UNIVERSIDAD NACIONAL AUTÓNOMA

DE MÉXICO

FACULTAD DE CIENCIAS

Origen y primeros problemas de la teoría aditiva de los números

TESIS

QUE PARA OBTENER EL TÍTULO DE:

Matemático

PRESENTA:

José Luis Ramírez Alatriste

DIRECTOR DE TESIS:

Mat. Julio César Guevara Bravo

2015

Ciudad Universitaria, D. F.

Datos

1. Datos del alumno
   Ramírez
   Alatriste
   José Luis
   5532735048
   Universidad Nacional Autónoma de México
   Facultad de Ciencias
   Matemáticas
   407075401
2. Datos del tutor
   Mat.
   Julio César
   Guevara
   Bravo
3. Datos del sinodal 1
   Dra.
   María del Carmen Heréndira
   Gómez
   Laveaga
4. Datos del sinodal 2
   M. en C.
   José Antonio
   Gómez
   Ortega
5. Datos del sinodal 3
   M. en C.
   José Rafael
   Martínez
   Enríquez
6. Datos del sinodal 4
   Mat.
   Anayanzi Delia
   Martínez
   Hernández
7. Datos del trabajo escrito
   Origen y primeros problemas de la teoría aditiva de los números
   88 p.
   2015

Agradecimientos

Esta parte me resulta tan especial y es que hay tanta gente a quien agradecer. No existe otra palabra como ***gracias*** para agradecer a todas aquellas personas que me han brindado su apoyo incondicional.

En primer lugar y desde mi más profundo ser, quiero agradecer a mis queridos padres que me brindaron su apoyo infinito con todo su corazón y que siempre se los voy agradecer inmensamente.

A mi padre, por ser un ejemplo para mí y mis hermanos, además de ser una de las personas a la cual admire por esa enorme inteligencia y que me dijo que estudiara desde muy pequeño. Aunque físicamente ya no está presente, sé que le hubiera encantado estar conmigo en estos momentos.

A la mujer más importante en mi vida, mi madre, por haberme apoyado en los malos momentos de la vida, por tenerme mucha paciencia y sobre todo por confiar en mí todo el tiempo.

A mis hermanos Luis Alfonso, Edgar, Alberto y Angelito, por estar siempre conmigo.

A toda mi demás familia, tíos, tías, y primos.

A mis tíos, Elena y Samuel por haberme dado un lugarcito en su casa y que me brindaron su apoyo de todo corazón.

A mis primos Jorge y Claudia por haberme soportado tanto tiempo, jejeje. Espero demostrarles todo el agradecimiento que les tengo por todo este tiempo de apoyo.

Y por último a mi asesor Julio César Guevara, por su gran paciencia, ayuda y sus enormes contribuciones para que este trabajo saliera adelante.

Solo me queda agradecer a la vida por haberme puesto en el camino a tan enormes y buenas personas. ***MUCHAS GRACIAS!***

Índice general

Introducción

Desde épocas remotas de la civilización uno de los intereses del hombre ha sido el de los números, y una de las razones para ocuparse en ellos fue para dar solución a las necesidades y a los problemas prácticos de la vida diaria. Bajo este contexto el primer concepto que sería importante abordar tendría que ser el de número; sin embargo la concepción de número trae consigo una multitud de significados si nos extendemos hacia disciplinas diversas como la filosofía. En el caso de las matemáticas, y en particular en lo que se refiere la teoría de números tenemos un sin fin de resultados, y esto se debe a que en esta rama se estudian las propiedades de los números y no el concepto mismo. De esta manera las propiedades del número le dan a dicha concepción un enfoque más matemático.

La teoría de números es sin duda una de las áreas de la matemática más antiguas. Sabemos que desde la época de oro de la matemática griega ya se manejaban conceptos básicos de lo que hoy conocemos como teoría de números,[1] y es sobresaliente que éstos son los que se usan actualmente en un primer curso de esta materia.

Ahora bien, así como la matemática se ha divido en muchas ramas, la teoría de números también lo ha hecho. Una de estas áreas, y de la que se desprende este trabajo, es la teoría aditiva de los números; en ella se tienen muchos teoremas, pero entre ellos existen los que son poco conocidos, y otros que si son muy identificados por la fama que han logrado. Se sabe que los babilónicos y otras culturas ya conocían lo que después se llamó ternas pitagóricas,[2] y lo mencionamos porque esto ya recae dentro de la teoría aditiva de los números (nos referiremos a la disciplina como TAN). Más aún, Euclides ya conocía las fórmulas para encontrar a todas las ternas, por lo que esta subrama es igual de antigua que la teoría de números.

