfrac{49}{64}y^2 + \tfrac{9}{4}z^2) + yz + (\tfrac{3}{2}z^2 - \tfrac{9}{4}z^2) + (-\tfrac{5}{2}y^2 - \tfrac{49}{64}y^2)] &= \\
2[(x^2 + \tfrac{49}{64}y^2 + \tfrac{9}{4}z^2 + \tfrac{7}{4}xy - 3xz) + yz - \tfrac{3}{4}z^2 - \tfrac{209}{64}y^2] &= \\
2[(x^2 + \tfrac{49}{64}y^2 + \tfrac{9}{4}z^2 + \tfrac{7}{4}xy - 3xz - \tfrac{21}{8}yz) + (yz + \tfrac{21}{8}yz) - \tfrac{3}{4}z^2 - \tfrac{209}{64}y^2] &= \\
2[(-x - \tfrac{7}{8}y + \tfrac{3}{2}z)^2 + \tfrac{29}{8}yz - \tfrac{3}{4}z^2 - \tfrac{209}{64}y^2] &= \\
2(-x - \tfrac{7}{8}y + \tfrac{3}{2}z)^2 + \tfrac{29}{4}yz - \tfrac{3}{2}z^2 - \tfrac{209}{32}y^2 &
\end{aligned}$$

Ahora sólo es cuestión de hacer la sustitución $(-x - \frac{7}{8}y + \frac{3}{2}z) \mapsto w$, para completar la diagonalización de la primera variable. Con frecuencia, a w se le rebautiza llamándole nuevamente x, aunque sería un error pensar que se trata de la misma variable. Con las otras letras se procede de igual modo, pero sin considerar los términos ya diagonalizados. $\diamondsuit$

El procedimiento descrito anteriormente puede ser aplicado a formas cuadráticas cuyo campo subyacente es cualquier subcampo de los complejos. En el lenguaje de las matrices, se puede expresar esta conclusión de la siguiente manera.

Teorema 15. *Sea $\mathbb{S}$ un subcampo de $\mathbb{C}$, y sea M una matriz simétrica cuyas entradas están en $\mathbb{S}$. Entonces existe una matriz A, cuyas entradas también están en $\mathbb{S}$, tal que AMA' es diagonal.*

En contraposición, si el conjunto subyacente es el de los enteros, no se dispone de un resultado semejante. Muchas $\mathbb{Z}$-formas cuadráticas no pueden ser diagonalizadas

sin recurrir a números que no sean enteros. Por ejemplo, la forma cuadrática $\mathfrak{q}(x,y) = xy$ tiene la matriz asociada $M_{\mathfrak{q}} = \begin{pmatrix} 0 & 1/2 \\ 1/2 & 0 \end{pmatrix}$, con determinante $-\frac{1}{4}$. Si se supone que existe una matriz $M_{\mathcal{T}}$, invertible en los enteros, tal que $M_{\mathcal{T}} M_{\mathfrak{q}} M'_{\mathcal{T}} = D$, una matriz diagonal con entradas enteras, entonces

$$\det(D) = \det(M_{\mathcal{T}}) \det(M_{\mathfrak{q}}) \det(M'_{\mathcal{T}}) = \det(M_{\mathfrak{q}})[\det(M_{\mathcal{T}})]^2 = \det(M_{\mathfrak{q}}) = -\frac{1}{4}$$

La penúltima igualdad se deduce del hecho que las matrices invertibles en los enteros son precisamente las unimodulares, es decir, aquellas cuyo determinante es ± 1. Ahora bien, si una matriz es diagonal con entradas enteras, entonces forzosamente su determinante debe ser entero. La conclusión es que $\mathfrak{q}$ no es diagonalizable.

5.1.2. La forma $x^2 - y^2$, el plano hiperbólico

Ya se ha hablado mucho de la forma $\mathfrak{q}(\mathbf{x}) = x^2 - y^2 = \mathfrak{D}\langle 1, -1\rangle$. Se sabe que es isotrópica, pues el par (ξ, ξ) es solución de $\mathfrak{q}(\mathbf{x}) = 0$, para cada ξ en cualquier anillo subyacente. En los enteros, es conocido que no es universal, pues no representa a los números congruentes con 2 en el módulo 4. Se verá que en los racionales sí es universal, y será probado de dos maneras distintas. A esta forma cuadrática se le conoce en la literatura como el *plano hiperbólico*, y será denotada por $\mathfrak{H}$. La clase de equivalencia a la que pertenece tiene mucha importancia teórica.

Teorema 16. *El plano hiperbólico $\mathfrak{H}(x,y) = x^2 - y^2$ es universal en $\mathbb{Q}$.*

Primera demostración. En la prueba del teorema 5 de la página 62, se planteó que $(\frac{n+1}{2}, \frac{n-1}{2})$ es una representación en enteros del número n, bajo la forma $\mathfrak{H}$, siempre que n sea impar. En el contexto de los racionales no existe la restricción de paridad, y se puede verificar inmediatamente que el par ordenado dado puede ser tomado como representación de cualquier número racional n. $\square$

Segunda demostración. Se recurrirá ahora a una forma cuadrática auxiliar de la que ya se ha hablado brevemente con anterioridad: $\mathfrak{q}(x,y) = xy$. $\mathfrak{q}$ es claramente universal, pues el par $(1,n)$ es representación de cualquier $n \in \mathbb{Q}$. Lo que se propone es

diagonalizar $\mathfrak{q}$ para mostrar que es equivalente a $\mathfrak{H}$, con lo que el teorema quedaría probado. Para esto hay que notar que, aunque $\mathfrak{q}$ no puede ser diagonalizada en los enteros, el teorema 15 asegura que es posible hacerlo en los racionales.

Considérese la transformación $(x, y) \overset{\mathcal{T}_1}{\longmapsto} (x, x + 2y)$, y complétese el cuadrado para diagonalizar la forma:

$$\mathfrak{q} \overset{\mathcal{T}_1}{\longmapsto} x(x + 2y) = x^2 + 2xy + y^2 - y^2 = (x + y)^2 - y^2$$

Ahora se debe añadir la transformación $(x, y) \overset{\mathcal{T}_2}{\longmapsto} (x - y, y)$. Es fácil probar que ambas transformaciones son invertibles, y así, $\mathfrak{q} \sim \mathfrak{H}$. $\square$

Para cerrar la sección, se verificará que el problema de la representación de racionales mediante $\mathbb{Q}$-formas n-arias se reduce al problema isotrópico, enunciado que se precisará en el teorema 17. El puente que conecta ambos conceptos es el plano hiperbólico, mediante el siguiente lema que afirma que las formas isotrópicas «contienen» de cierta manera a $\mathfrak{H}$ y son, por lo tanto, universales.

Lema 17. *Si* $\mathfrak{q}(\mathbf{x})$ *es una* $\mathbb{Q}$*-forma cuadrática* n*-aria isotrópica, con* $n \geq 2$*, entonces existe una* $\mathbb{Q}$*-forma* $(n-2)$*-aria* $\mathfrak{g}$ *tal que*

$$\mathfrak{q}(x_1, x_2, \ldots, x_n) \sim \mathfrak{H}(x_1, x_2) + \mathfrak{g}(x_3, \ldots, x_n)$$

Se puede obtener inspiración para demostrar el lema anterior buscando primero un conjunto completo de representantes diagonales para las clases de equivalencia bajo $\sim$ del conjunto de las $\mathbb{Q}$-formas n-arias (ver problemas 44 al 49 del apéndice D). Aún si esta búsqueda fracasa, muchos puntos clave son resaltados en el proceso.

Teorema 17. *Sea* $\mathfrak{q}(\mathbf{x})$ *una* $\mathbb{Q}$*-forma cuadrática* n*-aria, y sea* $a \neq 0$ *un número racional. Las siguientes proposiciones son equivalentes:*

a) *La forma* $(n+1)$*-aria* $\mathfrak{q}(\mathbf{x}) + (-a)x_{n+1}^2$ *es isotrópica.*

b) *La forma* $\mathfrak{q}$ *representa racionalmente al número* a*.*

Demostración. Primero se supondrá que (b) es cierta. Luego existen $x_1, \ldots, x_n \in \mathbb{Q}$, no todos ellos cero, tales que $\mathfrak{q}(x_1, \ldots, x_n) = a$, pero entonces se puede reescribir esta expresión para obtener

$$\mathfrak{q}(x_1, \ldots, x_n) + (-a)(1)^2 = 0.$$

Por el contrario, si se supone que (a) es cierta, deben existir $x_1, \ldots, x_n, x_{n+1} \in \mathbb{Q}$, no todos ellos cero, tales que $\mathfrak{q}(x_1, \ldots, x_n) + (-a)x_{n+1}^2 = 0$. Si $x_{n+1} \neq 0$, entonces se puede dividir la expresión entre x_{n+1}^2 y despejar la a para obtener una representación:

$$\mathfrak{q}\left(\tfrac{x_1}{x_{n+1}}, \ldots, \tfrac{x_n}{x_{n+1}}\right) = a$$

Finalmente, si $x_{n+1} = 0$, entonces $\mathfrak{q}(x_1, \ldots, x_n) = 0$, en donde no todas las variables son cero, lo que significa que $\mathfrak{q}$ es isotrópica. Por el lema anterior, $\mathfrak{q}$ debe contener al plano hiperbólico y, por ende, ser universal, lo que implica que puede representar a todos los racionales, y en particular al número a. □

El teorema permite afirmar que si existiera un algoritmo para decidir si una forma cuadrática n-aria dada es isotrópica, entonces también podría emplearse para decidir si la forma representa a un número racional dado. Sin embargo, si el algoritmo sólo funciona para valores de n menores que un natural N fijo, entonces la técnica sería útil solamente para problemas de representación en los que $n \leq N - 1$.

5.2. Teoremas fundamentales

Interesa ahora resolver el problema de la representación para $\mathbb{Q}$-formas cuadráticas binarias. En virtud del teorema 15 sólo se deben considerar las formas $aX^2 + bY^2$. Puesto que las variables toman valores racionales, si existiera una representación para un número $n \in \mathbb{Q}$, se podrían ajustar las variables para que posean el mismo denominador, sea z, y así el problema de la representación queda resumido en la siguiente ecuación:

$$a\left(\frac{x}{z}\right)^2 + b\left(\frac{y}{z}\right)^2 = n \tag{5.1}$$

Multiplicando ambos lados por z^2, y tomando $c := -n$, tal y como aconseja el teorema 17, se puede reescribir la ecuación como:

$$ax^2 + by^2 + cz^2 = 0 \tag{5.2}$$

No se necesita estudiar las variables x, y, z en los racionales, pero los coeficientes por el momento sí pertenecen a $\mathbb{Q}$. Mediante transformaciones lineales adecuadas de las variables racionales originales (X, Y), se puede convertir cualquier $\mathbb{Q}$-forma cuadrática en una cuyos coeficientes sean enteros libres de cuadrados. Esto indica que, si es posible resolver la ecuación ternaria (5.2), considerándola una ecuación diofantina con coeficientes enteros, se resolverá también el problema de la representación de racionales mediante formas binarias. Esto es precisamente lo que sugieren el teorema 17 y el principio de equivalencia homogénea.

La solución de este problema tan fundamental es un legado de Legendre,[3] y ya fue mencionada previamente en la página 13, aunque en esa ocasión fue invocada debido a su conexión con la reciprocidad cuadrática. Esa conexión y las implicaciones del lema de Legendre serán discutidas en el resto de esta sección.

5.2.1. El lema de Legendre

Para enunciar este importante resultado, se introducirá primero una notación que ayudará a simplificar su redacción.

Definición. Dados $a, b \in \mathbb{Z}\backslash\{0\}$, se escribirá $a \boxdot b$ cuando a sea un residuo cuadrático en el módulo $|b|$.

[3] **Adrien-Marie Legendre** (1752 – 1833) fue un matemático francés. Gran parte de su trabajo fue perfeccionado posteriormente por otros: sus trabajos en las raíces de los polinomios inspiró la teoría de Galois; los trabajos de Abel en las funciones elípticas se construyeron sobre los de Legendre; parte de la obra de Carl Friedrich Gauss sobre estadística y teoría de números complementaba la de Legendre. En 1830 ofreció una demostración del último teorema de Fermat para el exponente $n = 5$, casi simultáneamente con Dirichlet (1828). Su nombre es uno de los 72 inscritos en la torre Eiffel.

Proposición. *Sean $b, c \in \mathbb{Z} \setminus \{0\}$, tales que* $\text{MCD}(b, c) = 1$. *Entonces se cumple la siguiente equivalencia: $a \boxdot bc \iff a \boxdot b$, $a \boxdot c$.*

Empleando la definición dada y el teorema chino del residuo, es muy fácil demostrar el enunciado anterior. En cuanto al lema, puede reescribirse de la siguiente manera.

