UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE CIENCIAS

"LOS PROBLEMAS DE WARING EN LA TEORÍA ADITIVA DE LOS NÚMEROS."

T E S I S

QUE PARA OBTENER EL TÍTULO DE:

M A T E M Á T I C O

P R E S E N T A :

YUVAL MATARASSO POZAICER

FACULTAD DE CIENCIAS
UNAM

DIRECTOR DE TESIS: MAT. JULIO CÉSAR GUEVARA BRAVO

2006

Los problemas de Waring en la teoría aditiva de los números

Yuval Matarasso Pozaicer

Agradecimientos

A mis padres, por su apoyo incondicional en todos los momentos de mi vida, sin ustedes nada de esto sería posible. A mi hermano, mi abuela Carlota Sissa, mis primos y mis tíos muy en especial a mi tía Solange Matarasso que ha sido una segunda madre para mí. A la memoria de mi abuelo Samuel Matarasso que yo se que le encantaría tanto como a mi estar conmigo en este momento. A Patricia Moreleón por su apoyo en tantos momentos especiales. A los buenos amigos que me he encontrado en el camino; Carlos Galán, Israel Sardaneta, Ericka Calviño, Samuel Sánchez, Víctor Cruz, Ignacio González, Leonardo Faustinos y Jaime Lugo. A la Universidad Nacional Autónoma de México porque gracias a ella tuve –y tengo– la oportunidad de recibir una preparación de primer nivel. A todos mis profesores de la Facultad de Ciencias quienes me guiaron en esta aventura, muy en especial a César Guevara y Armando García quienes me dieron mis primeras oportunidades en el ámbito de la matemática. A mis alumnos de la facultad de Ciencias, ya que aprendí tanto o más que ellos en las aulas. A todas las personas que han estado de alguna manera en mi vida y me han dejado experiencias y enseñazas valiosas. ¡GRACIAS!

INDICE

INTRODUCCIÓN

Desde sus orígenes la matemática nos ha sorprendido y maravillado a través de ver que siempre ha mantenido una simbiosis frente a la modernidad científica en cada periodo de la historia[1].

Pero el interés de la matemática no sólo se ha dirigido a aquellas cuestiones que van a la vanguardia con los temas nuevos o con las aplicaciones novedosas. El interés por los problemas inconclusos ha sido una constante a lo largo de la historia, como si se tratara de ir cerrando —o ampliando— capítulos en la matemática.

Cabe mencionar que la matemática es una de las disiplinas con más problemas —y algunos muy longevos— que aún permanecen sin solución. Pero lo que es más importante es que dichos problemas siguen vigentes y sin grandes modificaciones en cuanto sus enunciados o planteamientos originales[2].

En este contexto, la teoría de los números siempre ha dado motivos para la incertidumbre y la ilusión. Desde Euclides (330 a.C.–275 a.C.) [1994], en sus libros aritméticos (VII al IX), contenidos en *Elementos*, tenemos la primera exposición teórica del estudio de los enteros positivos. Esta obra dio lugar a que los matemáticos —principalmente— del siglo XVI, y posteriores, enfrentaran los problemas como retos para construir lo que hoy conocemos como la teoría de los números.

---

[1] Esta relación —a través de la historia— de matemáticas y modernidad se podría, sin duda, extender a otras ramas de la ciencia. Se tiene que contemplar que la matemática desde la antigüedad pertenecía a un conjunto de disciplinas agrupadas en una sola, es decir, astronomía, música, geometría, entre otras, formaban parte de una sola. Asi, la matemática —en este trabajo— no se contempla como disciplina desvinculada de las otras ciencias, pero, para los objetivos de este trabajo contemplaremos sólo a la matemática.

[2] Aquí es importante mencionar que en otras áreas del conocimiento también han existido los problemas abiertos. Pero según las características mismas de cada materia los problemas no siempre logran trascender a través de la historia, y ello se debe a que por el avance mismo de la ciencia algunos problemas pierden importancia, o incluso, llegan a perderla totalmente. Como ejemplo tenemos el uso de sales para curar algunas enfermedades, las sangrías para liberar al cuerpo de los malos humores o, por otro lado, la búsqueda para perfeccionar las trayectorias de los planetas en el sistema ptolemaico, o Descartes cuando quiere describir por medio de los corpúsculos del viento porque una música nos es más agradable que otra. En todos estos casos los problemas a resolver quedaron estancados, y la razón fue porque los problemas perdieron vigencia, es decir, se desarrollaron otras teorías que rebasaron estas interrogantes. Así, existen problemas en áreas de las ciencias biológicas o físicas que son abiertos —desde cientos de años atrás— pero que ya no son de interés, los que siguen vigentes en estas asignaturas son escasos, pero no así en la matemática.

Para el presente trabajo de tesis hemos decidido abordar uno de los pasajes de la teoría aditiva de los números que consideramos que es importante para la matemática de los siglos XVII al XX. Pero antes de adentrarnos más es importante precisar qué es la teoría aditiva de los números. Esta rama de la teoría de los números estudia la representación de enteros positivos como suma de determinados conjuntos de enteros; entre estos conjuntos podemos mencionar el de los números cuadrados, que históricamente fue un problema central de la teoría moderna de los enteros. Se podría decir que un punto de partida de los problemas clásicos —en la teoría aditiva de los números— es el de la representación de enteros como suma de dos, tres o cuatro cuadrados (que corresponde a lo que conoceríamos después como los teoremas de Fermat, Gauss y Lagrange). Posteriormente se presentarían los problemas que plantean mayores dificultades, que son la representación de enteros como suma de cubos o de potencias mayores (lo que se conoce como los problemas de Waring).

Una de las principales motivaciones para desarrollar este trabajo fue el ver lo poco que se conoce del trabajo de Edward Waring. Nos hemos percatado que en algunos textos se mencionan los "problemas de Waring", pero sólo de manera complementaria, es decir, no se discuten las precisiones que él planteo, y sólo se mencionan como parte de otros problemas. Un ejemplo que ilustra esta situación lo tenemos en las frecuentes referencias a la conjetura de Goldbach donde se hace mención que es parte de los "problemas de Waring".

Una obra que aborda el tema de una manera extensa y moderna es la de Melvyn Nathanson [1996], *Additive Number Theory. The Classical Bases,* pero tiene el inconveniente que es un libro para estudiantes que se están especializando en teoría de los números o para ser utilizados en cursos de Posgrado, es decir, no es una obra para un lector novicio. El libro de Nathanson aborda los temas de manera avanzada y no presenta un enfoque muy didáctico para abordar los problemas originales de Waring, aunque su gran virtud es que sí se ocupa de ellos bajo un enfoque contemporáneo.

Por lo anterior consideramos que sería apropiado escribir una exposición de los problemas originalmente planteados por Waring y las soluciones ofrecidas por sus contemporáneos, así como las actuales, aunque todo restringido a la lista que Waring [1728] originalmente propuso en sus *Meditationes Algebraicae* en el año 1770.

El presente trabajo de tesis se divide en cuatro capítulos:

Capítulo I. Se exponen algunos datos biográficos de Edward Waring y un panorama amplio de lo que son los "problemas de Waring". Consideramos que en este caso sí es importante exponer los datos biográficos por el gran desconocimiento que se tiene de este personaje.

Capítulo II. Se hace una presentación del libro *Meditationes Algebraicae*. La intención es dar a conocer el libro ya que no alcanza el nivel de popularidad de obras como las de Newton, Fermat o Descartes, pero no por ello deja de ser importante para la historia de las matemáticas. La presentación se hará en dos etapas, i) se mostrarán algunas de las aportaciones de Waring y ii) se llevará a cabo una breve descripción de cada capítulo con la finalidad de tener una visión lo más amplia posible de las *Meditationes Algebraicae*.

Capítulo III. Será dedicado al teorema 47 del capítulo 5 de *Meditationes Algebraicae*. Aquí es donde aparece lo que conocemos como los "problemas de Waring". Se enunciarán en sus formas originales para después dar lugar a las demostraciones hechas por sus contemporáneos así como algunas más recientes.

Capítulo IV. Se describen algunos problemas actuales, así como algunas líneas de investigación que es hacia donde se dirigen los problemas de Waring. Entre ellos se puede mencionar el estudio de los números politopo, que actualmente constituyen uno de los focos de atención de los especialistas.

CAPÍTULO I

Su pasado

Edward Waring nació en Shrewsbury, Inglaterra, en 1736, y murió en Plealey, cerca de Shrewsbury, el 15 de agosto de 1798. De la vida de este matemático inglés se sabe realmente muy poco. En 1753 fue admitido en el Magdalene College en Cambridge —donde su talento matemático rápidamente atrajo la atención de sus profesores— y se graduó como *contendiente mayor*[3] en 1757.[4] Entre otras peculiaridades, esta escuela sometía a los alumnos, en su tercer año, a un examen muy complicado llamado *tripos*, y a los estudiantes se les conocía en forma individual por el resultado obtenido en dicho examen. Cada año, a quien obtenía la mejor calificación en esta prueba, se le llamaba contendiente mayor o primera clase, la segunda mejor calificación recibía el nombre de segundo contendiente o segunda clase, y así sucesivamente.

Waring fue electo miembro de la comunidad de la Universidad y, en 1760, recibió su M. A. a la vez que rechazaba una beca porque le favorecía más aceptar la cátedra lucasiana, libre como consecuencia de la muerte de John Colson. Así, él sería el sexto profesor Lucasiano (y el cuarto en el área de matemáticas).[5]

Debido a sus escasos 24 años de edad algunos de sus compañeros —también profesores de Cambridge— se opusieron a esta designación, pero pronto calló las críticas cuando publicó en 1762 su *Miscellanea analytica de aequationibus algebraicis et curvarum proprietatibus*, el cual fue una prueba irrefutable de su habilidad, demostrando así porque era contendiente mayor. Con estos antecedentes

[3] Senior wrangler.

[4] Cabe mencionar que por esta misma universidad han pasado matemáticos de la talla de Hardy y Littlewood.

[5] Los primeros cinco en ocupar la cátedra, sus respectivos periodos, fueron: Isaac Barrow 1664-1669, Isaac Newton 1669-1702, William Whiston 1702-1710, Nicolas Saunderson 1711-1739, John Colson 1739-1760.

no tuvo problema y fue electo miembro de la *Royal Society* al año siguiente.

La *Miscellanea* fue descrita por Charles Hutton [1815] como "el libro más complejo de las áreas más complicadas del álgebra". Este libro se ocupa en gran parte de la teoría de números (algunos de sus capítulos son "De fluxionibus fluentium inveniendis", "De methodo incrementorum" y "De infinitis seriebus"), una rama de las matemáticas en la cual Waring puso un interés especial. Este libro contiene, sin demostración, el teorema que dice que todo número entero es la suma de cuatro cuadrados, nueve cubos, 19 cuartas potencias, etcétera.

En 1770 Waring publicó su libro *Meditationes Algebraicae*, un trabajo que fue profundamente elogiado por Lagrange. Otras publicaciones de este matemático son: *Proprietates algebraicarum curvarum* [1772] y *Meditationes analyticae* [1776]. Además de estos importantes tratados, durante este periodo publicó trece artículos en el *Philosophical Transactions of the Royal Society*. Su último trabajo, titulado *Essay on the Principles of Human Knowledge*, publicado en 1794, es notable por la presentación de aplicaciones de la ciencia abstracta a la filosofía.

Waring recibió la medalla Copley de la Royal Society en 1784; también fue electo como miembro de varias sociedades científicas europeas, siendo dignas de mencionar las de Göttingen y Boloña. Trabajó como profesor Lucasiano hasta el día de su muerte. Sus actividades no fueron exclusivamente matemáticas; al mismo tiempo que escribía sus libros de matemáticas se interesó por la medicina y recibió la maestría por parte de la Universidad de Cambridge en 1770. Aparentemente nunca practicó la medicina, pero se cree que realizó disecciones en la privacidad de su laboratorio en Cambridge.

Su entorno

Para Waring el entorno inglés no le fue muy favorable debido a que las matemáticas inglesas atravesaban por un período incierto. Esto se debía en parte a la notación confusa que había utilizado Newton en su *Cálculo*, y al enfoque geométrico que dio a los *Principia*, considerada por algunos como un tanto arcaico. Y por otro lado los lectores ingleses fueron persuadidos para pensar que la nueva gran herramienta matemática forjada por Newton y Leibniz (la cual era empleada con gran vigor y habilidad en el continente, particularmente por los Bernoulli) no era realmente necesaria. Esta situación persistió por más de un siglo, a pesar de los esfuerzos de matemáticos distinguidos tales como Brook Taylor, Colin Maclaurin, John Wallis y Jérôme Lalande. Este

último escribió [1976] que no había un solo analista de primera en toda Inglaterra, pero Waring sostuvo consistentemente que su *Miscellanea Analytica* contradecía totalmente la observación de Lalande, y la justificación evidente bien podrían ser los elogios que recibió de d´Alembert, Lagrange y Euler.

A pesar de las mejoras en la notación matemática que fueron pronunciadas en el continente, Waring utilizó en sus propios trabajos el *deism* de Leibniz y el *dotage* de Newton —los dos grandes sistemas rivales— indistintamente, y no hizo ninguna contribución notable al establecimiento de una notación permanente en alguna rama de las matemáticas. Su método de escribir los exponentes era extremadamente tosco, por lo general sus presentaciones parecían poco atractivas, y sus obras eran difíciles de leer, esto es, sus escritos matemáticos resultaban algo confusos y casi imposibles de seguir en el manuscrito; mientras que sus trabajos publicados, quizás debido a su miopía extrema, están plagados de errores tipográficos. Como ejemplo podemos encontrar en Powell [1760] algunas críticas sobre el inconveniente de recurrir a Waring para calcular raíces, en lugar de utilizar el método de la regla de Newton.

A manera de resumen: los trabajos que publicó Waring son complicados pero innovadores; de alguna manera podemos pensar que una parte de los trabajos que publicó son una sintaxis de problemas algebraicos de los enteros que se venían proponiendo desde Diofanto, Fermat y Descartes. Por otra parte, sus artículos en los *Philosophical transactions of the Royal Society* son variados, abarcan tópicos de teoría de los números, polinomios, series y mecánica. Aquí es importante mencionar que no se tiene el registro preciso de cuántos artículos publicó para la *Royal Society*. Por ejemplo, la referencia que da Scott [1976] en el *Dictionary of Scientific Biography*, es que existen cinco artículos. Para el presente trabajo se realizó una búsqueda que arrojó una cantidad superior de artículos, trece, para ser más precisos.

De los diversos trabajos escritos por Waring, los que corresponden a teoría aditiva de los números constituyen el tema principal de esta tesis.

A continuación se dará una introducción a los problemas de Waring, y en el capítulo 3 se tratará de responder las siguientes preguntas: "¿Cuáles son estos problemas?" y "¿Tienen solución dichos problemas?, y si la tienen ¿Cómo se resuelven?".

¿Cuáles son los problemas de Waring?

Waring, en su libro *Meditationes algebraicae*, hizo conjeturas sobre la posibilidad de que los enteros pudieran escribirse como la suma de otros enteros elevados a diversas potencias. Por ejemplo, se puede escribir $13 = 9 + 4 = 3^2 + 2^2$. De aquí es posible observar que 13 puede escribirse como la suma de dos cuadrados. ¿Puede cualquier número escribirse como suma de dos cuadrados? La respuesta a esta pregunta es **NO**. Por ejemplo, si se considera el número 12 resulta que no se puede escribir de esa manera, dado que al intentarlo se obtienen las siguientes combinaciones:

$$12 = 1^2 + 11 \; ; \; 12 = 2^2 + 8 \text{ y } 12 = 3^2 + 3$$

Y con ellas se han agotado todas las posibilidades de escribir a 12 como suma de dos cuadrados, con lo que se constata que es imposible hacerlo.

Ahora sería natural hacer la siguiente pregunta: ¿cuál es el menor número de cuadrados necesarios para representar a todo número entero positivo? Ya se sabe que no son suficientes 2 cuadrados. De hecho, Joseph-Louis Lagrange demostró en 1770 que todo entero positivo puede escribirse como la suma de no más de cuatro cuadrados, es decir, cualquier número, sin importar lo grande que sea, puede escribirse utilizando un máximo de cuatro cuadrados. Más adelante se demostrará este resultado, hoy conocido como "Teorema de Lagrange".

Ahora se pide al lector que nos permita adentrarnos un poco más en algunas propiedades, pero sin llegar aún al planteamiento original de Waring y las demostraciones respectivas.

Para entender mejor cuántas potencias se requieren para representar a un entero, defínase $g(k)$ como el menor número requerido de potencias k para representar a todos los enteros positivos. Es decir, se sabe (gracias a Lagrange) que $g(2) = 4$, porque 4 es el menor número de cuadrados requeridos para representar a todos los enteros positivos. Waring propuso que $g(3) = 9$, es decir, que se requieren nueve cubos (o menos) para representar a cualquier entero (para el caso $k = 3$). Para esta cuestión es lógico pensar que algunos números muy grandes requieren de los nueve cubos, pero no es así. Considérese el número 23, y se verá que no podemos utilizar 3^3 como parte de la suma para 23 porque $27 > 23$; por lo tanto 23 debe representarse como la suma de cubos de 1 y 2. Así, la menor representación de 23 como la suma de cubos es la siguiente:

$$23 = 2^3 + 2^3 + 1^3 + 1^3 + 1^3 + 1^3 + 1^3 + 1^3 + 1^3$$

El siguiente número con esta propiedad —que requiere de nueve cubos— es 239:

$$239 = 5^3 + 3^3 + 3^3 + 3^3 + 2^3 + 2^3 + 2^3 + 2^3 + 1^3$$

Así, si se intenta escribir a todos los enteros como suma de 8 cubos, sólo se fracasará con 23 y 239.[6]

De todo lo anterior se pueden adelantar dos preguntas:

1.- ¿Realmente existe $g(k)$ para toda k? y

2.- Si ese es el caso, ¿cuál es su valor?

Como regla general se puede decir que $k+1 \leq g(k)$, (para una demostración de este resultado véase Loo [1982]). De lo contrario, si se intenta representar a todos los números como la suma de k números elevados a la potencia k, se fracasará. Sin embargo, ésta es solamente una cota inferior y no dice cual debe ser $g(k)$ para cada k en particular.

Se han hecho esfuerzos importantes para resolver este problema. Sin embargo, sólo se ha logrado resolver en algunos casos específicos, a saber, para $k = 2,...,10$. A continuación se presenta una tabla donde se indica quién es $g(k)$ o cuáles son sus cotas en dichos casos:

$g(2) = 4$	Conjetura de Fermat, demostrada por Lagrange en 1770
$g(3) = 9$	Conjetura de Waring, demostrada por Weiferich en 1912
$g(4) = 19$	Conjetura de Waring, demostrada en 1986
$g(5) = 37$	Demostrada por Chen en 1964
$g(6) = 73$	Demostrada por Pillai en 1940
$143 \leq g(7) \leq 3806$	
$279 \leq g(8) \leq 36,119$	
$548 \leq g(9) \leq ???$	
$1079 \leq g(10) \leq ???$	

[6] Para verificar este dato se puede consultar el artículo de Dickson [1939].

En esta lista se puede observar que solamente los casos particulares de $k = 2,3,4,5$ y 6 han logrado resolverse. Se tiene muy poca información del 7 al 10. Pero ¿habrá alguna formula general?

Otra parte de este fascinante problema es preguntarse: "¿Cuál es el menor número de potencias de k en el que existirá sólo un número finito de fallas?". Por ejemplo, se sabe que se necesitan cuatro cuadrados para representar a todos los enteros. ¿Pero si se intenta utilizar únicamente tres? ¿Será finito el número de enteros que no se pueden representar? En otras palabras, ¿existe alguna n suficientemente grande tal que todos los números mayores que n puedan representarse con sólo tres cuadrados? La respuesta es **NO**. Si se intenta utilizar solamente tres cuadrados para escribir números, existirá una cantidad infinita de excepciones.

Como otro ejemplo se pueden analizar los cubos. Se sabe que se requieren nueve cubos para representar a cualquier entero positivo[7]. Sin embargo, solamente dos números relativamente pequeños requieren el uso de los nueve cubos. También se sabe que todos los números mayores sólo requieren de ocho cubos o menos. Es decir, se requieren menos de nueve cubos para representar a todos los enteros positivos mayores que 239. ¿Se puede decir lo mismo para siete cubos? La respuesta es SÍ. ¿Y para seis cubos? Se empieza a tener problemas.

Ahora, sea $G(k)$ el menor número de potencias k en el que existen sólo un número finito de excepciones. Es decir, si se intenta representar los números con menos potencias k que $G(k)$, entonces se obtendrá un número infinito de fracasos. Se sabe que $G(2) = 4$, así como que $g(2) = 4$. Ahora, $g(3) = 9$, pero ¿cuánto vale $G(3)$? Sólo se puede decir que $4 \leq G(3) \leq 7$.

El segundo problema de Waring parece ser más difícil. Sin embargo, para los matemáticos tiene tanto interés como $g(k)$, porque parece ser que los números menores tienen sus propias peculiaridades que no comparten con los números más grandes. Esto significa que algunos teoremas sólo fallan para algunos números pequeños y nada más. Por lo tanto, $G(k)$ (que sólo tiene un número finito de fallas) es tan importante como $g(k)$ (que no tiene ninguna falla).

---

[7] El teorema que respalda esta afirmación es el de Wieferich-Kempner, que dice: *Todo entero no negativo es la suma de nueve cubos no negativos*. Más adelante en la tesis se demuestra dicho teorema (véase la pag. 76)

En general, se puede decir que $k+1 \le G(k) \le g(k)$. Para $G(k)$ específicos, donde $k = 2,...,10$, se sabe lo siguiente:

$$G(2) = 4$$
$$4 \le G(3) \le 7$$
$$G(4) = 16$$
$$6 \le G(5) \le 21$$
$$9 \le G(6) \le 31$$
$$8 \le G(7) \le 45$$
$$32 \le G(8) \le 62$$
$$13 \le G(9) \le 82$$
$$12 \le G(10) \le 102$$

En 1909, el matemático alemán David Hilbert (1862-1943) demostró que para cualquier *k* existe $g(k)$ y que este número es finito. Si $g(k)$ existe, entonces $G(k)$ también existe, porque en el peor de los casos se tendría que $G(k) = g(k)$. También se han realizado algunos esfuerzos para encontrar algún límite superior de $g(k)$ y $G(k)$ dependiendo únicamente de *k*. En 1954, G.J Mozzochi, demostró que:

$$G(k) \le \frac{-2\ln(3k) - \ln(6k)}{\ln\left(\frac{k-1}{k}\right)} - 4$$

(para ampliar la información de este resultado véase Andrews [1986])

Las desigualdades anteriores, producen un límite superior bastante grande para $g(k)$ y $G(k)$. Por ejemplo, si $k = 3$ se tendría que: $g(3) \le 2^{758}$ (un número bastante grande) y que $G(3) \le 14$, una cota superior mucho más razonable que la de $g(k)$, pero considerablemente mayor que el límite que actualmente se tiene que es 7.

Para entender mejor la relación existente entre las funciones $g(k)$ y $G(k)$ consideremos el caso $k = 4$, como ya vimos en las tablas presentadas anteriormente, $g(4) = 19$ y $G(4) = 16$, esto quiere decir que todos los enteros pueden ser expresados mediante la suma de 19 cuartas potencias, pero si solamente utilizamos 16, cuartas potencias, los eteros excluidos de esta notación son solamente un número finito.

CAPÍTULO II
Meditationes Algebraicæ

Introducción

En el presente capítulo se muestra un breve resumen del contenido de *Meditationes Algebraicæ*. El interés por exponer de manera compacta el contenido de esta obra de Waring obedece a que el libro no ha gozado de popularidad entre los científicos como los *Principia* (Newton), el *De revolutionibus* (Copérnico), *La geometría* (Descartes) o los *Elementos* (Euclides). Así, será importante, en primer lugar, exponer las principales ideas que Waring escribió en el prefacio de la obra, es decir, se presentarán las aportaciones al álgebra que Waring consideró importantes para su época y necesarias para el desarrollo de sus propuestas matemáticas. Al final del capítulo se dará a conocer el contenido de la obra.

Waring compiló en su prefacio una breve historia de las etapas del álgebra que consideró importante conocer, para poder así dar seguimiento a sus *Meditationes Algebraicæ*.

Abordó el trabajo de Diofanto de Alejandría (360 d.C.) sobre reducción de ecuaciones y menciona que hasta hace poco sus métodos (los de Diofanto) para encontrar soluciones racionales a dichos problemas no habían sido descritos con precisión y elegancia.

Waring retoma la historia de los numerales 0, 1, 2, 3, etc. inventados por los hindús, pasando por los árabes y los europeos como Al-Zarqali y Regiomontanus alrededor del año 1400 d.C. Se adentró en la *Aritmética* de Petrus Ramus, publicada en 1560, y comentó su aporte al sistema decimal. Proporciona una breve historia de las soluciones de ecuaciones cuadráticas y cúbicas; menciona a Mohammed ben Musa, Thebit ben Korah y a Omar ben Ibrahim, algebristas árabes que entre otras aportaciones redujeron el grado de las ecuaciones cúbicas, pero —comenta Waring— que para su época los manuscritos árabes no habían sido examinados detalladamente. Siguió con Cardano y el debate —actualmente más explorado—, para resolver ecuaciones cúbicas que involucró a Scipio del Ferro, Nicoló Tartaglia y a Ludovico Ferrari.

Con respecto a la notación matemática, Waring menciona que Buteo en su *Logística*, publicada en 1559, designó varias cantidades desconocidas mediante letras A, B, C, etc. También señala que Vieta (otro

pionero en la notación) empleó la sustitución de letras por cantidades conocidas; como ejemplo de ello se tiene el proceso de demostración de que el coeficiente del segundo término de una ecuación es la suma de las raíces, y que todos los coeficientes son constituidos similarmente; también hace señalamientos acerca de las elegantes demostraciones para encontrar soluciones racionales a una ecuación cuadrática. Siguiendo con Vieta, menciona —Waring— los elegantes métodos existentes para relacionar los términos del desarrollo de $(a+b)^n = a^n + na^{n-1}b + n\left(\frac{n-1}{2}\right)a^{n-2}b^2 + \ldots$ con los números triangulares, piramidales y así sucesivamente.[8]

En la primera edición del libro Waring publicó un método para decidir si todas las raíces de una ecuación dada son reales. Vale la pena mencionar que en las ecuaciones arbitrarias de grado mayor es raro que todas las raíces sean reales; por lo tanto él menciona que le gustaría tener una regla que estableciera primero el número de raíces imposibles —imaginarias— de una ecuación dada y, posteriormente, si el número de raíces imposibles está dado, entonces buscar el número de raíces positivas y negativas. Waring opinaba que estos dos problemas de ecuaciones de grado mayor, y que requieren cálculos laboriosos y complejos, casi nunca han sido resueltos. Por tal razón los incluyó en este libro.

Waring fue el primero en probar el principio racional de Schooten sobre la extracción de la n-ésima raíz de la cantidad binomial $a+\sqrt{b}$ siempre que la raíz pueda ser expresada de la forma

$$\frac{\left(x+\sqrt{y}\right)}{\sqrt[n]{Q}}$$

Siguiendo con la historia del álgebra, Waring nos menciona las "fracciones continuas", las cuales fueron discutidas por Viscount Brounker, quien también demostró diversas formas para encontrar valores enteros

[8] Agregando más a esta parte de la notación, señala que Harriot también influyó en la notación matemática. Él sustituyó *aa, aaa,* etc. por a^2, a^3, etc., y rescribió las ecuaciones como expresiones simples que le permitieron demostrar cómo las ecuaciones de grado mayor pueden ser construidas a partir de ecuaciones lineales. Descartes utilizó las últimas letras del alfabeto, ..., *x, y, z* para representar cantidades desconocidas y las primeras, *a, b, c,...*, para cantidades conocidas. Segner estableció que existen cuando mucho tantas raíces positivas como cambios en el signo de + a – y de – a +, y cuando mucho tantas raíces negativas como hay secuencias continuas + + y - - .

para x ó y en la ecuación $ax^2+1=y^2$. Una regla general para esto, que recurre al uso de series, fue propuesta por Waring.[9]

De las aportaciones de Fermat no se pudo abstraer, y entre muchos resultados menciona que todo entero es un número triangular o puede ser escrito como la suma de dos o tres triangulares. Otro teorema enuncia que si m es un número entero, entonces todo número primo de la forma $(4m+1)$ es la suma de dos cuadrados. En la segunda edición del *Meditationes Algebraicae* se muestran problemas semejantes, por ejemplo: todo número es un cubo o es la suma de 1, 2, 3, 4,..., 8 ó 9 cubos; también que todo número que sea más grande que otro cierto número es la suma de números de la forma $pa^2+qb^2+rc^2+sd^2$, donde a, b, c, d son números arbitrarios y p, q, r, s son primos entre sí. Waring afirma que la suma de dos cubos

$$a^3+b^3=(a+b)(a^2-ab+b^2)$$

no puede ser igual a un tercer cubo c^3 o igual a $ae(a^2-e^2)$, y de igual forma, $x\left(\frac{x+1}{2}\right)$ no puede ser un cuadrado (a menos de que $x=1$). Euler estableció las pruebas de estas proposiciones y añadió una similar que dice que $\alpha^3\beta x^4\pm\beta^3\alpha y^4$,... no pueden ser cuadrados, la cual él mismo probó con los mismos lineamientos.

En la primera edición Waring incluyó una regla para series que calcula la suma —directamente de los coeficientes de la ecuación dada— de las raíces de una ecuación dada, la suma de los cuadrados de las raíces, la suma de los cubos de las raíces, y así sucesivamente, hasta llegar a cierto grado. Cabe señalar que estos resultados también los abordaron en su momento Euler, Girard y Newton.

Con respecto al trabajo de Cramer, Waring en su primera edición presentó una regla sencilla para calcular las potencias de las raíces de

$$y^n-py^{n-1}+qy^{n-2}-ry^{n-3}+\ldots=0,$$

es decir, calcular los valores de $\alpha^a\beta^b\gamma^c\delta^d\cdots+\ldots$ usando las sumas de potencias enteras de las raíces; en la segunda edición, añadió un método para evaluar la misma expresión utilizando los coeficientes dados por la ecuación.

---

[9] No se deja de mencionar en el prefacio del *Meditationes Algebraicae* que Euler extendió este método a la ecuación $ax^2+bx+c=y^2$. Así como las aportaciones al tema por parte de Lagrange, Wallis, Bachet, Simpson.

En 1762 Waring publicó un método para transformar una ecuación dada en otra cuyas raíces sean cuadrados de las diferencias de las raíces de la ecuación dada, y notó que: "Si todos los signos de los términos de la ecuación resultante alternan + − y − +, entonces la ecuación dada no tiene raíces imposibles; de otra manera, tendrá alguna raíz imposible." En los *Philosophical Transactions* (Londres 1764), Waring dio ejemplos de esta transformación para ecuaciones de quinto grado, y ahí se afirma que la ecuación dada tiene dos raíces imposibles si el término final de la ecuación resultante es negativo; pero si es positivo, entonces ninguna o cuatro raíces serán imaginarias. En el mismo artículo, Waring menciona que: dada la ecuación $x^n - px^{n-1} + qx^{n-2} - ... = 0$, se pueden proponer ecuaciones $v^{n-1} - \frac{n-1}{n} pv^{n-2} + ... = 0$ y $v^n - pv^{n-1} + ... = z$, y transformar estas dos en una sola para eliminar a v. Por medio de la ecuación que resulta en z se puede detectar a menudo si hay raíces imposibles: se afirma que la ecuación dada no tiene ninguna raíz real si los signos de los términos de la ecuación con raíz z continuamente alternan + − y − +.[10]

En este libro, Waring prueba que si se tienen ecuaciones que son simétricas con respecto a x y y, y se toma una cantidad racional $P = z$, en la cual los cuadrados de x y y estén implicados, entonces la ecuación que tiene por raíz a z tiene raíces en parejas, una negativa y una positiva, de la misma magnitud, y consecuentemente se obtendrá una forma de bajar el grado a la mitad a la ecuación cuya raíz es x ó y. Al parecer Newton no sabía que el grado de la ecuación que tiene por raíz a z sería de la mitad del grado de la ecuación cuya raíz es x ó y. Waring fue el primero en afirmar y demostrar la siguiente proposición: "Dadas dos ecuaciones simétricas en x y y, la ecuación cuyas raíces son funciones simétricas racionales de x y y tendrá solamente la mitad del grado de la ecuación cuya raíz es x ó y.". En este trabajo añadió la siguiente pro-

---

[10] En este tenor, Waring consideró apropiado también mencionar que Maclaurin fue el primero en afirmar que las raíces de la ecuación $nx^{n-1} - (n-1)px^{n-2} + (n-2)qx^{n-3} - .... = 0$ son los límites de las raíces de la ecuación $x^n - px^{n-1} + qx^{n-2} - rx^{n-4} + ... = 0$. En el mismo contexto mencionó que Milner probó que la ecuación

$$ax^n - (a+b)px^{n-1} + (a+2b)qx^{n-2} - (a+3b)rx^{n-3} + ... = 0$$

no siempre tiene una raíz entre la raíz menor positiva y menor negativa de $x^n - px^{n-1} + qx^{n-2} - rx^{n-3} + ... = 0$. Finalmente agrega el trabajo de Newton sobre como extraer la raíz cuadrada de $a + \sqrt{b} + \sqrt{c} + \sqrt{d} + ...$, siempre que la raíz pueda ser expresada por una cantidad del mismo tipo, y él –Newton– redujo ecuaciones de grado $2n$ en ecuaciones de grado n. Waring hizo reducciones similares a grado $\frac{n}{2}$, siempre y cuando $\frac{n}{2}$ fuera entero.

posición: "Sea $x=\phi(z)$ tal que z está también en función de x, *i.e.*, $z=\phi(x)$. Entonces para cualquier ecuación dada $A=0$, la cual es función de x y y, si se escribe a x como su valor $\phi(z)$, y en la ecuación resultante para z se escribe x, y si se denota la ecuación resultante como $B=0$; entonces el valor de la cantidad x en la ecuación $x=\phi(x)$ será el mismo valor que el de la cantidad x asumida en las ecuaciones $A=0$ y $B=0$."

Leibnitz fue el primero en descomponer la fracción $\frac{1}{x^n-px^{n-1}+qx^{n-2}-\ldots}$ en fracciones $\frac{p}{x-\alpha}+\frac{q}{x-\beta}+\cdots$

Euler mostró que:

$$\frac{\alpha^r}{(\alpha-\beta)(\alpha-\gamma)(\alpha-\delta)}+\frac{\beta^r}{(\beta-\alpha)(\beta-\gamma)(\beta-\delta)}+\frac{\gamma^r}{(\gamma-\alpha)(\gamma-\beta)(\gamma-\delta)}+\cdots=0$$

siempre que r sea un entero menor que el número de letras α, β, γ, δ, etc. Waring generalizó esta proposición en los *Philosophical Transactions*; también lo demuestra utilizando un nuevo principio, cuando α^r, β^r, γ^r,... son reemplazados por productos, todos de la misma dimensión, de dos, tres o más raíces distintas. Waring deduce el valor de la suma cuando r es cualquier número, positivo o negativo, destacando una serie con la cual expresa dicha suma si r es una fracción.

Bezout establece que $y=\frac{x+a}{x+b}$ y sustituye esta expresión por y en la ecuación $y^n+h=0$, obteniendo como resultado la siguiente igualdad:

$$x^n+n\frac{a+hb}{1+h}x^{n-1}+n\cdot\frac{n-1}{2}\cdot\frac{a^2+hb^2}{1+h}x^{n-2}+\ldots=0$$

Waring presentó la siguiente serie:

$x^n=a^{n-1}b\pm a^{n-2}b^2+na^{n-2}bx+n\cdot\frac{n-3}{2}a^{n-3}bx^2+n\cdot\frac{n-4}{2}\cdot\frac{n-5}{3}a^{n-4}bx^3+\ldots$ cuya resolución es $x=\sqrt[n]{a^{n-1}b}+\sqrt[n]{a^{n-2}b^2}$. En los *Philosophical Transactions* y en este libro, Waring exhibe la igualdad:

$$x^{2n}-2b^npx^n-\frac{n}{1\cdot2}\cdot2nb^{n-1}a^2px^{n-1}-\frac{n\left(n^2-1\right)}{1\cdot2\cdot3\cdot4}2nb^{n-2}a^4px^{n-2}-\ldots=a^{2n}p-b^{2n}p^2$$

y además:

$$x^n-p\left(na^{n-1}bx^2+n\cdot\frac{n-5}{2}a^{n-6}b^2x^4+\ldots\right)\pm p^2\left(na^{\frac{n-3}{2}}b^{\frac{n-1}{2}}x-\ldots\right)=a^np+b^np^3,$$ cuya solución es $x=a\sqrt[n]{p}+b\sqrt[n]{p^3}$. Estas soluciones se pueden hacer más

generales aún de manera fácil, *i.e.*, se pueden construir las ecuaciones cuyas raíces estén dadas por

$$x = a\sqrt[n]{p^m} + b\sqrt[n]{p^{m+n}}$$

Euler estableció un método para reducir dos ecuaciones, $y^n + ay^{n-1} + by^{n-2} + ... = 0$ y $y^m + Ay^{m-1} + By^{m-2} + ... = 0$, a una sola en la que se eliminó y. Para hacer esto se tiene que multiplicar de ambos lados de las ecuaciones por estas dos cantidades: $Py^{m-1} + a'y^{m-2} + b'y^{m-3} + ...$ y $P'y^{n-1} + A'y^{n-2} + B'y^{n-3} + ...$; después se suman los dos productos y se impone la condición de que en la ecuación resultante las variables $P, a', b', ..., P', A', B', ...$, que involucren a y, deben desaparecer. Se pueden aplicar métodos similares para tres o más ecuaciones con tres o más variables. Waring fue el primero en publicar ésta y otras proposiciones del estilo en la segunda edición de su libro, las cuales podrían ser derivadas de manera más fácil directamente del principio presentado en el Problema 41, como él mismo indica en dicho problema. En la primera edición de su libro Waring demuestra cómo reducir dos ecuaciones a una —para eliminar variables— por medio de series infinitas, y en la tercera edición este método es extendido para casos de más ecuaciones con más incógnitas. También estableció un método para resolver este problema, y que combina los métodos de Cramer y de Bezout. A su vez, Lagrange resolvió este mismo problema utilizando logaritmos.