Tal pareciera que los libros aritméticos de Euclides nos dan una primera base axiomática de la teoría aditiva de los números, pero realmente ésta llegó hasta el siglo XVII, con la *Aritmética* de Diofanto y con las observaciones de Fermat. Varias de estas observa-

[1] Los libros VII – lX de los *Elementos* de Euclides nos muestran el interés que tenían los griegos por entender a los números.
[2] Véase Carrera, Josep [2009], pp. 139-144.

ciones hoy son problemas aún vigentes en la ciencia matemática y que recaen dentro de la TAN.

Los problemas (*teoremas*) que se estudian en este trabajo, y que pertenecen a la TAN, son principalmente de Waring, para los casos de cuadrados y cubos, y cuyas soluciones hacen honor a los matemáticos que intervinieron en ella.

Esta tesis inicia con los antecedentes históricos de la TAN que datan desde tiempos pitagóricos y llegan hasta Lagrange; esto dará la base para encontrar la solución del teorema de Waring para el caso de cuadrados.[3]

De manera general, este trabajo contiene los orígenes y los primeros problemas de la TAN pero escritos con la notación actual para que el lector pueda tener una lectura más fluida. Dejamos claro desde un principio que este trabajo no es una introducción a la TAN, pues no se abordan muchos de los temas que se necesitan y que forman parte de los contenidos de esta subrama; más bien se abordan todos los resultados que son necesarios para demostrar los teoremas antes mencionados, y que en general se encuentran separados en distintos libros y artículos. Se pasa en seguida a resumir los contenidos de cada capítulo

El **capítulo 1**, que trata los *Antecedentes históricos*, aquí proporcionamos algunos resultados particulares y otros generales concernientes a números cuadrados. Este capítulo nos brinda la cadena de los problemas de números cuadrados desde la época de oro de la matemática griega hasta la obra de Diez Freyle, titulada *Sumario Compendioso*, publicada en 1556.[4]

En el **capítulo 2** se demuestran y explican los resultados concernientes a la suma de dos, tres y cuatro cuadrados; el último resultado corresponde al *teorema de Lagrange*.

Por último, el objetivo principal del **capítulo 3** es demostrar el *teorema de Wieferich-Kempner*, que trata sobre la suma de cubos y cuya prueba conlleva algunos resultados previos incluyendo detalles de dos artículos publicados por L.E. Dickson en 1928 y 1935. Y al final se muestran algunas líneas del trabajo actual sobre algunas potencias mayores a las de cuadrados y cubos.

[3] Todo número entero positivo es suma de cuatro cuadrados.
[4] Esta obra titulada *Sumario Compendioso* [facsimilar, 2008], fue la primera obra de carácter científico que se publicó en América (1556), por Juan Díez Freyle.

Capítulo 1

Antecedentes históricos

La suma de cuadrados es un problema de interés centenario

Dentro de la teoría de los números la suma de cuadrados es de los primeros problemas que aborda el tema de la representación de un entero como suma de otros enteros, es decir, podríamos pensar que aquí inicia la teoría aditiva de los números, esto ha generado gran interés desde la época de oro de la matemática griega. Este tema se abordó principalmente desde la perspectiva de los números poligonales y fue Diofanto (siglo II d. C), en su *Aritmética*, que planteó diversas situaciones que involucraban a los números cuadrados. Pero es importante señalar que este conocimiento que aportó Diofanto no regresó directamente (a través de su obra) a Occidente en una etapa temprana del siglo XVI; lo que sucedió es que la teoría de los números cuadrados llegó a Occidente a través de otros autores correspondientes al bajo Medioevo y a la segunda mitad del siglo XV.

Una explicación de porqué no fue conocida su obra en el pleno despegue de la matemática a partir de la segunda mitad del siglo XVI, tiene que ver con que no se conoció directamente en ese siglo. Se sabe que la obra de Diofanto fue estudiada desde el siglo X por Abu Al-Wafa (segunda mitad del siglo X), y que Qusta-ben-Luqa-al-Balabakki escribió comentarios a la *Aritmética*.[5] El problema histórico que de inmediato se hace patente es que las obras árabes de la edad media que trataron estos temas prácticamente no fueron conocidas en Europa durante el siglo XVI, sólo se sabía de su existencia por listados que se encontraron en esa época.