Lema de Legendre. *Sean $a, b, c \in \mathbb{Z} \setminus \{0\}$, libres de cuadrados, primos relativos a pares, y no todos ellos positivos, ni todos negativos. Entonces la ecuación (5.2) posee una solución no trivial en enteros si, y sólo si, todas las siguientes condiciones se cumplen:*

- $-ab \boxdot c$
- $-bc \boxdot a$
- $-ca \boxdot b$

Bosquejo de la demostración. Para probar la *suficiencia*, se debe analizar localmente la ecuación (5.2) en los módulos a, b, c. Considerando por ejemplo el módulo c, se debe multiplicar ambos lados de la congruencia por $-b$ y demostrar que x es invertible en ese módulo; las otras dos condiciones son simétricas.

La *necesidad* puede demostrarse recurriendo a la versión modificada del lema de Legendre que se presentará a continuación, tal y como lo hacen Ireland y Rosen [22]. Ellos separan los casos $a = b$ y $a \neq b$, y utilizan para el segundo un argumento tipo descenso. Como es usual, esta parte de la demostración es considerablemente más difícil. $\square$

Lema de Legendre (versión de Ireland y Rosen)**.** *Dados $a, b \in \mathbb{Z}^+$, libres de cuadrados, la ecuación $ax^2 + by^2 = z^2$ tiene una solución en enteros no trivial si, y sólo si, todas las siguientes condiciones se cumplen:*

- $a \boxdot b$
- $b \boxdot a$
- $-\frac{ab}{d^2} \boxdot d$, *donde* $d = \text{MCD}(a, b)$

5.2.2. La ley de reciprocidad de Hilbert

Pete L. Clark [7] señala que el lema de Legendre tiene la siguiente consecuencia: una $\mathbb{Q}$-forma cuadrática ternaria $\mathfrak{D}\langle a, b, -1\rangle$ tiene una representación racional (o entera) no trivial de cero si, y sólo si, existe una representación en $\mathbb{R}$ y, para cada primo p y cada entero positivo a, la congruencia

$$ax^2 + by^2 \equiv z^2 \pmod{p^a} \tag{5.3}$$

tiene una solución no trivial. En otras palabras, existe una solución racional para el problema isotrópico si, y sólo si, existen soluciones locales en cada módulo potencia de primo (soluciones p-ádicas) además de una solución real. Conforme el valor de a se incrementa, cada congruencia implica a las anteriores, lo que apunta a reunir todas esas interrogantes de existencia en una sola para cada primo. Esto motiva la siguiente terminología:

Definición (Isotropía local)**.** Una forma cuadrática $\mathfrak{q}$ es llamada p-isotrópica si para todo $a \in \mathbb{Z}^+$, la congruencia $\mathfrak{q}(\mathbf{x}) \equiv 0 \pmod{p^a}$ tiene una solución no trivial. De lo contrario se dirá que $\mathfrak{q}$ es p-anisotrópica. Se dirá que $\mathfrak{q}$ es ∞-isotrópica si tiene una solución real.

Considerando el caso de las formas $\mathfrak{D}\langle a, b, -1\rangle$, para cada primo p y para ∞ se formula una pregunta tipo sí/no: ¿Es $\mathfrak{D}\langle a, b, -1\rangle$ p-isotrópica? Siendo así, tiene sentido asociar «sí» con $+1$ y «no» con -1.

Notación. Para cada primo p, el símbolo $[a, b]_p$ toma el valor $+1$ si $\mathfrak{D}\langle a, b, -1\rangle$ es p-isotrópica, y -1 si es p-anisotrópica. Se define $[a, b]_\infty$ análogamente. Con frecuencia se reemplaza la expresión «para cada primo p y para ∞» con «para $p \leq \infty$».

Con esto, el lema de Legendre puede ser reformulado de la siguiente manera: $\mathfrak{D}\langle a, b, -1\rangle$ *es isotrópica si, y sólo si,* $[a, b]_p = 1$ *para todo* $p \leq \infty$. Es claro que la notación es muy ventajosa por ser tan compacta. También pone en evidencia propiedades que de otra forma serían difíciles de notar, tal como lo muestra Hilbert.

Teorema 18 (Hilbert)**.**

a) *Dados $a, b \in \mathbb{Z} \setminus \{0\}$, se cumple que $[a, b]_p = +1$ para $p \leq \infty$, excepto a lo sumo para una cantidad finita de valores de p.*

b) *Dos $\mathbb{Q}$-formas cuadráticas $\mathfrak{D}\langle a, b, -1\rangle$ y $\mathfrak{D}\langle c, d, -1\rangle$ son equivalentes (racionalmente) si, y sólo si, $[a, b]_p = [c, d]_p$ para cada $p \leq \infty$.*

c) *Dados $a, b \in \mathbb{Z} \setminus \{0\}$, el conjunto finito de valores p para los cuales $[a, b]_p = -1$ tiene una cantidad par de elementos.*

d) *Para cada conjunto finito S de valores de p, que tenga cardinalidad par, existen $a, b \in \mathbb{Z} \setminus \{0\}$ tales que $[a, b]_p = -1$ si, y sólo si, $p \in S$.*

Este teorema resuelve varios problemas de interés. En particular, los incisos *(b)* y *(d)* constituyen un primer avance en el problema de la clasificación de $\mathbb{Q}$-formas según $\sim$, la equivalencia racional (ver el problema 49, en el apéndice D). El inciso *(a)* asegura que el producto $\prod_{p \leq \infty} [a, b]_p$ está definido sin ambigüedad. Finalmente, el inciso *(c)* permite demostrar la siguiente relación, conocida como la *ley de reciprocidad de Hilbert*:

$$\prod_{p \leq \infty} [a, b]_p = 1 \tag{5.4}$$

En referencia al lema de Legendre, la ley propuesta por Hilbert[4] permite omitir uno de los valores de p en la búsqueda de soluciones locales. En particular, se puede omitir $p = \infty$ y obtener el siguiente resultado, que parece difícil de creer: $\mathfrak{D}\langle a, b, -1\rangle$ *es isotrópica si, y sólo si,* $[a, b]_p = 1$ *para todo* $p < \infty$. En otras palabras, la restricción sobre los signos de a, b, c en el enunciado original de Legendre (página 120), que se traduce en la existencia de soluciones reales ($p = \infty$), es implicada por la isotropía en cada módulo. También puede notarse que el caso $p = 2$ no puede deducirse de las

[4]**David Hilbert** (1862 – 1943) fue un famoso matemático nacido en Königsberg, Alemania. Se dice que Hilbert fue el último de los grandes matemáticos universales, conocedor de todas las ramas y disciplinas de la época, hizo importantes contribuciones a todas ellas. Los artículos de Hilbert incluyen resultados impresionantes en Álgebra y Teoría de Números; por ejemplo, resolvió el problema de Waring mediante métodos del Análisis Matemático. Su trabajo de 1899, *Grundlagen der Geometrie*, lo elevó a la fama internacional, porque se basó en una nueva forma de concebir la naturaleza de los axiomas. Hilbert adoptó un punto de vista formalista, que lo llevó a plantearse la tarea de construir una base lógica que fundamentara toda la estructura de las matemáticas, creando en el proceso la teoría de la Meta-matemática.

condiciones sobre residuos cuadráticos propuestas por Legendre, motivo por el cual él se vio obligado a incluir la condición para $p = \infty$.

Hilbert también encontró fórmulas explícitas para $[a, b]_p$ en términos de símbolos de Legendre [20]. Conociéndolas, la relación (5.4) es equivalente a la conjunción de la ley de reciprocidad cuadrática y sus suplementos. Si p, q son primos impares distintos, las fórmulas más elementales son:

- $[p, q]_p = \left(\frac{q}{p}\right)$
- $[p, q]_2 = (-1)^{(p-1)(q-1)/4}$

Si se toma $a = p, b = q$ en la ecuación (5.4), después de simplificar se obtiene la expresión que le otorga la categoría de ley de reciprocidad (comparar con el enunciado de Legendre en la página 15):

$$[p, q]_p \, [p, q]_q \, [p, q]_2 = 1$$

5.2.3. Hasse-Minkowski y el principio local-global

El teorema de Hasse-Minkowski es, probablemente, el resultado más fundamental en la teoría de las formas cuadráticas. Es una generalización para formas n-arias del teorema de Hilbert. En su forma más elemental, puede enunciarse de la siguiente manera:

Teorema de Hasse-Minkowski. *Sea* $\mathfrak{q}(\mathbf{x})$ *una* $\mathbb{Z}$*-forma cuadrática* n*-aria. Las siguientes proposiciones son equivalentes:*

a) $\mathfrak{q}$ *es isotrópica (sobre* $\mathbb{Z}$ *o sobre* $\mathbb{Q}$*).*

b) $\mathfrak{q}$ *es isotrópica sobre* $\mathbb{R}$ *y, para cada* $m \in \mathbb{Z}^+$*, existen soluciones no triviales para la congruencia* $\mathfrak{q}(\mathbf{x}) \equiv 0 \pmod{m}$*.*

Es claro que *(a)* implica *(b)*. De hecho, en forma contrapositiva se trata del método conocido como *análisis local*, del cual se discutió en la sección 1.4.2, página

28. Lo que es realmente interesante es la necesidad, la cual asegura que si la ecuación diofantina $\mathfrak{q}(\mathbf{x}) = 0$ no tiene soluciones, entonces el análisis local es capaz de demostrarlo. En otras palabras, el método es completo para esta familia de problemas diofánticos, todos ellos están dentro de su alcance. La única modificación que debe ser hecha es agregar una búsqueda de soluciones reales, que en el caso de las formas binarias consiste en calcular el discriminante de la forma $\mathfrak{q}$.

Hermann Minkowski[5] demostró este teorema para $\mathbb{Q}$-formas, y Helmut Hasse[6] lo generalizó para otros campos y lo redactó en su forma más conocida, que involucra números p-ádicos. Su enunciado no es tan explícito como el del lema de Legendre, pues este último daba un listado finito de condiciones de congruencias a verificar. Sin embargo, también es cierto en este contexto más ampllio que, para cada forma específica, existe un conjunto finito de módulos de los cuales depende la existencia de soluciones.

Aún sin conocer el listado finito de módulos asociados a cada forma cuadrática, el teorema provee un algoritmo que permite resolver el problema isotrópico para cualquier forma. Cada uno de los siguientes problemas, para un N fijo, se pueden resolver en un número finito de pasos:

- Verificar si existe una n-upla $(x_1, \ldots, x_n) = \mathbf{x}$ de números enteros, con la restricción $\max_i |x_i| = N$, que cumpla $\mathfrak{q}(\mathbf{x}) = 0$.
- Verificar si $\mathfrak{q}(\mathbf{x}) \equiv 0 \pmod{N}$ posee sólo la solución trivial.

El algoritmo es, entonces, resolver en paralelo ambos problemas para valores de N que se incrementen progresivamente, hasta que una de las verificaciones resulte

[5]**Hermann Minkowski** (1864 – 1909) fue un matemático ruso de origen lituano que desarrolló la Teoría Geométrica de Números. Sus trabajos más destacados fueron realizados en la Teoría de Números, la Física Matemática y la Teoría de la Relatividad. Fue uno de los profesores de Einstein. En 1907 se percató de que la Teoría Especial de la Relatividad, presentada por su antiguo alumno en 1905, y basada en trabajos anteriores de Lorentz y Poincaré, podía entenderse mejor en una geometría no-euclidiana de un espacio de cuatro dimensiones, desde entonces conocido como espacio de Minkowski. Él y Hilbert compartieron una profunda amistad.

[6]**Helmut Hasse** (1898 – 1979) fue un matemático alemán que trabajó en Teoría Algebraica de Números, conocido por sus contribuciones fundamentales a la Teoría de Cuerpos de Clases, la aplicación de números p-ádicos a la Teoría de Cuerpos de Clases Locales, a la Geometría Diofántica (principio de Hasse), y a las funciones zeta locales.

afirmativa. El teorema de Hasse-Minkowski asegura que exactamente uno de los dos problemas se resolverá afirmativamente, al menos para las formas cuadráticas, aunque puede haber múltiples soluciones para dicho problema.

Se puede crear un algoritmo semejante para formas de grado superior a 2, pero éste no es capaz de resolver el problema de la isotropía sin una generalización de Hasse-Minkowski que lo acompañe [7]. Así, resulta natural preguntarse si tal generalización es posible, para formas de grado superior, o incluso para polinomios que no sean homogéneos, como $2x^2 + 5y^3 - 7z^5$. Pero, como había sido discutido previamente (página 21), el resultado obtenido por Matiyasevich dice que no es posible hacerlo en el caso más general, así que se debe aceptar la limitación a polinomios específicos o, a lo sumo, familias de éstos. Siempre que para un polinomio se pueda resolver el problema de isotropía inspeccionándolo en los reales y en cada módulo, se dirá que el principio local-global, o principio de Hasse, se cumple para dicho polinomio.