Euler desarrolló un método para generar ciertas ecuaciones de las cuales se conoce su solución, es decir, supongamos que

$$x = \sqrt[n]{\alpha} + \sqrt[n]{\beta} + \sqrt[n]{\gamma} + \sqrt[n]{\delta} + ...$$

es la solución, en donde $\alpha, \beta, \gamma, \delta, ...$ denotan respectivamente las m raíces distintas, todavía no determinadas, de una ecuación de grado m. En la primera edición del libro de Waring se encuentra el método general para encontrar una ecuación para esta solución, en donde se requiere únicamente eliminar cantidades racionales de la ecuación dada. En conexión con esto también desarrolla dos nuevos métodos generales para eliminar irracionalidades. Es importante hacer notar que Waring fue el primero en descubrir y revelar este método. También dedujo que si se asumen las distintas potencias 1, 2, 3, 4, ..., $n-2$, $n-1$, entonces $n-1$ variables independientes pueden ser introducidas sin que se agregue ninguna variable irracional nueva, llegando a la solución

$$x = a\sqrt[n]{p} + b\sqrt[n]{p^2} + c\sqrt[n]{p^3} + ... + B\sqrt[n]{p^{n-3}} + C\sqrt[n]{p^{n-2}} + D\sqrt[n]{p^{n-1}};$$

de la cual, si se eliminan las cantidades irracionales, se obtendría la siguiente ecuación: $x^n - n(aD + bC + cB + ...)x^{n-1} + ... = 0$. Este método está contenido en la primera edición y de la cual, a principios del año 1763, mandó copias a Euler. Luego, en mayo de 1770, fueron enviadas copias de la segunda edición a matemáticos, entre quienes se encontraban D'Alambert, Bezout, Montucla, Euler, Lagrange y Frisi, entre otros. No se sabe si estos ejemplares llegaron a su destino, ya que ninguno de estos personajes, a excepción de Frisi, le escribió a Waring para informarle de la recepción del libro.

Tschirnhaus propone la ecuación $y = ax^{n-1} + bx^{n-2} + cx^{n-3} + ...$ para eliminar el n-ésimo término de la ecuación dada $x^n - px^{n-1} + qx^{n-2} - rx^{n-3} + ... = 0$. De la ecuación que resulta, todos los términos intermedios también se hacen desaparecer, obteniendo finalmente la ecuación $y^n - H = 0$. Él usa este método para resolver la ecuación cúbica $x^3 + px^2 + qx + r = 0$, eliminando el segundo y tercer término $\left(px^2 \text{ y } qx\right)$. En la segunda edición de su libro Waring primero usa este método para eliminar el segundo y el cuarto término de la ecuación dada. A partir de ello deriva una solución de la ecuación bicuadrática. En esta misma versión también precisó, primeramente, que la solución $\sqrt[3]{-\frac{1}{2}b + \sqrt{\frac{1}{4}b^2 + \frac{a^3}{27}}}\,(=A) + \sqrt[3]{-\frac{1}{2}b - \sqrt{\frac{1}{4}b^2 + \frac{a^3}{27}}}\,(=B)$ tiene nueve valores, los cuales son las soluciones de las tres ecuaciones cúbicas: $x^3 + ax + b = 0$, $x^3 - \frac{1+\sqrt{-3}}{2}ax + b = 0$ y $x^3 - \frac{1-\sqrt{-3}}{2} = 0$; después mostró que las tres raíces de la ecuación $x^3 + ax + b = 0$ son: $A + B$, $\alpha A + \frac{B}{\alpha}$ y $\beta A + \frac{B}{\beta}$, en donde 1, α, β son las raíces de la ecuación $x^3 - 1 = 0$; y por último estableció una ecuación $x^3 + qx - r = 0$, cuyas raíces son α, β, $-\alpha - \beta$, tales que si se transforma esta última ecuación en otra cuya raíz sea z, y tal que $z^2 - zx = q = -\frac{\alpha^2 + \alpha\beta + \beta^2}{3}$, entonces z tendrá 6 valores: $z = \frac{\alpha}{2} \pm \frac{(\alpha + 2\beta)\sqrt{-3}}{6}$, $\frac{\beta}{2} \pm \frac{(\beta + 2\alpha)\sqrt{-3}}{6}$, $\frac{-\alpha - \beta}{2} \pm \frac{(-\alpha - \beta)\sqrt{-3}}{6}$.

De Moivre da un método para obtener la suma de una serie de términos que sean iguales, alternantes o cíclicos, sobre un intervalo de distancia dos, tres o más, $a + bx + cx^2 + ...$ Esto lo hace a través de dividir la unidad por la expresión multinomial $p + qx + rx^2 + ...$ En 1757, Waring envió la primera versión de este trabajo a la *Royal Society* de

Londres, la cual Simpson leyó, y después de su visto bueno, la insertó en los *Philosophical Transactions* en 1758.

En la segunda edición de su libro Waring presenta un método para determinar si una serie dada puede ser expresada como una fracción racional o no, y añadió que no existen n números primos escritos en progresión aritmética a menos que su diferencia común sea divisible por $1\cdot 2\cdot 3\cdot 4\cdots n$. Varias propiedades sobre los divisores de números fueron encontradas por Euler, Lagrange y Beguelin, entre otros. En su libro *Meditationes Algebraicae* Waring muestra que el número de residuos obtenidos al dividir los números 1^m, 2^m, 3^m, 4^m, ... por un número primo p será $\frac{p-1}{r}$, donde r es el máximo común divisor de m y $p-1$. Waring no vio la proposición de Euler hasta que su libro ya estaba impreso. Esta proposición es la siguiente: si $m\times s+1=p$, entonces s será el número de residuos de lo antedicho, lo cual es un caso especial de la proposición que Waring dio.

Waring probó que la suma $1^r+2^r+3^r+4^r+\ldots+x^r$ es siempre divisible por x ó $x+1$, siempre que x ó $x+1$ sea un número primo mayor que $r+1$. Del mismo modo probó que la suma de productos de la forma $\alpha^a\beta^b\gamma^c\delta^d\cdots$, donde α, β, γ, δ, ... representan números distintos 1, 2, 3, 4,..., x, y la suma $a+b+c+d+\ldots$ de índices dados es menor que $x-1$ ó x, siempre será divisible por el número primo x ó $x+1$. Se puede afirmar de manera más general que $1\cdot 2\cdot 3\cdot 4\ldots(r+1)\times S$ siempre es divisible por $(2x+1)\times(x+1)\times x$, si r es par, y por $x^2+(x+1)^2$ si r es impar; de aquí se pueden deducir elegantes propiedades de las parábolas similares a las propiedades canónicas de las parábolas de Arquímedes, publicadas por Waring [1772] en su *Proprietates Algebraicarum Curvarum*. La prueba también nos da una elegante propiedad de los números primos, la cual fue descubierta más adelante y que afirma lo siguiente: el número $1\cdot 2\cdot 3\cdot 4\cdots(n-1)+1$ es siempre divisible por n siempre que n sea primo; la prueba elegante de este teorema fue establecida primero por Lagrange.

En resumen, este prefacio de Waring da una introducción sobre la teoría contenida en el libro, así como toda la teoría existente y de la cual Waring se va a apoyar para poder realizar su propia teoría.

Finalmente Waring pone una nota para los lectores que a continuación se enunciará:

> "Después de tanta labor de tantos obreros en el campo del álgebra, algunos podrían asombrarse de que yo haya producido otro trabajo, uno con tantas páginas sobre el asunto. Pero la falta sería mía de no haberlo hecho; si fueran menos páginas que en mi primer libro no podría compilar todos los descubrimientos de recientes escritores y no podría dar énfasis a ninguno de ellos, ni a cualquiera de mis propios descubrimientos que también quizás merecen la elaboración. Pero de esto el lector erudito debe ser el juez. Mi deber ha sido de hecho servir fielmente, y para promover tanto cuanto yo puedo la causa del conocimiento. Yo le pido entonces aceptar este libro, a pesar de su verbosidad tediosa, para dominar un poco más el tema que busca explicar."

Resumen por capítulos de Meditationes Algebraicae

Capítulo I: "Un método para encontrar una ecuación cuyas raíces son cualquier función algebraica de las raíces de una ecuación dada o de varias ecuaciones dadas."

Aborda la teoría de *funciones simétricas*, esto es, aquellas funciones racionales integrales que no se alteran mediante ninguna permutación de las variables. Es más, Waring no se refiere a éstas con este nombre, simplemente las llama funciones algebraicas de la ecuación general.

Un método característico de Waring es establecer, donde sea posible, principios y reglas generales, y después aplicar éstos a los casos específicos. Presenta una ley general para la *m*-ésima potencia en función de las raíces de una ecuación dada; para esto no sólo calcula, al igual que Newton, las potencias en secuencia ascendente sino que presenta una fórmula general y después explica los pasos que condujeran a su deducción.
Por ejemplo: dada una ecuación de grado *n* cuyos exponentes están ordenados de manera descendente con los signos de los coeficientes alternados, se requiere encontrar una nueva ecuación cuyos coeficientes consistan en las sumas de las *m*-ésimas potencias de las raíces de la ecuación antedicha (*problema I*).

Al presentar este método general Waring discutió las funciones simétricas elementales. También están los dos sistemas de fórmulas establecidas que revelan las relaciones que existen entre las sumas de las potencias de las raíces de una ecuación con sus coeficientes, y que, escritas de esta manera general, son conocidas como las *formulas de Waring*. También dio pruebas para estas fórmulas pero no quedó satisfecho con solamente probar la corrección de éstas.

A las sumas de potencias Waring las pasó a funciones simétricas de la forma $\sum \alpha^a \beta^b \gamma^c + \alpha^b \beta^a \gamma^c + \ldots$ y mostró que toda función simétrica de esta forma puede ser expresada como una función integral de sumas de potencias y, de igual manera, como una función integral de los coeficientes de la ecuación dada cuyas raíces son α, β, γ, etc. (*problema III*).

Pero Waring fue más allá, y en su *problema V* busca para una ecuación dada, qué coeficientes son funciones simétricas de las raíces de dos o más ecuaciones. Para este problema, obtuvo resultados positivos que nadie encontró antes que él.

Como Waring no contaba con el actual símbolo de suma $\sum$, ni tenía la notación factorial a su disposición, sus fórmulas resultantes son muy incómodas. Pero de cualquier manera, incluso, los matemáticos modernos deberían referirse a Waring para cualquier investigación relacionada con estos temas.

CAPÍTULO II: "Raíces imaginarias"

La investigación de Waring sobre el número de raíces de una ecuación tuvo como punto de partida las raíces imaginarias. En su época él las llamó "imposibles" y las utilizó como nosotros utilizamos a $a+bi$ y a $a-bi$, pero si bien las denotó mediante $\left(a+\sqrt{-b^2}\right)$ y $\left(a-\sqrt{-b^2}\right)$.

Para la detección de raíces complejas Waring ofrece un estudio muy amplio, aunque debió conformarse con resolver casos especiales dado que no encontró una regla general. Además, Waring transforma una ecuación general, con algunas potencias no incluidas y con signos alternantes adjuntos a los coeficientes, en otra cuyas raíces son los cuadrados de las diferencias de las raíces de la ecuación dada. De donde resulta que si la ecuación resultante tiene coeficientes de signos continuamente alternantes entonces la ecuación dada no tiene raíces complejas, y de otra manera sí las tendrá (*problema XII*).

Bajo la misma suposición Waring presentó un método general para encontrar las raíces positivas y negativas de una ecuación bicuadrática (*problema XII*) y una de la ecuación de grado 5 (*problema XII*), las cuales no ofrecen una utilidad muy práctica. Sin embargo, años después, se pudo encontrar de manera mucho más sencilla el número máximo de raíces positivas y negativas (por medio del teorema de Descartes y Rolle) e incluso (a través del teorema de Sturm) el número exacto de raíces reales.

De la misma manera, conociendo el número de raíces reales positivas y negativas de la ecuación dada (*problema XVI*), Waring halló un método para obtener el número de raíces imaginarias de una ecuación cuyas raíces son iguales a los cuadrados de las diferencias de las raíces de una ecuación dada.

Waring [1728 (pp. 101-106)] conocía la regla de los signos de Descartes, y lo discute de la siguiente manera: "La regla de los signos de Descartes puede ser mencionada como sigue: una ecuación polinomial completa tiene tantas raíces positivas como cambios de signo, de + a − y de − a +, siempre y cuando la ecuación no tenga raíces imposibles. Cuando cualquier ecuación es multiplicada por $x-a$, donde a es

una cantidad positiva, el número de cambios en el signo será incrementado en al menos 1; pero si la ecuación dada es multiplicada por $x+a$, entonces entre el primer término y el penúltimo de la ecuación resultante habrá tantos o más (por un número par) signos idénticos como había en la ecuación original. Si la ecuación resultante tiene exactamente tantos signos cambiados, del primero al penúltimo término, como en la ecuación dada, entonces el penúltimo término de la ecuación resultante tendrá el mismo signo que el último término de la ecuación dada, de aquí que la ecuación resultante tendrá un signo más agregado a la progresión, la cual no se puede encontrar en la ecuación original. Así, en la ecuación que resulta habrá un número impar de las progresiones de los signos además de los que estaban en la ecuación dada."

Estas afirmaciones son importantes, porque aquí Waring revela un conocimiento o entendimiento más profundo de la regla de los signos, mismo que Gauss retomaría más adelante.

CAPÍTULO III: "Reducción y solución de ecuaciones."

Para Waring, la reducción *sensu latu* comprende la transformación de cualquier ecuación para hacer su solución mucho más sencilla; la reducción *sensu strictu* es para él la transformación a otra ecuación de grado menor. Por lo tanto, para Waring, la reducción no es simplemente un sinónimo de descomponer una ecuación polinomial en factores.

La ley de reducciones, tal y como la menciona Waring, señala que: "Las ecuaciones pueden ser reducidas si pueden ser separadas en dos partes iguales tales que las mismas raíces se puedan extraer de cualquiera de las dos partes". (*Teorema XIX*)

Waring también entiende que la eliminación del resto (que es independiente de la variable x) es precisamente la condición para que dos ecuaciones tengan una raíz en común. Pero solamente con la ayuda de determinantes puede ser posible enunciar de manera decente la regla por la cual las sucesiones polinomiales del resto podrían ser construidas fácilmente.

En cuanto a los métodos para encontrar soluciones de ecuaciones de grado superior, Waring conoce únicamente aquellos que dependen de transformaciones de la ecuación dada; los métodos basados en la resolución directa fueron diseñados por primera vez por Lagrange.

Respecto de las transformaciones de ecuaciones, Waring avanzó más allá del método de Tschirnhausen. Waring sabía más que solamente eliminar el segundo y el tercer término de una ecuación de cualquier

grado a partir de resolver una ecuación cuadrática: podía también, recurriendo a una ecuación bicuadrática, remover el segundo y el cuarto término (*problema XXIII*). Creía que con este método una ecuación de cualquier grado podría ser transformada en una ecuación *pura*, y que podría enunciar el teorema que afirmara que la ecuación reductora, en general pudiera ser de grado a lo más $(n-1)!$. Sin embargo Waring nunca aportó demostraciones de todas estas afirmaciones.

En este capítulo Waring también discute el tipo de ecuaciones que se conocen como *recíprocas* (*problema XVII*), y para su solución ofrece un método especial que se justifica solamente si contara con un conocimiento más profundo de la estructura de tales ecuaciones. Pero Waring utilizó otro camino para resolver estas ecuaciones, que de hecho resultó mucho más complicado.

Waring también conocía las ecuaciones *binomiales* (*problema XXVII*) y sus propiedades, si bien sus representaciones trigonométricas le resultaban desconocidas. Como un caso especial de las ecuaciones binomiales, Waring consideró la ecuación $x^n - 1 = 0$ y la utilizó para introducir el estudio de las llamadas *raíces de la unidad* (*Teorema XIV*). Esto a pesar de que no conocía la diferencia entre las raíces primitivas y las no primitivas.

Sobre este tema estaba familiarizado con el siguiente teorema: "La suma de las m potencias de las raíces de la ecuación $z^n - 1 = 0$ es 0, excepto cuando $n = m$ o cuando n es un factor de m; en este caso la suma será n."

Ampliando este teorema, Waring demostró que cualquier función simétrica de la n-ésima raíz de la unidad, $\sum \alpha^m \beta^r \gamma^s \delta^t$ es siempre igual a cero, excepto cuando $m+r+s+t$ es un múltiplo de n. Como es su costumbre, Waring busca expandir este teorema en varias combinaciones de potencias de sumas y desarrollar una fórmula general de este método.

CAPÍTULO IV: "Dos o más ecuaciones con dos o más incógnitas."

Waring sabía que hay un número específico de pares de raíces que satisfacen simultáneamente dos ecuaciones dadas; así mismo conocía el teorema de Bezout: "Dos ecuaciones independientes con dos incógnitas y coeficientes independientes de grado m y n respectivamente tienen al menos $n \cdot m$ soluciones." (*Teorema XXIV*). Pero el método de Ernest Fardinand Minding (1806-1885), el cual permite calcular el número exacto de soluciones para cada caso especial, naturalmente no era conocido por Waring.

Waring muestra más adelante en este capítulo cómo es que una de las dos incógnitas puede ser eliminada a través de encontrar divisores comunes (*problema XXIV*), o por medio de multiplicar cruzado y dividir (*problema XXXI*), o a través de series infinitas que se insertan en la segunda ecuación y después se multiplican los valores resultantes entre ellos, o multiplicando las dos ecuaciones por dos ecuaciones arbitrarias y resolviéndolas por medio del método de coeficientes correspondientes.

Además, a través de numerosos ejemplos, llega a la conclusión de que k ecuaciones con k incógnitas pueden ser transformadas en una sola ecuación con una sola variable; y cuando descubre que el grado de esta ecuación tiene que ser igual al producto de los grados de las k ecuaciones originales, puede enunciar un teorema (*problema XXXI*) que más adelante recibió el nombre de *Generalización del Teorema de Bezout*.

Subsecuentemente en este capítulo, Waring introduce su investigación sobre raíces repetidas de ecuaciones múltiples (*problema XXXIII*), pero no podía conseguir lo que es la noción de discriminante, que es una función integral homogénea de los coeficientes de grado $2(n-1)$.

Más adelante Waring establece un criterio para estimar las raíces reales e imaginarias de ecuaciones múltiples. Para investigar las raíces imaginaria ideó un método con el cual primero determina si hay alguna raíz real en la ecuación dada y después la elimina de la ecuación para luego ocuparse de las raíces imaginarias de la ecuación reducida (*Teorema XXXI* y *XXXII*).

Waring dio una calurosa bienvenida al *Teorema de Cauchy*, gracias al cual uno puede determinar el número de raíces, en cualquier ecuación, cuyas partes real e imaginaria se encuentran entre los dos conjuntos respectivos de cotas superiores e inferiores.

En la página 233 hace referencia a su libro *Proprietates Algebraicaarum Curvarum* y reporta que mediante su interpretación geométrica comienza a darse cuenta que si dos, tres o más arcos de curvas, cuyas ecuaciones son dadas, pasan a través de un punto P, entonces se define un doble (o múltiple) punto, y que este resultado es un equivalente geométrico de la propiedad que señala que dos o más ecuaciones tienen doble (o múltiple) raíz común.

CAPÍTULO V: "Cantidades racionales y enteras."

En este capítulo se encuentra el resultado que permite a Waring ocupar uno de los sitios de honor en la historia de la teoría de los números: el teorema 47, mismo que se ocupa de los problemas de teoría aditiva de los números, hoy conocidos como los 'problemas de Waring'.

Aunque este Teorema aparece sin demostración en el libro, sin embargo es uno de los resultados más enriquecedores y completos de la obra de este gran matemático.

Pero es importante mencionar que el capítulo V no sólo se reduce a este gran Teorema; el capítulo es extenso, y entre otras aportaciones cabe enunciar las siguientes:

- ✓ Se introducen métodos mediante los cuales se pueden encontrar raíces racionales en una ecuación con varias variables y, más aún, ofrece criterios para decidir si una ecuación puede ser resuelta por extracción de *raíces cuadradas o cúbicas* (*problema XLVI*).
- ✓ Busca soluciones enteras para las funciones exponenciales a^x y x^a (*problema LXIII*).
- ✓ Da ejemplos y métodos constructivos para *números perfectos* (*Teorema XLVI*) y *números amigos*[11].
- ✓ Demostró que si $(a+b)^n$ y $(a-b)^n$ no tienen factores comunes excepto 2^m, entonces a y b son primos relativos (*Teorema XLIII*).
- ✓ Se introducen teoremas teóricos-numéricos adicionales de diferentes autores:
  - ➢ La técnica de aproximación de *Wallis*, que convierte una fracción decimal infinita en una fracción equivalente racional (*problema LI*).
  - ➢ El método de Brounker para expresar una fracción común y su recíproco como una fracción continua (*problema XLV*).
  - ➢ El método de *Kirast*, que determina la divisibilidad por 7 de un número compuesto de la forma $a+b$ (*Teorema XLVI*).
  - ➢ El método de *J.A.Castelvetri* de división de un número a través de un proceso de aproximaciones.

[11]En esta parte, cuando Waring habla de *residuos* y *no-residuos*, se está refiriendo a nuestro concepto moderno de *congruencias*. Sin embargo, los residuos cuadráticos y residuos no cuadráticos eran desconocidos para él.

- ✓ El problema enunciado por Waring (página 379): "Todo número par es la suma de dos números primos y todo número impar es primo o la suma de tres primos." Esta afirmación —en nuestros días— es mejor conocida como la *conjetura de Goldbach.*
- ✓ El *último Teorema de Fermat*, aunque con otro nombre (*Teorema LII*).
- ✓ El teorema teórico-numérico más famoso en el libro de Waring es el *Teorema de Wilson*[12].

Cabe mencionar que todos los resultados conciernen únicamente a campos de números racionales. Pero Waring también se ocupaba de los campos cuadráticos imaginarios y produjo un acoplamiento elegante entre dos grandes disciplinas: el álgebra y la teoría de funciones.

[12]Del cual sabemos que Lagrange tuvo éxito en encontrar una demostración.

CAPÍTULO III

Los Problemas de Waring

El capítulo III es la parte central de este trabajo dado que es donde se expondrán los problemas de la teoría aditiva que anteriormente se han venido mencionando. Pero antes de presentar los enunciados de los problemas que corresponden al teorema 47, es conveniente contextualizar el teorema 47 respecto del contenido del capítulo V del *Meditationes*, que es donde aparece el teorema.

Como ya se vio en capítulos anteriores del *Meditationes Algebraicae*, una de las principales vertientes de la obra es estudiar las propiedades de las ecuaciones de una, dos o más variables, y el capítulo V no fue la excepción. Ya se sabe que el libro de Waring no se caracterizó por seguir una ruta bien definida para llegar a los objetivos, aunque debemos suponer que él sí los tenía claros. Por esta razón el capítulo V tiene contrastes temáticos que por momentos hacen que la lectura sea complicada y, por otro lado, enuncia resultados que parecen ser de poca importancia si bien ahora sabemos que son trascendentes para las matemáticas. Por ejemplo, al referirse a las propiedades de los enteros enuncia la conjetura binaria y terciaria de Goldbach, también menciona que la suma de los recíprocos de los primos forman una serie divergente, entre otros problemas.

El título del capítulo es "Sobre racionalidad y partes enteras". Aquí (Cáp. V) se abordan problemas tales como los siguientes: encontrar soluciones vía el método de Descartes de dividir entre binomios que contienen una raíz; resolver una ecuación a través de encontrar raíces cúbicas y cuadradas; métodos de aproximación; formas para convertir una fracción decimal con múltiples repeticiones a una fracción simple, los cual logra en parte a través de aproximar de raíces de ciertas series infinitas. También se adentra en la solución por enteros de la conocida ecuación de Pell $ax^2 + 1 = y^2$, la cual en realidad fue propuesta por Euler. Trabaja en soluciones enteras de funciones exponenciales. Menciona el tema de los residuos y no-residuos, la cual guarda una fuerte semejanza con lo que hoy conocemos como congruencias; sin embargo, desconocía lo que corresponde a los residuos cuadráticos y no-cuadráticos.

Después, en éste mismo capítulo, da un giro en la dirección temática y empieza a presentar algunos problemas que tenían que ver con primos, con divisibilidad y con enteros representados como sumas de enteros.

Así, se puede ver que el teorema 47, que dominó (por la fama que le dieron) sobre todo el libro *Meditationes Algebraicae*, no fue en su

momento un resultado principal en la obra, fue solamente una recopilación de problemas aditivos que se venían discutiendo desde la época de Fermat.

Como ya se sabe, los problemas del teorema 47 no fueron demostrados por Waring. En el capítulo III de la tesis se presentan algunas de las demostraciones que han surgido a lo largo de los años; así mimo, en un apéndice final se encuentran resultados que pueden ser necesarios para un mejor seguimiento de los mismos.

Teorema 47

1. Sean x y z enteros cualesquiera y a y b dos números sin divisores comunes. Entonces, cualquier número mayor que $ab-a-b$ puede ser expresado como $ax+bz$.
2. Si n es un entero, entonces cualquier número divisible por n que sea mayor que $nab-na-nb$ puede ser expresado por $nax+nbz$.
3. Todo número entero es un número triangular o la suma de dos o tres números triangulares, *i.e.*, está compuesto por uno, dos o tres de los números 1, 3, 6, 10, etc.
4. Todo número entero es un número pentagonal o la suma de dos, tres, cuatro o cinco números pentagonales. De la misma manera, todo entero es un número hexagonal o la suma de dos, tres, cuatro, cinco, seis, siete u ocho números hexagonales.
5. Todo entero es un cuadrado o la suma de dos, tres o cuatro cuadrados.
6. Todo entero puede ser expresado como la suma de cantidades de la forma a^2-b^2 y a^2-b^2-2, donde $a,b\in\mathbb{Z}$.
7. Todo número que sea mayor que cualesquiera números dados p, q, r, s (los cuales se consideran como parámetros y sin divisores comunes) puede ser expresado por la cantidad $pa^2+qb^2+rc^2+sd^2$, donde $a,b,c,d\in\mathbb{Z}$.
8. Todo entero puede ser escrito como la siguiente suma: $\left(a^2\pm ab+b^2\right)+\left(p^2\pm pq+q^2\right)$ donde $a,b,p,q\in\mathbb{Z}$.
9. Todo entero es un cubo o la suma de dos, tres, cuatro,..., nueve cubos; todo entero también es una cuarta potencia o suma de a lo más 19 cuartas potencias. Leyes similares pueden ser afirmadas para cualquier potencia.
10. Cualquier número de la forma $4n+2$ divisible por 2 pero no por 4, puede ser compuesto como la suma de dos o tres cuadrados.

Inciso 1

Sean x y z enteros cualesquiera y a y b dos números sin divisores comunes. Entonces, cualquier número mayor que $ab-a-b$ puede ser expresado como $ax+bz$.

Demostración:

Intrínsecamente se puede asumir que a y b son enteros positivos y como estos números no tienen divisores comunes, entonces $(a,b)=1$. Los números más pequeños que cumplen estas condiciones son $a=1$ y $b=2$ ó $a=2$ y $b=1$, de esta manera se tiene que la cota $ab-a-b$ es por lo menos $1\cdot 2-1-2=-1$, así, lo que se tiene que probar es que todo número entero $n>-1$ puede ser expresado como $ax+bz$, *i.e.*, los números que se pueden expresar de esta forma son los enteros positivos.

Por el algoritmo de la división, existen r, $s\in\mathbb{Z}$ tales que $ar+bs=1$. Sea n cualquier entero, entonces, multiplicando la ecuación $ar+bs=1$ por n de ambos lados de la igualdad se obtiene que $arn+bsn=n$.

Como r, s y n son enteros se tiene que $x=rn$ y $z=sn$ también son enteros, por lo tanto $n=ax+bz$ para cualquier n entero positivo, es decir, para n mayor que $ab-a-b$. □

Inciso 2

Si n es un entero, entonces cualquier número divisible por n que sea mayor que $nab - na - nb$ puede ser expresado por $nax + nbz$.

Demostración:

Sean $n, m \in \mathbb{Z}$ tales que n divide a m, entonces existe un entero k tal que $m = kn$. Como $k \in \mathbb{Z}$, entonces gracias al inciso 1 se tiene que $k = ax + bz$; multiplicando esta última igualdad por n de ambos lados se obtiene $kn = axn + bzn$, pero se sabe que $m = kn$, por lo tanto $m = nax + nbz$.

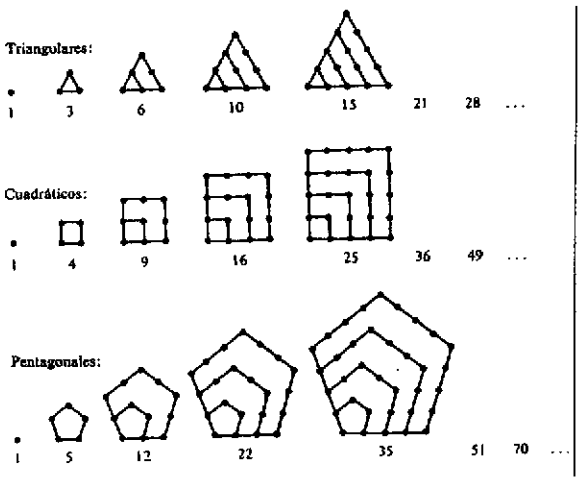
Nuevamente, por el inciso 1 se tiene que $k \geq ab - a - b$ y n es un entero positivo; entonces, si se multiplica la última desigualdad por n de ambos lados, la desigualdad no se altera y resulta que $kn \geq nab - na - nb$, es decir, el entero m es mayor que $nab - na - nb$ y puede ser expresado por $nax + nbz$. □

Inciso 3

Todo número entero es un número triangular o la suma de dos o tres números triangulares, es decir, está compuesto por la suma de uno, dos o tres de los números 1, 3, 6, 10, etc.

Antes de demostrar este inciso se necesita tener un panorama global de lo que es un número triangular, y más aún, lo que es un número poligonal. Para ello se necesitan algunos resultados que a continuación se presentan:

Los pitagóricos relacionaron los números con la geometría; introdujeron la idea de *números poligonales*, tales como los *números triangulares*, *números cuadrados*, *números pentagonales*, *números hexagonales*, etc. Una idea geométrica de esta clase de números figurados se muestra a continuación:



Definición 1: Un *número triangular* es un entero positivo que puede ser representado como puntos acomodados, de acuerdo con cierta regla, en los lados de un triángulo equilátero. Así, la sucesión de números triangulares quedaría escrita de la siguiente manera: 1, 3, 6, 10, 15, 21,... (ver figura). Se denotará al n-ésimo número triangular por t_n donde $n \geq 1$. En la construcción de t_n se observa que en la i-ésima fila, hay exactamente i puntos, así que el n-ésimo número triangular queda perfectamente definido por la siguiente fórmula:

$$t_n = \sum_{i=1}^{n} i = \frac{n(n+1)}{2} \quad \forall n \in \mathbb{N}$$

Una vez que se ha entendido la idea general de lo que es un número triangular se puede dar una definición que funcione para cualquier número figurado.

Definición 2: Para toda $m \geq 1$, se define el k-ésimo número poligonal de orden[13] $m+2$, denotado por $p_m(k)$, como la suma de los primeros k términos de la progresión aritmética con valor inicial 1 y diferencia m, esto es:

$$\begin{aligned} p_m(k) &= 1+(m+1)+(2m+1)+\ldots+((k-1)m+1) \\ &= \frac{mk(k-1)}{2}+k \end{aligned}$$

Con esta definición se tiene que los números triangulares son números poligonales de orden 3, es decir, $m+2=3$ y en consecuencia $m=1$, por lo tanto $p_1(k)=t_k=\frac{k(k+1)}{2}$.

Ahora que se conoce qué son los números poligonales ya se puede regresar al enunciado del inciso 3.

Primero se dará un panorama general de la demostración de este problema:

Lo que se quiere probar es que un número entero N se puede representar como la suma de tres números triangulares, es decir, que $N=\frac{a(a+1)}{2}+\frac{b(b+1)}{2}+\frac{c(c+1)}{2}$, para algunos $a, b, c \in \mathbb{Z}^+$. Para esto, primero se requiere analizar a los enteros que pueden ser escritos como suma de 3 cuadrados. Estos resultados se mostrarán en un Lema y un Teorema y a partir de ellos el inciso 3 se demuestra fácilmente.

Lema 1: Si n es un entero tal que $n \equiv 1, 3, \text{ó } 5 \pmod 8$, entonces n puede ser representado como suma de tres cuadrados.

Demostración:

Si $n=1$, entonces el resultado se obtiene de inmediato, ya que $1=1^2+0^2+0^2$. Ahora, supóngase que $n \geq 2$.

---

[13] El *orden* de un número poligonal no es mas que la dimensión de dicho número; por ejemplo, si se habla de números poligonales de orden tres nos referimos a números triangulares, los de orden cuatro son los cuadrados, y así sucesivamente.

Constrúyase el número entero c de la siguiente manera:

$$\text{Si } n \equiv 1 \pmod 8, \text{ entonces } c = 3$$
$$\text{Si } n \equiv 3 \pmod 8, \text{ entonces } c = 1$$
$$\text{Si } n \equiv 5 \pmod 8, \text{ entonces } c = 5$$

Por hipótesis se sabe que $n \equiv 1 \pmod 8$, $n \equiv 3 \pmod 8$ ó $n \equiv 5 \pmod 8$. Se estudiará cada caso por separado:

Si $n \equiv 1 \pmod 8$, entonces $c = 3$, entonces $cn \equiv 3 \pmod 8$, $cn - 1 \equiv 2 \pmod 8$ y por lo tanto se tiene que $\frac{cn-1}{2} \equiv 1 \pmod 4$. Además, como $cn - 1 = 2 + 8k$ para alguna $k \in \mathbb{Z}$, entonces $cn - 1$ es un número par, por lo tanto $\frac{cn-1}{2} \in \mathbb{Z}$.

Si $n \equiv 3 \pmod 8$, entonces $c = 1$, $cn \equiv 3 \pmod 8$, $cn - 1 \equiv 2 \pmod 8$ y por lo tanto se tiene que $\frac{cn-1}{2} \equiv 1 \pmod 4$ y de manera análoga al caso anterior se tiene que $\frac{cn-1}{2} \in \mathbb{Z}$.

Si $n \equiv 5 \pmod 8$, entonces $c = 3$, $cn \equiv 7 \pmod 8$, $cn - 1 \equiv 6 \pmod 8$ y por lo tanto se tiene que $\frac{cn-1}{2} \equiv 3 \pmod 4$. Además, como $cn - 1 = 6 + 8q$ para alguna $q \in \mathbb{Z}$, entonces $cn - 1$ es un número par, por lo tanto $\frac{cn-1}{2} \in \mathbb{Z}$.

En los tres casos se obtiene que $\left(4n, \frac{cn-1}{2}\right) = 1$.

Por el Teorema de progresiones aritméticas de Dirichlet[14] se sabe que existe un primo p de la forma $p = 4nj + \frac{cn-1}{2}$, para algún entero positivo j.

Ahora, se construye un entero d' que tenga la forma $d' = 8j + c$, después tómese el primo de Dirichlet tal que

[14] Teorema de progresiones aritméticas de Dirichlet: Si $k > 0$ y $(h, k) = 1$, entonces existe una infinidad de primos en la progresión aritmética $nk + h$; $n = 0, 1, 2, \ldots$

$2p = 2\left(4nj + \frac{cn-1}{2}\right) = 8nj + cn - 1 = n(8j+c) - 1 = nd' - 1$, por lo tanto se tiene que $2p = nd' - 1$ y $d' = 8j + c$.

Para poder continuar con la demostración se necesita un lema auxiliar que solamente se enunciará en el recuadro 1 y posteriormente se demostrará porque será util para otras pruebas.

Lema auxiliar: Sea $n \geq 2$. Si existe un entero positivo d' tal que $-d'$ es un residuo cuadrático[15] módulo $d'n-1$, entonces n puede ser representado como la suma de tres cuadrados.

Recuadro 1

Con ayuda de este lema, si se prueba que $-d'$ es un residuo cuadrático módulo $2p = nd' - 1$, entonces se tendrá que n es representable por medio de tres cuadrados.

Supóngase que $-d'$ es un residuo cuadrático modulo p, entonces existe un entero x_0 tal que $x_0^2 \equiv -d' \pmod{p}$, es decir, $x_0^2 + d' \equiv 0 \pmod{p}$. Lo cual implica que $(x_0 + p)^2 + d' \equiv x_0^2 + d' \equiv 0 \pmod{p}$.

Sea $x = \begin{cases} x_0 \text{ si } x_0 \text{ es impar} \\ x_0 + p \text{ si } x_0 \text{ es par} \end{cases}$, entonces x es impar y $x^2 + d'$ es par.

Como $x_0^2 + d'$ es un número par, entonces $x^2 + d' \equiv 0 \pmod{2}$ y se tiene que $x^2 + d' \equiv 0 \pmod{p}$, entonces $x^2 + d' \equiv 0 \pmod{2p}$; por lo tanto es suficiente probar que $-d'$ es un residuo cuadrático módulo p.

Resumiendo, si $2p = nd' - 1$, entonces es suficiente demostrar que $-d'$ es un residuo cuadrático módulo p y por tanto se tendrá que n es la suma de tres cuadrados.

Para probar esto, sea $d' = \prod_{q_i | d'} q_i^{k_i}$ la factorización del entero impar d' en potencias de primos impares distintos q_i. Como

[15] Un entero x es un *residuo cuadrático módulo m*, si y sólo si existe un entero y tal que $y^2 \equiv x \pmod{m}$, donde $(x, m) = 1$. En el apéndice A se profundiza más sobre residuos cuadráticos y el símbolo de Legendre.

$2p = nd' - 1 \equiv -1 \pmod{d'}$, entonces $2p \equiv -1 \pmod{q_i}$ y $(p, q_i) = 1$ para todo primo q_i que divida a d'.