Una de las aportaciones históricas más importantes sobre números cuadrados que se dio en el siglo XIII fue el *Liber Quadratorum* (*Libro de los números cuadrados*) de Leonardo de Pisa, conocido como Fibonacci. Esta obra fue escrita en 1225, las copias fueron escasas y

[5] Para más información sobre las obras de estos autores, véase Suter [1892] y [1890].

su difusión por el territorio europeo no le fue favorable en su época.[6] Las características propias de la obra la colocan dentro de un tipo de matemática que no se aplicaba directamente al comercio y por ello rápidamente quedó en desuso. Fue hasta 1799 que Pietro Cossali revivió a los números cuadrados de Fibonacci con motivo de un estudio que realizó acerca de los progresos del álgebra en Italia.[7]

Aún nos queda una vía para tratar de saber cómo llegaron los números cuadrados a los lectores del siglo XV. Esta opción consiste en revisar las *Aritméticas* que se publicaron en la segunda mitad del siglo XV y en las primeras décadas del XVI. Para esto la referencia obligada y el personaje que primero acude a la memoria es Luca Pacioli de Borgo Sansepolcro y su *Summa Arithmetica*. La obra se publicó por primera vez en 1494 y más tarde, en 1509, se imprimió su *Opere matematiche* (Venecia), la cual incluía a la *Summa*.

La obra de Pacioli contiene la justificación del estudio de los números cuadrados; allí define y añade propiedades de ellos y todo esto lo acompaña con diversos ejemplos.[8] Antes de que Pacioli se adentrara en los resultados importantes advierte al lector de la existencia de la obra de Fibonacci como fuente histórica.

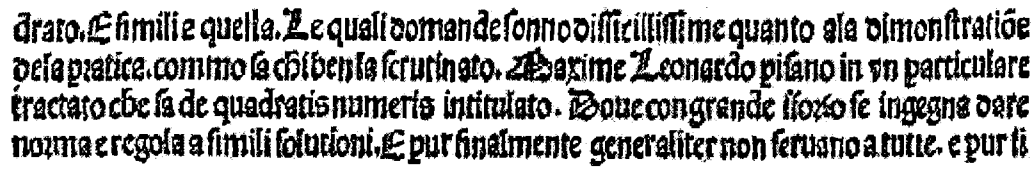

drato. E fimili e quella. Le quali domande fonno difficillifime quanto ala dimonftratiõe
dela pratica, commo fa chi bene fa ferutinato. Maxime Leonardo pifano in vn particulare
tractato che fa de quadratis numeris intitulato. Doue con grande ſforzo ſe ingegna dare
norma e regola a fimili ſolutioni. E pur finalmente generaliter non ſeruano a tutte. e pur ſi

Figura 1: Referencia en la *Summa Arithmetica* a Fibonacci.

En este contexto histórico cabe mencionar que las inquietudes matemáticas en México de mediados del siglo XVI sí incluyeron a los números cuadrados. En 1556 Juan Diez Freyle [2008] publicó una obra con el título *Sumario Compendioso*. El trabajo contiene una parte de problemas *"reservados al álgebra"* y en ellos se aborda la cuestión de los números cuadrados.[9] Diez Freyle no ofrece referencias de los autores cuyas obras pudo haber consultado, pero estudios recientes[10] nos permiten pensar que el *Libro de los números cuadrados* sí marcó el camino del *Sumario*, si bien no lo hizo directamente, esto se dio a través de Pacioli. Si

[6] Es importante señalar que aunque el *Liber Quadratorum* fue la última obra que escribió Fibonacci, en su *Liber Abaci* ya enuncia algunos problemas de cuadrados (véase el capítulo 14 (pág. 548) de la edición de Sigler [2002]).
[7] Consultar Cossali [1799].
[8] Véase Pacioli, Luca [1494], versión electrónica de la biblioteca virtual Miguel de Cervantes.
[9] Véase *Sumario compendioso* [2008], p. 70.
[10] Ver el estudio matemático que se presenta en la edición del *Sumario* [Diez 2008].

comparamos el contenido del *Sumario* con las obras de Pacioli y Fibonacci encontramos que en el tema de los números cuadrados existe la posibilidad de una cadena de influencias Diofanto –Fibonacci– Pacioli que finalmente alcanza a Diez Freyle.