El teorema de Matiyasevich aplica sólo a ecuaciones diofantinas, así que, por extraño que parezca, aún es posible que exista un algoritmo que determine si una ecuación con coeficientes racionales posee o no una solución racional. Por otro lado, uno podría pensar que los contraejemplos para el principio de Hasse podrían no ser tan «regulares» como las formas, que son polinomios homogéneos. Esta manera de pensar implica albergar la esperanza de generalizar Hasse-Minkowski a formas de orden superior, pero Selmer [34] niega categóricamente esta posibilidad, mostrando que la forma $3x^3+4y^3+5z^3$ viola el principio de Hasse. Para remarcar la singularidad del teorema, se puede señalar que, para cada grado arriba de 2, existen $\mathbb{Z}$-formas que violan el principio.

Regresando al tema de las formas cuadráticas binarias, las condiciones de congruencias que se deben satisfacer según el lema de Legendre son restricciones serias, pero, conforme el número de variables aumenta las restricciones se suavizan, hasta llegar a 5 o más variables, punto en el cual toda forma cuadrática posee soluciones no triviales en cualquier módulo. En otras palabras, el principio local-global se reduce al siguiente enunciado: *Dada una forma cuadrática n-aria $\mathfrak{q}$, con $n \geq 5$, la ecuación*

$\mathfrak{q}(\mathbf{x}) = 0$ *tiene una solución entera no trivial si, y sólo si, tiene una solución real no trivial.* Éste resultado sorprendente fue demostrado por Meyer [29].

5.3. La forma $x^2 + y^2$, sucesiones aritméticas de cuadrados enteros

Para cerrar el capítulo se mostrará explícitamente cómo la teoría de $\mathbb{Q}$-formas puede prestar auxilio en la solución de problemas sobre enteros que originalmente no parecen estar vinculados a los racionales. Esta idea encaja muy bien con el principio de equivalencia homogénea y el teorema 17 (página 117).

Si se consideran los primeros cuadrados perfectos: 1, 4, 9, 16, 25, 36, 49, 64, 81, 100, ... Puede apreciarse que tres de ellos están en progresión aritmética: 1, 25 y 49, cuya diferencia común es 24. Más adelante se encuentra la progresión: 289, 625 y 961. Si X^2, Z^2, Y^2 son tres enteros en progresión aritmética, en ese orden, entonces la diferencia común devuelve la ecuación $Y^2 - Z^2 = Z^2 - X^2$, o bien $X^2 + Y^2 = 2Z^2$, una ecuación cuasi-pitagórica. Conforme se continúa avanzando en la sucesión de cuadrados se encuentran otras ternas, y resulta natural conjeturar que existen infinitas soluciones. Esto se respalda en el hecho establecido de que la ecuación pitagórica original posee infinitas soluciones, que pueden ser parametrizadas con la fórmula de Euclides (página 26).

Problema. Determinar todas las ternas no triviales de enteros (X, Y, Z) que satisfagan la ecuación $X^2 + Y^2 = 2Z^2$. De ser posible, parametrizarlas con una fórmula generadora semejante a la de Euclides.

Por la homogeneidad de la ecuación, si una terna determinada es solución también lo será cualquiera de sus múltiplos, así que, cuando se conjeturó la existencia de infinitas soluciones, se pensaba sólo en las primitivas. Además, a excepción de la solución trivial, se tiene que $Z \neq 0$, así que se puede dividir entre Z^2 y tomar las nuevas variables racionales $x := \frac{X}{Z}$, $y := \frac{Y}{Z}$, para convertir el problema en uno de representabilidad en $\mathbb{Q}$. Considérese un par de racionales (x, y) que sea solución de la

ecuación $x^2 + y^2 = 2$, es decir, un punto racional en el círculo de radio 2 centrado en el origen. Reescribiendo x, y como fracciones empleando el mínimo común denominador: $\frac{X}{Z}, \frac{Y}{Z}$, se ve que (X, Y, Z) es solución primitiva del problema original, esto es, X^2, Z^2, Y^2 es una progresión aritmética de cuadrados enteros. Correspondientemente, $x^2, 1, y^2$ es una progresión aritmética de cuadrados racionales.

Problema equivalente. Determinar todos los puntos racionales (x, y) en el círculo $x^2 + y^2 = 2$. De ser posible parametrizar las soluciones.

La fórmula de Euclides emplea dos parámetros, primos relativos entre sí, para generar a las ternas. Este tipo de información se puede codificar igualmente en una fracción reducida, lo que promueve la idea de que, si es posible parametrizar los puntos racionales del círculo mencionado, bastaría un único parámetro racional. Esto se puede hacer de muchas maneras, se empleará una que resulta ventajosa para el propósito que se tiene. La respuesta del problema se enuncia como un teorema, y en su demostración se explica el proceso de parametrización elegido.

Teorema 19. *Los puntos racionales (ξ, η) en el círculo $x^2 + y^2 = 2$, a excepción del punto $(1, -1)$, están descritos por las fórmulas:*

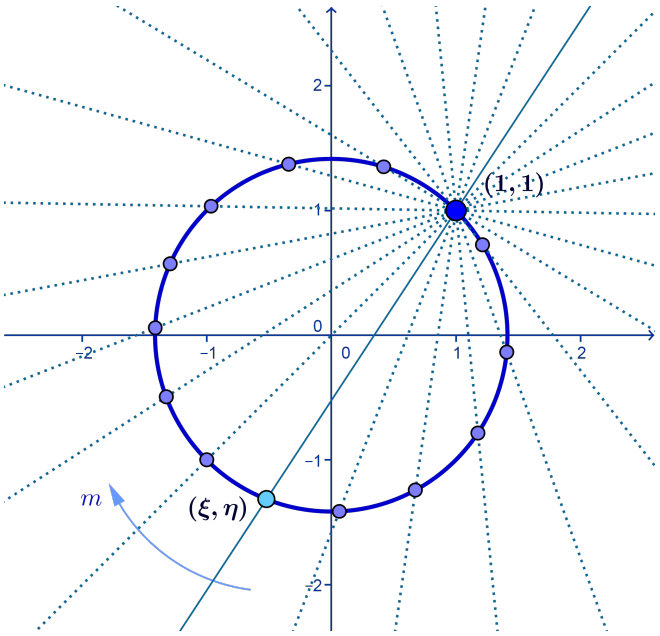
$$\xi = \frac{m^2 - 2m - 1}{m^2 + 1}, \qquad \eta = \frac{-m^2 - 2m + 1}{m^2 + 1}$$

donde $m \in \mathbb{Q}$. El punto $(1, -1)$ es generado tomando el límite cuando m tiende a $\pm\infty$. La correspondencia entre m y los otros puntos (ξ, η) es biunívoca.

Demostración. El punto $(1, 1)$ es una solución racional de la ecuación $x^2 + y^2 = 2$. Considere el haz de rectas que pasan por dicho punto (ver figura 6). Cada una de ellas, a excepción de la recta tangente, se intersectan nuevamente con el círculo en un punto distinto, esto es, los puntos en el círculo y los miembros del haz de rectas están asociados biunívocamente. Asimismo, a cada recta le corresponde biunívocamente una pendiente $m \in \mathbb{R}$ (a excepción de la recta vertical, que puede asociarse con $m = \pm\infty$), así que puede tomarse m como parámetro. Se quiere saber si, restringiendo m al conjunto $\mathbb{Q}$, la relación descrita lo asocia biunívocamente con todos los puntos de

coordenadas racionales en el círculo. Se obtendrán primero las fórmulas que asocian los puntos (ξ, η) en el círculo con el valor de m, y se estudiará después la restricción.

Figura 6. **Parametrización de las soluciones de $x^2 + y^2 = 2$**



Fuente: elaboración propia, mediante Geogebra 4.

Sea (ξ, η) un punto en el círculo distinto de $(1, -1)$. Si $(\xi, \eta) \neq (1, 1)$, se puede hallar la ecuación de la recta $y = mx + b$ que pasa por ambos puntos, encontrando el valor de b en términos de m. Si $(\xi, \eta) = (1, 1)$, entonces puede tomarse la recta tangente. En cualquier caso, se obtiene $b = 1 - m$. Sustituyendo la expresión $y = mx + (1 - m)$ en la ecuación del círculo, se obtiene una ecuación cuadrática cuyas soluciones deben ser 1 y ξ. La ecuación es

$$2 = x^2 + (mx + 1 - m)^2 = (m^2 + 1)x^2 + 2m(1 - m)x + (1 - m)^2$$

Restando 2 y dividiendo entre (m^2+1) se obtiene

$$x^2 + \frac{2m(1-m)}{m^2+1}x + \frac{m^2-2m-1}{m^2+1} = 0$$

Una vez más, las raíces del polinomio son $1, \xi$. Por las relaciones de Cardano-Vieta, el producto de las raíces debe ser igual al término independiente. Así se obtiene la fórmula para ξ. Sustituyendo en la ecuación de la recta se puede obtener la fórmula para η. Estas fórmulas son precisamente las del enunciado.

Ahora se procede a la inversa, hallando m en términos de (ξ, η). La fórmula de la pendiente entre dos puntos devuelve la relación $m = \frac{\eta-1}{\xi-1}$. Así, se tienen las siguientes correspondencias entre los puntos del círculo (exceptuando $(1,-1)$) y el parámetro m, que son inversas entre sí:

$$m \mapsto \left(\frac{m^2-2m-1}{m^2+1}, \frac{-m^2-2m+1}{m^2+1} \right), \qquad (\xi,\eta) \mapsto \begin{cases} \frac{\eta-1}{\xi-1} & \text{si } (\xi,\eta) \neq (1,1) \\ -1 & \text{si } (\xi,\eta) = (1,1) \end{cases}$$

La primera constata que si $m \in \mathbb{Q}$, entonces el punto (ξ, η) correspondiente tiene coordenadas racionales. La segunda indica que el recíproco también es cierto. La verificación del límite cuando m tiende a $\pm\infty$ es inmediata. Esto demuestra que el teorema es válido. $\square$

CONCLUSIONES

1. Las técnicas fundamentales en la resolución de problemas de representabilidad son: el descenso al infinito y el análisis local. Éstas son insuficientes para analizar el problema general, salvo para conjuntos específicos de formas. Tal es el caso de las formas cuadráticas.

2. La $\mathbb{Z}$-forma $x^2 - y^2$ representa a todos los enteros impares y a los múltiplos de 4. La $\mathbb{Z}$-forma $x^2 + y^2$ representa a los números tales que su factorización prima no incluya a un primo congruente con 3 en el módulo 4, elevado a una potencia impar. Una regla semejante es válida en el caso de $x^2 + xy + y^2$, para primos congruentes con 2 en el módulo 3.

3. Todo primo que sea representable en las formas $x^2 - y^2$ y $x^2 + y^2$ posee una única representación independiente. Las representaciones para números compuestos se pueden encontrar recursivamente en términos de las de sus divisores, empleando las cerraduras asociadas.

4. Existen (al menos) tres cerraduras generales para las $\mathbb{Z}$-formas cuadráticas binarias mónicas en una de las variables (página 98). Existe también una tricerradura general para todas las formas cuadráticas.

5. La estructura ternaria de la tricerradura se manifiesta en el conjunto de cerraduras de la forma $x^2 + xy + y^2$.

6. La ecuación diofantina pitagórica, y variaciones de ésta, como $x^2 + y^2 = 2z^2$, pueden ser resueltas de una manera más sencilla si se cambia el conjunto subyacente por $\mathbb{Q}$. Esta simplificación se observa de manera general en los problemas de representación.

RECOMENDACIONES

1. Si se desea estudiar el problema de determinar cotas para curvas de crecimiento de funciones $\mathcal{R}$, se debe profundizar más en la Teoría de Números Analítica. Lo mismo puede ser dicho acerca de la densidad del conjunto de números n para los cuales $\mathcal{R}(n)$ tenga un valor fijo.

2. Hace falta encontrar una demostración general, o un contraejemplo, para la hipótesis de que cualquier cerradura homogénea de una $\mathbb{Z}$-forma es reducida, salvo para las formas que son cuadrados perfectos. De cualquier manera, el interesado debe enfocarse en las formas de discriminante positivo.

3. El interesado en determinar un conjunto de representantes diagonales para las clases bajo $\sim$, de las $\mathbb{Q}$-formas cuadráticas n-arias, debe considerar las implicaciones del teorema de Hilbert (página 122), así como las del teorema de Hasse-Minkowski.

BIBLIOGRAFÍA

[1] AICARDI, Francesca; TIMORIN, Vladlen. "On binary quadratic forms with semigroup property". *Proceedings of the Steklov Institute of Mathematics*. 2007, vol. 258, núm. 1, p. 23–43. ISSN: 1531-8605.