Si $n \equiv 1 \pmod{8}$, entonces $\frac{cn-1}{2} \equiv 1 \pmod{4}$. De esta manera se tiene que $4nj + \frac{cn-1}{2} \equiv 4nj + 1 \pmod{4}$, lo cual implica que $p \equiv 4nj + 1 \pmod{4}$ y, como $4nj + 1 \equiv 1 \pmod{4}$, resulta que $p \equiv 1 \pmod{4}$. Análogamente, si $n \equiv 3 \pmod{8}$, entonces $\frac{cn-1}{2} \equiv 1 \pmod{4}$; de esta manera se tiene que $4nj + \frac{cn-1}{2} \equiv 4nj + 1 \pmod{4}$, lo cual implica que $p \equiv 4nj + 1 \pmod{4}$, y como $4nj + 1 \equiv 1 \pmod{4}$ resulta que $p \equiv 1 \pmod{4}$.

Por otra parte, como el símbolo de Legendre es multiplicativo (en la parte superior)[16], entonces $\left(\frac{-d'}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{d'}{p}\right)$, pero se sabe que $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$, y como $p \equiv 1 \pmod{4}$, entonces $\frac{p-1}{2}$ es un número par y de esta manera se tiene que $(-1)^{\frac{p-1}{2}} = 1$, y por lo tanto: $\left(\frac{-d'}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{d'}{p}\right) = \left(\frac{d'}{p}\right)$. Pero como $d' = \prod_{q_i | d'} q_i^{k_i}$, resulta que

$$\left(\frac{-d'}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{d'}{p}\right) = \left(\frac{d'}{p}\right) = \left(\frac{\prod_{q_i | d'} q_i^{k_i}}{p}\right).$$

Utilizando nuevamente que el símbolo de Legendre es multiplicativo se tiene que

$$\left(\frac{-d'}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{d'}{p}\right) = \left(\frac{d'}{p}\right) = \left(\frac{\prod_{q_i | d'} q_i^{k_i}}{p}\right) = \prod_{q_i | d'} \left(\frac{q_i}{p}\right)^{k_i} = \prod_{q_i | d'} \left(\frac{p}{q_i}\right)^{k_i}$$

Ya se analizó qué sucede si $n \equiv 1$ ó $3 \pmod{8}$; ahora bien, si $n \equiv 5 \pmod{8}$, se sigue el mismo procedimiento que en los dos casos anteriores, y resulta que $p \equiv 3 \pmod{4}$. Como $d' = 8j + c = 8j + 3$ para alguna $j \in \mathbb{Z}$, entonces $d' \equiv 3 \pmod{8}$. Así las cosas, para el ca-

[16] Propiedad 2 del Teorema 4 del apéndice A.

so $n \equiv 5 \pmod 8$ se emplea el hecho de que todos los números primos son congruentes con 1 o con 3 módulo 4, y entonces, se puede reescribir a d' de la siguiente manera:

$d' = \prod_{\substack{q_i \mid d' \\ q_i \equiv 1 \pmod 4}} q_i^{k_i} \prod_{\substack{q_i \mid d' \\ q_i \equiv 3 \pmod 4}} q_i^{k_i}$. Si se observa esta última igualdad y se reduce módulo 4 resulta que $\prod_{\substack{q_i \mid d' \\ q_i \equiv 1 \pmod 4}} q_i^{k_i} \equiv 1 \pmod 4$ puesto que $q_i \equiv 1 \pmod 4$.

De manera análoga se tiene que $\prod_{\substack{q_i \mid d' \\ q_i \equiv 3 \pmod 4}} q_i^{k_i} \equiv (-1)^{k_i} \pmod 4$ ya que $q_i \equiv 3 \pmod 4$. Por lo tanto se obtiene:

$$d' = \prod_{\substack{q_i \mid d' \\ q_i \equiv 1 \pmod 4}} q_i^{k_i} \prod_{\substack{q_i \mid d' \\ q_i \equiv 3 \pmod 4}} q_i^{k_i} \equiv \prod_{\substack{q_i \mid d' \\ q_i \equiv 3 \pmod 4}} (-1)^{k_i} \pmod 4.$$

Luego $d' \equiv \prod_{\substack{q_i \mid d' \\ q_i \equiv 3 \pmod 4}} (-1)^{k_i} \pmod 4$; pero $d' = 8j + 3$, por lo que $8j + 3 \equiv \prod_{\substack{q_i \mid d' \\ q_i \equiv 3 \pmod 4}} (-1)^{k_i} \pmod 4$. Claramente $4 \mid 8j$, y entonces $\prod_{\substack{q_i \mid d' \\ q_i \equiv 3 \pmod 4}} (-1)^{k_i} \equiv 3 \pmod 4$, pero $3 \equiv -1 \pmod 4$. Por lo que resulta que $\prod_{\substack{q_i \mid d' \\ q_i \equiv 3 \pmod 4}} (-1)^{k_i} \equiv -1 \pmod 4$, y de esta manera $d' \equiv -1 \pmod 4$. Como $\prod_{\substack{q_i \mid d' \\ q_i \equiv 3 \pmod 4}} (-1)^{k_i}$ sólo puede tomar el valor de 1 ó -1, y es congruente con -1 módulo 4 se tiene que: $\prod_{\substack{q_i \mid d' \\ q_i \equiv 3 \pmod 4}} (-1)^{k_i} = -1$.

Como se vio anteriormente, $\left(\frac{-d'}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{d'}{p}\right)$, pero en este caso $p \equiv 3 \pmod 4$, de donde resulta que $\left(\frac{-d'}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{d'}{p}\right) = -\left(\frac{d'}{p}\right)$. Utilizando la expansión de d' en primos se obtiene que:

$-\left(\frac{d'}{p}\right) = -\prod_{\substack{q_i \mid d' \\ q_i \equiv 1 \pmod 4}} \left(\frac{q_i}{p}\right)^{k_i} \prod_{\substack{q_i \mid d' \\ q_i \equiv 3 \pmod 4}} \left(\frac{q_i}{p}\right)^{k_i}$. Al utilizar la ley de reciprocidad cuadrática y su corolario[17] se obtiene lo siguiente:

$-\left(\frac{d'}{p}\right) = -\left(\prod_{\substack{q_i \mid d' \\ q_i \equiv 1 \pmod 4}} \left(\frac{p}{q_i}\right)^{k_i} \left(-\prod_{\substack{q_i \mid d' \\ q_i \equiv 3 \pmod 4}} \left(\frac{q_i}{p}\right)^{k_i}\right)\right)$. Si se sustituye el signo "-" que está junto a $\prod_{\substack{q_i \mid d' \\ q_i \equiv 3 \pmod 4}} \left(\frac{q_i}{p}\right)^{k_i}$ por $\prod_{\substack{q_i \mid d' \\ q_i \equiv 3 \pmod 4}} (-1)^{k_i}$, y dado que, como se vio anteriormente $\prod_{\substack{q_i \mid d' \\ q_i \equiv 3 \pmod 4}} (-1)^{k_i} = -1$, resulta que:

$-\left(\frac{d'}{p}\right) = -\prod_{\substack{q_i \mid d' \\ q_i \equiv 1 \pmod 4}} \left(\frac{p}{q_i}\right)^{k_i} \prod_{\substack{q_i \mid d' \\ q_i \equiv 3 \pmod 4}} \left(\frac{q_i}{p}\right)^{k_i} \prod_{\substack{q_i \mid d' \\ q_i \equiv 3 \pmod 4}} (-1)^{k_i}$, es decir,

$-\left(\frac{d'}{p}\right) = \prod_{\substack{q_i \mid d' \\ q_i \equiv 1 \pmod 4}} \left(\frac{p}{q_i}\right)^{k_i} \prod_{\substack{q_i \mid d' \\ q_i \equiv 3 \pmod 4}} \left(\frac{q_i}{p}\right)^{k_i}$, y entonces:

$-\left(\frac{d'}{p}\right) = \prod_{q_i \mid d'} \left(\frac{p}{q_i}\right)^{k_i}$. Por lo tanto $\left(\frac{-d'}{p}\right) = \prod_{q_i \mid d'} \left(\frac{p}{q_i}\right)^{k_i}$.

A continuación se muestra con más detalle cada uno de los desarrollos para dar mayor claridad:

$$\left(\frac{-d'}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{d'}{p}\right)$$

$$= -\left(\frac{d'}{p}\right)$$

$$= -\prod_{\substack{q_i \mid d' \\ q_i \equiv 1 \pmod 4}} \left(\frac{q_i}{p}\right)^{k_i} \prod_{\substack{q_i \mid d' \\ q_i \equiv 3 \pmod 4}} \left(\frac{q_i}{p}\right)^{k_i}$$

$$= -\prod_{\substack{q_i \mid d' \\ q_i \equiv 1 \pmod 4}} \left(\frac{p}{q_i}\right)^{k_i} \prod_{\substack{q_i \mid d' \\ q_i \equiv 3 \pmod 4}} \left(\frac{q_i}{p}\right)^{k_i} \prod_{\substack{q_i \mid d' \\ q_i \equiv 3 \pmod 4}} (-1)^{k_i}$$

$$= \prod_{q_i \mid d'} \left(\frac{p}{q_i}\right)^{k_i}$$

---

[17] Sean p y q dos primos impares distintos, entonces $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{(p-1/2)(q-1/2)}$. La demostración de este resultado y su corolario aparece en el apéndice A.

Nótese que independientemente del caso $n \equiv 1, 3\ 6\ 5 \pmod 8$ se tiene que $\left(\frac{-d'}{p}\right) = \prod_{q_i | d'} \left(\frac{p}{q_i}\right)^{k_i}$. Ahora bien, se sabe[18] que $\left(\frac{2^2}{l}\right) = \left(\frac{4}{l}\right) = 1$ para cualquier número primo impar l. Entonces se puede realizar la siguiente operación:

$\left(\frac{-d'}{p}\right) \cdot 1 = \prod_{q_i | d'} \left(\frac{p}{q_i}\right)^{k_i} \cdot \left(\frac{2 \cdot 2}{q_i}\right) = \prod_{q_i | d'} \left(\frac{2}{q_i}\right)^{k_i} \left(\frac{2p}{q_i}\right)^{k_i}$, es decir, $\left(\frac{-d'}{p}\right) = \prod_{q_i | d'} \left(\frac{2}{q_i}\right)^{k_i} \left(\frac{2p}{q_i}\right)^{k_i}$. Ahora bien, como $2p \equiv -1 \pmod{q_i}$, entonces[19] $\left(\frac{2p}{q_i}\right) = \left(\frac{-1}{q_i}\right)$, por lo tanto se obtiene que: $\left(\frac{-d'}{p}\right) = \prod_{q_i | d'} \left(\frac{2}{q_i}\right)^{k_i} \prod_{q_i | d'} \left(\frac{-1}{q_i}\right)^{k_i}$

Para efectos de la demostración, lo que se requiere es que $\left(\frac{-1}{q_i}\right) = (-1)$. Se sabe que[20] $\left(\frac{-1}{q_i}\right) = \begin{cases} 1 \text{ si } q_i \equiv 1 \pmod 4 \\ -1 \text{ si } q_i \equiv -1 \pmod 4 \end{cases}$, entonces para que se cumpla lo que se necesita, debe ocurrir que $q_i \equiv 3 \pmod 4$, es decir, $q_i = 4k + 3$ para alguna $k \in \mathbb{Z}$. Multiplicando de ambos lados de la última igualdad por 2 se tiene que $2q_i = 8k + 6$ para alguna $k \in \mathbb{Z}$, o lo que es lo mismo

$$2q_i \equiv 6 \pmod 8 \ldots\ldots (1).$$

Resolviendo (1) para q_i se tiene que como $(2,8) = 2$ divide a 6, entonces la congruencia tiene exactamente dos soluciones, a saber: $q_i \equiv \left(\frac{6}{2}\right) x_0 + t\left(\frac{8}{2}\right) \pmod 8$, *i.e.*, $q_i \equiv 3x_0 + 4t \pmod 8$; donde $t = 0, 1$ y x_0 es la solución de la congruencia $\left(\frac{2}{2}\right) x \equiv 1 \left(\mod \left(\frac{8}{2}\right)\right)$, es decir, de la congruencia $x \equiv 1 \pmod 4$. Claramente, $x_0 \equiv 5 \pmod 4$, de esta manera se tiene que $q_i \equiv 3 \cdot 5 + 4 \cdot 0 \equiv 15 \equiv 7 \pmod 8$ y $q_i \equiv 3 \cdot 5 + 4 \cdot 1 \equiv 19 \equiv 3 \pmod 8$. Por lo tanto, $\prod_{q_i | d'} \left(\frac{-1}{q_i}\right)^{k_i} = \prod_{\substack{q_i | d' \\ q_i \equiv 3,7 \pmod 8}} (-1)^{k_i}$.

[18] Gracias al Teorema 4, inciso 4.a del apéndice A.
[19] Por el Teorema 4, inciso 3 del apéndice A.
[20] Teorema 5 del apéndice A.

Ahora aparece $\prod_{q_i|d'}\left(\frac{2}{q_i}\right)^{k_i}$. Como[21] $\left(\frac{2}{q_i}\right)=\begin{cases} 1 \text{ si } q_i \equiv \pm 1 \pmod 8 \\ -1 \text{ si } q_i \equiv \pm 3 \pmod 8 \end{cases}$ y además $-3 \equiv 5 \pmod 8$, entonces $\prod_{q_i|d'}\left(\frac{2}{q_i}\right)^{k_i} = \prod_{\substack{q_i|d' \\ q_i \equiv 3,5 \pmod 8}} (-1)^{k_i}$.

Como consecuencia se tiene que $\left(\frac{-d'}{p}\right)= \prod_{\substack{q_i|d' \\ q_i \equiv 3,5 \pmod 8}} (-1)^{k_i} \prod_{\substack{q_i|d' \\ q_i \equiv 3,7 \pmod 8}} (-1)^{k_i}$.

Entonces se obtiene lo siguiente:

$$\left(\frac{-d'}{p}\right)= \prod_{\substack{q_i|d' \\ q_i \equiv 3,5 \pmod 8}} (-1)^{k_i} \prod_{\substack{q_i|d' \\ q_i \equiv 3,7 \pmod 8}} (-1)^{k_i}$$

$$= \prod_{\substack{q_i|d' \\ q_i \equiv 3 \pmod 8}} (-1)^{k_i} \prod_{\substack{q_i|d' \\ q_i \equiv 5 \pmod 8}} (-1)^{k_i} \prod_{\substack{q_i|d' \\ q_i \equiv 3 \pmod 8}} (-1)^{k_i} \prod_{\substack{q_i|d' \\ q_i \equiv 7 \pmod 8}} (-1)^{k_i}$$

$$= \prod_{\substack{q_i|d' \\ q_i \equiv 3 \pmod 8}} (-1)^{k_i} (-1)^{k_i} \prod_{\substack{q_i|d' \\ q_i \equiv 5,7 \pmod 8}} (-1)^{k_i}$$

$$= \prod_{\substack{q_i|d' \\ q_i \equiv 3 \pmod 8}} (-1)^{2k_i} \prod_{\substack{q_i|d' \\ q_i \equiv 5,7 \pmod 8}} (-1)^{k_i}$$

$$= \prod_{\substack{q_i|d' \\ q_i \equiv 5,7 \pmod 8}} (-1)^{k_i}$$

Lo que establece que $\left(\frac{-d'}{p}\right)= \prod_{\substack{q_i|d' \\ q_i \equiv 5,7 \pmod 8}} (-1)^{k_i}$.

Lo que dice esta última igualdad es que $-d'$ es un residuo cuadrático módulo $2p = d'n - 1$ siempre y cuando la suma de los exponentes k_i sea un número par o, lo que es lo mismo, que $\sum_{\substack{q_i|d' \\ q_i \equiv 5,7 \pmod 8}} k_i \equiv 0 \pmod 2$[22], por lo que, lo único que resta probar es que, en efecto, esta suma es congruente con 0 módulo 2.

Como todo primo es congruente con 1, 3, 5 ó 7 módulo 8, entonces se puede escribir $d' = \prod_{\substack{q_i|d' \\ q_i \equiv 1 \pmod 8}} q_i^{k_i} \prod_{\substack{q_i|d' \\ q_i \equiv 3 \pmod 8}} q_i^{k_i} \prod_{\substack{q_i|d' \\ q_i \equiv 5 \pmod 8}} q_i^{k_i} \prod_{\substack{q_i|d' \\ q_i \equiv 7 \pmod 8}} q_i^{k_i}$. Reduciendo esta ecuación módulo 8 se tiene que

[21] Teorema 6 del apéndice A.

[22] Ya que si $\sum_{\substack{q_i|d' \\ q_i \equiv 5,7 \pmod 8}} k_i \equiv 0 \pmod 2$, entonces $\left(\frac{-d'}{p}\right)= \prod_{\substack{q_i|d' \\ q_i \equiv 5,7 \pmod 8}} (-1)^{k_i} = 1$, lo cual es la definición de residuo cuadrático.

$d' \equiv \prod_{\substack{q_i \mid d' \\ q_i \equiv 3 \pmod 8}} 3^{k_i} \prod_{\substack{q_i \mid d' \\ q_i \equiv 5 \pmod 8}} (-3)^{k_i} \prod_{\substack{q_i \mid d' \\ q_i \equiv 7 \pmod 8}} (-1)^{k_i} \pmod 8$. Reagrupando los términos congruentes con 5 módulo 8 resulta que $d' \equiv \prod_{\substack{q_i \mid d' \\ q_i \equiv 3,5 \pmod 8}} 3^{k_i} \prod_{\substack{q_i \mid d' \\ q_i \equiv 5,7 \pmod 8}} (-1)^{k_i} \pmod 8$.

Si $n \equiv 1$ ó $5 \pmod 8$, entonces $c = 3$ y $d' = 8j + 3 \equiv 3 \pmod 8$. Esto implica que $\sum_{\substack{q_i \mid d' \\ q_i \equiv 3,5 \pmod 8}} k_i \equiv 1 \pmod 2$ y $\sum_{\substack{q_i \mid d' \\ q_i \equiv 5,7 \pmod 8}} k_i \equiv 0 \pmod 2$, que lleva a que $\sum_{\substack{q_i \mid d' \\ q_i \equiv 5,7 \pmod 8}} k_i \equiv 0 \pmod 2$.

Si $n \equiv 3 \pmod 8$, entonces $c = 1$ y $d' = 8j + 1 \equiv 1 \pmod 8$. Por lo tanto se tiene que:

$\sum_{\substack{q_i \mid d' \\ q_i \equiv 3,5 \pmod 8}} k_i \equiv 0 \pmod 2$ y $\sum_{\substack{q_i \mid d' \\ q_i \equiv 5,7 \pmod 8}} k_i \equiv 0 \pmod 2$, de donde $\sum_{\substack{q_i \mid d' \\ q_i \equiv 5,7 \pmod 8}} k_i \equiv 0 \pmod 2$.

Entonces, de ambos casos se concluye que $\sum_{\substack{q_i \mid d' \\ q_i \equiv 5,7 \pmod 8}} k_i \equiv 0 \pmod 2$, lo cual implica que $-d'$ es un residuo cuadrático módulo p. Ahora, ya que $\left(\frac{-d'}{p}\right) = 1$, entonces $-d'$ también es residuo cuadrático módulo $2p = d'n - 1$. Así, por el Lema auxiliar se tiene que n puede ser representado como la suma de tres cuadrados. □

Teorema 1: Si N es un entero positivo tal que $N \equiv 3 \pmod 8$, entonces N es la suma de tres cuadrados impares.

Demostración:

Se sabe que para cualquier entero $x \equiv 0, 1, 2, 3, 4, 5, 6$ ó $7 \pmod 8$, se tiene que $x^2 \equiv 0^2, 1^2, 2^2, 3^2, 4^2, 5^2, 6^2$ ó $7^2 \pmod 8$, por lo que $x^2 \equiv 0, 1$ ó $4 \pmod 8$.

Si $N \equiv 3 \pmod 8$, entonces, gracias al Lema 1, N es suma de tres cuadrados, es decir, existen $a, b, c \in \mathbb{Z}$ tales que $N = a^2 + b^2 + c^2$; como $N \equiv 3 \pmod 8$, entonces $a^2 + b^2 + c^2 \equiv 3 \pmod 8$, lo que lleva a que $a^2 \equiv b^2 \equiv c^2 \equiv 1 \pmod 8$ y cada uno de estos cuadrados debe de ser impar, ya que si $a^2 \equiv 1 \pmod 8$, entonces $a^2 - 1 \equiv 0 \pmod 8$, o lo que es lo mismo $(a-1)(a+1) \equiv 0 \pmod 8$, es decir, $8 \mid a-1$ ó $8 \mid a+1$. Si $8 \mid a+1$ entonces existe $w \in \mathbb{Z}$ tal que $a+1 = 8w$, de donde $a = 2(4w) - 1$ y por lo tanto a es impar. Análogamente, b y c son impares.

Por lo tanto, N es la suma de tres cuadrados impares. □

Con estos dos resultados (Lema 1 y Teorema 1), la demostración del inciso 3 se sigue de inmediato:

Demostración (del inciso 3: Todo número entero es la suma de tres números triangulares):

Se sabe que los números triangulares son de la forma $\frac{k(k+1)}{2}$. Sea $N \geq 1$ un entero arbitrario. Entonces, por el Teorema 1, el entero $8N+3$, que es congruente con 3 módulo 8 para cualquier N, es la suma de tres cuadrados impares. De donde resulta que existen enteros no negativos k_1, k_2, k_3 tales que:

$$\begin{aligned} 8N+3 &= (2k_1+1)^2 + (2k_2+1)^2 + (2k_3+1)^2 \\ &= 4k_1^2 + 4k_1 + 1 + 4k_2^2 + 4k_2 + 1 + 4k_3^2 + 4k_3 + 1 \\ &= 4\left(k_1^2 + k_1 + k_2^2 + k_2 + k_3^2 + k_3\right) + 3 \end{aligned}$$

Entonces $8N = 4\left(k_1^2 + k_1 + k_2^2 + k_2 + k_3^2 + k_3\right)$, o lo que es lo mismo, $N = \frac{1}{2}\left(k_1^2 + k_1 + k_2^2 + k_2 + k_3^2 + k_3\right)$ y por lo tanto:

$$N = \frac{k_1(k_1+1)}{2} + \frac{k_2(k_2+1)}{2} + \frac{k_3(k_3+1)}{2}$$

Así, todo número entero es la suma de tres números triangulares. □

Inciso 4

Todo número entero es un número pentagonal o la suma de dos, tres, cuatro o cinco números pentagonales, *i.e.*, está compuesto por uno, dos, tres, cuatro o cinco números 1, 4, 10, 20, 35, etc. De la misma manera, es la suma de dos, tres, cuatro, cinco, seis, siete u ocho números hexagonales 1, 5, 15, 35, 70, 126, 210, etc.[23]

Lo que se hará a continuación es presentar una reseña de la demostración que Nathanson [1996] incluyó en su libro *Additive Number Theory*, y que se ocupa del caso general de este inciso. En la tesis se toma la demostración de Nathanson para responder el inciso 4, pero se incluyen algunas anotaciones adicionales para que sea más comprensible.

Primeramente se recordará lo que es un número poligonal. Sea $m \geq 1$ un número entero. Se define el k-ésimo número poligonal de orden $(m+2)$ como la suma de los primeros k términos en la progresión aritmética $1, (1+m), (1+2m), (1+3m), \ldots$ De esta manera, y como ejemplo, los números poligonales de orden 3 y 4 son los números triangulares y cuadrados respectivamente.

Fermat fue el primero en enunciar el siguiente resultado: "Todo número es un número triangular o la suma de dos o tres triangulares; todo número es un cuadrado o la suma de dos, tres o cuatro cuadrados; todo número es un número pentagonal o la suma de dos, tres, cuatro o cinco pentagonales; y así *hasta el infinito*".

Como se vio en el inciso 3, Gauss probó que todo número es un triangular o la suma de dos o tres triangulares o, equivalentemente, que todo entero no negativo $n \equiv 3 \pmod 8$ es la suma de tres cuadrados impares. Más adelante en la tesis se demostrará el inciso 5, mismo que se

---

[23] Este enunciado tiene varios errores. Para Waring el conjunto de números pentagonales es $\{1, 4, 10, 20, 35, \ldots\}$ y no tiene correspondencia con los números figurados de orden 5, *i.e.*, los pentagonales, que son: $\{1, 5, 12, 22, 35, \ldots\}$. De la misma manera, Waring afirma que los números hexagonales son $\{1, 5, 15, 35, 70, 126, 210, \ldots\}$, y en realidad este conjunto es $\{1, 6, 15, 28, 45, 66, 91, \ldots\}$. Además, afirma que todo entero puede ser escrito como la suma de 1, 2, 3, …,7 ú 8 números hexagonales, pero se sabe que todo entero puede ser escrito como la suma de 1, 2, 3, 4, 5 ó 6 números hexagonales y no hacen falta ni 7 ni 8 de ellos.
Por lo tanto, el enunciado debería de decir:
"Todo número entero es un número pentagonal o la suma de dos, tres, cuatro o cinco números pentagonales, *i.e.*, está compuesto por uno, dos, tres, cuatro o cinco números 1, 5, 12, 22, 35, etc. De la misma manera, es la suma de dos, tres, cuatro, cinco o seis números hexagonales 1, 6, 15, 28, 45, 66, 91, etc."

debe a Lagrange, quien probó que todo número es la suma de cuatro cuadrados.

Para los casos $m \geq 5$, Cauchy probó que todo número entero es la suma de m números poligonales de orden m, con al menos cuatro de estos sumando distintos de cero o uno.

Pepin [1892-93] y Dickson [1927] publicaron tablas[24] de representación para todo entero $n \leq 120m$ como la suma de m números poligonales de orden m, con al menos cuatro de estos diferentes de 0 ó 1. Por lo tanto es suficiente probar el teorema de Cauchy solamente para $n \geq 120m$.

Notación: Se denotará al k-ésimo número poligonal de orden $(m+2)$ por medio de $p_m(k) = \frac{m}{2}(k^2 - k) + k$, de esta manera se tiene que $p_m(0) = 0$, $p_m(1) = 1$, $p_m(2) = m + 2$, ...

Una vez analizada someramente la historia de este resultado y fijado la notación con la cual se va a trabajar, se comenzará con la teoría que dará como resultado el inciso 4 y su caso general.

La vía a través de la cual se dará respuesta a este inciso será mediante el Teorema de Cauchy, y para la demostración de dicho resultado se necesitan algunas cualidades del intervalo $I = \left(\frac{1}{2} + \sqrt{\frac{6N}{m} - 3}\ , \frac{2}{3} + \sqrt{\frac{8N}{m} - 8} \right)$ y así encontrar cuatro enteros consecutivos para poder construir la suma de $(m + 1)$ números poligonales de orden $(m + 2)$ que sea la representación de cualquier entero. Para ello se requiere construir y demostrar tres lemas:

- El Lema 1 define el intervalo I, antes mencionado, y su longitud.
- El Lema 2 establece, mediante un par de desigualdades, las propiedades que tienen los números que pertenecen al intervalo I.
- En el Lema 3, a partir de las desigualdades construidas en el Lema 2, se representa a números enteros como la suma de cuadrados y otras representaciones necesarias para resolver el Teorema de Cauchy.

[24] En las cuales hay algunos errores que pueden ser corregidos.

Lema 1: Sean $m \geq 3$, $N \geq 2m$ y L la longitud del intervalo $I = \left(\frac{1}{2} + \sqrt{\frac{6N}{m} - 3}\ ,\ \frac{2}{3} + \sqrt{\frac{8N}{m} - 8} \right)$. Entonces:

i) $L > 4$ si $N \geq 108m$.
ii) Sea $l \in \mathbb{Z}$, entonces $L > lm$ si $l \geq 3$ y $N > 7l^2m^3$.

Demostración:

Para facilitar las cuentas, sea $x = \frac{N}{m} \geq \frac{2m}{m} = 2$ y $l_0 = l - \frac{1}{6}$. Con todos estos cambios se tiene que $L = \frac{2}{3} + \sqrt{8x-8} - \frac{1}{2} - \sqrt{6x-3} = \sqrt{8x-8} - \sqrt{6x-3} + \frac{1}{6}$. Entonces $L > l$ si y sólo si $\sqrt{8x-8} > \sqrt{6x-3} + l_0$, si se eleva al cuadrado ambos lados de la desigualdad y se reagrupan los términos, se tiene que $2x - l_0^2 - 5 > 2l_0\sqrt{6x-3}$. Ahora, elevando al cuadrado nuevamente y reagrupando se obtiene:

$$\left(2x - l_0^2 - 5\right)^2 > 4l_0^2\left(6x-3\right)$$
$$4x^2 + l_0^4 + 25 - 4xl_0^2 - 20x + 10l_0^2 > 24xl_0^2 - 12l_0^2$$
$$\left(4x^2 - 4xl_0^2 - 20x - 24xl_0^2\right) + \left(l_0^4 + 10l_0^2 + 25\right) + 12l_0^2 > 0$$
$$4x\left(x - \left(7l_0^2 + 5\right)\right) + \left(l_0^2 + 5\right)^2 + 12l_0^2 > 0$$

Esta última desigualdad se cumple si $x \geq 7l_0^2 + 5 = 7\left(l - \frac{1}{6}\right)^2 + 5$. Por lo tanto se tiene que $L > l$ siempre y cuando $x = \frac{N}{m} \geq 7\left(l - \frac{1}{6}\right)^2 + 5$. Como $7\left(4 - \frac{1}{6}\right)^2 + 5 = 107.86\bar{1}$, entonces se sigue que $L > 4$ siempre que $N \geq 108m$, lo cual demuestra el inciso *i*).

Como $7l^2 > 7\left(l - \frac{1}{6}\right)^2 + 5$ para $l \geq 3$, entonces resulta que $L > l$ si $l \geq 3$ y $\frac{N}{m} \geq 7l^2$. Por lo tanto, si $l \geq 3$ y $N > 7l^2m^3$, entonces $L > lm$ □

Lema 2: Sean $m \geq 3$ y $N \geq 2m$. Considérese los enteros no negativos a, b y r tales que $0 \leq r < m$ y

$$N = \frac{m}{2}(a-b)+b+r \quad \ldots\ldots\ldots\ldots\ldots\ldots \quad (1).$$

Si $b \in I$; donde $I = \left(\frac{1}{2}+\sqrt{\frac{6N}{m}-3}\,,\ \frac{2}{3}+\sqrt{\frac{8N}{m}-8}\right)$, entonces $b^2 < 4a$ y $3a < b^2 + 2b + 4$.

Demostración:

De la ecuación (1) se tiene que:

$$N = \frac{m}{2}(a-b)+b+r$$

$$N = a\frac{m}{2} - b\frac{m}{2} + b + r$$

$$a\frac{m}{2} = N + b\frac{m}{2} - b - r$$

$$a = N\frac{2}{m} + b - b\frac{2}{m} - r\frac{2}{m}$$

$$a = b\left(1-\frac{2}{m}\right)+2\left(\frac{N-r}{m}\right)$$

Entonces $b^2 - 4a = b^2 - 4\left(1-\frac{2}{m}\right)b - 8\left(\frac{N-r}{m}\right) < 0$ siempre y cuando $0 \leq b < 2\left(1-\frac{2}{m}\right)+\sqrt{4\left(1-\frac{2}{m}\right)^2+8\left(\frac{N-r}{m}\right)}$.

Si $b \in I$, entonces se tiene que:

$$\begin{aligned} 0 < b &< \frac{2}{3}+\sqrt{\frac{8N}{m}-8} \\ &< 2\left(1-\frac{2}{m}\right)+\sqrt{8\left(\frac{N-r}{m}\right)} \\ &< 2\left(1-\frac{2}{m}\right)+\sqrt{4\left(1-\frac{2}{m}\right)^2+8\left(\frac{N-r}{m}\right)} \end{aligned}$$

Por lo tanto $b^2 - 4a < 0$, es decir $b^2 < 4a$.

Nuevamente, considérese $b^2 + 2b + 4 - 3a$, lo que se quiere analizar es cuándo esta expresión es mayor que cero. Para esto se substituye $a = b\left(1-\frac{2}{m}\right)+2\left(\frac{N-r}{m}\right)$. Entonces se tiene que

$b^2+2b+4-3a=b^2-\left(1-\frac{6}{m}\right)b-\left(6\left(\frac{N-r}{m}\right)-4\right)>0$ siempre y cuando se cumpla que $b>\left(\frac{1}{2}-\frac{3}{m}\right)+\sqrt{\left(\frac{1}{2}-\frac{3}{m}\right)^2+6\left(\frac{N-r}{m}\right)-4}$. Pero si se supone que $b\in I$, entonces:

$$b>\frac{1}{2}+\sqrt{\frac{6N}{m}-3}$$
$$>\left(\frac{1}{2}-\frac{3}{m}\right)+\sqrt{\left(\frac{1}{2}-\frac{3}{m}\right)^2+\frac{6N}{m}-4}$$
$$>\left(\frac{1}{2}-\frac{3}{m}\right)+\sqrt{\left(\frac{1}{2}-\frac{3}{m}\right)^2+6\left(\frac{N-r}{m}\right)-4}$$

Por lo tanto $b^2+2b+4-3a>0$, es decir, $3a<b^2+2b+4$. □

El siguiente Lema a veces es llamado "Lema de Gauss".

Lema 3: Sean a y b dos enteros positivos impares tales que $b^2<4a$ y $3a<b^2+2b+4$. Entonces existen enteros no negativos s, t, u y v tales que $a=s^2+t^2+u^2+v^2$ y $b=s+t+u+v$.

Demostración:

Como a y b son ambos impares, entonces, observando un sistema completo de residuos módulo 8 se tiene que $a, b\equiv 1, 3, 5$ ó $7 \pmod 8$, entonces $4a\equiv 4, 12, 20$ ó $28 \pmod 8$, pero $4\equiv 12\equiv 20\equiv 28 \pmod 8$, por lo tanto $4a\equiv 4 \pmod 8$ y $b^2\equiv 1, 9, 25$ ó $49 \pmod 8$; pero $1\equiv 9\equiv 25\equiv 49 \pmod 8$, por lo tanto $b^2\equiv 1 \pmod 8$. De esta manera se tiene que $4a-b^2\equiv 4-1\equiv 3 \pmod 8$. Gracias al Teorema 1 del inciso 3 (véase la página 41) existen tres enteros positivos impares. Sean $x\geq y\geq z$ tales que $4a-b^2=x^2+y^2+z^2$.

Se puede escoger el signo de $\pm z$ de tal manera que $b+x+y\pm z\equiv 0 \pmod 4$. Se definen los enteros s, t, u y v de la siguiente manera:

$$s = \frac{b+x+y\pm z}{4}$$
$$t = \frac{b+x}{2} - s = \frac{b+x-y\mp z}{4}$$
$$u = \frac{b+y}{2} - s = \frac{b-x+y\mp z}{4}$$
$$v = \frac{b\pm z}{2} - s = \frac{b-x-y\pm z}{4}$$

Si se hacen las cuentas se puede verificar que con estas definiciones se obtiene: $a = s^2 + t^2 + u^2 + v^2$, $b = s+t+u+v$ y $s \geq t \geq u \geq v$. □

Teorema de Cauchy: Si $m \geq 4$ y $N \geq 108m$, entonces N puede ser escrito como la suma de $(m+1)$ números poligonales de orden $(m+2)$, con al menos cuatro de estos distintos de 0 ó 1. Si $N \geq 324$, entonces N puede ser escrito como la suma de cinco números pentagonales y al menos uno de estos es 0 ó 1.

Demostración:

Por el Lema 1, la longitud del intervalo $I = \left(\frac{1}{2} + \sqrt{\frac{6N}{m} - 3}\,,\, \frac{2}{3} + \sqrt{\frac{8N}{m} - 8}\right)$ es mayor que 4 gracias a que $N \geq 108m$. Entonces I contiene cuatro enteros consecutivos y como consecuencia dos números impares consecutivos, denotados por b_1 y b_2. Si $m \geq 4$, el conjunto de números de la forma $b+r$ donde $b \in \{b_1, b_2\}$ y $r \in \{0, 1, ..., m-3\}$ es un sistema completo de residuos módulo m y entonces se puede escoger a $b \in \{b_1, b_2\} \subseteq I$ y a $r \in \{0, 1, ..., m-3\}$ de tal manera que $N \equiv b + r \pmod{m}$.

Por lo tanto $a = 2\left(\frac{N-b-r}{m}\right) + b = \left(1 - \frac{2}{m}\right)b + 2\left(\frac{N-r}{m}\right)$ es un entero positivo impar y $N = \frac{m}{2}(a-b) + b + r$. Por el Lema 2, como $b \in I$, se tiene que $b^2 < 4a$ y $3a < b^2 + 2b + 4$.

Ahora bien, por el Lema 3, existen enteros no negativos s, t, u y v tales que $a = s^2 + t^2 + u^2 + v^2$ y $b = s+t+u+v$. De aquí que:

$$
\begin{aligned}
N &= \frac{m}{2}(a-b)+b+r \\
&= \frac{m}{2}\left(s^2-s+t^2-t+u^2-u+v^2-v\right)+(s+t+u+v)+r \\
&= \left(\frac{m\left(s^2-s\right)}{2}+s\right)+\left(\frac{m\left(t^2-t\right)}{2}+t\right)+\left(\frac{m\left(u^2-u\right)}{2}+u\right)+\left(\frac{m\left(v^2-v\right)}{2}+v\right)+r \\
&= p_m(s)+p_m(t)+p_m(u)+p_m(v)+r
\end{aligned}
$$

Como $0 \le r \le m-3$ y 0, 1 son números poligonales de orden $(m+2)$ para toda m, entonces se tiene el Teorema de Cauchy para $m \ge 4$, esto es, para números poligonales de orden al menos 6.

Para obtener el resultado de números pentagonales, es decir, para $m=3$, considérense números de la forma b_1+r y b_2+r, donde b_1 y b_2 son enteros consecutivos impares en el intervalo I y $r=0$ ó 1. □

Este resultado tiene varias aplicaciones en la teoría de los números. Una de ellas, bastante representativa en la teoría aditiva de números, es el siguiente teorema que se le acredita a Legendre:

Teorema de Legendre: Sea $m \ge 3$ y $N \ge 28m^3$. Si m es impar, entonces N es la suma de cuatro números poligonales de orden $(m+2)$. Si m es par, entonces N es la suma de cinco números poligonales de orden $(m+2)$, con al menos uno de ellos igual a 0 ó 1.