Pasamos ahora a la revisión de algunos problemas representativos de los autores mencionados en los párrafos anteriores.

Problema a)

Este problema plantea la solución simultánea de dos ecuaciones: se requiere encontrar un número X que al sumarle 15 dé como resultado un cuadrado, y que por otro lado, al restarle 4 genere otro cuadrado diferente al anterior. Esto es, se tiene que resolver el sistema

$$X + 15 = s^2$$
$$X - 4 = r^2.$$

En el *Sumario* el problema se aborda de manera insuficiente.[11] Por un lado se resuelve sólo para un caso particular, y cuando presenta la regla de solución no abre al lector la posibilidad de poder enfrentar problemas semejantes, es decir, no ofrece un camino para extraer una regla general.

Se puede ver que la solución se enmarca en la técnica que usa Fibonacci para resolver el problema IV de su *Libro de los números cuadrados*,[12] por ello aquí se resolverá el problema del *Sumario*, pero a través de la matemática de Fibonacci.

Solución

A las ecuaciones $X + 15 = s^2$ y $X - 4 = r^2$, réstese la segunda ecuación de la primera para obtener $19 = s^2 - r^2$; gracias a Euclides se sabía que $19 = (s + r)(s - r)$, por lo que se puede descomponer el producto en dos igualdades $(s + r) = 19$ y $(s - r) = 1$; se suman ambas para obtener $2s = 20$, y por tanto $s = 10$. Ya que se obtiene *s* se sustituye en la primera ecuación y resulta que $X + 15 = 10^2$, o lo que es lo mismo, $X = 100 - 15$. Así que $X = 85$, y también satisface la segunda ecuación.

Si se compara esta solución con la del *Sumario*, se verá que se sigue el mismo método, pero Diez no lo dice, y sólo se limita a describir las operaciones aritméticas del caso particular.

[11] Véase *Sumario* [Diez, 2008].
[12] Libro de los números cuadrados [Ver Eecke, 1973], pp. 39-44.

El caso general sería el de encontrar un número X que al sumarle A y restarle B genere cuadrados diferentes:

$$X + A = s^2$$
$$X - B = r^2.$$

El método general, extraído del procedimiento de Fibonacci, sería el siguiente: restar la segunda ecuación de la primera: $A + B = s^2 - r^2 = (s + r)(s - r)$.

Partir los productos y generar dos igualdades, que si se multiplican miembro a miembro generan la igualdad anterior:

$$A + B = (s + r)$$

$$1 = (s - r).$$

Se suman ambas igualdades y se despeja *s*, obteniéndose $s = \left(\frac{A + B + 1}{2}\right)$.

Finalmente se sustituye *s* en la primera ecuación para obtener[13] $X = \left(\frac{A + B + 1}{2}\right)^2 - A$,

y cuyo resultado también satisface a $X - B = r^2$.

Es importante señalar que la solución de este tipo de problemas que se presentan en el *Sumario* es para números enteros, y que si la suma de los términos A y B es par, entonces la expresión $\left(\frac{A + B + 1}{2}\right)$ no es un entero y en este se obtendrán soluciones fraccionarias.[14]

Las ternas pitagóricas

Ahora presentamos un problema sobre ternas pitagóricas. Se pide encontrar *a* y *b* tales que $a^2 + b^2 = r^2$, donde ya se conoce la terna $x^2 + y^2 = r^2$ (en ambas está *r*). Este problema se encuentra en el *Sumario* y es interesante ver cómo se usa la teoría de proporciones para encontrar la solución, y aunque aquí no es explícito el uso de esta herramienta, sí lo es en el problema III del *Libro de los números cuadrados*.[15]

[13] Cabe señalar que la solución también se puede obtener restando las ecuaciones $A + B = (s + r)$ y $1 = (s - r)$, (la segunda de la primera).

[14] Por ejemplo si A = 7, B = 5 $\Rightarrow X = \frac{141}{4}$, $s = \left(\frac{13}{2}\right)^2$ y $r = \left(\frac{11}{2}\right)^2$.

[15] *Libro de los números cuadrados* [Ver Eecke, 1973], pp. 36-39.