[2] ANDREESCU, Titu; ANDRICA, Dorin. *Number theory: structures, examples and problems*. Boston: Birkhäuser, 2009. 410 p. ISBN: 0-81-763245-X.

[3] ANDREWS, George E. *Number theory*. New York: Springer Verlag, 1974. 259 p. ISBN: 0-7216-1255-5.

[4] ARNOL'D, Vladimir. "Arithmetics of binary quadratic forms, symmetry of their continued fractions and geometry of their de Sitter world". *Bulletin of the Brazilian Mathematical Society, New Series*. 2003, vol. 34, núm. 1, p. 1–42. ISSN: 1678-7714.

[5] BARNING, F.J.M. "On Pythagorean and quasi-Pythagorean triangles and a generation process with the help of unimodular matrices". *Math. Centrum Amsterdam Afd. Zuivere Wisk*. 1963, ZW-001.

[6] BEILER, Albert H. *Recreations in the theory of numbers, the queen of mathematics entertains*. 2nd ed. New York: Dover Publications, 1966. 349 p. ISBN: 4-86-21096-0.

[7] CLARK, Pete L. *Rational quadratic forms and the local-global principle* [en línea]. Math 4400/6400 – Number theory (lecture notes), 2009. <`http://math.uga.edu/~pete/4400rationalqf.pdf`> [Consulta: 31 de julio de 2013].

[8] CONWAY, John H. "Universal quadratic forms and the fifteen theorem". *Contemporary Mathematics: International conference on quadratic forms and their applications (1999: University College Dublin)*. 1999, vol. 272, p. 23–26. ISBN: 0-8218-2779-0.

[9] COX, David. *Primes of the form x^2+ny^2: Fermat, class field theory and complex multiplication*. Hoboken, New Jersey: John Wiley & Sons, 1989. 351 p. ISBN: 3-7643-3044-9.

[10] DAVENPORT, Harold. *The higher arithmetic*. Cambridge: University Press, 1982. 248 p. ISBN: 0-521-28678-6.

[11] DE ALEJANDRÍA, Diofanto. *"Arithmetica"* [en línea]. Bachet, Claude (trad. griego-latín); Heath, Thomas (trad. latín-inglés). En: HEATH, Thomas. *Diophantus of Alexandria, a study in the history of Greek algebra*. 2nd ed. Cambridge: University Press, 1910, 01-02-2004. <`http://archive.org/details/diophantusofalex010687mbp`> (descargable o en línea) [Consulta: 7 de enero de 2013].

[12] DE ALEJANDRÍA, Euclides. *Thirteen books of Euclid's Elements*. De Novara, Campanus (trad. griego-latín); Heath, Thomas (trad. latín-inglés). 2nd ed. New York: Dover Publications, 2007. Tres tomos. ISBN: 0-4864-6118-1.

[13] EARNEST, Andrew; FITZGERALD, Robert. "Multiplicative properties of integral binary quadratic forms". *Contemporary Mathematics: International conference on the algebraic and arithmetic theory of quadratic forms (2007: Frutillar, Chile)*. 2009, vol. 493, p. 107–116. ISBN: 978-0-8218-4648-3.

[14] EULER, Leonhard. *Introduction to the analysis of the infinite*. Blanton, J. (trad. latín-inglés). New York: Springer Verlag, 1988. Dos tomos. ISBN: 0-3879-6824-5.

[15] GAUSS, Carl Friedrich. *Disquisitiones arithmeticae*. Clarke, Arthur (trad. latín-inglés). New Haven, Connecticut: Yale University Press, 1966. Reimpreso por Springer Verlag, 1986. 500 p. ISBN: 0-387-96254-9.

[16] GROSSWALD, Emil. *Topics from the theory of numbers*. 2nd ed. Boston: Birkhäuser, 1984. 333 p. ISBN: 3-7643-3044-9.

[17] HALMOS, Paul R. *Naive set theory*. New York: W. B. Saunders, 1971. 104 p. ISBN: 0-38-790092-6.

[18] HARDY, Godfrey; WRIGHT, Eduard. *An introduction to the theory of numbers*. 4th ed. Oxford: Oxford University Press, 1975. 421 p. ISBN: 0-19-853310-7.

[19] HERNSTEIN, I. N. *Abstract algebra*. 3rd ed. Hoboken, New Jersey: John Wiley & Sons, 1996. 274 p. ISBN: 0-47-136879-2.

[20] HILBERT, David. *The theory of algebraic number fields*. Adamson, Iain (trad. alemán-inglés). Berlin: Springer Verlag, 1998. 350 p. ISBN: 3-540-62779-0.

[21] HUXLEY, M. N. "Exponential sums and lattice points III". *Proceedings of the London Mathematical Society*. 2003, vol. 87, núm. 3, p. 591–609.

[22] IRELAND, Kenneth; ROSEN, Michael. *A classical introduction to modern number theory (Graduate Texts in Mathematics)*. 2nd ed. New York: Springer Verlag, 1990. 397 p. ISBN: 3-540-97329-X.

[23] KAYE, George R. "Indian mathematics". *Isis*. 1919, vol. 2, núm. 2, p. 326–356.

[24] KITAOKA, Yoshiyuki. *Arithmetic of quadratic forms*. Cambridge Tracts in Mathematics 106. United States of America: Cambridge University Press, 1993. 284 p. ISBN 0-521-40475-4, Zbl 0785.11021.

[25] LANG, Serge. *Introduction to linear algebra*. 2nd ed. New York: Springer Verlag, 1985. 304 p. ISBN: 0-38-796205-0.

[26] LEMMERMEYER, Franz. *Reciprocity laws: from Euler to Eisenstein*. Monographs in Mathematics. New York: Springer Verlag, 2000. 489 p. ISBN: 3-54-066957-4.

[27] LENSTRA, Hendrik W. "Solving the Pell Equation". *Notices of the American Mathematical Society*. 2002, vol. 49, núm. 2, p. 182–192.

[28] MATIYASEVICH, Yuri. *Hilbert's tenth problem*. Cambridge, Massachusetts: MIT Press, 1993. 288 p. ISBN: 0-26-213295-8.

[29] MEYER, A. "Mathematische Mittheilungen". *Vierteljahrschrift der Naturforschenden Gesellschaft in Zürich*. 1884, vol. 29, p. 209–222.

[30] NIVEN, Ivan. "Quadratic diophantine equations in the rational and quadratic fields". *Transactions of the American Mathematical Society*. 1942, vol. 52, núm. 1, p. 1–11.

[31] NEUKIRCH, Jürgen. *Algebraic number theory*, Grundlehren der mathematischen Wissenschaften 322. Berlin: Springer-Verlag, 1999. 574 p. ISBN 978-3-540-65399-8.

[32] PRICE, H. Lee. "The Pythagorean Tree: a new species" [en línea]. *ArXiv*. 2008, eprint arXiv: 0809.4324, 24-10-2011. <`http://arxiv.org/pdf/0809.4324v2.pdf`> [Consulta: 15 de enero de 2013].

[33] RAHN, Johann; PELL, John. *An introduction to algebra*. Brancker, Thomas (trad. altogermánico-inglés). London: W.G., 1668. 248 p. Early English Books Series. OCLC: 12255003.

[34] SELMER, Ernst S. "The Diophantine Equation $ax^3 + by^3 + cz^3 = 0$". *Acta Mathematica*. 1957, vol. 85, p. 203–362.

[35] STILLWELL, John. *Mathematics and its history*. 2nd ed. New York: Springer Verlag, 2002. 684 p. ISBN: 978-0-387-95336-6.

[36] WEIL, André. *Number theory: an approach through history; from Hammurapi to Legendre*. Boston: Birkhäuser, 1983. 375 p. ISBN: 3-7643-3141-0.

APÉNDICES

A. EXHAUSTIONES MAYORES

Para poder tomar directamente los valores de las exhaustiones menores, se ha colocado primero el cuarteto (h_1, k_1, h_2, k_2) y luego (h_3, k_3, h_4, k_4). Cuando se encuentren las soluciones, se deben reordenar para formar el octeto $(h_1, h_2, h_3, h_4; k_1, k_2, k_3, k_4)$ que corresponde a los coeficientes de X, Y en las cerraduras.

A.1. Exhaustión mayor de las cerraduras de $\langle 1, 0, 1 \rangle$

$$\begin{cases} 0 &= h_1h_3 + k_1k_3 & \text{(R-4)} \\ 0 &= h_1h_4 + h_2h_3 + k_1k_4 + k_2k_3 & \text{(R-5)} \\ 0 &= h_2h_4 + k_2k_4 & \text{(R-6)} \end{cases}$$

h_1	k_1	h_2	k_2	h_3	k_3	h_4	k_4	R-4	R-5	R-6	solución
1	0	0	1	1	0	0	1	1	0	1	·
1	0	0	1	1	0	0	−1	1	0	−1	·
1	0	0	1	−1	0	0	1	−1	0	1	·
1	0	0	1	−1	0	0	−1	−1	0	−1	·
1	0	0	1	0	1	1	0	0	2	0	·
1	0	0	1	0	1	−1	0	0	0	0	✓
1	0	0	1	0	−1	1	0	0	0	0	✓
1	0	0	1	0	−1	−1	0	0	−2	0	·
1	0	0	−1	1	0	0	1	1	0	−1	·
1	0	0	−1	1	0	0	−1	1	0	1	·
1	0	0	−1	−1	0	0	1	−1	0	−1	·
1	0	0	−1	−1	0	0	−1	−1	0	1	·
1	0	0	−1	0	1	1	0	0	0	0	✓
1	0	0	−1	0	1	−1	0	0	−2	0	·
1	0	0	−1	0	−1	1	0	0	2	0	·
1	0	0	−1	0	−1	−1	0	0	0	0	✓
−1	0	0	1	1	0	0	1	−1	0	1	·

continúa

h_1	k_1	h_2	k_2	h_3	k_3	h_4	k_4	R-4	R-5	R-6	solución
−1	0	0	1	1	0	0	−1	−1	0	−1	·
−1	0	0	1	−1	0	0	1	1	0	1	·
−1	0	0	1	−1	0	0	−1	1	0	−1	·
−1	0	0	1	0	1	1	0	0	0	0	✓
−1	0	0	1	0	1	−1	0	0	2	0	·
−1	0	0	1	0	−1	1	0	0	−2	0	·
−1	0	0	1	0	−1	−1	0	0	0	0	✓
−1	0	0	−1	1	0	0	1	−1	0	−1	·
−1	0	0	−1	1	0	0	−1	−1	0	1	·
−1	0	0	−1	−1	0	0	1	1	0	−1	·
−1	0	0	−1	−1	0	0	−1	1	0	1	·
−1	0	0	−1	0	1	1	0	0	−2	0	·
−1	0	0	−1	0	1	−1	0	0	0	0	✓
−1	0	0	−1	0	−1	1	0	0	0	0	✓
−1	0	0	−1	0	−1	−1	0	0	2	0	·
0	1	1	0	1	0	0	1	0	2	0	·
0	1	1	0	1	0	0	−1	0	0	0	✓
0	1	1	0	−1	0	0	1	0	0	0	✓
0	1	1	0	−1	0	0	−1	0	−2	0	·
0	1	1	0	0	1	1	0	1	0	1	·
0	1	1	0	0	1	−1	0	1	0	−1	·
0	1	1	0	0	−1	1	0	−1	0	1	·
0	1	1	0	0	−1	−1	0	−1	0	−1	·
0	1	−1	0	1	0	0	1	0	0	0	✓
0	1	−1	0	1	0	0	−1	0	−2	0	·
0	1	−1	0	−1	0	0	1	0	2	0	·
0	1	−1	0	−1	0	0	−1	0	0	0	✓
0	1	−1	0	0	1	1	0	1	0	−1	·
0	1	−1	0	0	1	−1	0	1	0	1	·
0	1	−1	0	0	−1	1	0	−1	0	−1	·
0	1	−1	0	0	−1	−1	0	−1	0	1	·
0	−1	1	0	1	0	0	1	0	0	0	✓
0	−1	1	0	1	0	0	−1	0	2	0	·
0	−1	1	0	−1	0	0	1	0	−2	0	·
0	−1	1	0	−1	0	0	−1	0	0	0	✓
0	−1	1	0	0	1	1	0	−1	0	1	·
0	−1	1	0	0	1	−1	0	−1	0	−1	·
0	−1	1	0	0	−1	1	0	1	0	1	·
0	−1	1	0	0	−1	−1	0	1	0	−1	·
0	−1	−1	0	1	0	0	1	0	−2	0	·
0	−1	−1	0	1	0	0	−1	0	0	0	✓

continúa

h_1	k_1	h_2	k_2	h_3	k_3	h_4	k_4	R-4	R-5	R-6	solución
0	−1	−1	0	−1	0	0	1	0	0	0	✓
0	−1	−1	0	−1	0	0	−1	0	2	0	·
0	−1	−1	0	0	1	1	0	−1	0	−1	·
0	−1	−1	0	0	1	−1	0	−1	0	1	·
0	−1	−1	0	0	−1	1	0	1	0	−1	·
0	−1	−1	0	0	−1	−1	0	1	0	1	·