Demostración:

Como $m \ge 3$, entonces como $N \ge 28m^3$ y $N \ge 28m^3 \ge 252m \ge 2m$. Por lo tanto $N \ge 2m$. Así, gracias al Lema 1, como $N \ge 7l^2m^3 = 28m^3$, haciendo $l=2$, la longitud del intervalo I es mayor que $2m$, y por ende I contiene m enteros impares consecutivos.

Si m es impar, entonces los m enteros impares consecutivos del intervalo I forman un sistema completo de residuos módulo m, por lo que $N \equiv b \pmod m$ para algún entero impar $b \in I$. Se toma la misma definición para el número a que se utilizó en la demostración del Teorema de Cauchy: $a = 2\left(\frac{N-b-r}{m}\right)+b$. Tómese a $r=0$, entonces $N = \frac{m}{2}(a-b)+b$. Ahora bien, $m \ge 3$, y ya se vio que $N \ge 2m$; claramente a, b y $r=0$ son enteros no negativos tales que $0 \le r < m$, en-

tonces se cumplen las hipótesis del Lema 2. Por lo tanto, si $b \in I$, se tiene que $b^2 < 4a$ y $3a < b^2 + 2b + 4$. De la misma manera se cumplen las hipótesis del Lema 3 por lo tanto existen enteros no negativos *s*, *t*, *u* y *v* tales que $a = s^2 + t^2 + u^2 + v^2$ y $b = s + t + u + v$. Entonces se tiene que:

$$
\begin{aligned}
N &= \frac{m(a-b)}{2} + b = \frac{m\left(s^2 + t^2 + u^2 + v^2 - s - t - u - v\right)}{2} + s + t + u + v \\
&= \frac{m\left[s(s-1) + t(t-1) + u(u-1) + v(v-1)\right]}{2} + s + t + u + v \\
&= \frac{ms(s-1) + mt(t-1) + mu(u-1) + mv(v-1) + 2s + 2t + 2u + 2v}{2} \\
&= \frac{ms(s-1)}{2} + s + \frac{mt(t-1)}{2} + t + \frac{mu(u-1)}{2} + u + \frac{mv(v-1)}{2} + v \\
&= p_m(s) + p_m(t) + p_m(u) + p_m(v)
\end{aligned}
$$

Por lo tanto N es la suma de cuatro números poligonales de orden $(m+2)$.

Si m es par y N es impar, entonces $N \equiv b \pmod{m}$ para algún entero impar $b \in I$, y por un razonamiento análogo se tiene que N es la suma de cuatro números poligonales de orden $(m+2)$. Si m es par y N es par, entonces $N - 1 \equiv b \pmod{m}$ para algún entero impar $b \in I$. Entonces $N - 1$ es impar y por lo tanto
$N - 1 = p_m(s) + p_m(t) + p_m(u) + p_m(v)$, es decir,
$N = p_m(s) + p_m(t) + p_m(u) + p_m(v) + 1$.

Por lo tanto N es la suma de cinco números poligonales de orden $(m+2)$, y alguno de ellos es $p_m(1) = 1$. □

Inciso 5

Todo entero es un cuadrado o la suma de dos, tres o cuatro cuadrados.

De este problema ya se tienen referencias que datan desde la época de Diofanto. Bachet señala que Diofanto asumió en diferentes partes de su *Aritmética* (libro V) que cualquier número es un cuadrado o la suma de 2, 3 ó 4 cuadrados, y él mismo había verificado esta hipótesis para todos los números hasta 325 y daría la entrada para una prueba. Descompuso en 4 o menos cuadrados a cada número hasta el 120, también mencionó –Bachet– la generalización de Diofanto, escrita en su libro IV, del problema que consiste en encontrar k números tales que la suma de sus cuadrados sea un número dado n. Atribuir a Diofanto un conocimiento más profundo de este teorema sería falso; él no hizo mención de una condición para que un número fuera la suma de cuatro cuadrados, pero sí dio condiciones necesarias para el estudio de que todo entero pueda ser representado como la suma de dos o tres cuadrados. Diofanto intentó dividir un número dado en cuatro porciones tales que la suma de cualesquiera tres de las partes fuera un cuadrado. Así, tres veces la suma de las cuatro partes es la suma de cuatro cuadrados.

Fermat indicó que ya tenía una prueba de que cada número es la suma de cuatro cuadrados, y también comentó que al parecer Diofanto sabía este resultado. Mencionó además que tenía muchos problemas en encontrar los nuevos principios necesarios para aplicar su método de descenso infinito en la demostración de que cada número es un cuadrado o la suma de 2, 3 ó 4 cuadrados.

Descartes enunció un teorema (sin demostrarlo): Cualquier número que sea la suma de tres cuadrados y mayor que 41 se puede expresar también como la suma de cuatro cuadrados, excepto solamente los productos de 6 ó 14 por 4, 4^2, 4^3, ... No existen otros números que no se compongan de cuatro cuadrados, excepto $2 \cdot 4^n$, que no es un cuadrado, ni suma de tres o cuatro cuadrados, y que solamente lo es de dos.

Una vez que se conoce un poco de la historia de este problema se procederá a dar la demostración con todo detalle de este inciso.

Primero se van a dar las condiciones necesarias para que un entero pueda ser representado como la suma de uno, dos o tres cuadrados y, posteriormente, se demostrará el caso general que dice que todo entero es la suma de cuatro cuadrados.

El problema de un cuadrado se puede escribir en un teorema que dice:

Teorema 1: Si $Q(x) = x^2$, entonces la ecuación $Q(x) = n$ tiene soluciones enteras si y sólo si $n = m^2$ para algún entero m.

Claramente este teorema es cierto, ya que está afirmando que los números enteros que son representables por un cuadrado son los mismos números cuadrados. Nótese también que si un entero n es representable por un cuadrado, también se puede ver como suma de cuatro cuadrados ya que si $n = m^2$ para algún $m \in \mathbb{Z}$, entonces también $n = m^2 + 0^2 + 0^2 + 0^2$.

Para el problema de los dos cuadrados, lo que se debe de hacer es caracterizar el conjunto de enteros para los cuales la ecuación diofantina $x^2 + y^2 = n$ tiene solución, donde $x, y, n \in \mathbb{Z}$. Emil Grosswald [1984], en su libro *Representations of integers as sums of squares*, afirma que este problema se demuestra si se prueba el siguiente teorema:

Teorema 2: La ecuación diofantina $x^2 + y^2 = n$ tiene solución si y sólo si todos los divisores primos q de n, tales que $q \equiv 3 \pmod 4$, aparecen en la descomposición de n con potencias pares.

Para la demostración de este resultado se necesitan un par de lemas auxiliares que a continuación se presentan:

Lema 1: Si $p \mid n$ y $p \equiv 3 \pmod 4$, entonces la ecuación diofantina $x^2 + y^2 = n$ no tiene solución primitiva[25].

Demostración:

Se va a suponer que x y y son solución de la ecuación $x^2 + y^2 = n$ con $(x, y) = 1$ y se tratará de llegar a una contradicción. Sea p un divisor primo de n. Si $p \mid n$ y $p \mid x$, entonces $p \mid y$, lo cual es una contradicción con el hecho de que $(x, y) = 1$. De esta manera se tiene que si $p \mid n$ entonces $p \nmid x$ y $p \nmid y$.

Por el pequeño Teorema de Fermat[26], $x^{p-1} \equiv 1 \pmod p$ y entonces $yx^{p-1} \equiv y \pmod p$. Si se hace un cambio de variable $z = yx^{p-2}$, se

[25] Se dice que x_1, y_1 es una *solución primitiva* de la ecuación $x^2 + y^2 = n$ si los enteros x_1, y_1 son primos relativos, *i.e.*, $(x_1, y_1) = 1$.

tiene que $xz \equiv y \pmod{p}$; elevando al cuadrado ambos lados de la congruencia y sumando x^2 se obtiene:

$$x^2\left(z^2+1\right) \equiv y^2 + x^2 \equiv n \equiv 0 \pmod{p}.$$

Como $p \nmid x$ y $x^2\left(z^2+1\right) \equiv 0 \pmod{p}$, entonces $z^2+1 \equiv 0 \pmod{p}$, o lo que es lo mismo, $z^2 \equiv -1 \pmod{p}$, *i.e.*, -1 es un residuo cuadrático[27] modulo p, entonces $\left(\frac{-1}{p}\right) = 1$, y como por otro lado se sabe que $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$. Por lo tanto $\frac{p-1}{2}$ es un número par, es decir, $\frac{p-1}{2} \equiv 0 \pmod{2}$; entonces $p-1 \equiv 0 \pmod{4}$ y por lo tanto $p \equiv 1 \pmod{4}$, lo cual contradice el hecho de que $p \equiv 3 \pmod{4}$.

Se concluye que la ecuación diofantina $x^2 + y^2 = n$ no tiene solución primitiva. □

Lema 2: La ecuación diofantina $x^2 + y^2 = n$ tiene solución si n es un número primo congruente con 1 módulo 4, *i.e.*, si $n = p \equiv 1 \pmod{4}$.

Demostración:

Si $p \equiv 1 \pmod{4}$, entonces $p-1 \equiv 0 \pmod{4}$, lo cual implica que $\frac{p-1}{2} \equiv 0 \pmod{2}$, es decir, $\frac{p-1}{2}$ es un número par y por consiguiente $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = 1$, lo cual quiere decir que la congruencia $x^2 + 1 \equiv 0 \pmod{p}$ tiene solución. Por lo tanto $x^2 + y^2 = mp$ es soluble con x, y y m enteros. Lo que se tiene que probar ahora es que $m = 1$.

Como x y y pertenecen al sistema completo de residuos modulo p, entonces se escoge $|x| < \frac{p}{2}$, $|y| < \frac{p}{2}$, entonces $x^2 + y^2 < \frac{p^2}{4} < \frac{p^2}{2}$ y $m < \frac{p}{2}$. Sea m_0 el menor entero tal que $x^2 + y^2 = m_0 p$ es soluble para x y y

---

[26] Pequeño Teorema de Fermat: Sea p un primo tal que $p \nmid a$, entonces $a^{p-1} \equiv 1 \pmod{p}$.

[27] Para ver definiciones, propiedades y resultados de residuos cuadráticos y símbolo de Legendre, revise el apéndice A.

enteros. Se supondrá que $m_0 > 1$ y se tratará de llegar a una contradicción.

Supóngase entonces que $m_0 > 1$ y que $m_0 \mid x$, entonces $m_0 \nmid y$.[28] Tómense los enteros c y d de tal manera que $x_1 = x - cm_o$ y $y_1 = y - dm_0$; con $|x_1| < \frac{m_0}{2}, |y_1| < \frac{m_0}{2}$ y ambos no cero. Entonces $0 < x_1^2 + y_1^2 < 2\left(\frac{m_0^2}{4}\right) = \left(\frac{m_o}{2}\right)m_0$. Como $x_1^2 + y_1^2 \equiv x^2 + y^2 \equiv 0 \pmod{m_0}$, se sigue que $x_1^2 + y_1^2 = m_0 m_1$, donde $0 < m_1 < \frac{m_0}{2}$.

Si se multiplica la ecuación $x^2 + y^2 = m_0 p$ por $x_1^2 + y_1^2 = m_0 m_1$ se tiene que:

$$m_0^2 m_1 p = \left(x^2 + y^2\right)\left(x_1^2 + y_1^2\right) = \left(xx_1 + yy_1\right)^2 + \left(xy_1 - yx_1\right)^2.$$

Como $x_1 = x - cm_o$ y $y_1 = y - dm_0$ entonces:

$$xx_1 + yy_1 = x\left(x - cm_0\right) + y\left(y - dm_0\right) = x^2 + y^2 - m_0\left(cx + dy\right) = m_0\left(p - cx - dy\right) = m_0 X$$

y de la misma manera se obtiene que:

$$xy_1 - yx_1 = x\left(y - dm_0\right) - y\left(x - cm_0\right) = m_0\left(cy - dx\right) = m_0 Y.$$

De donde claramente se está suponiendo que $X = p - cx - dy$ y $Y = cy - dx$. Por lo tanto $m_0^2 m_1 p = m_0^2\left(X^2 + Y^2\right)$, o lo que es lo mismo, $X^2 + Y^2 = m_1 p$, con $0 < m_1 < \frac{m_0}{2}$, lo cual contradice la minimalidad de m_0. Por lo tanto $m_0 = 1$ y esto prueba el lema 2. □

Una vez que se demostró el Lema 1, ya se puede pasar a la demostración del Teorema 2 y así resolver el problema de los dos cuadrados.

Demostración (del Teorema 2):

Supóngase que x y y son solución de la ecuación $x^2 + y^2 = n$, con $(x, y) = d$, y que $p \equiv 3 \pmod 4$ es tal que $p^r \mid d$ y $p^{r+1} \nmid d$.

---

[28] Ya que si se supone lo contrario, es decir, si $m_0 \mid y$ entonces $m_0^2 \mid x^2 + y^2$ lo cual implica que $m_0^2 \mid m_0 p$, *i.e.*, $m_0 \mid p$ y por lo tanto se tendría que $m_0 = 1$, lo cual es imposible.

Sean $x = dx_1$, $y = dy_1$ donde $(x_1, y_1) = 1$, entonces
$n = x^2 + y^2 = (dx_1)^2 + (dy_1)^2 = d^2(x_1^2 + y_1^2) = d^2 n_1$.

Si $p^c \mid n$ y $p^{c+1} \nmid n$, entonces $p^{c-2r} \mid n_1$ y $p^{c-2r-1} \nmid n_1$. Sin embargo, $x_1^2 + y_1^2 = n_1$, lo cual implica que x_1 y y_1 es una representación primitiva de n_1.[29] Por el Lema 1, $p \nmid n_1$, por lo tanto $c = 2r$ y es par.

Se puede entonces afirmar que si x y y son solución de la ecuación $x^2 + y^2 = n$ y p es un primo tal que $p \equiv 3 \pmod 4$, $p^r \mid d$ y $p^{r+1} \nmid d$, entonces p aparece en la descomposición de n con potencia par.

Inversamente, si se supone que todos los divisores primos q de n que son congruentes con 3 módulo 4 aparecen con potencias pares en la descomposición de n, lo que se quiere probar es que n puede ser escrita como la suma de dos cuadrados.

Gracias al Lema 1 se sabe que todos los primos congruentes con 1 módulo 4 son representables como suma de dos cuadrados; así mismo, las potencias de 2 también se pueden escribir como suma de dos cuadrados, y como el producto de dos números que son representables como suma de dos cuadrados se puede expresar nuevamente como suma de dos cuadrados[30], entonces $n_0 = 2^f n_1$ es la suma de dos cuadrados, donde $f \in \mathbb{N}$ y n_1 es el producto de primos congruentes con 1 módulo cuatro; por lo tanto existen dos enteros a y b tales que $n_0 = 2^f n_1 = a^2 + b^2$. Ahora considérense los primos congruentes con tres módulo 4, $n_2 = \prod_{q \equiv 3 \pmod 4} q^{2s} = \left(\prod_{q \equiv 3 \pmod 4} q^s \right)^2$, y sea $m = \prod_{q \equiv 3 \pmod 4} q^s$, entonces $n_2 = m^2$. Por lo tanto se tiene que $n_0 m^2 = m^2(a^2 + b^2) = (am)^2 + (bm)^2 = n$.

Por lo tanto n es la suma de dos cuadrados. □

Nótese que al igual que en el problema de un cuadrado, si un entero n es representable por la suma de dos cuadrados, también se puede ver como suma de cuatro cuadrados ya que si $n = a^2 + b^2$ para algunos enteros a y b, entonces también $n = a^2 + b^2 + 0^2 + 0^2$.

---

[29] Es decir, x_1, y_1 es solución primitiva de la ecuación $x_1^2 + y_1^2 = n_1$.

[30] Ya que $(a^2 + b^2)(c^2 + d^2) = (ac + bd)^2 + (ad - bc)^2 = (ac - bd)^2 + (ad + bc)^2$

Para ilustrar el Teorema 2 se observa que 3 no puede ser representado como la suma de dos cuadrados, pero en el caso de $n = 90$ sí se puede, ya que en su descomposición en primos aparece únicamente un primo congruente con 3 módulo 4, a saber, el 3, y figura con una potencia par, *i.e.*, $90 = 2 \cdot 5 \cdot 3^2 = 9^2 + 3^2$.

Para el problema de los 3 cuadrados se necesitan un par de lemas cuya demostración no se incluye en esta parte, ya que el primero no es más que el inciso 10 que más adelante se probará y el segundo lema es un resultado que ya se utilizó y está demostrado en el inciso 3, a saber, el Lema 1 (Pág. 33)

Lo que se quiere es clasificar a los enteros que pueden ser representados por la suma de tres cuadrados; esta clasificación está dada por los enteros que no son de la forma $N = 4^a(8k + 7)$ y a esto es a lo que se quiere llegar.

Lema 4[31]: Si n es un entero positivo y $n \equiv 2 \pmod 4$, entonces n puede ser representado como la suma de tres cuadrados.

Lema 5[32]: Si n es un entero positivo tal que $n \equiv 1, 3$ ó $5 \pmod 8$, entonces n puede ser representado como la suma de tres cuadrados.

Una vez que se tienen estos dos resultados, ya se puede demostrar el problema de los tres cuadrados, que no es más que demostrar el siguiente Teorema:

Teorema 3[33]: Un entero positivo N puede ser representado como la suma de tres cuadrados si y sólo si N no es de la forma $N = 4^a(8k + 7)$.

Demostración:

Se sabe que un entero x puede ser congruente con 0, 1, 2,...ó 7 módulo ocho, entonces $x^2 \equiv 0, 1$ ó $4 \pmod 8$. De esta manera se sigue que la suma de tres cuadrados nunca puede ser congruente con 7 módulo 8.

Si el entero $4m$ es la suma de tres cuadrados, entonces existen enteros x_1, x_2, x_3 tales que $4m = x_1^2 + x_2^2 + x_3^2$, *i.e.*, $x_1^2 + x_2^2 + x_3^2$ es un múltiplo de cuatro, y entonces los tres x_1, x_2, x_3 tienen que ser números pares,

[31] Este resultado es justamente el inciso 10.
[32] Este Lema es lo que llamamos Lema 1 en el inciso 3.
[33] El resultado se debe a Gauss.

de donde $m=\left(\frac{x_1}{2}\right)^2+\left(\frac{x_2}{2}\right)^2+\left(\frac{x_3}{2}\right)^2$. Por lo tanto $4^a m$ es la suma de tres cuadrados si y sólo si m es la suma de tres cuadrados. Esto demuestra que cualquier entero que no sea de la forma $4^a(8k+7)$ puede ser escrito como la suma de tres cuadrados.

Todo entero positivo N puede ser escrito de manera única en la forma $N=4^a m$, donde $m\equiv 2 \pmod 4$ ó $m\equiv 1, 3, 5$ ó $7 \pmod 8$. Entonces gracias a los Lemas 4 y 5 se tiene que el entero positivo N es la suma de tres cuadrados, excepto cuando $m\equiv 7 \pmod 8$. Por lo tanto si N no es de la forma $4^a(8k+7)$, entonces se puede escribir como suma de tres cuadrados. □

Claramente si un número se puede expresar como la suma de tres cuadrados, supóngase $n=x_1^2+x_2^2+x_3^2$, entonces también se puede ver como la suma de cuatro cuadrados haciendo $n=x_1^2+x_2^2+x_3^2+0^2$.

A continuación se presentará el problema de los cuatro cuadrados.

En la demostración del inciso 3, se introdujo la definición de número figurado. Así, los *números cuadrados* son números poligonales de orden $(m+2)$, por lo tanto, el orden de los números cuadrados es $m+2=4$, es decir, $m=2$ y $p_2(k)=\frac{2k(k-1)}{2}+k=k^2-k+k=k^2$. Una vez que se tiene esta definición ya se puede proceder a la demostración del caso general de este inciso[34].

Un esbozo de la demostración permite apreciar en qué consiste su estrategia.

Se requiere demostrar que cualquier $n\in\mathbb{Z}$ se puede representar como la suma de cuatro cuadrados. Se necesita para ello descomponer a n como producto de primos; con ello el problema se reduce a probar dos cosas: la primera es que todo número primo se puede escribir como la suma de cuatro cuadrados[35]; y la segunda es que el producto de sumas de cuatro cuadrados puede ser expresado nuevamente como suma de cuatro cuadrados[36].

A continuación se presentarán estos resultados con los cuales se responderá el inciso 5.

---

[34] Que se debe a Lagrange, el cual lo demostró en 1770.
[35] Lo cual va a ser consecuencia de lo que llamaremos Lema 7.
[36] Lo cual vamos a llamar Lema 6.

Lema 6 (Euler, 1743): El producto de sumas de cuatro cuadrados puede ser expresado como una suma de cuatro cuadrados.

Demostración:

La demostración de este lema se basa en la siguiente identidad algebraica:

$$\left(a^2+b^2+c^2+d^2\right)\left(e^2+f^2+g^2+h^2\right)=\left(ae+bf+cg+dh\right)^2+\left(af-be+ch-dg\right)^2+$$
$$+\left(ag-bh-ce+df\right)^2+\left(ah+bg-cf-de\right)^2$$

La cual es fácil de comprobar desarrollando ambos lados de la igualdad. □

Lema 7 (Euler, 1751): Si p es un primo impar, entonces existen enteros x y y tales que $1+x^2+y^2\equiv 0 \pmod p$, donde $0\le x,\ y<\frac{p}{2}$.

Demostración:

Considérese el conjunto $A=\left\{0^2,\ 1^2,\ ...,\ \left(\frac{p-1}{2}\right)^2\right\}$. Sean r y s cualesquiera dos elementos distintos de A, y supóngase que $r^2\equiv s^2 \pmod p$. Se demostrará que esto es imposible.

Si $r^2\equiv s^2 \pmod p$, entonces $(r+s)(r-s)\equiv 0 \pmod p$, lo cual indica que $p\mid r+s$ ó $p\mid r-s$; por lo tanto $r\equiv s \pmod p$ ó $r\equiv -s \pmod p$. Como $r\neq s$ y $r,s<p$, entonces $r\not\equiv s \pmod p$. Si $r\equiv -s \pmod p$, entonces $p\mid r+s$, lo cual es imposible, ya que $0<r+s<p$ y p es primo. Por lo tanto, si $r\neq s$, entonces $r\not\equiv s \pmod p$.

Análogamente, si a y b son dos elementos distintos de $B=\left\{-1-0^2,\ -1-1^2,\ ...,\ -1-\left(\frac{p-1}{2}\right)^2\right\}$, entonces no pueden ser congruentes entre sí módulo p. Supóngase que sí, es decir que $a\equiv b \pmod p$, entonces existen $x,\ y\in\mathbb{Z}$ con $0\le x,\ y\le\frac{p-1}{2}$ tales que $-1-x^2\equiv -1-y^2 \pmod p$, lo cual implica que $x^2\equiv y^2 \pmod p$, y repitiendo el proceso que se siguió para los elementos de A resulta que $x\equiv \pm y \pmod p$, lo cual da lugar a una contradicción.

Ahora bien, la cardinalidad del conjunto A es $|A| = \frac{p-1}{2} + 1$ y la de B es $|B| = \frac{p-1}{2} + 1$. De ello se sigue que la cardinalidad del conjunto $A \cup B$ es $|A \cup B| = \frac{p-1}{2} + 1 + \frac{p-1}{2} + 1 = p - 1 + 2 = p + 1$; como $A \cup B$ tiene $(p+1)$ elementos, entonces, por el principio del palomar[37], dos elementos distintos de $A \cup B$ tienen que ser congruentes módulo p. Pero ya se demostró que dos elementos distintos de A no pueden ser congruentes entre sí al igual que dos elementos distintos de B, por lo tanto algún elemento del conjunto A y otro del conjunto B son congruentes módulo p, *i.e.*, como dos elementos de A y dos de B no pueden ser congruentes, y el conjunto $A \cup B$ tiene $(p+1)$ elementos, entonces ya sea que $A \cup B$ constituye un sistema completo de residuos o no, debe de contener dos elementos congruentes entre sí módulo p. Por lo tanto $x^2 \equiv -1 - y^2 \pmod{p}$ para algunos enteros x, y; donde $0 \le x,\ y < \frac{p-1}{2} < \frac{p}{2}$. Por lo tanto $1 + x^2 + y^2 \equiv 0 \pmod{p}$. □

Corolario: Si p es un primo impar, entonces existe un entero positivo $k < p$ tal que kp puede ser expresado como suma de cuatro cuadrados.

Demostración:

Por el Lema 2, como p es un primo impar, entonces existen enteros x, y tales que $1 + x^2 + y^2 \equiv 0 \pmod{p}$, donde $0 \le x,\ y < \frac{p}{2}$, es decir, $p \mid 1 + x^2 + y^2$; entonces existe un entero k tal que $x^2 + y^2 + 1 = kp$, o lo que es lo mismo, $x^2 + y^2 + 1^2 + 0^2 = kp$. Como $0 \le x < \frac{p}{2}$ y $0 \le y < \frac{p}{2}$, entonces $0 \le x^2 < \left(\frac{p}{2}\right)^2$ y $0 \le y^2 < \left(\frac{p}{2}\right)^2$. De esta manera resulta que $x^2 + y^2 + 1 < \left(\frac{p}{2}\right)^2 + \left(\frac{p}{2}\right)^2 + 1 < \frac{p^2}{2} + 1 < p^2$, y $kp < p^2$, *i.e.*, $k < p$.
Por lo tanto kp es la suma de cuatro cuadrados con $k < p$. □

Lema 8: Todo primo se puede escribir como la suma de cuatro cuadrados.

[37] Si se tienen n nidos y en ellos duermen $(n + 1)$ palomas, entonces al menos hay un nido en el cual duerme más de una paloma.

Demostración

Sea p un primo, claramente $2 = 1^2 + 1^2 + 0^2 + 0^2$; entonces el resultado es válido para $p = 2$. Supóngase entonces que p es impar.

Gracias al Corolario del Lema 7, existe $k \in \mathbb{Z}$, con $k < p$, tal que kp es la suma de cuatro cuadrados. Por el principio del buen orden[38] ocurre que existe un entero positivo (mínimo) m tal que:

$$mp = w^2 + x^2 + y^2 + z^2 \ldots\ldots (i)$$

para algunos enteros w, x, y y z, donde $1 \leq m < p$.

Si $m = 1$, entonces $mp = 1 \cdot p = p = w^2 + x^2 + y^2 + z^2$, y por lo tanto p se puede representar por medio de la suma de cuatro cuadrados. Entonces lo que se requiere probar es que $m = 1$.

Primero se demostrará que m es impar; esto se hará por reducción al absurdo. Supóngase que m es par, entonces mp también es par. Así, $w^2 + x^2 + y^2 + z^2$ es par, lo cual implica que w, x, y y z deben de tener la misma paridad o dos a dos tener la misma paridad. Supóngase, sin pérdida de generalidad, que $w \equiv x \pmod 2$ y que $y \equiv z \pmod 2$; de esta manera se tienen las siguientes congruencias:

$$\begin{aligned} w + x &\equiv 2x \equiv 0 \pmod 2 \\ w - x &\equiv 0 \pmod 2 \\ y + z &\equiv 2z \equiv 0 \pmod 2 \\ y - z &\equiv 0 \pmod 2 \end{aligned}$$

Entonces, $\frac{w+x}{2}$, $\frac{w-x}{2}$, $\frac{y+z}{2}$ y $\frac{y-z}{2}$ son enteros, y además, $\left(\frac{w+x}{2}\right)^2 + \left(\frac{w-x}{2}\right)^2 + \left(\frac{y+z}{2}\right)^2 + \left(\frac{y-z}{2}\right)^2 = \frac{w^2 + x^2 + y^2 + z^2}{2} = \left(\frac{m}{2}\right)p$. Entonces $\left(\frac{m}{2}\right)p$ puede ser expresado como suma de cuatro cuadrados y $\frac{m}{2} < m$, y además, como se supuso que m es par resulta que $\frac{m}{2}$ es entero, lo cual contradice la minimalidad de m. Por lo tanto m es impar.

Ahora se mostrará que $m = 1$. Para esto supóngase que $m > 1$ y se llegará a una contradicción. Sean a, b, c y d enteros no negativos tales

[38] Todo subconjunto no vacío de números naturales tiene primer elemento.

que $w \equiv a \pmod{m}$, $x \equiv b \pmod{m}$, $y \equiv c \pmod{m}$ y $z \equiv d \pmod{m}$, donde $-\frac{m}{2} < a,\ b,\ c,\ d < \frac{m}{2}$; entonces $a^2 + b^2 + c^2 + d^2 \equiv w^2 + x^2 + y^2 + z^2 = mp \equiv 0 \pmod{m}$. Esto implica que $m \mid a^2 + b^2 + c^2 + d^2$, y por lo tanto existe un entero positivo n, de tal manera que:

$$mn = a^2 + b^2 + c^2 + d^2 \ldots\ldots\ldots (ii)$$

y además $0 \le a^2 + b^2 + c^2 + d^2 < \frac{m^2}{4} + \frac{m^2}{4} + \frac{m^2}{4} + \frac{m^2}{4} = 4\left(\frac{m}{2}\right)^2 = m^2$, y por ende $0 \le mn < m^2$ y así $0 \le n < m$.

Se afirma que $n \ge 1$, ya que si $n = 0$ entonces $a^2 + b^2 + c^2 + d^2 = 0$, lo cual implica que $a = b = c = d = 0$, y por lo tanto que $w \equiv x \equiv y \equiv z \equiv 0 \pmod{m}$. Esto último conduce a $w^2 \equiv x^2 \equiv y^2 \equiv z^2 \equiv 0 \pmod{m^2}$, y de esta manera se obtiene que $w^2 + x^2 + y^2 + z^2 \equiv 0 \pmod{m^2}$. Por lo tanto $m^2 \mid \left(w^2 + x^2 + y^2 + z^2\right)$, y entonces $m^2 \mid mp$ y de aquí se llega a que $m \mid p$, lo cual es una contradicción, ya que $1 < m < p$ y p es primo. De esta manera, $n \ge 1$ y por lo tanto $1 \le n < m$.

Al multiplicar las ecuaciones (i) y (ii) resulta que

$$\left(w^2 + x^2 + y^2 + z^2\right)\left(a^2 + b^2 + c^2 + d^2\right) = (wa + xb + yc + zd)^2 + (wb - xa + yd - zc)^2 + (wc - xd - ya + zb)^2 + (wd + xc - yb - za)^2$$

es decir:

$$m^2 np = (mp)(mn) = r^2 + s^2 + t^2 + u^2 \ldots (iii)$$

Esta ecuación se puede deducir con ayuda del Lema 1. De esta manera, se obtienen las siguientes igualdades:

$$r = wa + xb + yc + zd$$
$$s = wb - xa + yd - zc$$
$$t = wc - xd - ya + zb$$
$$u = wd + xc - yb - za$$

En virtud de que $w \equiv a \pmod{m}$, $x \equiv b \pmod{m}$, $y \equiv c \pmod{m}$ y $z \equiv d \pmod{m}$, ocurre que $r = wa + xb + yc + zd \equiv w^2 + x^2 + y^2 + z^2 \equiv 0 \pmod{m}$, y por consiguiente $r \equiv 0 \pmod{m}$. De una manera análoga se puede demostrar

que $s \equiv t \equiv u \equiv 0 \pmod{m}$. Por lo tanto $\frac{r}{m}, \frac{s}{m}, \frac{t}{m}, \frac{u}{m} \in \mathbb{Z}$. Entonces la ecuación (*iii*) se replantea de la siguiente manera:

$np = \frac{r^2 + s^2 + t^2 + u^2}{m^2} = \left(\frac{r}{m}\right)^2 + \left(\frac{s}{m}\right)^2 + \left(\frac{t}{m}\right)^2 + \left(\frac{u}{m}\right)^2$ con $n < m$. Esto contradice la manera de seleccionar *m*. Por lo tanto $m = 1$.

De esta forma se tiene que $mp = 1 \cdot p = p = w^2 + x^2 + y^2 + z^2$. Por lo tanto *p* puede ser escrito como la suma de cuatro cuadrados. □

Alcanzada esta etapa queda preparado el camino para demostrar el teorema de Lagrange. A continuación se presenta dicha prueba, misma que parecerá muy simple, pero es debido a los resultados anteriores:

Demostración (del inciso (5): Todo entero es la suma de cuatro cuadrados):

Sea *n* un entero positivo cualquiera. Como $1 = 1^2 + 0^2 + 0^2 + 0^2$, entonces el resultado es verdadero cuando $n = 1$.

Supóngase que $n \geq 2$ y sea $n = \prod p_i^{e_i}$ su descomposición en primos. Aplicando el Lema 8, y debido que cada p_i es un número primo, entonces estos pueden ser escritos como la suma de cuatro cuadrados.

Por lo tanto, y gracias al Lema 6, $p_i^{e_i}$ y consecuentemente $\prod p_i^{e_i} = n$ pueden ser escritos como suma de cuatro cuadrados. □

Inciso 6

Todo entero puede ser expresado como la suma de cantidades de la forma $a^2 - b^2$ y $a^2 - b^2 - 2$, donde $a, b \in \mathbb{Z}$[39].

Demostración:

Como todo número entero es congruente con 0, 1, 2 ó 3 módulo 4, entonces todos los enteros son de la forma $4n$, $4n+1$, $4n+2$ ó $4n+3$ con $n \in \mathbb{Z}$ [40]. Se va a demostrar este inciso haciendo cada caso por separado.

Caso 1. Sea m un entero de la forma $4n$ con $n \in \mathbb{Z}$, entonces se tiene:

$$\begin{aligned} m = 4n &= 2 \cdot 2n + \left(4n^2 - 4n^2\right) + \left(1 - 1\right) \\ &= \left(4n^2 + 2 \cdot 2n + 1\right) - 4n^2 - 1 \\ &= \left(2n+1\right)^2 - 4n^2 - 1 \\ &= \left(2n+1\right)^2 - \left(2n\right)^2 - 1 \\ &= \left(2n+1\right)^2 - \left(2n\right)^2 + \left(1 - 2\right) \\ &= \left(2n+1\right)^2 - \left(2n\right)^2 + \left(1^2 - 0^2 - 2\right) \end{aligned}$$

Por lo tanto m puede ser escrito como la suma de una cantidad de la forma $a^2 - b^2$ y una de la forma $a^2 - b^2 - 2$.

Caso 2. Sea m un entero de la forma $4n+1$ con $n \in \mathbb{Z}$, por el caso 1 se sabe que:

$m = 4n+1 = \left(2n+1\right)^2 - \left(2n\right)^2 + \left(1^2 - 0^2 - 2\right) + 1$, pero $1 = 1^2 - 0^2$. De esta manera se obtiene que:

$$m = \left[\left(2n+1\right)^2 - \left(2n\right)^2\right] + \left[1^2 - 0^2 - 2\right] + \left[1^2 - 0^2\right]$$

Por lo tanto, m puede ser escrito como la suma de dos cantidades de la forma $a^2 - b^2$ y una de la forma $a^2 - b^2 - 2$.

---

[39] Para Waring los enteros a y b en ambas expresiones no necesariamente son iguales, ya que si lo fueran lo que el teorema aseguraría es que todo entero que puede ser expresado por medio de $a^2 - b^2 + a^2 - b^2 - 2$, lo sería de la forma $2a^2 - 2b^2 - 2 = 2\left(a^2 - b^2 - 1\right)$ y claramente no se pueden expresar de esta manera a los números impares ya que la expresión por si misma es un número par.

[40] O dicho de otra forma, se va a representar a todos los números enteros por medio de las clases de equivalencia módulo 4 y de esta manera cada entero pertenece a la clase del cero, del uno, del dos o del tres y solamente a una de estas. De esta manera se puede asegurar que cada entero puede ser representado por $4n$, $4n+1$, $4n+2$ ó $4n+3$ para alguna $n \in \mathbb{Z}$.

Caso 3. Sea m un entero de la forma $4n+2$, pero como $2 \equiv -2 \pmod 4$, entonces se puede ver a m como un entero de la forma $4n-2$ con $n \in \mathbb{Z}$, por el caso 1 se tiene:

$m = 4n-2 = (2n+1)^2 - (2n)^2 + (1^2 - 0^2 - 2) - 2$, pero $-2 = 0^2 - 0^2 - 2$. Entonces:

$$m = \left[(2n+1)^2 - (2n)^2\right] + \left[1^2 - 0^2 - 2\right] + \left[0^2 - 0^2 - 2\right]$$

Por lo tanto, m puede ser escrito como la suma de una cantidad de la forma $a^2 - b^2$ y dos de la forma $a^2 - b^2 - 2$.

Caso 4. Sea m un entero de la forma $4n+3$, pero como $3 \equiv -1 \pmod 4$, entonces m puede ser visto como un entero de la forma $4n-1$ con $n \in \mathbb{Z}$, por el caso 1 se tiene:

$m = 4n-1 = (2n+1)^2 - (2n)^2 + (1^2 - 0^2 - 2) - 1$, pero $-1 = 0^2 - 1^2$. Entonces:

$$m = \left[(2n+1)^2 - (2n)^2\right] + \left[1^2 - 0^2 - 2\right] + \left[0^2 - 1^2\right]$$

Por lo tanto, m puede ser escrito como la suma de dos cantidades de la forma $a^2 - b^2$ y una de la forma $a^2 - b^2 - 2$.

Por lo tanto, cualquier entero m puede ser escrito como la suma de cantidades de la forma $a^2 - b^2$ y $a^2 - b^2 - 2$; donde a y b son enteros. □

Inciso 7

Todo número que sea mayor que cualesquiera números dados p, q, r, s (los cuales se consideran como parámetros y sin divisores comunes) puede ser expresado por la cantidad $pa^2 + qb^2 + rc^2 + sd^2$, donde $a,b,c,d \in \mathbb{Z}$.

La base de la demostración de este inciso al igual que la del inciso 8 son las formas cuadráticas, en el inciso 10 se profundiza sobre las definiciones y la teoría necesaria para comprender mejor este concepto.

Para la demostración de este inciso y del inciso 8 se requiere un teorema que facilitará la prueba, pero antes de enunciar dicho teorema se necesitan un par de definiciones para comprender mejor el resultado auxiliar.