Fibonacci usará las siguientes proporciones entre los triángulos rectángulos que aparecen en la figura 2.

$\frac{ZL}{ZD} = \frac{ZM}{ZE}$ y $\frac{ZL}{ZD} = \frac{LM}{DE}$.

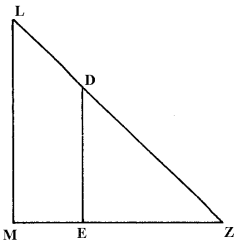


Figura 2

En la solución del *Sumario* se usa como el triángulo conocido el de lados X, Y, 8 (figura 3) que satisface la ecuación $X^2 + Y^2 = 8^2$; después, para encontrar un triángulo que tenga la misma hipotenusa se propone usar como triángulo auxiliar a $3^2 + 4^2 = 5^2$. Con ambas ternas pitagóricas se construye el triángulo de lados $\Delta XY8$ (con hipotenusa 8), y en su interior el de lados $\Delta 3, 4, 5$ (con hipotenusa 5). Por lo tanto, de las proporciones de Fibonacci se tiene que:

$$\frac{8}{5} = \frac{X}{3} \Rightarrow X = \frac{8\times 3}{5} = 4\tfrac{4}{5}$$

$$\frac{8}{5} = \frac{Y}{4} \Rightarrow Y = \frac{8\times 4}{5} = 6\tfrac{2}{5}$$

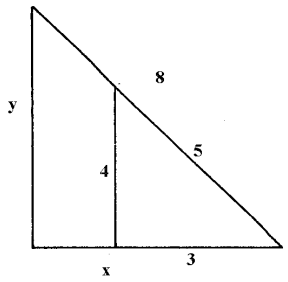


Figura 3

y como el triángulo de lados X, Y, 8 es rectángulo, entonces $\left(6\frac{2}{5}\right)^2 + \left(4\frac{4}{5}\right)^2 = 8^2$. Así, lo que obtenemos es un triángulo de lados diferentes al auxiliar, pero con la misma hipotenusa.

En el problema que sigue se pide resolver una suma de cuadrados conociendo previamente una solución, esto es, se pide encontrar valores para X, Y tales que $X^2 + Y^2 = 5^2$, sabiendo que $3^2 + 4^2 = 5^2$.

La solución del problema — que se presenta tanto en el *Sumario* como en la *Summa* (foja 17) — encierra nuevamente elementos euclidianos de la teoría de proporciones. Este problema es semejante al anterior y en ambos se usan proporciones entre triángulos rectán-

gulos. De igual manera, Fibonacci lo hace en el problema III[16] de su *Libro de los números cuadrados*. Las proporciones (figura 4) que usa Fibonacci son:

$$\frac{ZL}{ZD} = \frac{ZM}{ZE} \text{ y } \frac{DE}{LM} = \frac{ZD}{ZL}.$$

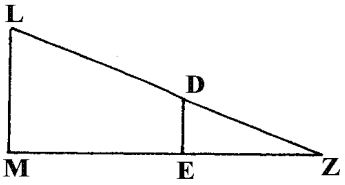
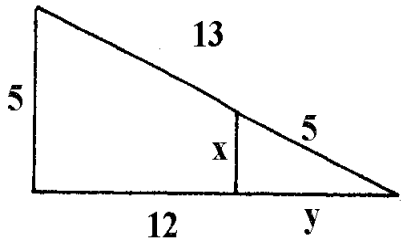


Figura 4

Para la solución del *Sumario* se propone usar la igualdad $5^2 + 12^2 = 13^2$ (arbitraria) y se construye el triángulo rectángulo de hipotenusa 13 (figura 5). Después se construye un triángulo semejante de hipotenusa 5. Por lo tanto, de las proporciones de Fibonacci se tiene que:

$$\frac{X}{5} = \frac{5}{13} \quad \text{y} \quad \frac{Y}{12} = \frac{5}{13},$$



$$X = \frac{5\times5}{13} \quad \text{y} \quad Y = \frac{5\times12}{13},$$

Figura 5

y como el triángulo de lados X, Y, 5 es rectángulo, entonces

$$\left(\frac{25}{13}\right)^2 + \left(\frac{60}{13}\right)^2 = 5^2.$$

Al igual que el problema III, Diez Freyle no usó los triángulos de manera explícita, pero se puede encontrar sin dificultad que las operaciones que se presentan de manera figurada en su respuesta son precisamente los cálculos de las proporciones

$$X = \frac{5\times5}{13} \quad \text{y} \quad Y = \frac{5\times12}{13}.$$

Diez y Pacioli no emplearon triángulos para acompañar sus explicaciones, pero a través de una cuidadosa lectura se ve que intrínsecamente siempre estuvieron presentes a través de las proporciones correspondientes, pero de manera explícita sí lo estuvieron en Fibonacci, que fue una guía para ambos.