A.2. Exhaustión mayor de las cerraduras de $\langle 1, 1, 1\rangle$

$$\begin{cases} 1 &= 2h_1h_3 + h_1k_3 + h_3k_1 + 2k_1k_3 & \text{(R-4)} \\ 1 &= 2(h_1h_4 + h_2h_3) + h_1k_4 + h_4k_1 + h_2k_3 + h_3k_2 + 2(k_1k_4 + k_2k_3) & \text{(R-5)} \\ 1 &= 2h_2h_4 + h_2k_4 + h_4k_2 + 2k_2k_4 & \text{(R-6)} \end{cases}$$

h_1	k_1	h_2	k_2	h_3	k_3	h_4	k_4	R-4	R-5	R-6	solución
1	−1	1	0	1	−1	1	0	2	2	2	·
1	−1	1	0	1	−1	0	−1	2	2	−1	·
1	−1	1	0	1	0	1	−1	1	4	1	·
1	−1	1	0	1	0	0	1	1	1	1	✓
1	−1	1	0	−1	0	−1	1	−1	−4	−1	·
1	−1	1	0	−1	0	0	−1	−1	−1	−1	·
1	−1	1	0	−1	1	−1	0	−2	−2	−2	·
1	−1	1	0	−1	1	0	1	−2	−2	1	·
1	−1	1	0	0	1	1	0	−1	2	2	·
1	−1	1	0	0	1	−1	1	−1	−1	−1	·
1	−1	1	0	0	−1	1	−1	1	1	1	✓
1	−1	1	0	0	−1	−1	0	1	−2	−2	·
1	−1	0	−1	1	−1	1	0	2	2	−1	·
1	−1	0	−1	1	−1	0	−1	2	2	2	·
1	−1	0	−1	1	0	1	−1	1	1	1	✓
1	−1	0	−1	1	0	0	1	1	−2	−2	·
1	−1	0	−1	−1	0	−1	1	−1	−1	−1	·
1	−1	0	−1	−1	0	0	−1	−1	2	2	·
1	−1	0	−1	−1	1	−1	0	−2	−2	1	·
1	−1	0	−1	−1	1	0	1	−2	−2	−2	·

continúa

h_1	k_1	h_2	k_2	h_3	k_3	h_4	k_4	R-4	R-5	R-6	solución
1	−1	0	−1	0	1	1	0	−1	−1	−1	·
1	−1	0	−1	0	1	−1	1	−1	−4	−1	·
1	−1	0	−1	0	−1	1	−1	1	4	1	·
1	−1	0	−1	0	−1	−1	0	1	1	1	✓
1	0	1	−1	1	−1	1	0	1	4	1	·
1	0	1	−1	1	−1	0	−1	1	1	1	✓
1	0	1	−1	1	0	1	−1	2	2	2	·
1	0	1	−1	1	0	0	1	2	2	−1	·
1	0	1	−1	−1	0	−1	1	−2	−2	−2	·
1	0	1	−1	−1	0	0	−1	−2	−2	1	·
1	0	1	−1	−1	1	−1	0	−1	−4	−1	·
1	0	1	−1	−1	1	0	1	−1	−1	−1	·
1	0	1	−1	0	1	1	0	1	1	1	✓
1	0	1	−1	0	1	−1	1	1	−2	−2	·
1	0	1	−1	0	−1	1	−1	−1	2	2	·
1	0	1	−1	0	−1	−1	0	−1	−1	−1	·
1	0	0	1	1	−1	1	0	1	1	1	✓
1	0	0	1	1	−1	0	−1	1	−2	−2	·
1	0	0	1	1	0	1	−1	2	2	−1	·
1	0	0	1	1	0	0	1	2	2	2	·
1	0	0	1	−1	0	−1	1	−2	−2	1	·
1	0	0	1	−1	0	0	−1	−2	−2	−2	·
1	0	0	1	−1	1	−1	0	−1	−1	−1	·
1	0	0	1	−1	1	0	1	−1	2	2	·
1	0	0	1	0	1	1	0	1	4	1	·
1	0	0	1	0	1	−1	1	1	1	1	✓
1	0	0	1	0	−1	1	−1	−1	−1	−1	·
1	0	0	1	0	−1	−1	0	−1	−4	−1	·
−1	0	−1	1	1	−1	1	0	−1	−4	−1	·
−1	0	−1	1	1	−1	0	−1	−1	−1	−1	·
−1	0	−1	1	1	0	1	−1	−2	−2	−2	·
−1	0	−1	1	1	0	0	1	−2	−2	1	·
−1	0	−1	1	−1	0	−1	1	2	2	2	·
−1	0	−1	1	−1	0	0	−1	2	2	−1	·
−1	0	−1	1	−1	1	−1	0	1	4	1	·
−1	0	−1	1	−1	1	0	1	1	1	1	✓
−1	0	−1	1	0	1	1	0	−1	−1	−1	·
−1	0	−1	1	0	1	−1	1	−1	2	2	·
−1	0	−1	1	0	−1	1	−1	1	−2	−2	·
−1	0	−1	1	0	−1	−1	0	1	1	1	✓
−1	0	0	−1	1	−1	1	0	−1	−1	−1	·

continúa

h_1	k_1	h_2	k_2	h_3	k_3	h_4	k_4	R-4	R-5	R-6	solución
−1	0	0	−1	1	−1	0	−1	−1	2	2	·
−1	0	0	−1	1	0	1	−1	−2	−2	1	·
−1	0	0	−1	1	0	0	1	−2	−2	−2	·
−1	0	0	−1	−1	0	−1	1	2	2	−1	·
−1	0	0	−1	−1	0	0	−1	2	2	2	·
−1	0	0	−1	−1	1	−1	0	1	1	1	✓
−1	0	0	−1	−1	1	0	1	1	−2	−2	·
−1	0	0	−1	0	1	1	0	−1	−4	−1	·
−1	0	0	−1	0	1	−1	1	−1	−1	−1	·
−1	0	0	−1	0	−1	1	−1	1	1	1	✓
−1	0	0	−1	0	−1	−1	0	1	4	1	·
−1	1	−1	0	1	−1	1	0	−2	−2	−2	·
−1	1	−1	0	1	−1	0	−1	−2	−2	1	·
−1	1	−1	0	1	0	1	−1	−1	−4	−1	·
−1	1	−1	0	1	0	0	1	−1	−1	−1	·
−1	1	−1	0	−1	0	−1	1	1	4	1	·
−1	1	−1	0	−1	0	0	−1	1	1	1	✓
−1	1	−1	0	−1	1	−1	0	2	2	2	·
−1	1	−1	0	−1	1	0	1	2	2	−1	·
−1	1	−1	0	0	1	1	0	1	−2	−2	·
−1	1	−1	0	0	1	−1	1	1	1	1	✓
−1	1	−1	0	0	−1	1	−1	−1	−1	−1	·
−1	1	−1	0	0	−1	−1	0	−1	2	2	·
−1	1	0	1	1	−1	1	0	−2	−2	1	·
−1	1	0	1	1	−1	0	−1	−2	−2	−2	·
−1	1	0	1	1	0	1	−1	−1	−1	−1	·
−1	1	0	1	1	0	0	1	−1	2	2	·
−1	1	0	1	−1	0	−1	1	1	1	1	✓
−1	1	0	1	−1	0	0	−1	1	−2	−2	·
−1	1	0	1	−1	1	−1	0	2	2	−1	·
−1	1	0	1	−1	1	0	1	2	2	2	·
−1	1	0	1	0	1	1	0	1	1	1	✓
−1	1	0	1	0	1	−1	1	1	4	1	·
−1	1	0	1	0	−1	1	−1	−1	−4	−1	·
−1	1	0	1	0	−1	−1	0	−1	−1	−1	·
0	1	1	0	1	−1	1	0	−1	2	2	·
0	1	1	0	1	−1	0	−1	−1	−1	−1	·
0	1	1	0	1	0	1	−1	1	1	1	✓
0	1	1	0	1	0	0	1	1	4	1	·
0	1	1	0	−1	0	−1	1	−1	−1	−1	·
0	1	1	0	−1	0	0	−1	−1	−4	−1	·

continúa

h_1	k_1	h_2	k_2	h_3	k_3	h_4	k_4	R-4	R-5	R-6	solución
0	1	1	0	−1	1	−1	0	1	−2	−2	·
0	1	1	0	−1	1	0	1	1	1	1	✓
0	1	1	0	0	1	1	0	2	2	2	·
0	1	1	0	0	1	−1	1	2	2	−1	·
0	1	1	0	0	−1	1	−1	−2	−2	1	·
0	1	1	0	0	−1	−1	0	−2	−2	−2	·
0	1	−1	1	1	−1	1	0	−1	−1	−1	·
0	1	−1	1	1	−1	0	−1	−1	−4	−1	·
0	1	−1	1	1	0	1	−1	1	−2	−2	·
0	1	−1	1	1	0	0	1	1	1	1	✓
0	1	−1	1	−1	0	−1	1	−1	2	2	·
0	1	−1	1	−1	0	0	−1	−1	−1	−1	·
0	1	−1	1	−1	1	−1	0	1	1	1	✓
0	1	−1	1	−1	1	0	1	1	4	1	·
0	1	−1	1	0	1	1	0	2	2	−1	·
0	1	−1	1	0	1	−1	1	2	2	2	·
0	1	−1	1	0	−1	1	−1	−2	−2	−2	·
0	1	−1	1	0	−1	−1	0	−2	−2	1	·
0	−1	1	−1	1	−1	1	0	1	1	1	✓
0	−1	1	−1	1	−1	0	−1	1	4	1	·
0	−1	1	−1	1	0	1	−1	−1	2	2	·
0	−1	1	−1	1	0	0	1	−1	−1	−1	·
0	−1	1	−1	−1	0	−1	1	1	−2	−2	·
0	−1	1	−1	−1	0	0	−1	1	1	1	✓
0	−1	1	−1	−1	1	−1	0	−1	−1	−1	·
0	−1	1	−1	−1	1	0	1	−1	−4	−1	·
0	−1	1	−1	0	1	1	0	−2	−2	1	·
0	−1	1	−1	0	1	−1	1	−2	−2	−2	·
0	−1	1	−1	0	−1	1	−1	2	2	2	·
0	−1	1	−1	0	−1	−1	0	2	2	−1	·
0	−1	−1	0	1	−1	1	0	1	−2	−2	·
0	−1	−1	0	1	−1	0	−1	1	1	1	✓
0	−1	−1	0	1	0	1	−1	−1	−1	−1	·
0	−1	−1	0	1	0	0	1	−1	−4	−1	·
0	−1	−1	0	−1	0	−1	1	1	1	1	✓
0	−1	−1	0	−1	0	0	−1	1	4	1	·
0	−1	−1	0	−1	1	−1	0	−1	2	2	·
0	−1	−1	0	−1	1	0	1	−1	−1	−1	·
0	−1	−1	0	0	1	1	0	−2	−2	−2	·
0	−1	−1	0	0	1	−1	1	−2	−2	1	·
0	−1	−1	0	0	−1	1	−1	2	2	−1	·
0	−1	−1	0	0	−1	−1	0	2	2	2	·

B. ℕ-FORMAS DIAGONALES UNIVERSALES Y CUASI-UNIVERSALES

Para representar a formas cuadráticas diagonales se usará el símbolo $\mathfrak{D}$ antes de la forma. Así, por ejemplo, $\mathfrak{D}\langle a,b,c,d\rangle$ representa a la expresión $aw^2+bx^2+cy^2+dz^2$. En este apartado se listan las 54 ℕ-formas digonales universales de Ramanujan, y también todas las ℕ-formas diagonales con déficit 1 o 2. D es el conjunto de números que no son representables en la forma dada. Eliminando del listado las variaciones triviales, Ramanujan exigió $a \leq b \leq c \leq d$, y aquí se seguirá el mismo convenio.