Definición 1: Una *función lineal* f es una función que cumple con lo siguiente:

i) $f(a+b) = f(a) + f(b)\ \forall a,b \in Dom(f)$

ii) $f(ca) = cf(a)\ \forall a \in Dom(f)$ y $\forall c \in \mathbb{R}$

Definición 2: Una función lineal f *es acotada* si y sólo si:
$|f(x)| \leq k\|x\|\ \forall x \in \mathrm{H}$ y para alguna $k \in \mathbb{R}^+$.

Una vez que se tienen estas definiciones, ya se puede enunciar el Teorema que ayudará a demostrar estos incisos. El resultado que se utilizará es un caso particular del Teorema de Lax-Milgram que dice lo siguiente:

Si Φ es una forma cuadrática tal que $\alpha\|x\|^2 \leq \Phi(x,x)$, para algún $\alpha \in \mathbb{R}^+$ y con $x \in \mathrm{H}$. Entonces, para cada funcional lineal acotada f existe un único elemento $y \in \mathrm{H}$ tal que $f(x) = \Phi(x,y)$.

En el Teorema de Lax-Milgram H es un espacio de Hilbert y lo único que se hace en el teorema que se ocupará es hacer a H igual a un $\mathbb{R}^n$ que también es un espacio de Hilbert y con esta suposición las funcionales lineales son funciones lineales.

Teorema auxiliar (Teorema 1): Sea Φ una forma cuadrática tal que $\alpha\|x\|^2 \leq \Phi(x,x)$, para algún $\alpha \in \mathbb{R}^+$ y con $x \in \mathbb{R}^n$ para alguna $n \in \mathbb{N}$. Entonces, para cada función lineal acotada f existe un único elemento $y \in \mathbb{R}^n$ tal que $f(x) = \Phi(x,y)$.

Demostración el inciso 7:

Sea n cualquier entero y considérese la forma cuadrática $\Phi : \mathbb{Z}^4 \times \mathbb{Z}^4 \to \mathbb{Z}$ dada por: $\Phi((x,y,z,w),(x,y,z,w)) = px^2 + qy^2 + rz^2 + sw^2$ con $p, q, r, s \in \mathbb{Z}^+$ y sea $\bar{x} = (x,y,z,w) \in \mathbb{Z}^4$.

$$px^2 + qy^2 + rz^2 + sw^2 \geq \min\{p, q, r, s\}(x^2 + y^2 + z^2 + w^2)$$

$$= \min\{p, q, r, s\}\|\bar{x}\|^2$$

es decir $\alpha\|\bar{x}\|^2 \leq \Phi(\bar{x}, \bar{x})$ con $\alpha = \min\{p, q, r, s\} \in \mathbb{R}^+$.

Entonces, por el Teorema 1 existe un único vector $\bar{a} = (a,b,c,d) \in \mathbb{Z}^4$ tal que para cada función lineal acotada $f : \mathbb{R}^4 \to \mathbb{R}$ se tiene que $f(\bar{x}) = \Phi(\bar{x}, \bar{a})$. En particular para $\bar{x} = \bar{a}$, *i.e.*, $f(\bar{a}) = \Phi(\bar{a}, \bar{a})$.

Sea $f(x,y,z,w) = \frac{nx}{a}$, claramente f es una función lineal acotada ya que $|f(\bar{x})| = \frac{nx}{a} \leq \frac{n}{a}\|\bar{x}\|$, entonces:

$$f(\bar{a}) = \frac{na}{a} = n = \Phi(\bar{a}, \bar{a}) = pa^2 + qb^2 + rc^2 + sd^2.$$

Por lo tanto cualquier entero n puede ser expresado por la cantidad $pa^2 + qb^2 + rc^2 + sd^2$, donde $a,b,c,d \in \mathbb{Z}$. □

Inciso 8

Todo entero puede ser escrito como la siguiente suma: $\left(a^2 \pm ab + b^2\right) + \left(p^2 \pm pq + q^2\right)$ donde $a, b, p, q \in \mathbb{Z}$.

Demostración:

La expresión $\left(a^2 \pm ab + b^2\right) + \left(p^2 \pm pq + q^2\right)$ se dividirá en cuatro casos:

$$\left(a^2 + ab + b^2\right) + \left(p^2 + pq + q^2\right)$$
$$\left(a^2 - ab + b^2\right) + \left(p^2 - pq + q^2\right)$$
$$\left(a^2 + ab + b^2\right) + \left(p^2 - pq + q^2\right)$$
$$\left(a^2 - ab + b^2\right) + \left(p^2 + pq + q^2\right)$$

Sea n cualquier entero, entonces se tiene que:

Caso 1: Se demostrará que todos los enteros pueden ser representados por medio de la expresión $\left(a^2 + ab + b^2\right) + \left(p^2 + pq + q^2\right)$.

Defínase la forma cuadrática $\Phi : \mathbb{Z}^4 \times \mathbb{Z}^4 \to \mathbb{Z}$ como sigue: $\Phi\left((a,b,p,q),(a,b,p,q)\right) = a^2 + ab + b^2 + p^2 + pq + q^2$ y supóngase que $ab \geq 0$, entonces $a^2 + ab + b^2 + p^2 + pq + q^2 \geq a^2 + b^2 + p^2 + q^2 = \left\|\bar{a}\right\|^2$ donde $\bar{a} = (a,b,p,q)$. Entonces se tiene que $\alpha\left\|\bar{a}\right\|^2 \leq \Phi\left(\bar{a}, \bar{a}\right)$ con $\alpha = 1$. Así mismo, sea $f : \mathbb{R}^4 \to \mathbb{R}$ definida mediante $f(x,y,z,w) = \frac{nx}{a}$, como ya se vio en el inciso anterior (inciso 7), f es una función lineal acotada, entonces por el Teorema 1 existe un único vector $\bar{y} = (y_1, y_2, y_3, y_4) \in \mathbb{R}^4$ de tal manera que $f\left(\bar{a}\right) = \Phi\left(\bar{a}, \bar{y}\right)$, en particular sea $\bar{a} = \bar{y}$, entonces:

$$f\left(\bar{a}\right) = \frac{na}{a} = n = \Phi\left(\bar{a}, \bar{a}\right) = a^2 + ab + b^2 + p^2 + pq + q^2$$

Por lo tanto todo entero n puede ser expresado por $\left(a^2 + ab + b^2\right) + \left(p^2 + pq + q^2\right)$.

Caso 2: Se demostrará que todos los enteros pueden ser representados por medio de la expresión $\left(a^2 - ab + b^2\right) + \left(p^2 - pq + q^2\right)$.

Defínase la forma cuadrática $\Phi : \mathbb{Z}^4 \times \mathbb{Z}^4 \to \mathbb{Z}$ como sigue:
$\Phi\left((a,b,p,q),(a,b,p,q)\right) = a^2 - ab + b^2 + p^2 - pq + q^2$.

Claramente[41] $-ab \geq -\frac{a^2+b^2}{2}$, entonces $a^2 + b^2 - ab \geq a^2 + b^2 - \frac{a^2+b^2}{2}$ y por lo tanto $a^2 + b^2 - ab \geq \frac{a^2+b^2}{2}$. De manera análoga se prueba que $p^2 + q^2 - pq \geq \frac{p^2+q^2}{2}$.

Entonces $a^2 - ab + b^2 + p^2 - pq + q^2 \geq \frac{a^2+b^2+p^2+q^2}{2} = \frac{1}{2}\left(\left\|a\right\|^2\right)$. Por lo tanto se tiene que $\alpha\left\|a\right\|^2 \leq \Phi\left(\bar{a}, \bar{a}\right)$ con $\alpha = \frac{1}{2}$ y $\bar{a} = (a,b,p,q)$.

Entonces, por el Teorema 1, para cada función lineal acotada f existe un único vector $\bar{a} \in \mathbb{R}^4$ tal que $f\left(\bar{x}\right) = \Phi\left(\bar{x}, \bar{a}\right)$ con $\bar{x} = (x,y,z,w)$ en particular se cumple para la función lineal acotada $f : \mathbb{R}^4 \to \mathbb{R}$ definida mediante $f(x,y,z,w) = \frac{nx}{a}$ y para $\bar{a} = \bar{x}$, así se obtiene:

$$f\left(\bar{a}\right) = \frac{na}{a} = n = \Phi\left(\bar{a}, \bar{a}\right) = a^2 + b^2 - ab + p^2 + q^2 - pq$$

Por lo tanto todo entero n puede ser expresado por $\left(a^2 - ab + b^2\right) + \left(p^2 - pq + q^2\right)$.

Caso 3: Se demostrará que todos los enteros pueden ser representados por medio de la expresión $\left(a^2 + ab + b^2\right) + \left(p^2 - pq + q^2\right)$.

Defínase la forma cuadrática $\Phi : \mathbb{Z}^4 \times \mathbb{Z}^4 \to \mathbb{Z}$ como sigue:
$\Phi\left((a,b,p,q),(a,b,p,q)\right) = a^2 + b^2 + ab + p^2 + q^2 - pq$.

Como se vio en el caso anterior $p^2 + q^2 - pq \geq \frac{p^2+q^2}{2}$, además se sabe que si $ab \geq 0$, entonces $a^2 + b^2 + ab \geq a^2 + b^2$. Sumando las dos des-

[41] Se sabe que $(r-s)^2 \geq 0$, entonces $0 \leq r^2 + s^2 - 2rs$ lo cual implica que $2rs \leq r^2 + s^2$ y por lo tanto $rs \leq \frac{r^2+s^2}{2}$ $\forall r, s \in \mathbb{R}$

igualdades anteriores resulta que $\Phi\left(\bar{a},\bar{a}\right)\geq\frac{p^2+q^2}{2}+a^2+b^2\geq\frac{a^2+b^2+p^2+q^2}{2}=\frac{1}{2}\left(\left\|\bar{a}\right\|^2\right)$, es decir, $\alpha\left\|\bar{a}\right\|^2\leq\Phi\left(\bar{a},\bar{a}\right)$ con $\alpha=\frac{1}{2}$ y $\bar{a}=\left(a,b,p,q\right)$.

Entonces, por el Teorema 1 (visto en el inciso 7), para cada función lineal acotada f existe un único vector $\bar{a}\in\mathbb{R}^4$ tal que $f\left(\bar{x}\right)=\Phi\left(\bar{x},\bar{a}\right)$ con $\bar{x}=\left(x,y,z,w\right)$ en particular se cumple para la funcional lineal acotada $f:\mathbb{R}^4\rightarrow\mathbb{R}$ definida mediante $f\left(x,y,z,w\right)=\frac{nx}{a}$ y para $\bar{a}=\bar{x}$, de esta manera se obtiene:

$$f\left(\bar{a}\right)=\frac{na}{a}=n=\Phi\left(\bar{a},\bar{a}\right)=a^2+b^2+ab+p^2+q^2-pq$$

Por lo tanto todo entero n puede ser expresado por $\left(a^2+ab+b^2\right)+\left(p^2-pq+q^2\right)$.

Caso 4: Haciendo un procedimiento análogo al de la demostración del caso 3 se tiene que todo entero n puede ser expresado por $\left(a^2-ab+b^2\right)+\left(p^2+pq+q^2\right)$.

Por lo tanto, cualquiera que sea el caso, todo entero puede ser escrito como la siguiente suma: $\left(a^2\pm ab+b^2\right)+\left(p^2\pm pq+q^2\right)$ donde $a,b,p,q\in\mathbb{Z}$. Lo cual demuestra el inciso 8. □

Inciso 9

Todo entero es un cubo o la suma de dos, tres, cuatro,..., nueve cubos; todo entero también es una cuarta potencia o suma de a lo más 19 cuartas potencias. Leyes similares pueden ser afirmadas para cualquier potencia.

Cuando se enunció el Teorema 47, se dio una pequeña reseña histórica sobre este resultado, cabe recordar que en la mayoría de los textos se refieren al inciso 9 como "Los problemas de Waring".

La demostración de este inciso se hará en tres partes:

Se demostrará el caso $k=3$, es decir, se probará que todo número entero puede ser representado como la suma de 9 cubos, o en nuestra notación, se probará que $g(3)=9$.

Se hará un bosquejo de la demostración del Teorema de Hilbert-Waring, el cual es el caso general de este inciso.

Se dará una serie de tablas en las cuales se puede observar el avance de esta conjetura y el estado actual de la misma para valores específicos de *k*, a saber, para $k=3,\ldots,10$.

A continuación se demostrará con detalle que todo entero es la suma de a lo más 9 cubos, *i.e.*, $g(3)=9$, esta demostración se le debe a Wieferich y Kempner. Antes de entrar a los detalles, para que el lector entienda de una mejor manera esta prueba, se dará una reseña de la demostración:

Lo que se quiere demostrar es que todo entero *N* puede ser escrito como la suma de nueve cubos no negativos. Nathanson [1996] presenta un resultado en el cual se caracterizan los enteros que pueden ser representados como suma de 9, 8, 7 ó 6 cubos no negativos[42]. Gracias a esta proposición, todo entero menor que 40,000 es la suma de 9 cubos no negativos, entonces nuestro problema se reduce a demostrar que todo entero mayor que esta cota, también es representable como la suma de 9 cubos no negativos. Después se construye un entero de la forma $N-a^3$ y se ve, gracias a lo que se llamará Lema 2, que este entero es congruente con un cubo impar módulo una potencia de 8. Después se hacen una serie de sustituciones en la cual se requiere de otro resultado[43], el cual afirma que para todo entero *r* mayor que 22^3, existen un par de números *d* y *m* tales que $0\le d\le 22$ y *m* se puede

[42] El cual llamaremos Lema 4.
[43] Que llamaremos Lema 3.

escribir como suma de 3 cuadrados, de tal manera que $r = d^3 + 6m$. Finalmente se llega a una expresión de la forma $N = a^3 + b^3 + c^3 + 6A\left(A^2 + m\right)$, entonces lo que haría falta para que N fuera suma de 9 cubos no negativos es que la expresión $6A\left(A^2 + m\right)$ fuera suma de 6 cubos no negativos, pero este resultado es justamente lo que será el Lema 1.

Una vez que se ha aclarado un poco el panorama de la demostración, se entrará a la parte técnica de dicha prueba.

Lema 1: Sean A y m enteros no negativos tales que $m \leq A^2$ y m puede ser escrito como la suma de tres cuadrados, entonces $6A\left(A^2 + m\right)$ es la suma de seis cubos no negativos.

Demostración:

Sean m_1, m_2 y m_3 enteros no negativos tales que $m = m_1^2 + m_2^2 + m_3^2$, entonces, se tiene que $6A\left(A^2 + m\right) = 6A\left(A^2 + m_1^2 + m_2^2 + m_3^2\right)$. Se afirma que: $6A\left(A^2 + m_1^2 + m_2^2 + m_3^2\right) = \sum_{i=1}^{3}\left(\left(A + m_i\right)^3 + \left(A - m_i\right)^3\right)$. Para probar esta afirmación, se desarrolla cada término y se compara el resultado:

Para cada $i = 1, 2, 3$, se tiene que:
$\left(A + m_i\right)^3 = A^3 + 3A^2 m_i + 3Am_i^2 + m_i^3$ y también
$\left(A - m_i\right)^3 = A^3 - 3A^2 m_i + 3Am_i^2 - m_i^3$, entonces
$\left(A + m_i\right)^3 + \left(A - m_i\right)^3 = 2A^3 + 6Am_i^2$, pero como es para cada $i \in \{1, 2, 3\}$, entonces:

$$\begin{aligned}\sum_{i=1}^{3}\left(\left(A + m_i\right)^3 + \left(A - m_i\right)^3\right) &= 2A^3 + 6Am_1^2 + 2A^3 + 6Am_2^2 + 2A^3 + 6Am_3^2 \\ &= 6A^3 + 6Am_1^2 + 6Am_2^2 + 6Am_3^2 \\ &= 6A\left(A^2 + m_1^2 + m_2^2 + m_3^2\right) \\ &= 6A\left(A^2 + m\right)\end{aligned}$$

Por lo tanto se tiene que $6A\left(A^2 + m\right)$ es la suma de seis cubos. Lo único que falta probar es que estos cubos no son negativos. Así, los cubos que conforman la expresión de $6A\left(A^2 + m\right)$ son de la forma

$(A+m_i)$ y $(A-m_i)$, entonces lo que se debe mostrar es que $A+m_i \geq 0$ y $A-m_i \geq 0$ para cada $i=1, 2, 3$:

Sea $i \in \{1, 2, 3\}$ arbitraria, entonces $m_i \geq 0$ ya que m_i son los números que al elevarlos al cuadrado conforman a m, el cual es un entero no negativo. Como $m = m_1^2 + m_2^2 + m_3^2$ y $m_i \geq 0$, entonces $m_i^2 \leq m$ y por lo tanto $m_i \leq \sqrt{m}$. Por hipótesis se sabe que $m \leq A^2$, entonces $\sqrt{m} \leq A$. De esta manera se llega a la siguiente cadena de desigualdades: $0 \leq m_i \leq \sqrt{m} \leq A$. Como $m_i \leq A$, entonces $A - m_i \geq 0$ y también, $0 \leq m_i \leq 2m_i \leq A + m_i$, lo cual implica que $A + m_i \geq 0$.

Por lo tanto $6A\left(A^2 + m\right)$ es la suma de seis cubos no negativos. □

Lema 2: Sea $t \geq 1$. Para todo entero impar w, existe un entero impar b tal que $w \equiv b^3 \pmod{2^t}$.

Demostración[44]:

Tómese un sistema completo de residuos módulo 2^t, $A = \{0, 1, 2, ..., 2^t - 1\}$. Ahora, divídase este conjunto A en dos, A_1 y A_2, donde los elementos de A_1 son los números pares del conjunto A y los elementos de A_2 los impares, *i.e.*, $A_1 = \{0, 2, ..., (2^t - 2)\} = \{0\} \cup \{2^k \ / \ k = 1, ..., t-1\}$ y $A_2 = \{1, 3, ..., 2^t - 1\}$. Por lo tanto $A = A_1 \cup A_2$.

Sea n un número impar arbitrario, entonces $n^3 \not\equiv a \pmod{2^t} \ \forall a \in A_1$ ya que a es un número par y al ser n impar resulta que n^3 también es impar y no es posible que un número impar sea congruente con un número par módulo un número par (2^t es par para todo $t \geq 1$). Como A es un sistema completo de residuos, entonces existe $m \in A_2$ tal que $n^3 \equiv m \pmod{2^t}$, esto quiere decir que todo número impar es congruente con un cubo impar módulo 2^t.

[44] La demostración que presenta Nathanson [1996] no es del todo clara, por lo tanto, la prueba que se presenta es original.

Ahora bien, si b_1 y b_2 son enteros impares de diferentes clases residuales tales que $b_1^3 \equiv b_2^3 \pmod{2^t}$, entonces 2^t divide a $b_2^3 - b_1^3 = (b_2 - b_1)(b_2^2 + b_2 b_1 + b_1^2)$. Como $b_2^2 + b_2 b_1 + b_1^2$ es impar, se sigue que 2^t divide a $b_2 - b_1$, es decir, $b_1 \equiv b_2 \pmod{2^t}$. Pero, si b_1 y b_2 son enteros impares tales que $0 < b_1 < b_2 < 2^t$, entonces $b_2 - b_1 < 2^t$ y ya se vio que $2^t \mid b_2 - b_1$ lo cual es imposible, por lo tanto $b_1^3 \not\equiv b_2^3 \pmod{2^t}$.

Resumiendo, todo número impar es congruente con un cubo impar módulo 2^t y cualesquiera dos cubos de impares caen en diferentes clases de equivalencia. Por lo tanto se puede sustituir al conjunto A_2 por $A_2' = \left\{1^3, 3^3, ..., (2^t - 1)^3\right\}$.

Si w es un entero impar, entonces existe $b' \in A_2'$ tal que $w \equiv b' \pmod{2^t}$, pero como $b' \in A_2'$, entonces $b' = b^3$ para algún entero impar b. Por lo tanto, para todo entero impar w, existe un entero impar b tal que $w \equiv b^3 \pmod{2^t}$. □

Lema 3: Si $r \geq 10648 = 22^3$, entonces existe un entero $d \in [0,22]$ y un entero m que es la suma de tres cuadrados tal que $r = d^3 + 6m$.

Demostración:

Se analizará qué sucede si se supone que el entero no negativo m NO es la suma de tres cuadrados, para de esa manera poder construir el entero $d^3 + 6m$ y poder demostrar que es igual al entero r.

Si m NO es la suma de tres cuadrados, entonces[45] existen enteros no negativos s y t tales que $m = 4^s(8t + 7)$. Entonces $6m = 6 \cdot 4^s(8t + 7)$. Ahora se observarán cuáles son los posibles residuos de $6m$ módulo 96:

Si $s \geq 2$, entonces :
$6 \cdot 4^s(8t + 7) = 6 \cdot 4^2(8t + 7)(4^{s-2}) = 96(8t + 7)(4^{s-2}) \equiv 0 \pmod{96}$.

[45] Gracias al Teorema 3 del inciso 5 (página 56).

Si $s=1$, entonces:
$6\cdot 4^s(8t+7)=6\cdot 4(8t+7)=96(2t)+168\equiv 168\equiv 72\pmod{96}$.
Si $s=0$ y t es un número par (supóngase $t=2k$; $k\in\mathbb{Z}$), entonces:
$6\cdot 4^s(8t+7)=6(8(2k)+7)=96k+42\equiv 42\pmod{96}$.
Si $s=0$ y t es un número impar ($t=2k+1$; $k\in\mathbb{Z}$), entonces:
$6\cdot 4^s(8t+7)=6(8(2k+1)+7)=96k+90\equiv 90\pmod{96}$.

Resumiendo, se tiene que:

$$6m\equiv\begin{cases}0 \pmod{96} \text{ si } s\geq 2\\ 72 \pmod{96} \text{ si } s=1\\ 42 \pmod{96} \text{ si } s=0 \text{ y } t \text{ es par}\\ 90 \pmod{96} \text{ si } s=0 \text{ y } t \text{ es impar}\end{cases}$$

Ahora bien, considérese la congruencia $6m\equiv h\pmod{96}$, claramente, h sólo puede ser múltiplo de 6 módulo 96, es decir, h puede tomar valores en el conjunto $\{0,6,12,18,24,30,36,42,48,54,60,66,72,78,84,90\}$, pero como ya se vio anteriormente, si se quiere que m sea suma de tres cuadrados, entonces h no puede ser 0, 42, 78 ni 90. Por lo tanto $h\in H=\{6,12,18,24,30,36,48,54,60,66,78,84\}$.

A continuación se presenta una tabla (denotada como Tabla 1) en la cual se construyen los enteros d^3+h módulo 96 con $h\in H$ y $d\in[0,22]$ en la cual se demuestra que estos enteros forman un sistema completo de residuos módulo 96. No es necesario considerar todo el intervalo $[0,22]$ ya que $12^3\equiv 0^3, 16^3\equiv 4^3$ y $20^3\equiv 8^3\pmod{96}$ y además cuando se consideran $d=19$ y $d=21$, los valores de d^3+h se repiten en los renglones anteriores. De esta manera se puede suponer que $d\in D=\{0,1,2,3,4,5,6,7,8,9,10,11,13,14,15,17,18,22\}$.

	6	12	18	24	30	36	48	54	60	66	78	84
0	6	12	18	24	30	36	48	54	60	66	78	84
1	7	13	19	25	31	37	49	55	61	67	79	85
2	14	20	26	32	38	44	56	62	68	74	86	92
3	33	39	45	51	57	63	75	81	87	93	9	15
4	70	76	82	88	94	4	16	22	28	34	46	52
5	35	41	47	53	59	65	77	83	89	95	11	17
6	42	72	90									
7	73	91	43									
8	50	80	2									
9	69	21	27									
10	58	64	10									
11	5	23	71									
13	1											
14	8											
15	3											
17	29											
18	0											
22	40											

Tabla 1[46]

De esta manera, se muestra que los números de la forma $d^3 + h$ con $h \in H$ y $d \in D$ son un sistema completo de residuos módulo 96.

Para cada $d \in D$ es claro que $0 \le d \le 22$. Entonces, si $r \ge 22^3$ se sigue que existe un entero $d \in D$ no negativo tal que $r - d^3 \equiv h \pmod{96}$ para alguna $h \in H$. Por lo tanto, $r - d^3 = 6m$, donde m es la suma de tres cuadrados. □

Lema 4: Si $1 \le N \le 40,000$, entonces:
(*i*) N es la suma de nueve cubos no negativos.
(*ii*) Si $N \ne 23$ ó 239, entonces N es la suma de ocho cubos no negativos.
(*iii*) Si $N \ne 23$ ó 239, y si N no es ninguno de los siguientes 15 números:

15	22	50	114	167
175	186	212	231	238
303	364	420	428	454

Entonces, N es la suma de siete cubos no negativos.

[46] Los elementos de H están listados en el primer renglón y los elementos de D en la primer columna. Los renglones que no están completos es porque los demás valores se repiten en renglones anteriores y en esta tabla sólo se consideran números distintos

(*iv*) Si $N > 8042$, entonces N es la suma de seis cubos no negativos.

Demostración:

La demostración de este lema es cien por ciento técnica, todos los resultados se siguen de cálculos hechos por computadoras. □

Una vez que se tienen estos cuatro lemas y el bosquejo inicial de la demostración del Teorema de Wieferich-Kempner, se pasará de inmediato a la demostración de dicho resultado.

Teorema (Wieferich-Kempner): Todo entero no negativo es la suma de nueve cubos no negativos, *i.e.*, $g(3) = 9$.

Demostración:

Gracias al Lema 4, se sabe que todo entero N tal que $1 \leq N \leq 40,000$ es la suma de 9 cubos no negativos, entonces lo que se tiene que probar es que el resultado es válido para enteros $N > 40,000$. Para esto, la prueba se dividirá en dos casos:

1. $N > 8^{10}$
2. $40,000 < N \leq 8^{10}$

Para el primer caso considérese el entero $n = \left[N^{1/3}\right]$, claramente, como $N > 8^{10}$ por hipótesis, entonces $N^{1/3} > \sqrt[3]{8^{10}} = 2^{10}$. Tomando parte entera de ambos lados se tiene que $\left[2^{10}\right] = 2^{10} < \left[N^{1/3}\right] = n$, por lo tanto $2^{10} < n$. Como el valor más pequeño que puede tomar N es $8^{10} + 1 = 1,073,741,825$, cuya raíz cúbica es $N^{1/3} = n = 1,024 = 2 \cdot 8^3$, entonces para toda $k \geq 2$ se tiene que $n \leq 2 \cdot 8^{k+1}$. Por lo tanto

$$2^{10} \leq n \leq 2 \cdot 8^{k+1} \ldots\ldots\ldots\ldots (1)$$

De la misma manera se afirma que existe un entero $k \geq 3$ de tal manera que $8 \cdot 8^{3k} < N \leq 8 \cdot 8^{3(k+1)}$.

Sea $N_i = N - i^3$, para $i = 1,\ldots,n$, y defínase $d_i \doteq N_{i-1} - N_i$, entonces:

$$d_i = N - (i-1)^3 - N + i^3 = i^3 - (i-1)^3 = i^3 - \left(i^3 - 3i^2 + 3i - 1\right) = 3i^2 - 3i + 1$$

Se sabe que $3i^2 - 3i + 1 < 3i^2 \Leftrightarrow -3i + 1 < 0 \Leftrightarrow 3i > 1$, pero por hipótesis, $i > 1$, entonces $3i > 3 > 1$. Lo cual implica que $3i > 1$. Por lo tanto $d_i = 3i^2 - 3i + 1 < 3i^2$.

Ahora, $3i^2 \leq 3N^{2/3} \Leftrightarrow i^2 \leq N^{2/3} \Leftrightarrow i \leq N^{1/3}$, pero se sabe que i es a lo más $n = \left[N^{1/3} \right]$, entonces, i es a lo más $N^{1/3}$, *i.e.*, $i \leq N^{1/3}$. Por lo tanto se tiene que $d_i = 3i^2 - 3i + 1 < 3i^2 \leq 3N^{2/3}$.

Finalmente se tiene la siguiente cadena de dobles implicaciones:

$$3N^{2/3} \leq \frac{3 \cdot 8^{2k+3}}{2} \Leftrightarrow 2N^{2/3} \leq 8^{2k+3} \Leftrightarrow 2N^{2/3} \leq 2^{2k+3} \cdot 4^{2k+3} \Leftrightarrow N^{2/3} \leq 2^{2k+3-1} \cdot 4^{2k+3}$$

$$\Leftrightarrow N^{2/3} \leq 2^{2k+2} \cdot 4^{2k+3} \Leftrightarrow N^{2/3} \leq 2^{2(k+1)} \cdot 4^{2k+3} \Leftrightarrow N^{2/3} \leq \left(2^{k+1}\right)^2 \cdot \left(2^{2k+3}\right)^2 \Leftrightarrow$$

$$\Leftrightarrow N^{1/3} \leq 2^{k+1} \cdot 2^{2k+3} \Leftrightarrow N^{1/3} \leq 2^{3k+4} \Leftrightarrow N^{1/3} \leq 2^{3k} \cdot 2^4 \Leftrightarrow N^{1/3} \leq 8^k (2 \cdot 8) \Leftrightarrow$$

$$\Leftrightarrow N^{1/3} \leq 2.8^{k+1} \Leftrightarrow \left[N^{1/3} \right] \leq \left[2.8^{k+1} \right] \Leftrightarrow n \leq 2 \cdot 8^{k+1}$$

Pero gracias a la desigualdad (1) se sabe que $n \leq 2 \cdot 8^{k+1}$. Por lo tanto:

$$d_i = 3i^2 - 3i + 1 < 3i^2 \leq 3N^{2/3} \leq \frac{3 \cdot 8^{2k+3}}{2}.$$

Ahora, escójase $i \in \{1, 2, ..., n\}$ de tal manera que

$$N_{i+1} \leq 8 \cdot 8^{3k} \leq N_i \text{ ..... (2).}$$

Claramente $i \geq 1$, ahora tómese $k \geq 3$, entonces se tienen las siguientes afirmaciones:

Por la definición de N_i se tiene que $N_n = N - n^3$ y también:

$$N - n^3 \leq (n+1)^3 - n^3 - 1 \Leftrightarrow N \leq (n+1)^3 - 1 \Leftrightarrow N \leq n^3 + 3n^2 + 3n + 1 - 1 \Leftrightarrow$$

$$\Leftrightarrow N \leq \left[N^{1/3} \right]^3 + 3\left[N^{1/3} \right]^2 + 3\left[N^{1/3} \right] \Leftrightarrow N \leq N + 3n^2 + 3n \Leftrightarrow 3n^2 + 3n \geq 0$$

Pero $3n^2 + 3n \geq 0$. Por lo tanto $N_n = N - n^3 \leq (n+1)^3 - n^3 - 1$.

Ahora bien, $(n+1)^3 - n^3 - 1 = n^3 + 3n^2 + 3n + 1 - n^3 - 1 = 3n^2 + 3n$, de esta manera se tiene que $N_n = N - n^3 \leq 3n^2 + 3n$.

Se observa que $3n^2 + 3n < 6n^2 \Leftrightarrow 3n < 3n^2 \Leftrightarrow n < n^2$, pero $n = \left[N^{1/3} \right] > 1$, por lo tanto $n < n^2$. De esto se sigue que $N_n = N - n^3 \leq 3n^2 + 3n < 6n^2$.

Por la desigualdad (1) se sabe que $n \leq 2 \cdot 8^{k+1}$, elevando al cuadrado de ambos lados se tiene $n^2 \leq 2^2 \cdot 8^{2(k+1)}$ y multiplicando por 6 de ambos lados, $6n^2 \leq 24 \cdot 8^{2k+2}$. Por lo tanto $6n^2 \leq 3 \cdot 8^{2k+3}$. De esta manera se tiene que $N_n = N - n^3 \leq 3n^2 + 3n < 6n^2 \leq 3 \cdot 8^{2k+3}$.

Finalmente, $3 \cdot 8^{2k+3} \leq 8 \cdot 8^{3k} \Leftrightarrow 3 \cdot 8^{2k} \cdot 8^3 \leq 8 \cdot 8^{3k} \Leftrightarrow 3 \cdot 8^3 \leq 8 \cdot 8^k \Leftrightarrow 3 \leq 8^{k-2}$, pero por hipótesis se tiene que $k \geq 3$, lo cual implica que $k - 2 \geq 1$ y por lo tanto $3 \leq 8^{k-2}$. Por lo tanto $N_n = N - n^3 \leq 3n^2 + 3n < 6n^2 \leq 3 \cdot 8^{2k+3} \leq 8 \cdot 8^{3k}$.

Se afirma que $i \leq n-1$, ya que si no sucediera, entonces, como $i \leq n$ e i NO es menor o igual que $n-1$, entonces $i = n$. Ahora, gracias a la desigualdad anterior se sabe que $N_n \leq 8 \cdot 8^{3k}$ y por la desigualdad (2) se tiene $8 \cdot 8^{3k} \leq N_n$. Por lo tanto $N_n = 8 \cdot 8^{3k}$. Así, se tiene que $N - n^3 = 8 \cdot 8^{3k}$, es decir, $8 \cdot 8^{3k} = 0$ lo cual es una contradicción. Por lo tanto $i \leq n-1$.

Se sabe, gracias a la siguiente cadena de doble implicaciones que:
$N_i < N_{i-1} \Leftrightarrow N - i^3 < N - (i-1)^3 \Leftrightarrow -i^3 < -i^3 + 3i^2 - 3i + 1 \Leftrightarrow 3i^2 - 3i + 1 > 0 \Leftrightarrow$
$\Leftrightarrow 3(i-1) + 1 > 0$
pero $i > 1$. Por lo tanto $N_i < N_{i-1}$.

Ahora bien, $N_{i-1} = (N_{i-1} + N_i) + (N_i - N_{i+1}) + N_{i+1} = d_i + d_{i+1} + N_{i+1}$.
Como ya se sabe, $d_i < \frac{3 \cdot 8^{2k+3}}{2} \; \forall i$ y también, como $i \leq n-1$, entonces $i+1 \leq n$; por lo tanto, haciendo $i+1 = n$, se tiene que $N_n \leq 8 \cdot 8^{3k}$. Por lo tanto:
$d_i + d_{i+1} + N_{i+1} < \frac{3 \cdot 8^{2k+3}}{2} + \frac{3 \cdot 8^{2k+3}}{2} + 8 \cdot 8^{3k} = 3 \cdot 8^{2k+3} + 8 \cdot 8^{3k}$ y de esta manera se obtiene $N_{i-1} < 3 \cdot 8^{2k+3} + 8 \cdot 8^{3k}$.

Finalmente se tiene que:
$3 \cdot 8^{2k+3} + 8 \cdot 8^{3k} \leq 11 \cdot 8^{3k} \Leftrightarrow 8^{3k}\left(3 \cdot 8^{2k+3-3k} + 8\right) \leq 11 \cdot 8^{3k} \Leftrightarrow 3 \cdot 8^{3-k} + 8 \leq 11 \Leftrightarrow$
$\Leftrightarrow 3 \cdot 8^{3-k} \leq 3 \Leftrightarrow 8^{3-k} \leq 1$
pero por hipótesis $k \geq 3$, entonces $0 \geq 3 - k$. Por lo tanto $8^{3-k} \leq 1$. De esta manera se tiene que:

$$N_{i-1} < 3 \cdot 8^{2k+3} + 8 \cdot 8^{3k} \leq 11 \cdot 8^{3k} \ldots (3)$$

Ahora considérese $d_i = N_{i-1} - N_i$, claramente d_i es impar ya que:

$$\begin{aligned} N_{i-1} - N_i &= N - (i-1)^3 - N + i^3 \\ &= -i^3 + 3i^2 - 3i + 1 + i^3 \\ &= 3i^2 - 3i + 1 \end{aligned}$$

Entonces:

1.- Si i es un número par entonces i^2, $3i^2$ y $3i$ son pares, entonces $3i^2 - 3i$ es par y $3i^2 - 3i + 1$ es impar. Por lo tanto d_i es impar.

2.- Si i es un número impar, entonces i^2, $3i^2$ y $3i$ son impares, entonces $3i^2 - 3i$ es par y $3i^2 - 3i + 1$ es impar. Por lo tanto d_i es impar.

Por lo tanto, exactamente N_{i-1} ó N_i es impar. Escójase $a \in \{i-1, i\}$ de tal manera que $N_a = N - a^3$ sea un número impar. Por el Lema 2 se sabe que existe un entero impar $b \in [1, 8^k - 1]$ tal que $N - a^3 \equiv b^3 \pmod{8^k}$. Entonces se tiene que $7 \cdot 8^{3k} = 8 \cdot 8^{3k} - 8^{3k} < N - a^3 - b^3$. Como $b^3 > 0$, entonces $N - a^3 - b^3 < N - a^3 = N_a$ y por la desigualdad (3) se tiene $N_a < 11 \cdot 8^{3k}$. Por lo tanto:

$$7 \cdot 8^{3k} < N - a^3 - b^3 < N_a < 11 \cdot 8^{3k} \ldots (4)$$

Como $N - a^3 \equiv b^3 \pmod{8^k}$, entonces existe $q \in \mathbb{Z}$ de tal manera que $N - a^3 - b^3 = 8^k \cdot q$. Por la desigualdad (4) se sabe que $8 \cdot 8^{3k} - 8^{3k} < N - a^3 - b^3$, entonces factorizando 8^k del lado izquierdo de la desigualdad se tiene que $8^k (8 \cdot 8^{2k} - 8^{2k}) < 8^k \cdot q$, si se elimina de ambos lados 8^k se tiene $8 \cdot 8^{2k} - 8^{2k} < q$. Por lo tanto $7 \cdot 8^{2k} < q$. Nuevamente, por (4) se tiene $N - a^3 - b^3 < 11 \cdot 8^{3k}$, entonces $8^k \cdot q < 11 \cdot 8^{3k}$. Por lo tanto $q < 11 \cdot 8^{2k}$. Así, se tiene la siguiente desigualdad:

$$7 \cdot 8^{2k} < q < 11 \cdot 8^{2k} \ldots (5)$$

Sea $r = q - 6 \cdot 8^{2k}$, entonces es claro que $22^3 < 8^6$; como $k \geq 3$ entonces se tiene $8^6 \leq 8^{2k}$. Ahora bien, gracias a la desigualdad (5) se tiene que $7 \cdot 8^{2k} < q$, entonces $8^{2k} < q - 6 \cdot 8^{2k}$. Por lo tanto $8^{2k} < r$; de

igual manera, por la desigualdad (5) se tiene que $q < 11 \cdot 8^{2k}$, entonces $q - 6 \cdot 8^{2k} < 5 \cdot 8^{2k}$. Por lo tanto $r < 5 \cdot 8^{2k}$. De esta manera se tiene que:

$$22^3 < 8^6 \leq 8^{2k} < r < 5 \cdot 8^{2k} \ldots (6)$$

Como $r > 22^3$ entonces, gracias al Lema 3, r puede ser escrito como $r = d^3 + 6m$; donde $0 \leq d \leq 22$ y m es la suma de tres cuadrados.