[16] El problema dice: *Encontrar dos números cuyos cuadrados reunidos den un cuadrado formado por la unión de los cuadrados de otros dos números dados*.

El siguiente problema es un buen ejemplo de una interpretación aditiva de enteros que usan los elementos matemáticos más sobresalientes de la teoría de los números hasta el siglo XV. Con este ejemplo nos percatamos que la TAN se estaba gestando en torno de sumas más generales y no sólo con los ejemplos antes señalados.

La suma de grandes cantidades *"in infinitum"* de cuadrados también es un cuadrado

Un problema entre los autores antes mencionados es el de poder construir sumas de más de dos cuadrados cuyo resultado también sea un cuadrado; aquí ya no consideramos la suma de dos cuadrados que da lugar a otro cuadrado, dado que son las ternas pitagóricas, y de ellas ya sabemos cómo encontrar una infinidad de soluciones. Se pasa a exponer la manera de construir tres cuadrados cuya suma sea un cuadrado, o pensar en la suma de cuatro cuadrados, y así hasta tener una cantidad indeterminada de cuadrados cuya suma sea un cuadrado.

La exposición de Fibonacci y la de Pacioli son semejantes: ambas pretendían mostrar que se puede encontrar una cantidad indeterminada de números cuadrados tales que juntos o tomados por grupos formen un cuadrado[17]. Por otro lado la de Diez Freyle está usando el hecho de que *la suma de los n primeros números impares es un cuadrado*. En Fibonacci la exposición es muy clara —a pesar de que también es retórica—, y menciona que está utilizando los resultados de los problemas I y II de su libro[18].

Para construir la solución de la suma de cuadrados ellos parten de una condición inicial que es importante, y que sí menciona Pacioli, y que se refiere a que el número cuadrado inicial que se tome siempre debe de ser un cuadrado impar. En el caso de Diez Freyle pide que se tome el primero impar, pero no menciona que siempre se debe de tomar así.

Antes veamos un caso particular. Sea nueve el primer cuadrado impar, es importante elegir un cuadrado impar pues dado que la suma de impares es un cuadrado, entonces la suma de los impares anteriores al 9 — que son 1, 3, 5, 7 — es un cuadrado, es decir,

[17] Proposición XIX de *El libro de los números cuadrados* [Ver Eecke], pp. 87-88. *Summa Arithmetca* [Pacioli, 1974], versión electrónica de la biblioteca virtual Miguel de Cervantes.
[18] El problema II dice: *Quiero demostrar porqué surge una serie ordenada de cuadrados de la suma de los números impares que van desde la unidad hasta el infinito*.

$\left(\frac{9-1}{2}\right)^2 = 4^2$. La interpretación diagramática de este razonamiento — que era una de las formas de presentación típica de las épocas de Fibonacci y Pacioli respectivamente — se puede ver en la figura siguiente:

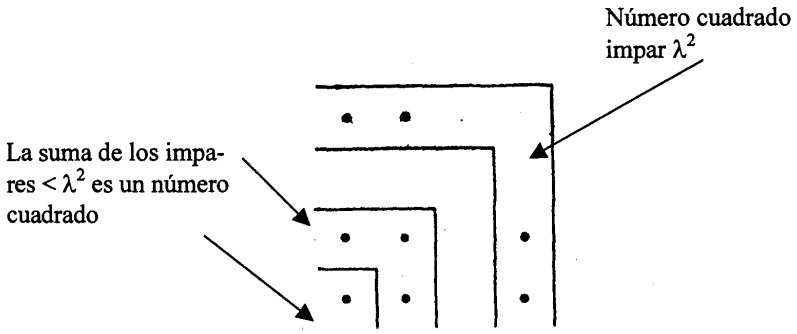


Figura 6: Interpretación diagramática de suma de impares.

Ahora damos lugar a la justificación.