B.1. ℕ-formas universales de Ramanujan

$\mathfrak{D}\langle 1,1,1,1\rangle$	$\mathfrak{D}\langle 1,1,1,2\rangle$	$\mathfrak{D}\langle 1,1,1,3\rangle$	$\mathfrak{D}\langle 1,1,1,4\rangle$	$\mathfrak{D}\langle 1,1,1,5\rangle$	$\mathfrak{D}\langle 1,1,1,6\rangle$
$\mathfrak{D}\langle 1,1,1,7\rangle$	$\mathfrak{D}\langle 1,1,2,2\rangle$	$\mathfrak{D}\langle 1,1,2,3\rangle$	$\mathfrak{D}\langle 1,1,2,4\rangle$	$\mathfrak{D}\langle 1,1,2,5\rangle$	$\mathfrak{D}\langle 1,1,2,6\rangle$
$\mathfrak{D}\langle 1,1,2,7\rangle$	$\mathfrak{D}\langle 1,1,2,8\rangle$	$\mathfrak{D}\langle 1,1,2,9\rangle$	$\mathfrak{D}\langle 1,1,2,10\rangle$	$\mathfrak{D}\langle 1,1,2,11\rangle$	$\mathfrak{D}\langle 1,1,2,12\rangle$
$\mathfrak{D}\langle 1,1,2,13\rangle$	$\mathfrak{D}\langle 1,1,2,14\rangle$	$\mathfrak{D}\langle 1,1,3,3\rangle$	$\mathfrak{D}\langle 1,1,3,4\rangle$	$\mathfrak{D}\langle 1,1,3,5\rangle$	$\mathfrak{D}\langle 1,1,3,6\rangle$
$\mathfrak{D}\langle 1,2,2,2\rangle$	$\mathfrak{D}\langle 1,2,2,3\rangle$	$\mathfrak{D}\langle 1,2,2,4\rangle$	$\mathfrak{D}\langle 1,2,2,5\rangle$	$\mathfrak{D}\langle 1,2,2,6\rangle$	$\mathfrak{D}\langle 1,2,2,7\rangle$
$\mathfrak{D}\langle 1,2,3,3\rangle$	$\mathfrak{D}\langle 1,2,3,4\rangle$	$\mathfrak{D}\langle 1,2,3,5\rangle$	$\mathfrak{D}\langle 1,2,3,6\rangle$	$\mathfrak{D}\langle 1,2,3,7\rangle$	$\mathfrak{D}\langle 1,2,3,8\rangle$
$\mathfrak{D}\langle 1,2,3,9\rangle$	$\mathfrak{D}\langle 1,2,3,10\rangle$	$\mathfrak{D}\langle 1,2,4,4\rangle$	$\mathfrak{D}\langle 1,2,4,5\rangle$	$\mathfrak{D}\langle 1,2,4,6\rangle$	$\mathfrak{D}\langle 1,2,4,7\rangle$
$\mathfrak{D}\langle 1,2,4,8\rangle$	$\mathfrak{D}\langle 1,2,4,9\rangle$	$\mathfrak{D}\langle 1,2,4,10\rangle$	$\mathfrak{D}\langle 1,2,4,11\rangle$	$\mathfrak{D}\langle 1,2,4,12\rangle$	$\mathfrak{D}\langle 1,2,4,13\rangle$
$\mathfrak{D}\langle 1,2,4,14\rangle$	$\mathfrak{D}\langle 1,2,5,6\rangle$	$\mathfrak{D}\langle 1,2,5,7\rangle$	$\mathfrak{D}\langle 1,2,5,8\rangle$	$\mathfrak{D}\langle 1,2,5,9\rangle$	$\mathfrak{D}\langle 1,2,5,10\rangle$

B.2. ℕ-formas diagonales cuasi-universales de déficit 1

forma	D	forma	D	forma	D	forma	D
$\mathfrak{D}\langle 1,1,1,9\rangle$	$\{7\}$	$\mathfrak{D}\langle 1,1,1,10\rangle$	$\{7\}$	$\mathfrak{D}\langle 1,1,1,12\rangle$	$\{7\}$	$\mathfrak{D}\langle 1,1,1,14\rangle$	$\{7\}$
$\mathfrak{D}\langle 1,1,1,15\rangle$	$\{7\}$	$\mathfrak{D}\langle 1,1,2,15\rangle$	$\{14\}$	$\mathfrak{D}\langle 1,1,2,17\rangle$	$\{14\}$	$\mathfrak{D}\langle 1,1,2,18\rangle$	$\{14\}$
$\mathfrak{D}\langle 1,1,2,19\rangle$	$\{14\}$	$\mathfrak{D}\langle 1,1,2,20\rangle$	$\{14\}$	$\mathfrak{D}\langle 1,1,2,21\rangle$	$\{14\}$	$\mathfrak{D}\langle 1,1,2,23\rangle$	$\{14\}$
$\mathfrak{D}\langle 1,1,2,19\rangle$	$\{14\}$	$\mathfrak{D}\langle 1,1,2,20\rangle$	$\{14\}$	$\mathfrak{D}\langle 1,1,2,21\rangle$	$\{14\}$	$\mathfrak{D}\langle 1,1,2,23\rangle$	$\{14\}$

continúa

forma	D	forma	D	forma	D	forma	D
$\mathfrak{D}\langle 1,1,2,24\rangle$	$\{14\}$	$\mathfrak{D}\langle 1,1,2,25\rangle$	$\{14\}$	$\mathfrak{D}\langle 1,1,2,27\rangle$	$\{14\}$	$\mathfrak{D}\langle 1,1,2,28\rangle$	$\{14\}$
$\mathfrak{D}\langle 1,1,2,29\rangle$	$\{14\}$	$\mathfrak{D}\langle 1,1,2,30\rangle$	$\{14\}$	$\mathfrak{D}\langle 1,1,3,7\rangle$	$\{6\}$	$\mathfrak{D}\langle 1,1,3,8\rangle$	$\{6\}$
$\mathfrak{D}\langle 1,1,3,10\rangle$	$\{14\}$	$\mathfrak{D}\langle 1,1,3,11\rangle$	$\{14\}$	$\mathfrak{D}\langle 1,1,3,13\rangle$	$\{6\}$	$\mathfrak{D}\langle 1,1,3,14\rangle$	$\{6\}$
$\mathfrak{D}\langle 1,1,3,15\rangle$	$\{6\}$	$\mathfrak{D}\langle 1,1,4,5\rangle$	$\{3\}$	$\mathfrak{D}\langle 1,1,4,6\rangle$	$\{3\}$	$\mathfrak{D}\langle 1,1,5,5\rangle$	$\{3\}$
$\mathfrak{D}\langle 1,1,5,6\rangle$	$\{3\}$	$\mathfrak{D}\langle 1,1,5,10\rangle$	$\{3\}$	$\mathfrak{D}\langle 1,1,5,11\rangle$	$\{3\}$	$\mathfrak{D}\langle 1,1,6,7\rangle$	$\{3\}$
$\mathfrak{D}\langle 1,1,6,8\rangle$	$\{3\}$	$\mathfrak{D}\langle 1,1,6,10\rangle$	$\{3\}$	$\mathfrak{D}\langle 1,1,6,11\rangle$	$\{3\}$	$\mathfrak{D}\langle 1,2,2,9\rangle$	$\{7\}$
$\mathfrak{D}\langle 1,2,2,10\rangle$	$\{7\}$	$\mathfrak{D}\langle 1,2,2,12\rangle$	$\{7\}$	$\mathfrak{D}\langle 1,2,2,14\rangle$	$\{7\}$	$\mathfrak{D}\langle 1,2,2,15\rangle$	$\{7\}$
$\mathfrak{D}\langle 1,2,3,11\rangle$	$\{10\}$	$\mathfrak{D}\langle 1,2,3,12\rangle$	$\{10\}$	$\mathfrak{D}\langle 1,2,3,13\rangle$	$\{10\}$	$\mathfrak{D}\langle 1,2,3,15\rangle$	$\{10\}$
$\mathfrak{D}\langle 1,2,3,17\rangle$	$\{10\}$	$\mathfrak{D}\langle 1,2,3,19\rangle$	$\{10\}$	$\mathfrak{D}\langle 1,2,3,20\rangle$	$\{10\}$	$\mathfrak{D}\langle 1,2,3,21\rangle$	$\{10\}$
$\mathfrak{D}\langle 1,2,3,22\rangle$	$\{10\}$	$\mathfrak{D}\langle 1,2,3,23\rangle$	$\{10\}$	$\mathfrak{D}\langle 1,2,3,24\rangle$	$\{10\}$	$\mathfrak{D}\langle 1,2,3,25\rangle$	$\{10\}$
$\mathfrak{D}\langle 1,2,3,26\rangle$	$\{10\}$	$\mathfrak{D}\langle 1,2,4,15\rangle$	$\{14\}$	$\mathfrak{D}\langle 1,2,4,17\rangle$	$\{14\}$	$\mathfrak{D}\langle 1,2,4,18\rangle$	$\{14\}$
$\mathfrak{D}\langle 1,2,4,19\rangle$	$\{14\}$	$\mathfrak{D}\langle 1,2,4,20\rangle$	$\{14\}$	$\mathfrak{D}\langle 1,2,4,21\rangle$	$\{14\}$	$\mathfrak{D}\langle 1,2,4,23\rangle$	$\{14\}$
$\mathfrak{D}\langle 1,2,4,24\rangle$	$\{14\}$	$\mathfrak{D}\langle 1,2,4,25\rangle$	$\{14\}$	$\mathfrak{D}\langle 1,2,4,27\rangle$	$\{14\}$	$\mathfrak{D}\langle 1,2,4,28\rangle$	$\{14\}$
$\mathfrak{D}\langle 1,2,4,29\rangle$	$\{14\}$	$\mathfrak{D}\langle 1,2,4,30\rangle$	$\{14\}$	$\mathfrak{D}\langle 1,2,5,5\rangle$	$\{15\}$	$\mathfrak{D}\langle 1,2,5,11\rangle$	$\{10\}$
$\mathfrak{D}\langle 1,2,5,12\rangle$	$\{10\}$	$\mathfrak{D}\langle 1,2,5,13\rangle$	$\{10\}$	$\mathfrak{D}\langle 1,2,5,14\rangle$	$\{10\}$	$\mathfrak{D}\langle 1,2,6,6\rangle$	$\{5\}$
$\mathfrak{D}\langle 1,2,6,10\rangle$	$\{5\}$	$\mathfrak{D}\langle 1,2,6,11\rangle$	$\{5\}$	$\mathfrak{D}\langle 1,2,6,12\rangle$	$\{5\}$	$\mathfrak{D}\langle 1,2,6,13\rangle$	$\{5\}$
$\mathfrak{D}\langle 1,2,7,8\rangle$	$\{5\}$	$\mathfrak{D}\langle 1,2,7,10\rangle$	$\{5\}$	$\mathfrak{D}\langle 1,2,7,11\rangle$	$\{5\}$	$\mathfrak{D}\langle 1,2,7,12\rangle$	$\{5\}$
$\mathfrak{D}\langle 1,2,7,13\rangle$	$\{5\}$	$\mathfrak{D}\langle 1,3,3,5\rangle$	$\{2\}$	$\mathfrak{D}\langle 1,3,5,6\rangle$	$\{2\}$	$\mathfrak{D}\langle 2,2,3,4\rangle$	$\{1\}$
$\mathfrak{D}\langle 2,3,4,5\rangle$	$\{1\}$	$\mathfrak{D}\langle 2,3,4,8\rangle$	$\{1\}$				