Sea $A = 8^k$, entonces, como $r = d^3 + 6m$ y $d^3 > 0$ se sigue que $6m \leq r$, por lo tanto $m \leq \frac{r}{6}$. También, gracias a la desigualdad (6) se sabe que $r < 5 \cdot 8^{2k}$. Por lo tanto $\frac{r}{6} < \frac{5 \cdot 8^{2k}}{6}$. Por último, como $\frac{5}{6} < 1$, entonces $\frac{5 \cdot 8^{2k}}{6} < 8^{2k}$. Por lo tanto $\frac{5 \cdot 8^{2k}}{6} < A^2$. Así, se obtiene:

$$m \leq \frac{r}{6} < \frac{5 \cdot 8^{2k}}{6} < A^2 \ldots (7)$$

Con todos estos datos y haciendo $c = 2^k d$ se tiene:

$$\begin{aligned} N &= a^3 + b^3 + 8^k \cdot q \\ &= a^3 + b^3 + 8^k \left(6 \cdot 8^{2k} + r\right) \\ &= a^3 + b^3 + 8^k \left(6 \cdot 8^{2k} + d^3 + 6m\right) \\ &= a^3 + b^3 + 8^k d^3 + 8^k \left(6 \cdot 8^{2k} + 6m\right) \\ &= a^3 + b^3 + \left(2^k d\right)^3 + 8^k \left(6 \cdot 8^{2k} + 6m\right) \\ &= a^3 + b^3 + c^3 + A\left(6A^2 + 6m\right) \end{aligned}$$

Gracias a la desigualdad (7) se sabe que $m < A^2$, y m es la suma de tres cuadrados, entonces por el Lema 1 se sabe que $6A\left(A^2 + 6m\right)$ es la suma de seis cubos, supóngase que tales cubos son: $6A\left(A^2 + 6m\right) = u_1^3 + u_2^3 + u_3^3 + u_4^3 + u_5^3 + u_6^3$; $u_i \in \mathbb{Z}\ \forall i = 1, 2, ..., 6$.

Así, $N = a^3 + b^3 + c^3 + u_1^3 + u_2^3 + u_3^3 + u_4^3 + u_5^3 + u_6^3$, es decir, N es la suma de nueve cubos y esto demuestra el caso 1.

Para el caso 2, se va a suponer que $40,000 < N \leq 8^{10}$. Constrúyase el entero $a = \left[\left(N - 10,000 \right)^{1/3} \right]$. Como $N > 40,000$, entonces $N - 10,000 > 30,000$ y por lo tanto $a > 30,000^{1/3}$. También $30,000^{1/3} = 31.072... > 31$. Por lo tanto:

$$a > 30,000^{1/3} > 31$$

Sea $d = (a+1)^3 - a^3 = a^3 + 3a^2 + 3a + 1 - a^3 = 3a^2 + 3a + 1$. Ahora bien, se tiene que $3a^2 + 3a + 1 < 4a^2 \Leftrightarrow 3a + 1 < 3a^2 \Leftrightarrow 1 < 3a^2 - 3a \Leftrightarrow 1 < 3a(a-1)$, pero a es un número menor o igual que 31, entonces $3a^2 + 3a + 1 < 4a^2$. También se tiene que $4a^2 < 4N^{2/3} \Leftrightarrow a^2 < N^{2/3} \Leftrightarrow a < N^{1/3}$, pero $N - 10,000 < N$, entonces $(N - 10,000)^{1/3} < N^{1/3}$, por lo tanto $a < \left[N^{1/3} \right] \leq N^{1/3}$. Así, se obtiene que:

$$d = (a+1)^3 - a^3 = 3a^2 + 3a + 1 < 4a^2 < 4N^{2/3} \ldots (8)$$

Por lo tanto $N - (a+1)^3 < 10,000$, ya que:

$N - (a+1)^3 < 10,000 \Leftrightarrow N - 10,000 < (a+1)^3 \Leftrightarrow (N - 10,000)^{1/3} < a + 1 \Leftrightarrow$

$\Leftrightarrow a < a + 1 \Leftrightarrow 0 < 1$

También resulta que $10,000 \leq N - a^3$, esto es porque:

$10,000 \leq N - a^3 \Leftrightarrow a^3 \leq N - 10,000 \Leftrightarrow a \leq (N - 10,000)^{1/3} \Leftrightarrow$

$\Leftrightarrow \left[(N - 10,000)^{1/3} \right] \leq (N - 10,000)^{1/3}$

Pero $N - a^3 = N - (a+1)^3 + d = N - (a+1)^3 + (a+1)^3 - a^3 = N - (a+1)^3 + d$ y $N - (a+1)^3 + d < 10,000 + 4N^{2/3}$ ya que $d < 4N^{2/3}$ y $N - (a+1)^3 < 10,000$. Así:

$$N - (a+1)^3 < 10,000 \leq N - a^3 = N - (a+1)^3 + d < 10,000 + 4N^{2/3}$$

Si $N - a^3 \leq 40,000$, entonces por el Lema 4 $N - a^3$ es la suma de seis cubos y ya se tendría el resultado.

Si $N - a^3 > 40,000$, se construye el entero $b = \left[\left(N - a^3 - 10,000 \right)^{1/3} \right] > 31$ de tal manera que:

$$N-a^3-(b+1)^3<10,000\le N-a^3-b^3<10,000+4\left(N-a^3\right)^{2/3}$$

Si $N-a^3-b^3\le 40,000$, entonces por el Lema 4 $N-a^3-b^3$ es la suma de seis cubos y ya se tendría el resultado.

Si $N-a^3-b^3>40,000$, se construye $c=\left\lfloor\left(N-a^3-b^3-10,000\right)^{1/3}\right\rfloor>31$ de tal manera que:

$$\begin{aligned}
N-a^3-b^3-(c+1)^3 &<10,000\\
&\le N-a^3-b^3-c^3\\
&<10,000+4\left(N-a^3-b^3\right)^{2/3}\\
&<10,000+4\left(10,000+4\left(10,000+4N^{2/3}\right)^{2/3}\right)^{2/3}\\
&\le 10,000+4\left(10,000+4\left(10,000+4\left(8^{10}\right)^{2/3}\right)^{2/3}\right)^{2/3}\\
&=10,000+4\left(10,000+4\left(10,000+4,194,304\right)^{2/3}\right)^{2/3}\\
&=10,000+4\left(10,000+4\left(26049.301\right)\right)^{2/3}\\
&=10,000+4\left(2353.804...\right)\\
&=19,415.21637...<20,000
\end{aligned}$$

Por lo tanto, si $40,000<N<8^{10}$, entonces existen $a, b, c\in\mathbb{Z}^+$ tales que $10,000<N-a^3-b^3-c^3\le 40,000$. Entonces, por el Lema 4, $N-a^3-b^3-c^3$ es suma de 6 cubos no negativos, *i.e.*, existen $z_1, z_2, z_3\in\mathbb{Z}^+$ tales que $N-a^3-b^3-c^3=z_1^3+z_2^3+z_3^3$. Por lo tanto se tiene que:
$N=a^3+b^3+c^3+z_1^3+z_2^3+z_3^3$, es decir, N es la suma de nueve cubos. □

Como ya se mencionó en el capítulo I el resultado importante de los problemas de Waring es el de dar certidumbre a que siempre se puede expresar un número entero como suma de cualesquiera potencias que se elijan, es decir, que todo número es la suma de k-ésimas potencias, para toda k en los enteros positivos. David Hilbert demostró que todo entero puede ser representado por una cantidad finita de k-ésimas potencias, cabe señalar que no demostró cuantos sumandos se requieren para cada potencia k, sólo demostró que sí es posible representar a cada entero de tal forma.

Melvyn B. Nathanson [2000], en su libro *Elementary Methods in Number Theory*, da la demostración de este teorema. Cabe mencionar que este teorema se enuncia en términos de *bases* y *bases asintóticas*,

así que, primeramente, se recordarán estos conceptos para después poder pasar a la prueba.

Definición 1: Sea A un conjunto de enteros no negativos, entonces:

- A es llamado *base de orden h* si todo entero positivo puede ser escrito como la suma de exactamente h elementos de A.
- El conjunto A es llamado *base de orden finito* si A es una base de orden h para alguna h.

Por ejemplo, gracias al Teorema de Lagrange, el conjunto de números cuadrados es una base de orden cuatro.

Con esta notación, el Teorema de Waring-Hilbert queda escrito de la siguiente manera: "Para todo entero $k \geq 2$, el conjunto de k-ésimas potencias no negativas es una base de orden finito".

Ya que se utiliza esta notación para la demostración del teorema, es importante introducir la siguiente definición para que quede completamente claro cada uno de los conceptos:

Definición 2: Sea B un conjunto de enteros no negativos, entonces:

- B es llamado *base asintótica de orden k* si todo entero positivo suficientemente grande puede ser escrito como la suma de exactamente k elementos de B.
- Se llamará a B una *base asintótica de orden finito* si B es una base asintótica de orden k para alguna k.

Por ejemplo, el conjunto de cubos forman una base asintótica de orden 8, ya que se necesitan 9 cubos para representar a todos los enteros, pero únicamente se requieren exactamente los 9 para representar al 23 y al 239, entonces, a partir del 239 todos los enteros pueden ser escritos como suma de 8 cubos.

Para la prueba, Nathanson utiliza un par de teoremas los cuales implican directamente al Teorema de Waring-Hilbert:

Teorema 11.9: Sea $f(x) = \sum_{i=0}^{k} a_i x^i = a_k x^k + a_{k-1} x^{k-1} + \ldots + a_1 x + a_0$ un polinomio valuado en los enteros de grado k con $a_k > 0$ y el máximo común divisor $\text{mcd}(A(f)) = 1$, es decir, $(f(0), f(1), \ldots) = 1$. Entonces $A(f) = \{f(0), f(1), \ldots\} \cup \{0\}$ es una base asintótica de orden finito, es decir, para alguna h y para todo entero suficientemente gran-

de n, existe un entero positivo $h_n \leq h$ y enteros no negativos $x_1,...,x_{h_n}$ tales que $f(x_1)+...+f(x_{h_n})=n$

A partir de este resultado, se sigue de inmediato el siguiente teorema, el cual a su vez implica el resultado de Waring-Hilbert:

Teorema 11.10: Sea $f(x)$ un polinomio de grado k valuado en los enteros con coeficiente principal $a_k > 0$. Si $0,1 \in A(f)=\{f(x) / x \in N_0\}$; donde $N_0 = \mathbb{N} \cup \{0\}$, entonces $A(f)$ es una base de orden finito.

Una vez que tenemos este par de resultados, el Teorema de Waring-Hilbert se sigue de inmediato. A continuación se enunciará el enunciado de este famoso resultado:

Teorema (Waring-Hilbert)[47]:

Para todo entero $k \geq 2$, el conjunto de k-ésimas potencias no negativas forman una base de orden finito.

Por último, se hará un estudio sobre la conjetura de Waring en casos particulares para que, de esta manera, al lector le quede más claro el avance de dicho problema así como los resultados que aún no tienen solución.

Alrededor del año de 1772, Johannes Albert Euler (hijo de Leonhard Euler) hizo la siguiente observación: Si se considera un entero $k \geq 2$, entonces, dividiendo 3^k entre 2^k se obtiene la siguiente igualdad: $3^k = (q \times 2^k)+r$ donde $1 \leq r \leq 2^k$. Por lo tanto $q=\left[\frac{3^k}{2^k}\right]$. Una vez que se tiene este entero q, se construye el entero $s=(q \times 2^k)-1 < 3^k$, ahora bien, si s es la suma de k-ésimas potencias, entonces dichas potencias solamente pueden ser 1 ó 2^k, pero s puede ser factorizado como $s=(q-1)\times 2^k+(2^k-1)\times 1$, por lo tanto s es la suma de $q-2+2^k$ (y no menos) k-ésimas potencias. De esta manera se obtiene que $g(k) \geq \left[\left(\frac{3}{2}\right)^k\right]-2+2^k$ y por lo tanto se tienen cotas inferiores para

[47] Este teorema es un caso especial del Teorema 11.10 aplicado a la función polinomial $f(x)=x^k$.

$g(k)$, es decir, $g(k) \geq 9, 19, 37, 73, 143, 279, 548, 1079, \ldots$ para cada $k = 3, 4, 5, 6, 7, 8, 9, 10, \ldots$ respectivamente.

Maillet, en el año de 1908 dio una cota inferior para $G(k)$. Él demostró que $G(k) \geq k+1$ para toda k, aunque esta cota es muy pobre, lo que Maillet afirmó es que existen números naturales arbitrarios muy grandes los cuales NO pueden ser representeados como la suma de k k-ésimas potencias.

Más adelante Hardy y Littlewood publicaron, en 1920 y en los años siguientes, una serie de artículos de gran relevancia para la conjetura de Waring. Ellos desarrollaron un nuevo método analítico el cual fue utilizado para crear una nueva prueba del teorema de Hilbert, la cual produjo la siguiente estimación:

$$G(k) \leq 2^{k-1}(k-2)+5$$

Sin embargo, la prueba de Hardy y Littlewood fue mejorada por Vinogradov en 1935 y éstas a su vez fueron simplificadas por Helibronn un año más tarde. Con estas mejoras, Vinogradov obtuvo en 1947 que $G(k) \leq k(3\log k + 11)$ y, más aún, para 1959, el mismo mejoró este resultado para $k \geq 170000$.

Pero la cota de $G(k)$ dada por Vinogradov no es la mejor. Chen en 1958 llega a la conclusión de que $G(k) \leq k(3\log k + 5.2)$ la cual se mejora una vez más en 1984 gracias a Balasubramanian y Mozochi, ellos afirmaron que

$$G(k) \leq [2A_2 + A_1 - 4]; \text{ donde } A_1 = -\frac{\log(3k)}{\log \rho},\ A_2 = -\frac{\log(6k)}{\log \rho} \text{ y } \rho = \frac{k-1}{k}$$

De la misma manera, se dieron cotas para $g(k)$ cada vez mejores, pero nunca llegando a su valor exacto para cada entero k.

Sin más preámbulo, se darán una serie de tablas, hechas por Ribenboim [1989] en las cuales se realiza un estudio sobre los valores de $g(k)$ y $G(k)$ para $k = 3, \ldots, 10$, así como también el estado actual de la conjetura de Waring para dichos valores:

$k = 3$

Año	Autor	$g(3)$	$G(3)$	Nota
1862	J.A. Euler	≥ 9		
1895	E. Maillet	≤ 21	≥ 4	$g(3)$ existe
1906	A. Fleck	≤ 13		
1909	A. Wieferich	≤ 9		El mejor valor posible de $g(3)$
1909	E. Landau		≤ 8	
1943	Yu. V. Linnik		≤ 7	

En 1939, Dickson demostró que todos los números enteros, excepto el 23 y el 239 pueden ser representados como la suma de ocho cubos.

El estado actual de este resultado es el siguiente:
$4 \leq G(3) \leq 7$; El valor exacto de $G(3)$ se desconoce, sin embargo, gracias a los cálculos de Bohman y Fröberg en 1981 así como Romani en 1982, se puede afirmar que la posibilidad más acertada es que $G(3) = 4$.

$k = 4$

Año	Autor	$g(4)$	$G(4)$	Nota
1859	J. Liouville	≤ 53		$g(4)$ existe
1862	J.A. Euler	≥ 19		
1878	S. Réalis	≤ 47		
1878	E. Lucas	≤ 41		
1895	E. Maillet		≥ 5	
1906	A. Fleck	≤ 39		
1907	E. Landau	≤ 38		
1909	A. Wieferich	≤ 37		
1912	A.J. Kempner		≥ 16	
1921	Hardy y Littlewood		≤ 21	
1939	H. Davenport		≤ 16	El mejor valor posible de $G(4)$
1971	F. Dress	≤ 30		
1974	J.R. Chen	≤ 27		
1974	H.E. Thomas	≤ 22		
1979	R. Balasubramanian	≤ 21		
1986	R. Balasubramanian, J.M. Deshouillers y F. Dress	≤ 19		El mejor valor posible de $g(4)$

El estado actual de este resultado es el siguiente:
$G(4)=16$ y $g(4)=19$, por lo tanto, el problema está resuelto.

$k=5$

Año	Autor	$g(5)$	$G(5)$	Nota
1862	J.A. Euler	≥ 37		
1892	E. Maillet	≤ 192	≥ 16	$g(5)$ existe
1907	A. Fleck	≤ 156		
1907	A. Wieferich	≤ 59		
1913	W.S. Baer	≤ 58		
1922	G.H. Hardy y J.E. Littlewood		≤ 53	
1933	L.E. Dickson	≤ 54		
1942	H. Davenport		≤ 23	
1964	J.R. Chen	≤ 37		El mejor valor posible de $g(5)$
1985	K. Thanigasalam		≤ 22	
1986	R.C. Vaughan		≤ 21	

El estado actual de este resultado es el siguiente:
$g(5)=37$ y $6\leq G(5)\leq 21$.

$k=6$

Año	Autor	$g(6)$	$G(6)$	Nota
1862	J.A. Euler	≥ 73		
1895	E. Maillet		≥ 7	
1907	A. Fleck	$\leq 184g(3)+59$ ≤ 2451		$g(6)$ existe
1912	A.J. Kempner	≤ 970		
1913	W.S. Baer	≤ 478		
1922	G.H. Hardy y J.E. Littlewood		≤ 133 ≥ 9	
1940	S.S. Pillai	≤ 73		El mejor valor posible de $g(6)$
1942	H. Davenport		≤ 36	
1985	K. Thanigasalam		≤ 34	
1986	R.C. Vaughan		≤ 31	

El estado actual de este resultado es el siguiente:
$g(6)=73$ y $9\leq G(6)\leq 31$

$k = 7$

Año	Autor	$g(7)$	$G(7)$	Nota
1862	J.A. Euler	≥ 143		
1895	E. Maillet		≥ 8	
1909	A. Wieferich	≤ 3806		$g(7)$ existe
1922	G.H. Hardy y J.E. Littlewood		≤ 325	
1942	H. Davenport		≤ 53	
1964	R.M. Stemmler	143		
1985	K. Thanigasalam		≤ 50	
1986	R.C. Vaughan		≤ 45	

El artículo en donde K. Sambasiva Rao, en 1941, afirma que $G(7) \leq 52$ es incorrecto. El estado actual de este resultado es el siguiente: $g(7) = 143$ y $8 \leq G(7) \leq 45$.

$k = 8$

Año	Autor	$g(8)$	$G(8)$	Nota
1862	J.A. Euler	≥ 279		
1895	E. Maillet		≥ 9	
1908	E. Maillet	$< \infty$		$g(8)$ existe
1908	A. Hurwitz	$\leq 840g(4)+273$ ≤ 36119		$g(8)$ existe
1922	G.H. Hardy y J.E. Littlewood		≤ 773 ≥ 32	
1941	V. Narasimhamurti		≤ 73	
1964	R.M. Stemmler	279		
1985	K. Thanigasalam		≤ 68	
1986	R.C. Vaughan		≤ 62	

El estado actual de este resultado es el siguiente:
$g(8) = 279$ y $32 \leq G(8) \leq 62$.

$k = 9$

Año	Autor	$g(9)$	$G(9)$	Nota
1862	J.A. Euler	≥ 548		
1895	E. Maillet		≥ 10	
1922	G.H. Hardy y J.E. Littlewood		≥ 13	
1941	V. Narasimhamurti		≤ 99	
1964	R.M. Stemmler	548		
1973	R.J. Cook		≤ 96	
1977	R.C. Vaughan		≤ 91	
1985	K. Thanigasalam		≤ 87	
1986	R.C. Vaughan		≤ 82	

La existencia de $g(9)$ se sigue del teorema de Hilbert. El estado actual de este resultado es el siguiente: $g(9) = 548$ y $13 \leq G(9) \leq 82$.

$k = 10$

Año	Autor	$g(10)$	$G(10)$	Nota
1862	J.A. Euler	≥ 1079		
1895	E. Maillet		≥ 11	
1909	J. Schur	$< \infty$		$g(10)$ existe
1922	G.H. Hardy y J.E. Littlewood		≥ 12	
1941	V. Narasimhamurti		≤ 122	
1964	R.M. Stemmler	1079		
1973	R.J. Cook		≤ 121	
1977	R.C. Vaughan		≤ 107	
1984	R. Balasubramanian y C.J. Mozzochi		≤ 106	
1985	K. Thanigasalam		≤ 102	

El estado actual de este resultado es el siguiente:
$g(10) = 1079$ y $12 \leq G(10) \leq 102$.

Para que se entienda un poco mejor esta serie de tablas, se presenta una nueva tabla la cual resumirá, el estado actual de la conjetura de Waring para $k = 2, 3, ..., 10$.

k	$g(k)$	$G(k)$	**Autor** ($g(k)$)	**Año** ($g(k)$)	**Autor** ($G(k)$)	**Año** ($G(k)$)
2	4	4	Lagrange	1770	Lagrange	1770
3	9	4	Wieferich	1909	Bohman, Fröberg y Romani	1981 y 1982
4	19	16	Balasubramanian, Deshouillers y Dress	1986	Davenport	1939
5	37	$6 \leq G(5) \leq 21$	Chen	1964		
6	73	$9 \leq G(6) \leq 31$	Pillai	1940		
7	143	$8 \leq G(7) \leq 45$	Stemmler	1964		
8	279	$32 \leq G(8) \leq 62$	Stemmler	1964		
9	548	$13 \leq G(9) \leq 82$	Stemmler	1964		
10	1079	$12 \leq G(10) \leq 102$	Stemmler	1964		

Inciso 10

Cualquier número de la forma $4n+2$, divisible por 2 pero no por 4, puede ser compuesto como la suma de dos o tres cuadrados.

Nathanson [1996] demuestra este teorema en su libro *Additive Number Theory*, su prueba esta basada en formas cuadráticas. De hecho, utiliza la teoría de formas cuadráticas para demostrar los Lemas 1 al 6 y los Teoremas 1 y 2. Con estos resultados se deduce a lo que se llamará Lema 7. Este último resultado es el que va a implicar directamente el inciso 10, ya que el problema se reduce a demostrar que cierto entero $-d'$ es un residuo cuadrático módulo otro número p. Así que primeramente se dará una pequeña introducción a este tema, así como los resultados necesarios para la demostración de este inciso.

Considérese el conjunto $SL_n(\mathbb{Z})$, como el grupo de matrices de tamaño $n \times n$ con discriminante 1. Se afirma que este grupo actúa en el anillo $M_n(\mathbb{Z})$[48] de la siguiente manera:

Si $A \in M_n(\mathbb{Z})$ y $U \in SL_n(\mathbb{Z})$, se define $\cdot : SL_n(\mathbb{Z}) \times M_n(\mathbb{Z}) \to SL_n(\mathbb{Z})$ de la siguiente manera $\cdot(U, A) \doteq A \cdot U = U^T A U$. Este es una acción de grupo ya que:

$\cdot(Id, A) = A \cdot Id = Id^t A\, Id = A$ ya que $Id^t = Id$ y es para $A \in M_n(\mathbb{Z})$

Además se cumple que:

$$(UV, A) = A \cdot (UV) = (UV)^T A(UV) = V^T (U^T A U) V =$$
$$= (U^T A U) \cdot V = (A \cdot U) \cdot V = \cdot(V, \cdot(U, A))$$

Una vez definida esta acción, se introduce una relación entre matrices de la siguiente manera:

Dos matrices $A, B \in M_n(\mathbb{Z})$ son *equivalentes* ($A \sim B$) si A y B pertenecen a la misma orbita de la acción de grupo, *i.e.*, si $B = A \cdot U = U^T A U$ para alguna $U \in SL_n(\mathbb{Z})$. Se puede verificar fácilmente que ésta relación es una relación de equivalencia, así que induce una partición: para cualquier entero d, la partición de la acción de

---

[48] Recordar que un *grupo G actúa en un conjunto X* si existe un mapeo $\Phi : G \times X \to X$ con las siguientes propiedades:

1) $\Phi(e, x) = x \quad \forall x \in X$; donde e es la identidad en G

2) $\Phi(g, \Phi(h, x)) = \Phi(gh, x) \quad \forall x \in X$ y $\forall h, g \in G$

grupo es el conjunto de matrices simétricas[49] de tamaño $n \times n$ con discriminante *d*.

Para toda matriz simétrica $A = (a_{i,j})$ de tamaño $n \times n$, le asociamos la *forma cuadrática* F_A definida mediante $F_A(x_1, ..., x_n) = \sum_{i=1}^{n} \sum_{j=1}^{n} a_{i,j} x_i x_j$.

F_A es una función homogénea de grado 2 en *n* variables $x_1, ..., x_n$.[50]

Esta es una función homogénea de grado dos en *n* variables $x_1, ..., x_n$. Por ejemplo, si I_n es la matriz identidad de tamaño $n \times n$, entonces la forma cuadrática asociada a esta matriz es $F_{I_n}(x_1, ..., x_n) = x_1^2 + x_2^2 + \cdots + x_n^2$.

Sea *x* la matriz de tamaño $n \times 1$ (o vector columna) $x = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$. Entonces se puede escribir la forma cuadrática de esta matriz como $F_A(x_1, ..., x_n) = x^T Ax$. Se define el *discriminante* de la forma cuadrática F_A como el determinante de la matriz *A*.

Se define una nueva relación (ahora entre formas cuadráticas) de la siguiente manera:

Sean *A* y *B* matrices simétricas de tamaño $n \times n$ y sean F_A y F_B sus correspondientes formas cuadráticas. Se dice que estas formas son *equivalentes* ($F_A \sim F_B$) si las matrices *A* y *B* son equivalentes, es decir, $A \sim B$. La equivalencia de formas cuadráticas es, nuevamente, una relación de equivalencia y formas cuadráticas equivalentes tienen el mismo discriminante.

---

[49] Se dice que una matriz $A \in M_n(\mathbb{Z})$ es *simétrica* si $A^T = A$. Obsérvese que si *A* es una matriz simétrica y *U* es cualquier matriz en $M_n(\mathbb{Z})$, entonces $U^T AU$ es también una matriz simétrica ya que $(U^T AU)^T = U^T A^T (U^T)^T = U^T AU$.

Obsérvese que si *A* es una matriz simétrica y *U* es cualquier matriz en $M_n(\mathbb{Z})$, entonces $U^T AU$ es también una matriz simétrica ya que $(U^T AU)^T = U^T A^T (U^T)^T = U^T AU$.

[50] Por ejemplo, si I_n es la matriz identidad de tamaño $n \times n$, entonces la forma cuadrática asociada a esta matriz es $F_{I_n}(x_1, ..., x_n) = x_1^2 + x_2^2 + \cdots + x_n^2$.

Se dice que la forma cuadrática F_A *representa al entero* N si existen enteros $x_1, ..., x_n$ tales que $F_A(x_1, ..., x_n) = N$. De esta manera, si $F_A \sim F_B$, entonces $A \sim B$ y por lo tanto existe una matriz $U \in SL_n(\mathbb{Z})$ tal que $A = B \cdot U = U^T BU$, de aquí se sigue que $F_A(x) = x^T Ax = x^T U^T BUx = (Ux)^T B(Ux) = F_B(Ux)$; donde x es la matriz de tamaño $n \times 1$ antes definida.

Así, si la forma cuadrática F_A representa al entero N, entonces toda forma equivalente a F_A también representa a N. Como la equivalencia de formas cuadráticas es una relación de equivalencia, entonces cualesquiera dos formas cuadráticas en la misma clase de equivalencia representan exactamente el mismo conjunto de enteros.[51]

Se dirá que la forma cuadrática F_A es *positiva-definida* si $F_A(x_1, ..., x_n) \geq 1$ para todo $(x_1, ..., x_n) \neq (0, ..., 0)$.[52]

Finalmente, una forma cuadrática en dos variables se llamará *forma cuadrática binaria* y, análogamente, una forma cuadrática en tres variables se llamará *forma cuadrática ternaria*.[53]

Una vez que se tienen los conceptos básicos de formas cuadráticas, se puede continuar con los resultados necesarios para demostrar el inciso 10. Cabe señalar que no se demostrarán, con todo rigor, todos estos resultados ya que las demostraciones son muy técnicas y a lo que se quiere llegar es a la prueba del inciso 10. Para consultar dichas pruebas, refiérase a Nathanson [1996].

---

[51] A manera de ejemplo, el Teorema de Lagrange de los cuatro cuadrados se puede reescribir en términos de formas cuadráticas de la siguiente manera:
"Para $n \geq 4$, cualquier forma equivalente a la forma $x_1^2 + \cdots + x_n^2$ representa a todos los enteros no negativos".

[52] Toda forma equivalente a una forma cuadrática positiva-definida es también una forma positiva-definida.

[53] Para las formas cuadráticas binarias y ternarias se puede probar que hay solamente una clase de equivalencia de formas positivas-definidas de discriminante 1.

Lema 1: Sean $A=\begin{pmatrix} a_{1,1} & a_{1,2} \\ a_{1,2} & a_{2,2} \end{pmatrix}$ una matriz simétrica de tamaño 2×2 y $F_A(x_1,x_2)=a_{1,1}x_1^2+2a_{1,2}x_1x_2+a_{2,2}x_2^2$ su forma cuadrática asociada. Entonces, la forma cuadrática binaria F_A es positiva-definida si y sólo si $a_{1,1}\geq 1$. Además, el discriminante d satisface que $d=\det(A)=a_{1,1}a_{2,2}-a_{1,2}^2\geq 1$.

Demostración:

De la suposición de que F_A es positiva-definida, se considera $F_A(1,0)=a_{1,1}\geq 1$ y de esta manera resulta que $a_{1,1}\geq 1$ y mediante una serie de cálculos sencillos se llega a que $d\geq 1$.

Del hecho de que $a_{1,1}\geq 1$ y $d\geq 1$, se sigue de inmediato que $F_A(x_1,x_2)=0$ si y sólo si $(x_1,x_2)=(0,0)$. Por lo tanto F_A es positiva-definida. □

Lema 2: Toda clase de equivalencia de formas cuadráticas binarias positivas-definidas de discriminante d contiene al menos una forma $F_A(x_1,x_2)=a_{1,1}x_1^2+2a_{1,2}x_1x_2+a_{2,2}x_2^2$ para la cual, $2|a_{1,2}|\leq a_{1,1}\leq\frac{2}{\sqrt{3}}\sqrt{d}$.

Demostración:

Para esta prueba, se construye una matriz B y su correspondiente forma cuadrática (positiva-definida) $F_B(x_1,x_2)=b_{1,1}x_1^2+2b_{1,2}x_1x_2+b_{2,2}x_2^2$ y una matriz $U\in SL_2(\mathbb{Z})$ de tal manera que $A=U^TBU$.

Después se prueba que $A\sim B$ y por tanto la forma F_B es equivalente a la forma $F_A(x_1,x_2)=a_{1,1}x_1^2+2a_{1,2}x_1x_2+a_{2,2}x_2^2$ donde $2|a_{1,2}|\leq a_{1,1}\leq a_{2,2}$.

Por último, mediante una serie de cálculos a partir del discriminante d se llega a que $a_{1,1}\leq\frac{2}{\sqrt{3}}\sqrt{d}$. □

Teorema 1: Toda forma cuadrática binaria positiva-definida con discriminante 1 es equivalente a la forma $x_1^2+x_2^2$.

Demostración:

Se considera una forma cuadrática binaria positiva-definida F con discriminante 1, utilizando el Lema 2 se llega a que F es equivalente a la forma $a_{1,1}x_1^2 + 2a_{1,2}x_1x_2 + a_{2,2}x_2^2$ para la cual $2|a_{1,2}| \le a_{1,1} \le \frac{2}{\sqrt{3}}\sqrt{d} < 2$.

Del hecho de que el discriminante de F es 1 junto con una serie de consideraciones para los elementos $a_{1,1}$, $a_{1,2}$ y $a_{2,2}$ se llega a que la forma F es equivalente a la forma $x_1^2 + x_2^2$. □

A continuación se presentaran los resultados análogos a los exhibidos hasta este momento pero para formas cuadráticas ternarias positivas-definidas. Por lo tanto las demostraciones, aunque un poco más largas y complejas, no son más que los casos generales de los resultados anteriores.

Lema 3: Sea $A = \begin{pmatrix} a_{1,1} & a_{1,2} & a_{1,3} \\ a_{1,2} & a_{2,2} & a_{2,3} \\ a_{1,3} & a_{2,3} & a_{3,3} \end{pmatrix}$ una matriz simétrica de 3×3 y sea F_A la correspondiente forma cuadrática ternaria. Sea d el discriminante de F_A. Entonces:

$a_{1,1}F_A(x_1,x_2,x_3) = (a_{1,1}x_1 + a_{1,2}x_2 + a_{1,3}x_3)^2 + G_{A^*}(x_2,x_3)$; donde G_{A^*} es la forma cuadrática binaria correspondiente a la matriz $A^* = \begin{pmatrix} a_{1,1}a_{2,2} - a_{1,2}^2 & a_{1,1}a_{2,3} - a_{1,2}a_{1,3} \\ a_{1,1}a_{2,3} - a_{1,2}a_{1,3} & a_{1,1}a_{3,3} - a_{1,3}^2 \end{pmatrix}$ y G_{A^*} tiene por discriminante a $a_{1,1}d$. Si F_A es positiva-definida, entonces G_{A^*} es positiva-definida.

Más aún, la forma F_A es positiva-definida si y sólo si los siguientes tres determinantes son positivos:

$$a_{1,1} = \det(a_{1,1}) \ge 1$$

$$d' = \det\begin{pmatrix} a_{1,1} & a_{1,2} \\ a_{1,2} & a_{2,2} \end{pmatrix} \ge 1$$

$$d = \det(A) \ge 1$$

Lema 4: Sea $B=\left(b_{i,j}\right)$ una matriz simétrica de tamaño 3×3 tal que la forma cuadrática ternaria F_B es positiva-definida.

Sea G_{B^*} la única forma cuadrática binaria positiva-definida tal que $b_{1,1}F_B\left(y_1,y_2,y_3\right)=\left(b_{1,1}y_1+b_{1,2}y_2+b_{1,3}y_3\right)^2+G_{B^*}\left(y_2,y_3\right)$.

Para cualquier matriz $V^*=\left(v_{i,j}^*\right)\in SL_2\left(\mathbb{Z}\right)$, sea $A^*=\left(V^*\right)^T B^*V^*$ ... (1) y considérese G_{A^*} la forma cuadrática binaria positiva-definida correspondiente a la matriz simétrica A^* y equivalente a la forma G_{B^*}.

Para cualesquiera enteros r y s, sean $V_{r,s}=\left(v_{i,j}\right)=\begin{pmatrix}1 & r & s\\ 0 & v_{1,1}^* & v_{1,2}^*\\ 0 & v_{2,1}^* & v_{2,2}^*\end{pmatrix}\in SL_3\left(\mathbb{Z}\right)$ y $A_{r,s}=V_{r,s}^T BV_{r,s}=\left(a_{i,j}\right)$ y $F_{A_{r,s}}$ la correspondiente forma cuadrática ternaria.

Entonces $a_{1,1}=b_{1,1}$ y $a_{1,1}F_{A_{r,s}}\left(x_1,x_2,x_3\right)=\left(a_{1,1}x_1+a_{1,2}x_2+a_{1,3}x_3\right)^2+G_{A^*}\left(x_2,x_3\right)$, donde la matriz A^* definida por (1) es independiente de r y s.

Lema 5: Sean $u_{1,1}$, $u_{2,1}$ y $u_{3,1}$ enteros tales que $\left(u_{1,1},u_{2,1},u_{3,1}\right)=1$. Entonces existen enteros $u_{i,j}$ con $i=1, 2, 3$ y $j=2, 3$ tales que la matriz $U=\left(u_{i,j}\right)\in SL_3\left(\mathbb{Z}\right)$, *i.e.*, $\det\left(U\right)=1$.

Lema 6: Toda clase de equivalencia de formas cuadráticas ternarias positivas-definidas de discriminante d contiene al menos una forma $\sum_{i,j=1}^{3}a_{i,j}x_ix_j$ para la cual $2\max\left(\left|a_{1,2}\right|,\left|a_{1,3}\right|\right)\le a_{1,1}\le\frac{4}{3}\sqrt[3]{d}$.

Teorema 2: Toda forma cuadrática ternaria positiva-definida de discriminante 1 es equivalente a la forma $x_1^2+x_2^2+x_3^2$.

Una vez que se tienen todos estos resultados relacionados con formas cuadráticas (tanto binarias como ternarias) se presentará el último resultado auxiliar que, junto con todos los anteriores, ayudarán a la resolución del inciso 10.

Lema 7: Sea $n \geq 2$. Si existe un entero positivo d' tal que $-d'$ es un resido cuadrático módulo $d'n-1$, entonces n puede ser representado como la suma de tres cuadrados.

Demostración:

Como $-d'$ es un residuo cuadrático módulo $d'n-1$, entonces[54] existe $a_{1,2} \in \mathbb{Z}$ tal que $a_{1,2}^2 \equiv -d' \pmod{d'n-1}$, *i.e.*, $a_{1,2}^2 + d' \equiv 0 \pmod{d'n-1}$. Por lo tanto, existe $a_{1,1} \in \mathbb{Z}$ tal que $a_{1,1}(d'n-1) = a_{1,2}^2 + d'$ ya que $d'n-1 \mid a_{1,2}^2 + d'$. Ahora, sustitúyase $d'n-1 = a_{2,2}$, entonces se tiene que $a_{1,2}^2 + d' = a_{1,1}a_{2,2}$.