B.3. ℕ-formas diagonales cuasi-universales de déficit 2

forma	D	forma	D	forma	D
$\mathfrak{D}\langle 1,1,1,11\rangle$	$\{7,39\}$	$\mathfrak{D}\langle 1,1,1,13\rangle$	$\{7,28\}$	$\mathfrak{D}\langle 1,1,1,17\rangle$	$\{7,15\}$
$\mathfrak{D}\langle 1,1,1,18\rangle$	$\{7,15\}$	$\mathfrak{D}\langle 1,1,1,20\rangle$	$\{7,15\}$	$\mathfrak{D}\langle 1,1,1,22\rangle$	$\{7,15\}$
$\mathfrak{D}\langle 1,1,1,23\rangle$	$\{7,15\}$	$\mathfrak{D}\langle 1,1,2,22\rangle$	$\{14,78\}$	$\mathfrak{D}\langle 1,1,2,26\rangle$	$\{14,56\}$
$\mathfrak{D}\langle 1,1,2,31\rangle$	$\{14,30\}$	$\mathfrak{D}\langle 1,1,2,33\rangle$	$\{14,30\}$	$\mathfrak{D}\langle 1,1,2,34\rangle$	$\{14,30\}$
$\mathfrak{D}\langle 1,1,2,35\rangle$	$\{14,30\}$	$\mathfrak{D}\langle 1,1,2,36\rangle$	$\{14,30\}$	$\mathfrak{D}\langle 1,1,2,37\rangle$	$\{14,30\}$
$\mathfrak{D}\langle 1,1,2,39\rangle$	$\{14,30\}$	$\mathfrak{D}\langle 1,1,2,40\rangle$	$\{14,30\}$	$\mathfrak{D}\langle 1,1,2,41\rangle$	$\{14,30\}$
$\mathfrak{D}\langle 1,1,2,43\rangle$	$\{14,30\}$	$\mathfrak{D}\langle 1,1,2,44\rangle$	$\{14,30\}$	$\mathfrak{D}\langle 1,1,2,45\rangle$	$\{14,30\}$
$\mathfrak{D}\langle 1,1,2,46\rangle$	$\{14,30\}$	$\mathfrak{D}\langle 1,1,3,16\rangle$	$\{6,15\}$	$\mathfrak{D}\langle 1,1,3,17\rangle$	$\{6,15\}$
$\mathfrak{D}\langle 1,1,3,19\rangle$	$\{6,15\}$	$\mathfrak{D}\langle 1,1,3,20\rangle$	$\{6,15\}$	$\mathfrak{D}\langle 1,1,3,22\rangle$	$\{6,15\}$
$\mathfrak{D}\langle 1,1,3,23\rangle$	$\{6,15\}$	$\mathfrak{D}\langle 1,1,4,7\rangle$	$\{3,35\}$	$\mathfrak{D}\langle 1,1,4,10\rangle$	$\{3,7\}$
$\mathfrak{D}\langle 1,1,5,7\rangle$	$\{3,19\}$	$\mathfrak{D}\langle 1,1,5,9\rangle$	$\{3,12\}$	$\mathfrak{D}\langle 1,1,5,12\rangle$	$\{3,11\}$
$\mathfrak{D}\langle 1,1,6,12\rangle$	$\{3,39\}$	$\mathfrak{D}\langle 1,1,6,13\rangle$	$\{3,12\}$	$\mathfrak{D}\langle 1,1,6,14\rangle$	$\{3,12\}$
$\mathfrak{D}\langle 1,1,6,16\rangle$	$\{3,12\}$	$\mathfrak{D}\langle 1,1,6,17\rangle$	$\{3,12\}$	$\mathfrak{D}\langle 1,1,6,19\rangle$	$\{3,12\}$
$\mathfrak{D}\langle 1,1,6,20\rangle$	$\{3,12\}$	$\mathfrak{D}\langle 1,2,2,11\rangle$	$\{7,39\}$	$\mathfrak{D}\langle 1,2,2,13\rangle$	$\{7,28\}$

continúa

forma	D	forma	D	forma	D
$\mathfrak{D}\langle 1,2,2,17\rangle$	$\{7,15\}$	$\mathfrak{D}\langle 1,2,2,18\rangle$	$\{7,15\}$	$\mathfrak{D}\langle 1,2,2,20\rangle$	$\{7,15\}$
$\mathfrak{D}\langle 1,2,2,22\rangle$	$\{7,15\}$	$\mathfrak{D}\langle 1,2,2,23\rangle$	$\{7,15\}$	$\mathfrak{D}\langle 1,2,3,14\rangle$	$\{10,40\}$
$\mathfrak{D}\langle 1,2,3,18\rangle$	$\{10,58\}$	$\mathfrak{D}\langle 1,2,3,27\rangle$	$\{10,26\}$	$\mathfrak{D}\langle 1,2,3,28\rangle$	$\{10,26\}$
$\mathfrak{D}\langle 1,2,3,29\rangle$	$\{10,26\}$	$\mathfrak{D}\langle 1,2,3,31\rangle$	$\{10,26\}$	$\mathfrak{D}\langle 1,2,3,33\rangle$	$\{10,26\}$
$\mathfrak{D}\langle 1,2,3,35\rangle$	$\{10,26\}$	$\mathfrak{D}\langle 1,2,3,36\rangle$	$\{10,26\}$	$\mathfrak{D}\langle 1,2,3,37\rangle$	$\{10,26\}$
$\mathfrak{D}\langle 1,2,3,38\rangle$	$\{10,26\}$	$\mathfrak{D}\langle 1,2,3,39\rangle$	$\{10,26\}$	$\mathfrak{D}\langle 1,2,3,40\rangle$	$\{10,26\}$
$\mathfrak{D}\langle 1,2,4,22\rangle$	$\{14,78\}$	$\mathfrak{D}\langle 1,2,4,26\rangle$	$\{14,56\}$	$\mathfrak{D}\langle 1,2,4,31\rangle$	$\{14,30\}$
$\mathfrak{D}\langle 1,2,4,33\rangle$	$\{14,30\}$	$\mathfrak{D}\langle 1,2,4,34\rangle$	$\{14,30\}$	$\mathfrak{D}\langle 1,2,4,35\rangle$	$\{14,30\}$
$\mathfrak{D}\langle 1,2,4,36\rangle$	$\{14,30\}$	$\mathfrak{D}\langle 1,2,4,37\rangle$	$\{14,30\}$	$\mathfrak{D}\langle 1,2,4,39\rangle$	$\{14,30\}$
$\mathfrak{D}\langle 1,2,4,40\rangle$	$\{14,30\}$	$\mathfrak{D}\langle 1,2,4,41\rangle$	$\{14,30\}$	$\mathfrak{D}\langle 1,2,4,43\rangle$	$\{14,30\}$
$\mathfrak{D}\langle 1,2,4,44\rangle$	$\{14,30\}$	$\mathfrak{D}\langle 1,2,4,45\rangle$	$\{14,30\}$	$\mathfrak{D}\langle 1,2,4,46\rangle$	$\{14,30\}$
$\mathfrak{D}\langle 1,2,5,16\rangle$	$\{10,15\}$	$\mathfrak{D}\langle 1,2,5,17\rangle$	$\{10,15\}$	$\mathfrak{D}\langle 1,2,5,18\rangle$	$\{10,15\}$
$\mathfrak{D}\langle 1,2,5,19\rangle$	$\{10,15\}$	$\mathfrak{D}\langle 1,2,5,21\rangle$	$\{10,15\}$	$\mathfrak{D}\langle 1,2,5,22\rangle$	$\{10,15\}$
$\mathfrak{D}\langle 1,2,5,23\rangle$	$\{10,15\}$	$\mathfrak{D}\langle 1,2,5,24\rangle$	$\{10,15\}$	$\mathfrak{D}\langle 1,2,5,26\rangle$	$\{10,15\}$
$\mathfrak{D}\langle 1,2,5,27\rangle$	$\{10,15\}$	$\mathfrak{D}\langle 1,2,5,28\rangle$	$\{10,15\}$	$\mathfrak{D}\langle 1,2,5,29\rangle$	$\{10,15\}$
$\mathfrak{D}\langle 1,2,5,31\rangle$	$\{10,15\}$	$\mathfrak{D}\langle 1,2,5,32\rangle$	$\{10,15\}$	$\mathfrak{D}\langle 1,2,5,33\rangle$	$\{10,15\}$
$\mathfrak{D}\langle 1,2,5,34\rangle$	$\{10,15\}$	$\mathfrak{D}\langle 1,2,6,7\rangle$	$\{5,20\}$	$\mathfrak{D}\langle 1,2,6,9\rangle$	$\{5,29\}$
$\mathfrak{D}\langle 1,2,6,14\rangle$	$\{5,13\}$	$\mathfrak{D}\langle 1,2,6,18\rangle$	$\{5,13\}$	$\mathfrak{D}\langle 1,2,6,19\rangle$	$\{5,13\}$
$\mathfrak{D}\langle 1,2,6,20\rangle$	$\{5,13\}$	$\mathfrak{D}\langle 1,2,7,9\rangle$	$\{5,14\}$	$\mathfrak{D}\langle 1,2,7,17\rangle$	$\{5,14\}$
$\mathfrak{D}\langle 1,2,7,18\rangle$	$\{5,14\}$	$\mathfrak{D}\langle 1,2,7,19\rangle$	$\{5,14\}$	$\mathfrak{D}\langle 1,2,7,20\rangle$	$\{5,14\}$
$\mathfrak{D}\langle 1,2,8,9\rangle$	$\{5,7\}$	$\mathfrak{D}\langle 1,2,8,12\rangle$	$\{5,7\}$	$\mathfrak{D}\langle 1,2,9,10\rangle$	$\{5,7\}$
$\mathfrak{D}\langle 1,2,9,11\rangle$	$\{5,7\}$	$\mathfrak{D}\langle 1,2,9,13\rangle$	$\{5,7\}$	$\mathfrak{D}\langle 1,2,9,14\rangle$	$\{5,7\}$
$\mathfrak{D}\langle 1,2,10,12\rangle$	$\{5,7\}$	$\mathfrak{D}\langle 1,3,4,6\rangle$	$\{2,30\}$	$\mathfrak{D}\langle 1,3,5,7\rangle$	$\{2,22\}$
$\mathfrak{D}\langle 1,3,5,8\rangle$	$\{2,10\}$	$\mathfrak{D}\langle 1,4,5,6\rangle$	$\{2,3\}$	$\mathfrak{D}\langle 1,4,6,7\rangle$	$\{2,3\}$
$\mathfrak{D}\langle 1,4,6,8\rangle$	$\{2,3\}$	$\mathfrak{D}\langle 1,4,6,11\rangle$	$\{2,3\}$	$\mathfrak{D}\langle 1,5,6,7\rangle$	$\{2,3\}$
$\mathfrak{D}\langle 1,5,6,8\rangle$	$\{2,3\}$	$\mathfrak{D}\langle 2,2,2,3\rangle$	$\{1,17\}$	$\mathfrak{D}\langle 2,2,3,5\rangle$	$\{1,6\}$
$\mathfrak{D}\langle 2,2,3,6\rangle$	$\{1,15\}$	$\mathfrak{D}\langle 2,3,3,4\rangle$	$\{1,13\}$	$\mathfrak{D}\langle 2,3,4,4\rangle$	$\{1,17\}$
$\mathfrak{D}\langle 2,3,4,6\rangle$	$\{1,23\}$	$\mathfrak{D}\langle 2,3,4,7\rangle$	$\{1,17\}$	$\mathfrak{D}\langle 2,3,4,10\rangle$	$\{1,23\}$
$\mathfrak{D}\langle 2,3,4,11\rangle$	$\{1,10\}$				

C. TABLA DE COMPOSICIONES DE LAS TRANSFORMACIONES SIMÉTRICAS

Para encontrar la composición $\mathcal{T}_i \circ \mathcal{T}_j$, se debe buscar en la fila i, columna j. Este grupo no es abeliano, es isomorfo al grupo diédrico del cuadrado: Dih_4 (véase el problema 28, en el apéndice D).

	$\mathcal{T}_1$	$\mathcal{T}_2$	$\mathcal{T}_3$	$\mathcal{T}_4$	$\mathcal{T}_5$	$\mathcal{T}_6$	$\mathcal{T}_7$	$\mathcal{T}_8$
$\mathcal{T}_1$	$\mathcal{T}_1$	$\mathcal{T}_2$	$\mathcal{T}_3$	$\mathcal{T}_4$	$\mathcal{T}_5$	$\mathcal{T}_6$	$\mathcal{T}_7$	$\mathcal{T}_8$
$\mathcal{T}_2$	$\mathcal{T}_2$	$\mathcal{T}_1$	$\mathcal{T}_4$	$\mathcal{T}_3$	$\mathcal{T}_7$	$\mathcal{T}_8$	$\mathcal{T}_5$	$\mathcal{T}_6$
$\mathcal{T}_3$	$\mathcal{T}_3$	$\mathcal{T}_4$	$\mathcal{T}_1$	$\mathcal{T}_2$	$\mathcal{T}_6$	$\mathcal{T}_5$	$\mathcal{T}_8$	$\mathcal{T}_7$
$\mathcal{T}_4$	$\mathcal{T}_4$	$\mathcal{T}_3$	$\mathcal{T}_2$	$\mathcal{T}_1$	$\mathcal{T}_8$	$\mathcal{T}_7$	$\mathcal{T}_6$	$\mathcal{T}_5$
$\mathcal{T}_5$	$\mathcal{T}_5$	$\mathcal{T}_6$	$\mathcal{T}_7$	$\mathcal{T}_8$	$\mathcal{T}_1$	$\mathcal{T}_2$	$\mathcal{T}_3$	$\mathcal{T}_4$
$\mathcal{T}_6$	$\mathcal{T}_6$	$\mathcal{T}_5$	$\mathcal{T}_8$	$\mathcal{T}_7$	$\mathcal{T}_3$	$\mathcal{T}_4$	$\mathcal{T}_1$	$\mathcal{T}_2$
$\mathcal{T}_7$	$\mathcal{T}_7$	$\mathcal{T}_8$	$\mathcal{T}_5$	$\mathcal{T}_6$	$\mathcal{T}_2$	$\mathcal{T}_1$	$\mathcal{T}_4$	$\mathcal{T}_3$
$\mathcal{T}_8$	$\mathcal{T}_8$	$\mathcal{T}_7$	$\mathcal{T}_6$	$\mathcal{T}_5$	$\mathcal{T}_4$	$\mathcal{T}_3$	$\mathcal{T}_2$	$\mathcal{T}_1$

D. LISTADO DE PROBLEMAS

El siguiente es un listado de problemas directa o indirectamente relacionados con el estudio hecho en el documento. No tiene ningún orden en lo que se refiere a dificultad o tema.