Entonces, $a_{2,2} = d'n-1 \geq 2d'-1$ ya que $d'n-1 \geq 2d'-1 \Leftrightarrow d'n \geq 2d' \Leftrightarrow n \geq 2$, pero por hipótesis $n \geq 2$. También se tiene que $2d'-1 \geq 1$ ya que por hipótesis $d' \geq 0$, entonces $2d' \geq 2$, por lo tanto $2d'-1 \geq 1$. De esta manera se obtiene que $a_{2,2} = d'n-1 \geq 2d'-1 \geq 1$

Como $a_{1,2}^2 + d' = a_{1,1}a_{2,2}$ y, además, $a_{1,2}^2 > 0$ (por ser un cuadrado) y $d' \geq 0$ por hipótesis, entonces $a_{1,2}^2 + d' > 0$ o equivalentemente $a_{1,1}a_{2,2} > 0$. Pero se acaba de probar que $a_{2,2} \geq 1$. Por lo tanto, por ser $a_{1,1}$ un entero, se tiene que $a_{1,1} \geq 1$.

Nuevamente, como $a_{1,2}^2 + d' = a_{1,1}a_{2,2}$, entonces $d' = a_{1,1}a_{2,2} - a_{1,2}^2$. Considérese entonces la matriz simétrica $A = \begin{pmatrix} a_{1,1} & a_{1,2} & 1 \\ a_{1,2} & a_{2,2} & 0 \\ 1 & 0 & n \end{pmatrix}$ y calcúlese su determinante:

$$\begin{aligned}
\det(A) &= \begin{vmatrix} a_{1,2} & a_{2,2} \\ 1 & 0 \end{vmatrix} + n \begin{vmatrix} a_{1,1} & a_{1,2} \\ a_{1,2} & a_{2,2} \end{vmatrix} \\
&= -a_{2,2} + n\left(a_{1,1}a_{2,2} - a_{1,2}^2\right) \\
&= \left(a_{1,1}a_{2,2} - a_{1,2}^2\right)n - a_{2,2} \\
&= \left(a_{1,2}^2 + d' - a_{1,2}^2\right)n - a_{2,2} \\
&= nd' - a_{2,2} \\
&= nd' - d'n + 1 = 1
\end{aligned}$$

[54] Gracias a la definición 1 del apéndice A.

Por lo tanto $\det(A)=1$, como se vio anteriormente $a_{1,1}\geq 1$ y también $d'\geq 1$, entonces gracias al Lema 3, la forma cuadrática F_A (correspondiente a la matriz A) es positiva. Más aún, F_A tiene discriminante 1 y además $F_A(0,0,1)=n$ ya que $\begin{pmatrix}0 & 0 & 1\end{pmatrix}\begin{pmatrix}a_{1,1} & a_{1,2} & 1\\ a_{1,2} & a_{2,2} & 0\\ 1 & 0 & n\end{pmatrix}\begin{pmatrix}0\\0\\1\end{pmatrix}=n$. Por lo tanto F_A representa al entero n.

Como F_A es una forma cuadrática ternaria positiva definida de discriminante 1, entonces (por el Teorema 2) es equivalente a la forma $x_1^2+x_2^2+x_3^2$. Pero F_A representa a n, entonces $x_1^2+x_2^2+x_3^2$ también representa a n.

Por lo tanto $n=x_1^2+x_2^2+x_3^2$ es la suma de tres cuadrados. □

Ya se tiene toda la herramienta para demostrar el inciso (10), así que a continuación se presenta la demostración de dicha proposición:

Demostración (del inciso 10: Cualquier número de la forma $4n+2$, divisible por 2 pero no por 4, puede ser compuesto como la suma de dos o tres cuadrados):

Tómese un entero de la forma $4n+2$, es decir, $n\equiv 2\pmod 4$, entonces $4n\equiv 0\pmod 4$ y $n-1\equiv 1\pmod 4$, entonces $(4n,n-1)=1$. Por lo tanto, y gracias al Teorema de progresiones aritméticas de Dirichlet, $\{4nj+n-1 \,/\, j=1,2,...\}$ contiene una cantidad infinita de primos. Escójase $j\geq 1$ tal que $p=4nj+n-1$ sea un número primo y considérese $d'=4j+1$. Como $n\equiv 2\pmod 4$, entonces $p\equiv 1\pmod 4$ ya que $p=d'n-1=(4j+1)n-1=4jn+n-1\equiv n-1\equiv 2-1\equiv 1\pmod 4$.

Gracias al Lema 7, si se prueba que $-d'$ es un residuo cuadrático módulo $p=d'n-1$, entonces n es la suma de tres cuadrados que es lo que se quiere probar.

Tómese la factorización en primos de d': $d'=\prod_{q_i|d'} q_i^{k_i}$, donde los q_i son primos distintos. De esta manera se tiene que

$p = d'n - 1 \equiv \prod_{q_i | d'} q_i^{k_i} \cdot n - 1 \equiv 1 \pmod{q_i} \ \forall i,$ entonces

$$d' \equiv \prod_{\substack{q_i | d' \\ q_i \equiv 3 \pmod 4}} q_i^{k_i} \cdot \prod_{\substack{q_i | d' \\ q_i \equiv 1 \pmod 4}} q_i^{k_i} \equiv \prod_{\substack{q_i | d' \\ q_i \equiv 3 \pmod 4}} (-1)^{k_i} \pmod 4.$$

Como $d' = 4j + 1 \equiv 1 \pmod 4,$ entonces

$d' \equiv \prod_{\substack{q_i | d' \\ q_i \equiv 3 \pmod 4}} (-1)^{k_i} \equiv 1 \pmod 4$. Como este producto solo puede tomar los valores 1 ó -1 y es congruente con 1 módulo 4, además $1 \not\equiv -1 \pmod 4$, entonces $\prod_{\substack{q_i | d' \\ q_i \equiv 3 \pmod 4}} (-1)^{k_i} = 1.$

Del hecho de que $p \equiv 1 \pmod 4$ se sigue, gracias al Teorema 5 del apéndice A, que $\left(\frac{-1}{p}\right) = 1.$

Que no se olvide que lo que se quiere probar es que $-d'$ es un residuo cuadrático módulo p, *i.e.*, $\left(\frac{-d'}{p}\right) = 1.$

Gracias a la propiedad 2 del Teorema 4 del apéndice A se sabe que $\left(\frac{-d'}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{d'}{p}\right)$, pero $\left(\frac{-1}{p}\right) = 1$, entonces $\left(\frac{-d'}{p}\right) = \left(\frac{d'}{p}\right)$. Ahora bien, tomando de nuevo la foctorización en primos de d' se tiene que $\left(\frac{-d'}{p}\right) = \left(\frac{d'}{p}\right) = \left(\frac{\prod_{q_i | d'} q_i^{k_i}}{p}\right)$, aplicando varias veces la propiedad 2 del Teorema 4 del apéndice A resulta que $\left(\frac{\prod_{q_i | d'} q_i^{k_i}}{p}\right) = \prod_{q_i | d'} \left(\frac{q_i}{p}\right)^{k_i}$, ahora bien, como $p \equiv 1 \pmod 4$ entonces por el corolario de la ley de reciprocidad cuadrática de Gauss[55] $\prod_{q_i | d'} \left(\frac{q_i}{p}\right)^{k_i} = \prod_{q_i | d'} \left(\frac{p}{q_i}\right)^{k_i}$. Como $p \equiv -1 \pmod{q_i}$, entonces por la propiedad 3 del Teorema 4 del apéndice A se sigue que

[55] Véase el apéndice A

$\prod_{q_i|d'}\left(\frac{p}{q_i}\right)^{k_i}=\prod_{q_i|d'}\left(\frac{-1}{q_i}\right)^{k_i}$ .Pero por el Teorema 5 del apéndice A se tiene que $\prod_{q_i|d'}\left(\frac{-1}{q_i}\right)^{k_i}=\prod_{\substack{q_i|d'\\ q_i\equiv 3(\mathrm{mod}\,4)}}(-1)^{k_i}$ y como ya se vio anteriormente $\prod_{\substack{q_i|d'\\ q_i\equiv 3(\mathrm{mod}\,4)}}(-1)^{k_i}=1$.

Por lo tanto $\left(\frac{-d'}{p}\right)=1$.

Resumiendo, las cuentas que se hicieron en esta parte son:

$$\begin{aligned}\left(\frac{-d'}{p}\right)&=\left(\frac{-1}{p}\right)\left(\frac{d'}{p}\right)\\&=\left(\frac{d'}{p}\right)\\&=\prod_{q_i|d'}\left(\frac{q_i}{p}\right)^{k_i}\\&=\prod_{q_i|d'}\left(\frac{p}{q_i}\right)^{k_i}\\&=\prod_{q_i|d'}\left(\frac{-1}{q_i}\right)^{k_i}\\&=\prod_{\substack{q_i|d'\\ q_i\equiv 3(\mathrm{mod}\,4)}}(-1)^{k_i}\\&=1\end{aligned}$$

Entonces $\left(\frac{-d'}{p}\right)=1$, es decir, $-d'$ es un residuo cuadrático módulo $p=d'n-1$. Por lo tanto y gracias al Lema 7 se tiene que n es la suma de tres cuadrados. □

Otros problemas aditivos del Capítulo V de *Meditationes Algebraicae*

En la sección anterior se estudió el Teorema 47 (que pertenece al capítulo 5), sin embargo, a continuación se analizarán algunos otros resultados de este capítulo para tener una idea más global sobre los problemas de teoría aditiva de los números en el libro de Waring.

El Teorema 46 trata propiedades de los números enteros, en este resultado se observan varios corolarios y notas, las cuales son muy útiles en la teoría aditiva de números y en particular para los problemas de Waring. De este resultado se analizará el inciso 10 el cual se dedica a estudiar las propiedades de la función "suma de divisores" de un entero n.

Teorema 46 (inciso 10):

Considérese la siguiente fórmula:

$$S(n)=S(n-1)+S(n-2)-S(n-5)-S(n-7)+S(n-12)+S(n-15)$$
$$-S(n-22)-S(n-26)+S(n-35)+S(n-40)-\ldots$$

Donde $S(n)$ denota la suma de los divisores de n y los signos + y − se alternan por pares de términos. Esta fórmula contiene todos los números de la forma $\frac{3z^2 \pm z}{2}$ $\forall z \in \mathbb{Z}$.

La serie determina cuando el argumento del término $S(x)$ se volverá negativo o cero; si se vuelve exactamente cero, entonces para éste último se escribirá n.

Además de este resultado, Waring presenta una serie de notas y corolarios que son de gran utilidad en la matemática, a continuación se hará una pequeña reseña de estos resultados.

Nota 1. Considérese la siguiente ecuación:

$$(x-1)(x^2-1)(x^3-1)\cdots(x^n-1)=x^h-px^{h-1}+qx^{h-2}-rx^{h-3}+sx^{h-4}-\ldots$$
$$=x^h-x^{h-1}-x^{h-2}+x^{h-5}+x^{h-7}-x^{h-12}-\ldots\pm x^{h-n}\pm\ldots$$
$$=A=0$$

Los signos + y − se alternan en pares hasta el término x^{h-n}. Los coeficientes de los términos hasta x^{h-n} son +1, −1 ó 0; estos serán:

+1 para los términos de la forma x^{h-v} donde $v=\frac{3z^2 \pm z}{2}$ y z un número par.

-1 para $v=\frac{3z^2 \pm z}{2}$ y z un número impar.

Cero en cualquier otro caso.

Los números 1, 2, 5, 7, 12, 15, 22, 26, 35, 40, ..., que son restados del índice h son obtenidos como suma de los números 1, 1, 3, 2, 5, 3, 7, 4, 9, 5, 11, 6, ... los cuales son derivados de intercalar las siguientes series: 1, 3, 5, 7, 9, 11, ... y 1, 2, 3, 4, 5, 6, 7, ...

Nota 2. La suma de las m-ésimas potencias de las raíces de $A=0$ serán $S(m)$, donde $S(m)$ es la suma de los divisores de m siempre que $m \le n$.

Corolario 10.1: Con esta regla se observa que:

$$S(m) = pS(m-1) - qS(m-2) + rS(m-3) - sS(m-4) + \ldots$$
$$= S(m-1) + S(m-2) - S(m-5) - S(m-7) + S(m-12) +$$
$$+ S(m-15) - S(m-22) - S(m-26) + \ldots$$

Las cuales son las propiedades, dadas por Euler, de los divisores.

Corolario 10.2: Si en la siguiente ecuación (dada)
$S(m) = S(m-1) + S(m-2) - S(m-5) - S(m-7) + \ldots$ se sustituyen los valores:
$S(m-2) + S(m-3) - S(m-6) - S(m-8) + \ldots$,
$S(m-3) + S(m-4) - S(m-7) - S(m-9)$, etc. por $S(m-1)$, $S(m-2)$, etc. respectivamente, se puede derivar una expresión para $S(m)$ en términos de los divisores de los números menores que $(m-1)$ o, recursivamente, menores que $(m-2)$ y así sucesivamente.

Corolario 10.5: Sea L el coeficiente de $x^{h'-m}$, entonces:
$\pm 1 \cdot 2 \cdot 3 \cdots m \times L = 1 - m \cdot \frac{m-1}{2} S'(2) + m(m-1)\frac{m-2}{3} S'(3) \pm \ldots$ es una ecuación que expresa una relación entre los divisores primos de los números 1, 2, 3,..., m y sus potencias.

Corolario 10.6: El coeficiente $\pm L$ es igual a la diferencia entre el número de maneras que puede ser construido m como suma de primos 2, 3, 5, 7, 11, 13, ... y el número de maneras que puedes ser construido m sin incluir al 2.

Aunque Waring no demostró el Teorema 47 en su libro, más adelante da resultados que ayudan a la resolución de dicho teorema, tal es el caso del Teorema 50 y del Teorema 51, los cuales hablan sobre representación de enteros como suma de cuatro cuadrados.

Teorema 50 : Sea $(a^2+b^2+c^2+d^2)(p^2+q^2+r^2+s^2)=x^2+y^2+z^2+v^2$, donde a, b, c, d y p, q, r, s son enteros; entonces x, y, z, v también son enteros[56], de hecho se tiene que:

$$x = ap + bq + cr + ds$$
$$y = aq - bp \pm cs \mp dr$$
$$z = ar \mp bs - cp \pm dq$$
$$v = as \pm br \mp cq - dp$$

Teorema 51:

$$\begin{aligned}(a^2+ab+b^2)(c^2+cd+d^2) &= (ac+ad+bd)^2+(ac+ad+bd)(bc-ad)-(bc-ad)^2\\ &= (ac+bd+bc)^2+(ac+bd+bc)(ad-bc)+(ad-bc)^2\\ &= (ac+ad+bc)^2+(ac+ad+bc)(bd-ac)+(bd-ac)^2\\ &= (ad+bd+bc)^2+(ad+bd+bc)(ac-bd)+(ac-bd)^2\\ &= P\end{aligned}$$

Corolario 1: Si una cantidad de la forma $p^2 \pm pq + q^2$ (con p y q enteros o cero) es multiplicada por otra cantidad de la misma forma, entonces el producto será otra cantidad de la misma forma.

Corolario 2: El producto $(a^2+ab+b^2)(c^2+cd+d^2)$ puede ser compuesto de dos diferentes maneras con cantidades de la forma p^2+pq+q^2. De la misma manera, puede ser compuesto de dos diferentes maneras con cantidades de la forma p^2-pq+q^2 (donde p y q son enteros positivos o cero).

Corolario 3: Si los números N y M son compuestos, en n y m maneras respectivamente, por cantidades de la forma p^2+pq+q^2. Entonces el número $N \times M$ es compuesto de $2nm$ maneras con cantidades de la misma forma.

Corolario 4: Todo divisor de un número de la forma $p^2 \pm pq + q^2$, donde p y q son primos relativos, es también un número de esta misma forma.

Corolario 5: Si el número P no tiene por divisor a a^2, no es divisible por 3 y puede ser resuelto en sólo una manera como un número de la forma p^2+pq+q^2, entonces P será un número primo. También, por

[56] Este resultado ya se demostró cuando se resolvió el Teorema de los cuatro cuadrados de Lagrange.

el mismo principio, si $A = a^2 + mb^2$ no tiene por divisores ni a a^2 ni a ma^2 y puede ser expresado por $a^2 + mb^2$ de una sola manera, entonces A es un número primo.

Corolario 6: La suma de dos cubos, $a^3 + b^3$ tiene divisores los cuales son también divisores del número $a+b$, y estos contienen un número de la forma $p^2 \pm pq + q^2$. En estas instancias a y b son primos relativos.

También, en el corolario 6 del Teorema 52, Waring habla sobre la suma de dos cuadrados, todos estos resultados fueron de gran utilidad para que Lagrange, en 1770, pudiera resolver el Teorema de los cuatro cuadrados.

Corolario 6 (del Teorema 52):

La suma de dos cuadrados no puede ser dividida por ningún primo de la forma $4n-1$ a menos que a y b, ambos, sean divisibles por $4n-1$. La diferencia $a^{4n-2} - b^{4n-2}$ puede ser dividida por $4n-1$, pero $a^{4n-2} - b^{4n-2} + 2b^{4n-2} = a^{4n-2} + b^{4n-2}$ no es divisible por $4n-1$. Pero $a^{4n-2} - b^{4n-2}$ es divisible por $a^2 + b^2$ y por lo tanto $a^2 + b^2$ no es divisible por $4n-1$.

En el Teorema 54, Waring presenta una serie de resultados de gran utilidad para el problema de Hilbert-Waring, ya que en estos podemos encontrar aparentes condiciones para que un número pueda ser expresado como la suma de cierta cantidad de potencias de enteros. A continuación se presenta el corolario 2 de este teorema y una serie de ejemplos que clarifican el resultado, así como el corolario 3.3 que no es más que la generalización del corolario 2.

Teorema 54:

Corolario 2: Sean a', b', c', ... enteros tales que no se pueden representar por medio de sumar de dos residuos α, β, γ, ...; sean a'', b'', c'', ... enteros tales que no se puedan representar por medio de sumar tres residuos; y así sucesivamente. Entonces, ningún número de la forma $nr + a'$, $nr + b'$, ... puede ser representado como suma de dos m-ésimas potencias $h^m + k^m$ y de la misma manera, ningún número de la forma $nr + a''$, $nr + b''$, ... puede ser representado como la suma de tres números $h^m + k^m + l^m$.

Ejemplo 2.1: Considérese el sistema completo de residuos módulo 7: $\{0, 1, 2, 3, 4, 5, 6\}$, entonces los cubos módulo 7 son:

$0^3, 1^3, 2^3, 3^3, 4^3, 5^3, 6^3 \equiv 0, 1, 1, 6, 1, 6, 6 \pmod 7$, es decir, cualquier cubo es congruente con 0, 1 ó 6 módulo 7. Ahora bien, la suma de cualesquiera dos de éstos residuos puede ser únicamente 0, 1, 2, 5 ó 6, entonces, ni 3 ni 4 pueden ser escritos como la suma de dos residuos de cubos módulo 7. Por lo tanto se tiene que $7r+3$ y $7r+4$ para cualquier $r \in \mathbb{Z}$ NO pueden ser representados como la suma de dos cubos positivos.

Ejemplo 2.2: Ahora considérese el sistema completo de residuos módulo 11, se observa que los residuos de dividir $0^5, 1^5, ..., 10^5$ entre 11 son 0, 1 ó 10; y la suma de cualesquiera dos de estos residuos puede ser igual a 0, 1, 2, 9 ó 10. Como 3, 4, 5, 6, 7 y 8 no pueden ser escritos como la suma de dos residuos de potencias de 5 módulo 11, entonces $11r+3, 11r+4, ..., 11r+8$ NO pueden ser representados como suma de dos potencias quintas $h^5 + k^5$ para toda $r \in \mathbb{Z}$.

Ejemplo 2.3: Retomando el ejemplo anterior, la suma de cualesquiera tres residuos de potencias de 5 módulo 11 puede ser igual a 0, 1, 2, 3, 8, 9 y 10. Como 4, 5, 6 y 7 no aparecen en estas sumas, entonces los enteros $11r+4, 11r+5, 11r+6$ y $11r+7$ para cualquier $r \in \mathbb{Z}$, NO pueden ser representados como la suma de tres potencias quintas $h^5 + k^5 + l^5$.

Ejemplo 2.4: Tomando el ejemplo 3.2.1, se tiene que los posibles residuos son 0, 1 ó 6 módulo 7, entonces, si se considera la diferencia de cualesquiera dos de estos residuos se tiene que los resultados únicamente pueden ser 0, 1, 2, 5 ó 6; lo cual quiere decir que ningún número de la forma $7r+3$ ó $7r+4$ puede ser escrito como $h^3 \pm k^3$. Análogamente, la diferencia de cualesquiera dos residuos de potencias de 5 módulo 11 puede tomar únicamente el valor 0, 1, 2, 9 ó 10. Por lo tanto, ningún número de la forma $11r+3, 11r+4, 11r+5, 11r+6, 11r+7$ ú $11r+8$ puede ser representado por $h^5 \pm k^5$.

Corolario 3.3: En general, sean $\alpha, \beta, \gamma, \delta, ...$ los residuos de dividir los números $1^m, 2^m, 3^m, 4^m, ...$ por n; sean $\alpha', \beta', \gamma', \delta', ...$ los residuos de dividir los números $1^{m'}, 2^{m'}, 3^{m'}, 4^{m'}$ por n. Si el número H no puede ser expresado por ningún número de la forma $A\alpha \pm B\beta \pm C\gamma \pm ...$, entonces $nr+H$ no puede ser un número de la forma $Ah^m \pm Bk^m \pm Cl^m \pm ...$; y si H' no puede ser expresado por la siguiente fórmula:
$A\alpha \pm B\beta \pm C\gamma \pm ... \pm A'\alpha' \pm B'\beta' \pm C'\gamma' \pm ...$, entonces $nr+H'$ no puede ser un número de la forma

$Ah^m \pm Bk^m \pm Cl^m \pm ... \pm A'h'^{m'} \pm B'k'^{m'} \pm C'l'^{m'} \pm ...$; donde $h, k, l, ..., h', k', l', ..., m, m', ..., A, B, C, ..., A', B', C', ...$ son todos números enteros.

En el Problema LXI, Waring hace un estudio sobre la relación de distintos tipos de números poligonales así como la representación de enteros como suma de números figurados.

Problema LXI, caso 2

Corolario 2.1: Si no existen dos números a y b tales que n sea la suma del cuadrado a^2 y del número triangular $\frac{b^2+b}{2}$, entonces $8n+1$ no puede ser igual a
$8a^2+4b^2+4b+1=2\left(4a^2\right)\left(2b+1\right)^2=2p^2+q^2$, y en consecuencia no es un número primo.

Entre el Teorema 55 y el 56, Waring presenta un Lema en el cual toca el tema de ternas pitagóricas, si bien es cierto que Waring no demuestra este resultado, queda claro que él tenía un conocimiento muy profundo sobre este tema.

Lema: Supóngase que a^2+b^2 es un número cuadrado, con a y b primos relativos. Entonces $a=p^2-q^2$ y $b=2pq$, y así $a^2+b^2=\left(p^2+q^2\right)^2$; donde p y q también son primos relativos. Uno de los cuales debe de ser par y el otro impar. De otra manera, a y b no serían primos relativos.

Supóngase que a^2-b^2 es un número cuadrado, con a y b primos relativos. Entonces $a=p^2+q^2$ y $b=p^2-q^2$ ó $b=2pq$, donde p y q son primos relativos, uno de ellos debe de ser par y el otro impar.

En el Teorema 56, como ejemplos, Waring introduce los casos conocidos —hasta ese momento— sobre *El último Teorema de Fermat*, aunque sin ese título. En el ejemplo 1 de este resultado, Waring aborda el caso $x^4+ay^4=z^2$ con $a\in\mathbb{Z}$. Cabe señalar que en la demostración de dicho ejemplo, Waring utiliza una prueba de descenso infinito. Después, el ejemplo 2 lo divide en dos casos, los cuales son muy conocidos en la teoría de números:

1.- La suma de dos cuartas potencias $\left(\alpha^4+\beta^4\right)$ no puede ser un cuadrado.

2.-[57] $a^4 - b^4$ y por lo tanto $ab\left(a^2 - b^2\right)$, $2ab\left(a^2 + b^2\right)$ y $2a^4 + 2b^4 = \left(a^2 + b^2\right)^2 + \left(a^2 - b^2\right)^2$ no son números cuadrados, a menos que $a = b$.

Después, se presentan dos corolarios de gran importancia, en los cuales el autor incluye algunos ejemplos. El corolario 5 habla de la relación entre los números triangulares y las cuartas potencias y en el 6, Waring dice cuando un número puede ser un "generador" de un número cuadrado.

Corolario 5: Ningún número triangular $\frac{x(x+1)}{2}$, excepto la unidad, puede ser una cuarta potencia. Para x y $\frac{x+1}{2}$, ó $\frac{x}{2}$ y $x+1$, son primos relativos, y así ambos tendrían que ser cuartas potencias.

Ejemplo 3: Ningún número de la forma $a^4 + 2b^4$ puede ser un cuadrado.

Corolario 6: Si $a^4 + kb^4$ no es un cuadrado, entonces $2k\alpha\beta^3 y^4 - 2\alpha^3\beta x^4$ nunca será capaz de generar un cuadrado.

Ejemplo 4: Ningún cubo (excepto el 8) es 1 menos que un cuadrado, *i.e.*, $\frac{a^3}{b^3} + 1 = v^2$ no es verdadero, y tampoco es cierto que $a^3 b + b^4 = b^4 v^2 = u^2$.

[57] Cabe señalar que el caso 2, no es más que un caso análogo al 1.

CAPÍTULO IV

Presente y futuro de los problemas de Waring

En este último capitulo, el objetivo es responder la siguiente pregunta: "¿Hacia donde van los problemas de Waring?". Al principio de la tesis se trató de explicar un poco los orígenes de estos problemas, más adelante vio cuales son los problemas más representativos y sus soluciones y, ahora, se quiere mostrar cuáles son las rutas actuales de dichos problemas.

Números politopos

0. Introducción

Hyun Kwang Kin [2002] en su artículo *On the regular polytope numbers* trabaja la generalización del teorema de Lagrange sobre los cuatro cuadrados pero llevado a números poligonales y al problema de Hilbert-Waring. En su artículo, Kwang asocia una sucesión de enteros no negativos que les llamará números politopo, con politopos regulares V en un espacio euclidiano, con ellos ya definidos, considera el problema de encontrar el orden g(V) del conjunto de números politopo regulares asociados a V.

En este capítulo de la tesis se presentan las principales ideas del trabajo de Kwang, y es importante señalar que esta investigación es actual, se sigue desarrollando y prácticamente los resultados de Kwang son los únicos a la mano de los interesados en el tema.

Gauss probó que los números triangulares forman una base de orden tres[58], es decir $\# = \Delta + \Delta + \Delta$.

Teorema de Gauss: Todo entero no negativo es la suma de tres números triangulares.

Más adelante, Cauchy dio un resultado más fuerte y más general:

---

[58] Un conjunto no vacío A de enteros no negativos es llamado *base de orden g* si g es el número mínimo con la propiedad de que todo entero no negativo puede ser escrito como la suma de g elementos de A.
Por ejemplo, el Teorema de Lagrange (suma de cuatro cuadrados) lo podemos reescribir como sigue:
El conjunto $\{n^2 / n = 0, 1, 2, ...\}$ de cuadrados no negativos forman una base de orden 4.

Teorema de Cauchy: Si $m \geq 4$ y $N \geq 108m$, entonces N puede ser escrito como la suma de $m+1$ números poligonales de orden $(m+2)$; a lo más cuatro de ellos diferentes de cero o uno. Si $N \geq 324$, entonces N puede ser escrito como la suma de cinco números pentagonales; al menos uno de ellos es cero o uno.

Edward Waring conjeturó en 1770 que todo entero no negativo es la suma de cuatro cuadrados (Teorema de Lagrange), 9 cubos, 19 cuartas potencias y así sucesivamente.

El problema de Waring es: "Probar que para todo entero $k \geq 2$, el conjunto de k-ésimas potencias no negativas es una base de orden finito".

Denótese por $g(3)$ al número de cubos que se necesitan para representar a cualquier entero como la suma de $g(3)$ cubos. Wieferich y Kempner probaron que $g(3)=9$. Entonces, rescribiendo el problema de Waring se tendría que: "Probar que $g(k)$ es finito". Hilbert probó esto en 1909.

Teorema de Hilbert-Waring: Las k-ésimas potencias forman una base de orden finito para todo entero positivo N.

Una vez que se tiene la idea de los números poligonales, se puede generalizarla e introducir la idea de los *números politopos*. En matemáticas, un politopo regular es una figura geométrica con un alto grado de simetría. Ejemplos en dos dimensiones incluyen el cuadrado, el pentágono, el hexágono regular, etc. En tres dimensiones los politopos regulares incluyen los sólidos platónicos o sea, los poliedros regulares. Existen ejemplos también en dimensiones superiores. Los círculos y las esferas, aunque altamente simétricos, no son considerados politopos porque no tienen caras planas. Si se toma un politopo regular V en el espacio Euclidiano y se le asocia una sucesión de enteros no negativos, a los elementos de esta sucesión se les llamarán números politopos (regulares).

La aplicación de los problemas de Waring en los números politopos es la siguiente: Generalizar el Teorema de los cuatro cuadrados de Lagrange, encontrar el orden de $g(V)$ del conjunto de los números politopos asociados a V y generalizar el Teorema de los números poligonales de Cauchy.

Kim, en su artículo *On regular polytope numbers*, da la siguiente fórmula para el n-ésimo número poligonal de orden k:

$$p_k^2(n) = n + (k-2)\frac{(n-1)n}{2} \quad \text{.....(1)}$$

Por otro lado, como ya se había visto, Nathanson da la siguiente fórmula:

$$p_k(n) = \frac{n(n-1)(k-2)}{2} + n \quad \text{.....(2)}$$

Aunque estas dos fórmulas parezcan distintas, se verá que son equivalentes:

$$(1) = p_k^2(n) = n + (k-2)\frac{(n-1)n}{2} = n + \frac{n(n-1)(k-2)}{2} = p_k(n) = (2).$$

La diferencia entre las notaciones es que Nathanson denota al k-ésimo número poligonal de orden $(m+2)$ como $p_m(k) = \frac{mk(k-1)}{2} + k$, esto lo hace para evitarse escribir $(m-2)$, pero con esta notación se tiene que $p_k(n) = \frac{n(n-1)(k-2)}{2} + n$ es el n-ésimo número poligonal de orden k.

En lo sucesivo se utilizará la siguiente notación:

$\mathbb{Z}^{\geq} \doteq \{n \in \mathbb{Z} / n \geq 0\}$

V (respectivamente V^d) $\doteq$ Un politopo regular (respectivamente de dimensión d) en el espacio Euclidiano.

$V(n) \doteq$ El n-ésimo número politopo asociado a V.

$\partial V(n) \doteq$ El número de puntos en la n-ésima línea en la frontera de V.

$V(n)^{\#} \doteq$ El número de puntos en la n-ésima línea en el interior de V.

1. Construcción de números politopos (regulares)

Lo que hace el autor en esta sección es dar el método para construir la sucesión $\{V(n)/n\in\mathbb{Z}^+\}$ de números politopos (regulares) asociados al politopo regular V y lo hace por inducción.

Convención: $V(0)=0$ y $V(1)=1$.

Esto suena bastante lógico, pues sucede lo mismo para los números poligonales:

$p_k^2(0)=0+(k-2)\dfrac{(-1)(0)}{2}=0+0=0$. Por lo tanto $p_k^2(0)=0$

$p_k^2(1)=1+(k-2)\dfrac{(0)(1)}{2}=1+0=1$. Por lo tanto $p_k^2(1)=1$

La manera de construir los politopos es muy semejante a los polígonos. Se toma el politopo X y se asume que $V(n-1)$ está construido. Se considera el vértice x de X (uno de ellos) y se extiende el extremo de X que contiene a x para formar un politopo regular más grande $\widetilde{X}$ que contiene a x. Después se toma la n-ésima línea de puntos asociados a V en $\widetilde{X}$. En primer lugar la $(n-1)$-ésima línea de puntos en X, después a cada nueva cara k-dimensional de $\widetilde{X}$, $0\le k\le d-1$. Se pone la n-ésima línea de puntos asociados en el correspondiente k-dimensional politopo regular. Por convención, consideramos el n-ésimo 0-dimensional número politopo en el 1, si $n\ge 1$. Finalmente, se cuentan todos los puntos de $\widetilde{X}$ que definen a $V(n)$.

Para continuar con nuestra construcción de números politopos es necesario introducir *el símbolo de Schläfli* denotado por $\{p, q\}$ (para el caso de polígonos regulares) donde p es el número de lados del polígono y q es el número de ellos que concurren en un vértice. El cubo, por ejemplo, es un poliedro regular cuyo símbolo de Schläfli es {4, 3}. Esto mismo se puede hacer con politopos de dimension k, con k un entero positivo.

Teorema de Schläfli: Los únicos posibles símbolos de Schläfli para un politopo regular en el espacio Euclidiano $\mathbb{R}^d$ están dados por la siguiente lista:

$d=2$: $\{n\}$, donde $n\ge 3$ es un entero arbitrario.

$d=3$: $\{3,3\},\{3,4\},\{4,3\},\{3,5\},\{5,3\}$

$d=4$: $\{3,3,3\},\{3,3,4\},\{4,3,3\},\{3,4,3\},\{3,3,5\},\{5,3,3\}$

$d\ge 5$: $\{3^{d-1}\},\{3^{d-2},4\},\{4,3^{d-2}\}$

Además, para cada símbolo en la lista existe un politopo regular con ese símbolo y dos politopos regulares con el mismo símbolo son similares.

A continuación se presenta una serie de tablas en las cuales se dan los politopos más representativos así como la fórmula explícita de los n-ésimos números politopos para los casos de dimensión 3, 4 y d con $d \geq 5$:

Dimensión 3

Nombre del politopo	Símbolo de Schläfli	N_0	N_1	N_2	n-ésimo número politopo
Tetraedro	{3 ,3}	4	6	4	$\frac{1}{6}n(n+1)(n+2)$
Cubo	{4, 3}	8	12	6	n^3
Octaedro	{3, 4}	6	12	8	$\frac{1}{3}n(2n^2+1)$
Dodecaedro	{5, 3}	20	30	12	$\frac{1}{2}n(9n^2-9n+2)$
Icosaedro	{3, 5}	12	30	20	$\frac{1}{2}n(5n^2-5n+2)$

Dimensión 4

Nombre del politopo	Símbolo de Schläfli	N_0	N_1	N_2	N_3	n-ésimo número politopo
5 celdas	{3, 3 ,3}	5	10	10	5	$\frac{1}{4}n(n+1)(n+2)(n+3)$
16 celdas	{3, 3, 4}	8	24	32	16	$\frac{1}{3}n^2(n^2+2)$
Tessaract	{4, 3, 3}	16	32	24	8	n^4
24 celdas	{3, 4, 3}	24	96	96	24	$n^2(3n^2-4n+2)$
600 celdas	{3, 3, 5}	120	720	1200	600	$\frac{1}{6}n(145n^3-280n^2+179n-38)$
120 celdas	{5, 3, 3}	600	1200	720	120	$\frac{1}{2}n(261n^3-504n^2+283n-38)$

Dimensión $d \geq 5$

Nombre del politopo	Símbolo de Schläfli	$N_j \ (0 \leq j \leq d-1)$	n-ésimo número politopo
Simple regular α^d	$\{3^{d-1}\}$	$\binom{d+1}{j+1}$	$\frac{1}{d!}n(n+1)\cdots(n+d-1)$
Cruzado β^d	$\{3^{d-2}, 4\}$	$2^{j+1}\binom{d}{j+1}$	$\sum_{r=0}^{d-1}(-1)^r\binom{d-1}{r}2^{d-1-r}\alpha^{d-r}(n)$
Medible γ^d	$\{4, 3^{d-2}\}$	$2^{d-j}\binom{d}{j}$	n^d

$\alpha^s(n) = \frac{1}{s!}n(n+1)\cdots(n+s-1) = \binom{n+s-1}{s}$, donde $\alpha^s(n)$ es el n-ésimo número simple regular de dimensión s.

En estas tablas se utilizaron los términos N_0, N_1, N_2, ..., N_k. A continuación se definen estos términos:

$N_0 \doteq$ El número de vértices del politopo (dimensión 0)

$N_1 \doteq$ El número de líneas del politopo (dimensión 1)

$N_2 \doteq$ El número de caras del politopo (dimensión 2)

$\vdots$

$N_k \doteq$ El número de caras del politpo ("caras" de dimensión k)

2. Relación entre los números politopos (regulares).

El propósito de esta sección es dar una analogía entre los números politpos cruzados y los números politopos medibles. Para hacer esto, se enuncia (y demuestra) el siguiente Teorema:

Teorema 2.1: Todo número politopo regular de dimensión d puede ser escrito como una combinación lineal de números simples regulares de dimensión d con coeficientes enteros no negativos.

Demostración:

$d=2$; $p_k(n)=p_3(n)+(k-3)p_3(n-1)$, $k\geq 3$

$d=3$;

n-ésimo número cubo $=\alpha^3(n)+4\alpha^3(n-1)+\alpha^3(n-2)$

n-ésimo número octaedro $=\alpha^3(n)+2\alpha^3(n-1)+\alpha^3(n-2)$

n-ésimo número dodecaedro $=\alpha^3(n)+16\alpha^3(n-1)+10\alpha^3(n-2)$

n-ésimo número icosaedro $=\alpha^3(n)+8\alpha^3(n-1)+6\alpha^3(n-2)$

$d=4$;

n-ésimo número $\{3,3,4\}=\alpha^4(n)+3\alpha^4(n-1)+3\alpha^4(n-2)+\alpha^4(n-3)$

n-ésimo número $\{4,3,3\}=\alpha^4(n)+11\alpha^4(n-1)+11\alpha^4(n-2)+\alpha^4(n-3)$

n-ésimo número $\{3,4,3\}=\alpha^4(n)+19\alpha^4(n-1)+43\alpha^4(n-2)+9\alpha^4(n-3)$

n-ésimo número $\{3,3,5\}=\alpha^4(n)+115\alpha^4(n-1)+357\alpha^4(n-2)+107\alpha^4(n-3)$

n-ésimo número $\{5,3,3\}=\alpha^4(n)+45\alpha^4(n-1)+1993\alpha^4(n-2)+543\alpha^4(n-3)$

$d\geq 5$;

Se sabe que $3^d(n)=\sum_{r=0}^{d-1}(-1)^r\binom{d-1}{r}2^{d-1-r}\alpha^{d-r}(n)$. Ahora, nótese que $\alpha^{d-1}(n)=\alpha^d(n)-\alpha^d(n-1)$. Por la aplicación sucesiva de esta relación se obtiene que :

$\alpha^{d-r}(n)=\sum_{i=0}^{r}(-1)^i\binom{r}{i}\alpha^d(n-i)$. Por lo tanto:

$$\begin{aligned}\beta^d(n)&=\sum_{r=0}^{d-1}(-1)^r\binom{d-1}{r}2^{d-1-r}(-1)^i\binom{r}{i}\alpha^d(n-i)\\&=\sum_{i=0}^{d-1}\sum_{r=i}^{d-1}(-1)^r\binom{d-1}{r}2^{d-1-r}(-1)^i\binom{r}{i}\alpha^d(n-i)\\&=\sum_{i=0}^{d-1}a_i\alpha^d(n-i)\end{aligned}$$

Donde $a_i = (-1)^i \sum_{r=i}^{d-1} (-1)^r \binom{d-1}{r}\binom{r}{i} 2^{d-1-r}$.