Problema 1 (caso especial del último teorema de Fermat)**.** Demostrar que la ecuación diofantina $x^4 + y^4 = z^4$ no posee soluciones en enteros positivos.

Problema 2. Hallar una $\mathbb{Z}$-forma cuadrática n-aria, para algún n en particular, que no sea cerrada bajo el producto, es decir, que no tenga ninguna identidad de cerradura.

Problema 3. Demuestre que la ecuación diofantina $(x^2 + y^2 + z^2) = 4(u^2 + v^2 + w^2)$ no posee soluciones, salvo la trivial.

Problema 4. Hallar todas las cerraduras homogéneas de la $\mathbb{Z}$-forma $x^2 + 5y^2$.

Problema 5. ¿Cómo se podría generalizar el concepto de *cerraduras reducidas* a las formas cuadráticas ternarias, en caso de que existieran?

Problema 6. Encuentre dos enteros representables en la $\mathbb{Z}$-forma $x^2 + y^2 + z^2$, pero tales que su producto no sea representable.

Problema 7. Generalice la definición de *transformaciones simétricas* a las formas ternarias. ¿Cuántas hay? ¿Y para formas n-arias?

Problema 8. Sean $a, b \in \mathbb{Z}^+$, tales que $ab \mid a^2+b^2+1$. Demostrar que $a^2+b^2+1 = 3ab$.

Problema 9. Demostrar que si se multiplica una terna pitagórica primitiva por una matriz de Barning, el resultado es otra terna primitiva.

Problema 10. Demostrar que cada terna pitagórica primitiva aparece exactamente una vez en el árbol diagramado en la figura 2.

Problema 11. Sean A, B, C las tres matrices de Barning. Describir los patrones que se generan en las ternas pitagóricas aplicando A^n a $(3, 4, 5)$, conforme n varía en los naturales. Hacer lo mismo para B^n y C^n (agradecimientos a Fabiola Ramírez por su contribución).

Problema 12. Demostrar que los exradios de un triángulo que corresponde a una terna pitagórica primitiva, son los inradios de los tres triángulos que se generan con las matrices de Barning a partir del triángulo anterior.

Problema 13. Hallar todas las soluciones en enteros positivos de la ecuación $a^b = b^a$.

Problema 14 (IMO 1997, #5)**.** Hallar todas las soluciones en enteros positivos de la ecuación $a^b = b^{a^2}$.

Problema 15 (IMO 1980, Inglaterra #1)**.** Probar que la ecuación $4x^3 - 3x + 1 = 2y^2$ tiene infinitas soluciones en los enteros positivos.

Problema 16 (IMO 1988, #6)**.** Sean $a, b \in \mathbb{Z}^+$, tales que $ab + 1 \mid a^2 + b^2$. Probar que $\frac{a^2+b^2}{ab+1}$ es un cuadrado perfecto.

Problema 17. Hallar todas las cerraduras homogéneas de la forma $x^2 + 3xy + 4y^2$.

Problema 18. Hallar el mínimo n para el cual $\langle 1, 0, -1\rangle\, \mathcal{R}(n)$ vale 5.

Problema 19. Demostrar que la gráfica de $\langle 1, 0, -1\rangle\, \overline{\mathcal{R}}(n)$ no es acotada por arriba, es decir, que para cualquier $m \in \mathbb{N}$ existe $n \in N$, tal que $\langle 1, 0, -1\rangle\, \overline{\mathcal{R}}(n) > m$.

Problema 20. Demostrar la aseveración contenida en el primer párrafo de la página 100, que dice: una $\mathbb{Z}$-forma es una forma cuadrado perfecto si, y sólo si, su discriminante vale cero.

Problema 21. Probar que si un número es congruente con 3 en el módulo 4, existe un primo, también congruente con 3, que lo divide.

Problema 22. Haciendo uso del problema anterior, demostrar que existen infinitos primos congruentes con 3 en el módulo 4. Para hacer esto, suponga que existe sólo un conjunto finito de ellos $\{p_1, p_2, \ldots, p_k\}$ y, considerando el número $N = 3 + 4\prod_{i=1}^{k} p_i$, llegue a una contradicción.

Problema 23. Sea $n \in \mathbb{Z}^+$, y considere el número $N = (n!)^2+1$. Sea p el menor primo que sea un divisor de N. Demuestre que $p > n$. También demuestre que $(n!)^{p-1} \equiv (-1)^{(p-1)/2} \pmod{p}$.

Problema 24. Usando el pequeño teorema de Fermat y la congruencia del problema anterior, concluya que $p \equiv 1 \pmod 4$. Explique por qué motivo el argumento anterior implica que existen infinitos primos de la forma $4k + 1$.

Problema 25. Demuestre la cota de error (3.9) de la página 81, propuesta por Gauss para la aproximación del área de un círculo en términos de los puntos reticulares que encierra. *Pista: considere todos los cuadrados unitarios con vértices de coordenadas enteras tales que al menos uno de sus vértices se encuentre en uno de los puntos reticulares encerrados.*

Problema 26. Hallar 10 cerraduras independientes para la forma de Pell $\langle 1, 0, -2\rangle$ (se recomienda emplear una computadora).

Problema 27. Hallar todos los pares de enteros (a, b) tales que a^2+b^2 divide a a^3+b y también a $a + b^3$.

Problema 28. Demostrar la isomorfía mencionada en el apéndice C.

Problema 29. A cada matriz cuadrada $\mathbf{M}$ de tamaño $n > 1$, se le asocia la forma cuadrática n-aria dada por la expresión $\mathbf{xMx}'$, donde $\mathbf{x}$ es el vector de variables $(x_1, x_2, \ldots, x_n)$, y $\mathbf{x}'$ es su transpuesto. Demuestre que esta asociación no es biyectiva, ya que dos matrices distintas pueden estar asociadas a la misma forma cuadrática. De entre todas las matrices que comparten la forma cuadrática con la matriz $\mathbf{M}$, existe una que es simétrica. Exprese esa matriz simétrica en términos de la matriz $\mathbf{M}$.

Problema 30. Demostrar que un número n posee una representación propia en una forma cuadrática $\mathfrak{q}$ cuyo discriminante es Δ si, y sólo si, Δ es un residuo cuadrático en el módulo $4n$.

Problema 31. Sea p un primo tal que $p \equiv 1 \pmod 4$. Considere el conjunto $S = \{a + bm \ : \ a, b \in \mathbb{Z}, 0 \leq a, b \leq \lfloor\sqrt{p}\rfloor\}$, donde m es cualquier número que cumpla $m^2 \equiv -1 \pmod p$. Probar que existen (al menos) dos elementos en este conjunto que son congruentes en el módulo p.

Problema 32. En referencia al problema anterior, si los elementos congruentes son $a_1 + b_1m$, $a_2 + b_2m$, mostrar que la siguiente es una representación de p como suma de dos cuadrados: $p = (a_1 - a_2)^2 + (b_1 - b_2)^2$.

Problema 33. Hallar todas las cerraduras homogéneas de la forma $x^2 - xy + y^2$. Elaborar un multigrafo como el mostrado en la figura 5, en la página 86.

Problema 34. Demostrar que si la $\mathbb{Z}$-forma $\mathfrak{q}$ representa al número n, entonces la $\mathbb{Z}$-forma $n\mathfrak{q}$ es perfecta (i.e. cerrada bajo el producto).

Problema 35 (IMO 1981, #3)**.** Determine el máximo valor que puede tomar la expresión $m^2 + n^2$, donde m, n son enteros positivos menores o iguales a 1981, que satisfacen $(n^2 - mn - m^2)^2 = 1$.

Problema 36. Sea p un primo tal que $2p - 1$ también es primo. Hallar todos los pares de números naturales (x, y) tales que $(xy - p)^2 = x^2 + y^2$.

Problema 37. Demostrar el lema 12 de la página 106. Se puede utilizar la nota de la página siguiente como una pista.

Problema 38. Demostrar que la composición de Dirichlet de dos formas primitivas es otra forma primitiva.

Problema 39. Sea $a \in \mathbb{Z}$. Demuestre que la $\mathbb{Z}$-forma cuadrática binaria $\mathfrak{q}$ representa al número a si, y sólo si, $\mathfrak{q}$ es propiamente equivalente a una forma $\langle a, b, c\rangle$, para algún par de números $b, c \in \mathbb{Z}$.

Problema 40. Demuestre que toda $\mathbb{Z}$-forma cuadrática binaria primitiva, definida positiva, es propiamente equivalente a una forma $\langle a, b, c\rangle$ que cumple:

$$\begin{cases} |b| \leq a \leq c & \text{siempre} \\ b \geq 0 & \text{si } \ |b| = a \ \text{ o si } \ a = c \end{cases}$$

Pista: Considere las transformaciones dadas por las siguientes matrices unimodulares

$$T_n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}, \qquad U = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

Qué se puede decir respecto de formas definidas negativas? ¿y de formas indefinidas?

Problema 41. Hallar un representante para cada clase de equivalencia bajo $\sim$ del conjunto de las $\mathbb{R}$-formas cuadráticas binarias. Descartar los casos en los que las formas binarias se reducen a formas unarias. Hallar $\mathscr{D}(\mathfrak{q})$ para cada $\mathfrak{q}$ que sea un representante de los hallados. Determinar cuáles de los conjuntos $\mathscr{D}(\mathfrak{q})$ son cerrados bajo el producto.

Problema 42. Demuestre que, si $\Delta \neq 0$ es un entero fijo, tal que existan $\mathbb{Z}$-formas cuadráticas con discriminante Δ, entonces

a) Existe al menos una forma con discriminante Δ que representa al número 1.
b) Todas las formas con discriminante Δ que representan al 1 son equivalentes.

Problema 43. Demostrar que la $\mathbb{Z}$-forma $\langle 4, -2, 12\rangle$ es multiplicativa pero no parametrizable.

Problema 44. Sea $a \neq 0$ un número racional. Demostrar que la $\mathbb{Q}$-forma $ax^2 - ay^2$ es equivalente a $x^2 - y^2$.

Problema 45. Demostrar que la $\mathbb{Q}$-forma cuadrática $x^2 + y^2$ no representa al 3.

Problema 46. Demostrar que la $\mathbb{Q}$-forma $x^2 + y^2$ es equivalente a $2x^2 + 2y^2$ y a $5x^2 + 5y^2$, pero no a $3x^2 + 3y^2$. ¿Para qué valores de $a \in \mathbb{Q}$ se cumple que $x^2 + y^2 \sim ax^2 + ay^2$?

Problema 47. Demostrar que la conclusión del lema 17 de la página 117 es válida para la forma $x^2 + y^2 - 2z^2$.

Problema 48. Demostrar el lema 17 de la página 117.

Problema 49 (**propuesto**)**.** Sea $n > 0$ un natural cualquiera. Hallar un conjunto completo de representantes diagonales para las clases de equivalencia bajo $\sim$ de las $\mathbb{Q}$-formas cuadráticas n-arias; es decir, un conjunto $\mathcal{A}$ de $\mathbb{Q}$-formas cuadráticas n-arias diagonales tal que no hay dos dentro del conjunto que sean equivalentes entre sí, y para cualquier $\mathbb{Q}$-forma $\mathfrak{q}$ existe $\mathfrak{g} \in \mathcal{A}$ tal que $\mathfrak{q} \sim \mathfrak{g}$. El problema se puede fraccionar enunciándolo para valores específicos de n.

Problema 50 (**propuesto**)**.** Determinar si existe una relación algebraica entre el número de cerraduras que posee una forma cuadrática capaz de representar a la unidad, la cantidad de simetrías que tenga, y el número de representaciones de la unidad que posea. Si r es la cantidad de representaciones de la unidad, c es el número de cerraduras, c^* es la cantidad de cerraduras independientes, y s, la cantidad de simetrías, la conjetura propuesta es $c = 4r$, o bien $c^* = \frac{4r}{s}$. Se permite que r, c, c^* valgan ∞, para ciertas formas.

Problema 51 (**propuesto**)**.** Determinar si existen cerraduras no reducidas de $\mathbb{Z}$-formas cuadráticas binarias cuyo discriminante sea distinto de cero. Se debe demostrar su imposibilidad o presentar un ejemplo. Se puede plantear el mismo problema respecto a cerraduras no homogéneas, es decir, aquellas en las cuales se sustituyen los polinomios X, Y (ver la ecuación 2.2, página 38) por funciones más generales con dominio $\mathbb{S}$ y rango contenido en el mismo conjunto.