Ahora se tiene que:

$$\begin{aligned} a_i &= (-1)^i \sum_{r=i}^{d-1} (-1)^r \binom{d-1}{r}\binom{r}{i} 2^{d-1-r} \\ &= (-1)^i \sum_{r=i}^{d-1} (-1)^r \binom{d-1}{i}\binom{d-1-i}{d-1-r} 2^{d-1-r} \\ &= \binom{d-1}{i} \sum_{s=0}^{d-1-i} (-1)^{d-1-i-s} \binom{d-1-i}{s} 2^s = \binom{d-1}{i} \end{aligned}$$

Esto prueba que $\beta^d(n) = \sum_{i=0}^{d-1} \binom{d-1}{i} \alpha^d(n-i)$. □

3. Resultados numéricos.

En esta sección, se dan los datos numéricos del orden de g del conjunto de números politopos (regulares).

Dimensión 3

Símbolo de Schläfli	n-ésimo número politopo	g
{3, 3}	$\frac{1}{6}n(n+1)(n+2)$	5
{4, 3}	n^3	9*
{3, 4}	$\frac{1}{3}n(2n^2+1)$	7
{5, 3}	$\frac{1}{2}n(9n^2-9n+2)$	22
{3, 5}	$\frac{1}{2}n(5n^2-5n+2)$	15

Dimensión 4

Símbolo de Schläfli	n-ésimo número politopo	g
{3, 3 ,3}	$\frac{1}{4}n(n+1)(n+2)(n+3)$	8
{3, 3, 4}	$\frac{1}{3}n^2(n^2+2)$	11
{4, 3, 3}	n^4	19*
{3, 4, 3}	$n^2(3n^2-4n+2)$	28
{3, 3, 5}	$\frac{1}{6}n(145n^3-280n^2+179n-38)$	125
{5, 3, 3}	$\frac{1}{2}n(261n^3-504n^2+283n-38)$	606

Dimensión 5

Símbolo de Schläfli	n-ésimo número politopo	g
{3, 3, 3, 3}	$\frac{1}{5!}n(n+1)(n+2)(n+3)(n+4)$	10
{3, 3, 3, 4}	$\frac{1}{15}n(2n^4+10n^2+3)$	14
{4, 3, 3, 3}	n^5	37*

Dimensión 6

Símbolo de Schläfli	n-ésimo número politopo	g
$\{3^5\}$	$\frac{1}{6!}n(n+1)\cdots(n+5)$	13
$\{3^4, 4\}$	$\frac{1}{45}n^2\left(2n^4+20n^2+23\right)$	19
$\{4, 3^4\}$	n^6	73*

Dimensión 7

Símbolo de Schläfli	n-ésimo número politopo	g
$\{3^6\}$	$\frac{1}{7!}n(n+1)\cdots(n+6)$	15
$\{3^5, 4\}$	$\frac{1}{315}n\left(4n^6+70n^4+196n^2+45\right)$	21
$\{4, 3^5\}$	n^7	143

Los números que tienen * son los que tienen valores exactos:

$g(\{4,3\})=9$ Probado por Wieferich y Kempner.

$g(\{4,3,3\})=19$ Probado por Balasubramanian, Deshouillers y Dress.

$g(\{4,3,3,3\})=37$ Probado por Chen.

$g(\{4,3,3,3,3\})=73$ Probado por Pillai.

Otras Vertientes

Para terminar este capítulo, mostraremos algunas de las vertientes por la que se han dirigido los problemas de Waring, se debe señalar que estos ejemplos corresponden a propuestas hechas en su mayoría en el siglo XX:

1. Se considera escribir números como sumas de potencias de k, pero sólo cuando los números que se utilizan en las sumas son primos. A esta generalización la podríamos llamar *"El Problema Primo de Waring"*. Cuando $k=1$, se obtiene la *Conjetura de Goldbach*. Es decir, ¿cualquier número suficientemente grande puede representarse como la suma de dos o tres primos elevados a la primera potencia? En 1938, Vinogradov demostró que para toda k, existe un entero $V(k)$, tal que todo número suficientemente grande es la suma de $V(k)$ primos elevados a la potencia k. Como ejemplo, se tiene que $38=5^2+3^2+2^2$, donde $k=2$ y cada número que se eleva a la potencia k es primo. Es obvio que no todos los números pueden escribirse en esta forma. Sin embargo, Vinogradov demostró que si se deja que n sea suficientemente grande, entonces todo número mayor que n puede escribirse como la suma de cuadrados de primos. El problema es encontrar $V(2)$, o cuantos cuadrados se necesitan. A esto se le conoce como el *Problema de Waring-Goldbach*.

2. Otra generalización bastante natural es preguntarse: "Si $f(x)$ es un polinomio valuado en enteros que toma el valor de 1, entonces "¿se puede expresar a cada entero como la suma de un número acotado de valores de $f(x)$?". El *Problema clásico de Waring* corresponde al caso cuando $f(x)=x^k$. De cierta manera, este problema tiene su origen en Fermat, quien en 1640 afirmó: "Un entero positivo es triangular o es la suma de dos o tres triangulares; es cuadrado o la suma de 2, 3 ó 4 cuadrados; es pentagonal o la suma de 2, 3, 4 ó 5 pentagonales, etc." Es increíble que este problema también se encuentra en el *Meditationes Algebraicae* apenas precediendo al problema de Waring.
   El problema de Fermat fue resuelto por Cauchy, la prueba es bastante elemental. Kamke dio una solución más general a dicho problema, su argumento está basado en el método de Hilbert. Después, la maquinaria analítica fue aplicada en el problema y un número análogo a $G(k)$ apareció. Hua dio una cota superior de este núme-

ro, con características similares a la estimación de Vinogradov para $G(k)$.

3. Quizás la generalización más natural del problema de Waring es preguntarse sobre campos de números algebraicos o sobre campos arbitrarios. Siegel aborda el problema de campos numéricos. Él demostró que si A_k es un conjunto de enteros algebraicos del campo numérico K en el cual pueden ser escritos como suma de k-ésimas potencias de enteros algebraicos, entonces existe una cota $g(k,K)$ que depende de k y K de tal manera que cada entero $\theta \in A_k$ puede ser escrito de la forma $\theta = \sum_{i=1}^{N} \alpha_i^k$, donde $N \le g(k,K)$ y $\alpha_1,...,\alpha_n$ son enteros algebraicos.

4. Como generalización del problema de Waring en una dirección totalmente opuesta, uno puede tomar una sucesión $n_1 \le n_2 \le ...$ de enteros positivos y preguntarse si todo entero positivo N puede ser escrito de la forma $N = \sum_{i=1}^{r} x_i^{n_i}$, donde r es menor que alguna cota que depende únicamente de la sucesión $\{n_i\}$.
   Resulta que hay una caracterización muy buena de tales sucesiones probada por Scourfield: "Una condición necesaria y suficiente para que exista una cota es que $\sum_{i=1}^{\infty} \frac{1}{n_i} = \infty$."

5. Hay un problema más simple en una pauta similar. Sea $r(n)$ que denota el último entero r tal que la ecuación $N = u_1 + \cdots + u_s$, con $s \le r$, es soluble para todo entero positivo N, donde cada u_i es un entero de la forma x_i^m con $m \ge n$. Pillai mostró que $r(n) \le 2^n + k - 1$ para toda $n \ge 32$, donde $k = \left[\frac{\log l}{\log 2}\right]$ y $l = \left[\left(\frac{3}{2}\right)^k\right]$.

6. Otro problema, conocido como el problema de Waring "más fácil", considera la representación del entero n de la forma $n = \pm x_1^k \pm \cdots \pm x_s^k$. Es bastante fácil probar que existe el análogo de $g(k)$, pero la obtención de una información más exacta es en gran parte un problema sin resolver.

CONCLUSIONES

Como se mencionó en la Introducción, el Teorema 47 —contenido en *Meditationes Algebraicae*— es la parte central del presente trabajo de tesis, sin embargo, a través del capítulo II y III queda la evidencia de que los problemas de Waring no fueron sólo el teorema 47. El trabajo de Waring —por lo menos— en la obra arriba mencionada fue extenso, con temas muy diversos en el campo del álgebra, principalmente en la solución de ecuaciones, pero como ya se mencionó, aquí sólo se abordó el análisis del teorema 47. A lo largo de la tesis quedó de manifiesto que los problemas de dicho teorema aún son vigentes, es frecuente encontrar artículos de investigación en el *Journal of Number Theory* que estudian problemas derivados de los originales de Waring.

En la tesis se presentan soluciones ya existentes, pero rescritas para una mejor comprensión, y en algunos casos la demostración es propia de este trabajo. Es importante señalar que varias de las demostraciones no son únicas, podemos mencionar por ejemplo el famoso artículo de Andrews [1986] para la demostración de la suma de tres números triangulares, o la demostración de Gauss [1801] que da en su *Disquisitiones Arithmeticae*.

Es importante mencionar que la conjetura de Goldbach ha sido también indirectamente una de las difusoras de los problemas de Waring, ello se debe a que es frecuente que cuando se menciona la conjetura de Goldbach se haga en el marco de una discusión de problemas aditivos de la teoría de los números, sin embargo, lo que no se menciona con frecuencia es que la conjetura antedicha es un caso particular de los problemas de Waring, en particular de lo que hoy conocemos como bases clásicas.

Otra línea importante de investigación que no se puede dejar de mencionar es la del estudio de los números politopo, gracias a la investigación de Kim [2002], es importante hacer un alto en el camino del estudio de los problemas aditivos, para mirar las generalizaciones de los números poligonales que nos presenta este autor. Ésta es una de las líneas de investigación en teoría aditiva de los números que vale la pena seguir de cerca por su modernidad.

Otro ejemplo de cómo el trabajo de Waring ha contribuido a la matemática moderna es la demostración del teorema de los cuatro cuadrados de Lagrange (que es un caso particular del Teorema de Hilbert-Waring), la cual da pie a introducir las nociones de bases finitas y bases asintóticas finitas. Nathanson [1996, 2000] rescribe los

problemas de Waring en términos de bases, la cual es una notación mucho más moderna y de esta manera se relaciona la matemática clásica con la actual.

Desde el inicio del trabajo, quedó manifiesto que nunca se tuvo la intención de escribir la vida y obra de Waring, pero sí darlo a conocer, porque es de los personajes poco reconocidos dentro de la matemática, de esta manera esperamos de un panorama global sobre Waring y su libro *Meditationes Algebraicae,* y que así el lector conozca un poco sobre la vida y trabajo de este gran matemático.

APÉNDICE A

Residuos cuadráticos y símbolo de Lagrange

Definición1: Sea $m \in \mathbb{Z}^+$ y a un entero tal que $(a,m)=1$. Entonces a es llamado un *residuo cuadrático de m* si existe un entero x tal que $x^2 \equiv a \pmod{m}$.

Observación: Si $b \equiv a \pmod{m}$ y a es un residuo cuadrático de m, entonces b también es un residuo cuadrático de m.

Teorema 1: Todo primo impar tiene exactamente $\frac{p-1}{2}$ residuos cuadráticos y $\frac{p-1}{2}$ residuos no cuadráticos.

Demostración:

Sea $A=\{1, 2, ..., p-2, p-1\}$ un sistema completo de residuos módulo p un primo impar. Este conjunto puede ser reescrito de la siguiente manera:
$A=\left\{1, 2, ..., \frac{p-1}{2}\right\}\cup\left\{-1, -2, ..., -\frac{p-1}{2}\right\}$. Se sabe que $(1)^2 \equiv (-1)^2 \pmod{p}$, $(2)^2 \equiv (-2)^2 \pmod{p}$, ..., $\left(\frac{p-1}{2}\right)^2 \equiv \left(-\frac{p-1}{2}\right)^2 \pmod{p}$.

Sea n el número de residuos cuadráticos de p, entonces $1 \le n \le \frac{p-1}{2}$. Lo que se quiere demostrar es que $n=\frac{p-1}{2}$.

Tómense dos enteros x y y tales que $x^2 \equiv y^2 \pmod{p}$. Si se demuestra que $x=y$ se obtendría el resultado deseado. Como $x=y$, entonces $p \mid x+y$ ó $p \mid x-y$, esto junto con el hecho de que p es primo se tiene que $1 \le x \le \frac{p-1}{2}$ y $1 \le y \le \frac{p-1}{2}$. Entonces $2 \le x+y \le p-1$, lo cual implica que $p \nmid x+y$, entonces $p \mid x-y$, *i.e.*, $x \equiv y \pmod{p}$, pero como p es primo entonces $x=y$.

Por lo tanto $n=\frac{p-1}{2}$ y así se tiene que p tiene exactamente $\frac{p-1}{2}$ residuos cuadráticos. □

Teorema 2: Si a es un residuo cuadrático modulo p, $(p,a)=1$ y p es un primo impar, entonces $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$.

Demostración:

Como a es un residuo cuadrático (R.C) modulo p, entonces la congruencia $x^2 \equiv a \pmod{p}$ tiene solución.

Como $x^2 \equiv a \pmod{p}$, entonces $\left(x^2\right)^{\frac{p-1}{2}} \equiv a^{\frac{p-1}{2}} \pmod{p}$, lo cual implica que $x^{p-1} \equiv a^{\frac{p-1}{2}} \pmod{p}$, por lo tanto $\left(x^{p-1}, p\right) = \left(a^{\frac{p-1}{2}}, p\right)$. Como $(p,a)=1$, entonces $\left(a^{\frac{p-1}{2}}, p\right)=1$ y $\left(x^{p-1}, p\right)=1$. Así, por el pequeño teorema de Fermat[59] se tiene que $x^{p-1} \equiv 1 \pmod{p}$, pero $x^{p-1} \equiv a^{\frac{p-1}{2}} \pmod{p}$, entonces por transitividad se obtiene que $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$. □

Teorema 3: Sea p un primo impar, si a no es un residuo cuadrático modulo p y $(p,a)=1$, entonces $a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$.

Demostración:

Gracias al Teorema 1, se sabe que el número de R.C contenidos en el sistema completo de residuos modulo p es $\frac{p-1}{2}$, es decir, el número de R.C es el mismo que las soluciones de $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$. Entonces, los R.C agotan todas las soluciones de $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ y no puede tener más de $\frac{p-1}{2}$ soluciones.

[59] Pequeño Teorema de Fermat: Sea p un primo tal que $p \nmid a$, entonces $a^{p-1} \equiv 1 \pmod{p}$.

Como $(p,a)=1$, por el pequeño Teorema de Fermat se tiene que $a^{p-1}\equiv 1 \pmod p$, entonces $\left(a^{\frac{p-1}{2}}-1\right)\left(a^{\frac{p-1}{2}}+1\right)\equiv 0 \pmod p$, de esto se obtiene, $p\left|\left(a^{\frac{p-1}{2}}-1\right)\left(a^{\frac{p-1}{2}}+1\right)\right.$ pero $p\left|\left(a^{\frac{p-1}{2}}-1\right)\right.$ ó $p\left|\left(a^{\frac{p-1}{2}}+1\right)\right.$ y no a ambos, ya que si lo hiciera se tendría que:

$p \mid a^{\frac{p-1}{2}}-1-a^{\frac{p-1}{2}}-1$ y entonces $p \mid -2$, lo cual es imposible pues p es un primo impar. □

Definición: Si p denota a un primo impar y $(p,a)=1$, se define el *símbolo de Legendre* de la siguiente manera:

$$\left(\frac{a}{p}\right)=\begin{cases}1 & \text{si } a \text{ es un residuo cuadrático modulo } p\\ -1 & \text{si } a \text{ no es residuo cuadrático modulo } p\end{cases}$$

Observación: Si $p \mid a$ entonces $\left(\frac{a}{p}\right)=0$.

Teorema 4: Si p es un primo impar y $(a,p)=1=(b,p)$, entonces:

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

2.- $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right)=\left(\frac{ab}{p}\right)$.

3.- Si $a\equiv b \pmod p$, entonces $\left(\frac{a}{p}\right)=\left(\frac{b}{p}\right)$.

4.- a) $\left(\frac{a^2}{p}\right)=1$

b) $\left(\frac{1}{p}\right)=1$

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

5.- $\left(\frac{a^2b}{p}\right)=\left(\frac{b}{p}\right)$.

Demostración:

1.- Por los Teoremas anteriores se tiene que: si a es R.C, entonces $a^{\frac{p-1}{2}}\equiv 1 \pmod p$ y si a no es R.C, entonces $a^{\frac{p-1}{2}}\equiv -1 \pmod p$. Así,

si a es R.C entonces $\left(\frac{a}{p}\right)=1$ y por lo tanto $\left(\frac{a}{p}\right)\equiv a^{\frac{p-1}{2}} \pmod p$, análogamente, si a no es R.C entonces $\left(\frac{a}{p}\right)=-1$ y por lo tanto $\left(\frac{a}{p}\right)\equiv a^{\frac{p-1}{2}} \pmod p$. En ambos casos resulta que $\left(\frac{a}{p}\right)\equiv a^{\frac{p-1}{2}} \pmod p$.

2.- Por el inciso anterior se sabe que $\left(\frac{a}{p}\right)\equiv a^{\frac{p-1}{2}} \pmod p$ y $\left(\frac{b}{p}\right)\equiv b^{\frac{p-1}{2}} \pmod p$. Entonces $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right)\equiv a^{\frac{p-1}{2}} b^{\frac{p-1}{2}} \pmod p$, *i.e.*, $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right)\equiv (ab)^{\frac{p-1}{2}} \pmod p$ y de nuevo por el inciso 1 se obtiene $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right)=\left(\frac{ab}{p}\right) \pmod p$. Si ambos lados de la última congruencia son iguales entonces se obtiene el resultado, pero en caso contrario resulta una contradicción ya que si $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right)=1$ y $\left(\frac{ab}{p}\right)=-1$, entonces se tiene que $1\equiv -1 \pmod p$ lo cual implica que p divide a 2 lo cual es imposible. Por lo tanto $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right)=\left(\frac{ab}{p}\right)$.

3.- Como $a\equiv b \pmod p$, entonces $a^{\frac{p-1}{2}}\equiv b^{\frac{p-1}{2}} \pmod p$, por el inciso 1 se tiene que $\left(\frac{a}{p}\right)\equiv\left(\frac{b}{p}\right) \pmod p$ y haciendo un análisis análogo al realizado en el inciso 2 se obtiene que $\left(\frac{a}{p}\right)=\left(\frac{b}{p}\right)$.

4.- a) Por el inciso 2 se sabe que $\left(\frac{a^2}{p}\right)=\left(\frac{a}{p}\right)\left(\frac{a}{p}\right)$. Por lo tanto $\left(\frac{a^2}{p}\right)=1$.

b) Por 4.a) se tiene que $\left(\frac{1}{p}\right)=\left(\frac{1^2}{p}\right)=1$.

c) Sea $a=-1$, por el inciso 1 se tiene que $\left(\frac{-1}{p}\right)=(-1)^{\frac{p-1}{2}}$.

5.- Por el inciso 2 se tiene que $\left(\frac{a^2b}{p}\right)=\left(\frac{a^2}{p}\right)\left(\frac{b}{p}\right)$ y por 4.a) $\left(\frac{a^2b}{p}\right)=1\left(\frac{b}{p}\right)$. Por lo tanto $\left(\frac{a^2b}{p}\right)=\left(\frac{b}{p}\right)$. □

Teorema 5: Si p es un primo impar entonces se tiene que:

$$\left(\frac{-1}{p}\right)=\begin{cases} 1 \text{ si } p\equiv 1 \pmod 4 \\ -1 \text{ si } p\equiv -1 \pmod 4 \end{cases}$$

Demostración:

Por la propiedad 4.c. del Teorema 4, se sabe que $\left(\frac{-1}{p}\right)=(-1)^{\frac{p-1}{2}}$. Pero $(-1)^{\frac{p-1}{2}}\equiv \pm 1 \pmod p$, entonces $(-1)^{\frac{p-1}{2}}=\begin{cases} 1 \text{ si } \frac{p-1}{2}=2k \text{ p.a. } k\in\mathbb{Z} \\ -1 \text{ si } \frac{p-1}{2}=2k+1 \text{ p.a. } k\in\mathbb{Z} \end{cases}$.

Del hecho de que $\frac{p-1}{2}=2k$, se sigue que $p-1=4k$ lo cual implica que $p=4k+1$, *i.e.*, $p\equiv 1 \pmod 4$. Análogamente, de que $\frac{p-1}{2}=2k+1$ se sigue que $p-1=4k+2$ lo cual implica que $p=4k+3$, *i.e.*, $p\equiv 3\equiv -1 \pmod 4$. Por lo tanto se tiene que:

$$\left(\frac{-1}{p}\right)=\begin{cases} 1 \text{ si } p\equiv 1 \pmod 4 \\ -1 \text{ si } p\equiv -1 \pmod 4 \end{cases}$$

□

Lema de Gauss: Sea p un primo impar y a un entero tal que $(p,a)=1$. Considere los enteros: a, $2a$, $3a$, ..., $\left(\frac{p-1}{2}\right)a$ y sus residuos no negativos modulo p. Si n denota el número de los residuos que exceden a $\frac{p}{2}$, entonces $\left(\frac{a}{p}\right)=(-1)^n$.

Demostración:

Sean $r_1, r_2, ..., r_n$ los residuos que exceden a $\frac{p}{2}$ y $s_1, s_2, ..., s_k$ los residuos que no exceden a $\frac{p}{2}$. Los r_i y s_j son distintos de cero y distintos

entre si[60]. Además se sabe que $n+k=\frac{p-1}{2}$, $0<p-r_i<\frac{p}{2}$ para $i=1,...,n$, los $p-r_i$ son distintos y ninguno de los $p-r_i$ es igual a un s_j, esto es ya que:

Sea $r_i \equiv \rho a \pmod p$ y $s_j \equiv \sigma a \pmod p$; donde $1 \le \rho,\sigma \le \frac{p-1}{2}$. Por lo tanto si se supone que $p-r_i=s_j$, entonces $p-r_i \equiv p-\rho a \pmod p$, *i.e.*, $s_j \equiv p-\rho a \pmod p$. Lo cual implica que $\sigma a \equiv p-\rho a \pmod p$, entonces $\sigma a+\rho a \equiv p \pmod p$. Por lo tanto $p \mid \sigma a+\rho a = a(\sigma+\rho)$, pero $(p,a)=1$ entonces $p \mid \sigma+\rho$ y por otro lado, como $\sigma+\rho \le p-1$ y p es primo entonces $p \nmid \sigma+\rho$ lo cual es una contradicción. Por lo tanto, ninguno de los $p-r_i$ es igual a un s_j y son todos (los $p-r_i$ y los s_j) por lo menos 1 y menos que $\frac{p}{2}$ y en número son $n+k=\frac{p-1}{2}$. Con todo esto, se puede afirmar que existen solamente los enteros 1, 2, 3, ..., $\left(\frac{p-1}{2}\right)$ en algún orden.

Ahora, $(p-r_1)\cdots(p-r_n)\cdot s_1\cdots s_k=\left(\frac{p-1}{2}\right)!$, pero $(p-r_1)\equiv -r_1 \pmod p$ entonces se tiene que $(p-r_1)\cdots(p-r_n)\equiv(-r_1)\cdots(-r_n)\pmod p$, entonces se da la congruencia $(p-r_1)\cdots(p-r_n)\cdot s_1\cdots s_k \equiv (-r_1)\cdots(-r_n)\cdot s_1\cdots s_k \pmod p$, lo cual implica que

$(-r_1)\cdots(-r_n)\cdot s_1\cdots s_k \equiv \left(\frac{p-1}{2}\right)! \pmod p$. De esta manera, resulta que

$(-1)^n r_1\cdots r_n\cdot s_1\cdots s_k \equiv 1\cdot 2\cdots\frac{p-1}{2}\pmod p$, pero,

$a\cdot 2a\cdots\left(\frac{p-1}{2}\right)a \equiv r_1\cdots r_n\cdot s_1\cdots s_k \pmod p$, entonces

$(-1)^n a\cdot 2a\cdots\left(\frac{p-1}{2}\right)a \equiv (-1)^n r_1\cdots r_n\cdot s_1\cdots s_k \pmod p$ y por lo tanto resulta que $(-1)^n a^{\frac{p-1}{2}}\cdot 1\cdot 2\cdots\left(\frac{p-1}{2}\right)\equiv 1\cdot 2\cdots\left(\frac{p-1}{2}\right)\pmod p$.

---

[60] Supongamos que $Ka=pq+r$ y $\Gamma a=p\lambda+r$, entonces $Ka-\Gamma a=pq-p\lambda$. Por lo tanto $a(K-\Gamma)=p(q-\lambda)$, pero $(p,a)=1$, entonces $p \mid K-\Gamma$ pero $K, \Gamma \le \frac{p-1}{2}$. Así $p \nmid K-\Gamma$ lo cual es imposible. Por lo tanto Ka y Γa tienen residuos distintos.

Como p es un primo impar, se tiene que $\left(1\cdot 2\cdots\left(\frac{p-1}{2}\right), p\right)=1$, entonces resulta que $(-1)^n a^{\frac{p-1}{2}} \equiv 1 \pmod p$ o lo que es lo mismo $(-1)^n(-1)^n a^{\frac{p-1}{2}} \equiv (-1)^n \pmod p$. Por lo tanto $a^{\frac{p-1}{2}} \equiv (-1)^n \pmod p$.

Entonces, si se utiliza el inciso 1 del Teorema 4 se tiene que $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod p$ y por otra parte $a^{\frac{p-1}{2}} \equiv (-1)^n \pmod p$. Entonces $\left(\frac{a}{p}\right) \equiv (-1)^n \pmod p$. Por lo tanto $\left(\frac{a}{p}\right) = (-1)^n$. □

Corolario: Sea p un primo impar y $(p,a)=1$. Sea n que denota el número de residuos (los menores positivos) de $a, 2a, 3a, \ldots, \left(\frac{p-1}{2}\right)a$ que exceden a $\frac{p}{2}$. Entonces $\left(\frac{a}{p}\right)=1$ si y solo si n es par.

Teorema 6: Sea p un primo impar, entonces se tiene que:

$$\left(\frac{2}{p}\right) = \begin{cases} 1 \text{ si } p \equiv \pm 1 \pmod 8 \\ -1 \text{ si } p \equiv \pm 3 \pmod 8 \end{cases}$$

Demostración:

Gracias al Lema de Gauss se sabe que $\left(\frac{2}{p}\right) = (-1)^v$ y $v = \frac{p-1}{2} - \left\lfloor \frac{p}{4} \right\rfloor$.

Caso 1.- Si $p \equiv 1 \pmod 8$

Como $p \equiv 1 \pmod 8$, entonces $p = 8k+1$ para algún entero k. De esta manera se tiene que $v = \frac{8k+1-1}{2} - \left\lfloor \frac{8k+1}{4} \right\rfloor = 4k - 2k = 2k$, por lo tanto $v = 2k$ es un número par.

Por lo tanto $\left(\frac{2}{p}\right) = (-1)^{2k} = 1$.

Caso 2.- Si $p \equiv -1 \pmod 8$

Como $p \equiv -1 \pmod 8$, entonces $p = 8k-1$ para algún entero k. De esta manera se tiene que $v = \frac{8k-1-1}{2} - \left\lfloor \frac{8k-1}{4} \right\rfloor = 4k-1-(2k-1) = 2k$, por lo tanto $v = 2k$ es un número par. Por lo tanto $\left(\frac{2}{p}\right) = (-1)^{2k} = 1$.

Caso 3.- Si $p \equiv 3 \pmod 8$

Como $p \equiv 3 \pmod 8$, entonces $p = 8k+3$ para algún entero k. De esta manera se tiene que $v = \frac{8k+3-1}{2} - \left\lfloor \frac{8k+3}{4} \right\rfloor = 4k+1-2k = 2k+1$, por lo tanto $v = 2k+1$ es un número impar. Por lo tanto $\left(\frac{2}{p}\right) = (-1)^{2k+1} = -1$.

Caso 4.- Si $p \equiv -3 \pmod 8$

La demostración es análoga a la de los tres casos anteriores.

Por lo tanto

$$\left(\frac{2}{p}\right) = \begin{cases} 1 \text{ si } p \equiv \pm 1 \pmod 8 \\ -1 \text{ si } p \equiv \pm 3 \pmod 8 \end{cases}$$

□

Ley de reciprocidad cuadrática de Gauss: Sean p y q dos primos impares distintos, entonces $\left(\frac{p}{p}\right)\left(\frac{q}{p}\right) = (-1)^{\left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right)}$.

Demostración:

Sean $r_1, r_2, ..., r_k$ los residuos modulo p (positivos mínimos) de los enteros $q, 2q, ..., \frac{p-1}{2}q$ y que son menores que $\frac{p}{2}$ y sean $s_1, s_2, ..., s_v$ los residuos que exceden a $\frac{p}{2}$. Entonces $k+v = \frac{p-1}{2}$ y por el Lema de Gauss se tiene que $\left(\frac{q}{p}\right) = (-1)^v$.

En la demostración del Lema de Gauss se estableció que los $\frac{p-1}{2}$ enteros $(r_1, r_2, ..., r_k, p-s_1, ..., p-s_v)$ son una permutación de los enteros $1,..., \frac{p-1}{2}$, entonces

$\sum_{i=1}^{k} r_i + \sum_{i=1}^{v} p - s_i = \sum_{k=1}^{\frac{p-1}{2}} k = 1+2+...+\frac{p-1}{2} = \frac{\frac{p-1}{2}\cdot\frac{p+1}{2}}{2} = \frac{p^2-1}{8}$. Por lo tanto $\sum_{i=1}^{k} r_i + vp - \sum_{j=1}^{v} s_j = \frac{p^2-1}{8}$. Únicamente por comodidad, se escribe $R = \sum_{i=1}^{k} r_i$ y $S = \sum_{j=1}^{v} s_j$. Entonces se tiene que:

$$\frac{p^2-1}{8} = R + vp - S \quad ...(1)$$

Regresando a los kq, $\left(q, 2q, ..., \frac{p-1}{2}q\right)$ donde $1 \le k \le \frac{p-1}{2}$, se tiene que: $\left\lfloor \frac{kq}{p} \right\rfloor$ denota la parte entera de la división de kq entre p. Se denotará por tk al residuo de $\frac{kq}{p}$ con $0 \le tk \le p$. Con estos datos se obtiene que:

$kq = \left\lfloor \frac{kq}{p} \right\rfloor \cdot p + tk$, entonces $\sum_{k=1}^{\frac{p-1}{2}} kq = \sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{kq}{p} \right\rfloor \cdot p + \sum_{k=1}^{\frac{p-1}{2}} tk$, de esta manera, se tiene que $q\sum_{k=1}^{\frac{p-1}{2}} k = pS'(p,q) + R + S$; donde $S'(p,q)$ es el número de los enteros que están por debajo de la recta $y = \frac{kq}{p}$. De esta manera resulta

$$q\left(\frac{p^2-1}{8}\right) = pS'(p,q) + R + S \quad ...(2).$$

Restando las ecuaciones (1) y (2) se obtiene:

$(q-1)\left(\frac{p^2-1}{8}\right) = p\left(S'(p,q) - v\right) + 2S$, entonces $\left(S'(p,q) - v\right)$ es un número par. Por lo tanto $(-1)^{S'(p,q)-v} = 1$, *i.e.*, $(-1)^{S'(p,q)} \cdot (-1)^{-v} = 1$. Por lo tanto $(-1)^{S'(p,q)} = (-1)^{-v}$. Pero se tenía que $\left(\frac{q}{p}\right) = (-1)^{v}$, entonces $\left(\frac{q}{p}\right) = (-1)^{S'(p,q)}$ y en forma similar se obtiene que $\left(\frac{p}{q}\right) = (-1)^{S'(q,p)}$. Por lo tanto $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{S'(q,p)+S'(p,q)}$.

De esta manera[61] resulta que $\left(\frac{p}{p}\right)\left(\frac{q}{p}\right)=(-1)^{\left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right)}$. □

Corolario: Sean p y q primos impares distintos, entonces:

$$\left(\frac{q}{p}\right)=\begin{cases}\left(\frac{p}{q}\right) & \text{si } p\equiv 1 \text{ ó } q\equiv 1 \pmod 4\\ -\left(\frac{p}{q}\right) & \text{si } p\equiv 3\equiv q \pmod 4\end{cases}$$

Demostración:

Si $p\equiv 1 \pmod 4$, entonces $4\mid p-1$. Como $(p-1)$ es par, entonces $\frac{p-1}{2}$ es par y de esta manera se tiene que $\frac{p-1}{2}\cdot\frac{q-1}{2}$ es un número par. Por la ley de reciprocidad cuadrática se sabe que $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right)=(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}=1$, entonces, como $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right)=1$ y $\left(\frac{p}{q}\right)=\pm 1=\left(\frac{q}{p}\right)$. Por lo tanto $\left(\frac{p}{q}\right)=\left(\frac{q}{p}\right)$. Análogamente si $4\mid q-1$.

Ahora, se analizará cuando $p\equiv q\equiv 3 \pmod 4$. Si $p\equiv 3 \pmod 4$ entonces $4\mid p-3$, $p-3=4\lambda$ y $\frac{p-3}{2}=2\lambda$ para alguna $\lambda\in\mathbb{Z}$. Por lo tanto $\frac{(p-1)-2}{2}=2\lambda$, lo cual implica que $\frac{p-1}{2}=2\lambda+1$, *i.e.*, $\frac{p-1}{2}$ es un número impar. Análogamente se llega a que $\frac{q-1}{2}$ es impar. Por lo tanto $\left(\frac{p-1}{2}\cdot\frac{q-1}{2}\right)$ es un número par.

Ahora bien, por la ley de reciprocidad cuadrática se sabe que $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right)=(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}=-1$. Por lo tanto $\left(\frac{q}{p}\right)=-\left(\frac{p}{q}\right)$. □

---

[61] Gracias al siguiente resultado: Sean p y q primos impares distintos. Entonces:

$$\sum_{k=1}^{\frac{p-1}{2}}\left\lfloor\frac{kq}{p}\right\rfloor+\sum_{k=1}^{\frac{q-1}{2}}\left\lfloor\frac{kp}{q}\right\rfloor=\frac{p-1}{2}\cdot\frac{q-1}{2}$$

BIBLIOGRAFIA

Andrews, George E. 1986. " EYPHKA! num = Δ+Δ+Δ". Journal of number theory, 23: 285-293.

Clawson, Calvin C. 1999. "Misterios matemáticos". Editorial Diana, México.

Dickson, Leonard Eugene 1927. "History of the Theory of Numbers". Carnegie Institute of Washington, Washington: 1919.

Dickson, Leonard Eugene 1939. "All integers except 23 and 239 are sums of 8 cubes". Bull. American Mathematical Society. Vol. 45. Páginas: 588-591.

Dickson, Leonard Eugene 1952. "History of the Theory of Numbers". Tres volúmenes. New York: Chelsea.

Euclides 1994. "Elementos". Traducción y notas de María Luisa Puertas Castaños. Madrid: Gredos.

Gauss, Carl Friedrich 1801. "Disquisitiones Arithmeticae". Traducido por Arthur A. Clarke. Yale University press: 1996.

Grosswald, Emil 1984. "Representations of integers as sum of squares". New York: Springer-Verlag.

Lalande, 1776. "Una notice sur la vie de cocorcet". Contenido en: Mercure de France, 20 de enero de 1796. Pág. 143

Loo, Hua Keng 1982. "Introduction to Number Theory". New York: Springer-Verlag.

Hutton, Charles 1815. "A Philosophical and Mathematical Dictionary". Londres: imprso por el autor y Simpkin y Marshall.

Kim, Hyun Kwang 2002. "On regular polytope numbers". Proceedings of the American Mathematical Society, volumen 131, número 1, páginas 65-75. Artículo electrónico publicado el 12 de junio de 2002.

Nathanson, Melvyn 1996, "Additive number theory the classical bases". New York: Springer-Verlag.

Nathanson, Melvyn 2000. "Elementary Methods in Number Theory". New York: Springer-Verlag.

Pepin, T. 1892-93. "Démonstration du théoreme de Fermat sur les nombres polygones". Atti. Accad Pont. Nuovi Lincei, 46: 1892-93.

Powell, W.S. 1760. "Observations on the first chapter of a book called Miscellanea Analytica". Londres: Impreso por T. Mernl.

Ribenboim, Paulo 1989. "The new Book of Prime Number Records". New York: Springer-Verlag.

Scott J.F. † 1976. "Dictionary of scientific biography" Vol. XIV, Pág.179-181 Colección editada por Charles Coulston Gillispie. Princeton University.

Waring, Edward 1762. "Miscellanea Analytica, de Aequationibus Albebraicis et Curvarum Proprietatibus". Cantabrigiae: Typis academicis excudebat J. Bentham.

Waring, Eward 1772. "Proprietates Algebraicarum Curvarum". Cantabrigiae: Typis academicis excudebat J. Archdeacon, veneunt apud J. Woodyer.

Waring, Eward 1776. "Meditationes Analyticae". Segunda edición. Cantabrigiae: Typis academicis excudebat J. Archdeacon, veneunt apud J. Nicholson.

Waring, Edward 1782, "Meditationes Algebraicae". Traducción de Dennis Weeks en 1991. Rhode Island: American Mathematical Society.