Sea λ^2 un entero impar y como la suma de los impares anteriores a λ^2 es un cuadrado, entonces la suma total de λ^2 más los impares hasta (λ^2 - 2) que es un cuadrado al que llamamos β^2, es también un cuadrado, entonces β^2+ λ^2 es una suma de cuadrados, y esto da como resultado un cuadrado.

Así, en el caso de tomar al 9 y siguiendo el método gráfico de arriba, se suman los impares menores a 9 y se obtiene que $\left(\frac{9-1}{2}\right)^2 = 4^2$ es el segundo cuadrado, después se suman ambos cuadrados y se obtiene que $3^2 + 4^2 = 5^2$. Ahora se hace lo mismo para 5^2, con el objetivo de encontrar una suma de tres cuadrados que dé como resultado un cuadrado.

Ahora, se toma la suma de los impares menores a 25, es decir, 1 + 3 + 5 + 7 +...+ 23, y el resultado es $\left(\frac{25-1}{2}\right)^2 = 12^2$. Así, se sigue que $12^2 + 5^2 = 13^2$, y sabiendo que $4^2 + 3^2 = 5^2$, se llega a $4^2 + 3^2 + 12^2 = 12^2 + 5^2 = 13^2$.

Ahora extendamos el ejemplo para el caso en que se toma la suma de cuatro cuadrados (aunque ya no está contenido en el *Sumario,* sí lo está en la *Summa* y en *Los números cuadrados*). Ya se tiene que $3^2 + 4^2 + 12^2 = 13^2$; enseguida tómese la suma de los impares

menores que 13^2=169, es decir, 1+3+5+7+...+165 + 167 = $\left(\frac{169-1}{2}\right)^2 = 7056 = 84^2$, por tanto $13^2 + 84^2 = 85^2 = 7225$. Finalmente a $3^2 + 4^2 + 12^2 = 13^2$ se le suma de ambos lados 84^2 para obtener: $3^2 + 4^2 + 12^2 + 84^2 = 13^2 + 84^2 = 85^2$. Lo mismo se puede hacer para los impares menores que 85^2 y se llega a que:

$$3^2 + 4^2 + 12^2 + 84^2 + 3612^2 = 3613^2,$$

y así, como escribió Diez Freyle al final del ejemplo: *"y nota que por esta vía lo podrás hacer in infinitum"*.

Para generalizar esta idea primero consideremos un cuadrado impar m^2. Así, si $m = 4k \pm 1$, entonces $m^2 = 4q + 1$, y sabemos que la suma de los impares anteriores a él es $\left(\frac{m^2-1}{2}\right)^2$ que también es un cuadrado y par, entonces $\left[m^2 + \left(\frac{m^2-1}{2}\right)^2\right]$ es un impar, pero a la vez es un cuadrado. Finalmente se tiene que la suma de un cuadrado impar m^2 más la suma de un cuadrado par $\left(\frac{m^2-1}{2}\right)^2$, da como resultado otro cuadrado impar, $\left[m^2 + \left(\frac{m^2-1}{2}\right)^2\right]$ al que llamamos n^2.

Como ya tenemos otro cuadrado impar n^2, entonces podemos hacer el mismo proceso como en el caso de m^2, y se llega a que $\left[n^2 + \left(\frac{n^2-1}{2}\right)^2\right]$ es nuevamente otro cuadrado impar al que llamamos t^2.

Entonces por los dos procesos anteriores se tiene que

$$\left[m^2 + \left(\frac{m^2-1}{2}\right)^2\right] = n^2,$$

y como

$$\left[n^2 + \left(\frac{n^2-1}{2}\right)^2\right] = t^2,$$

entonces de ambas expresiones se llega a

$$\left[m^2 + \left(\frac{m^2-1}{2}\right)^2 + \left(\frac{n^2-1}{2}\right)^2\right] = n^2 + \left(\frac{n^2-1}{2}\right)^2 = t^2.$$

Como se puede ver, hemos obtenido tres cuadrados cuya suma es un cuadrado t^2, y nótese que como este último cuadrado es nuevamente impar, entonces podemos repetir el proceso y construir de manera general que la suma de cuatro cuadrados es un cuadrado, y así se puede seguir el proceso como lo propuso Diez Freyle, *in infinitum.*

Con esto llegamos al inicio del camino del estudio de la suma de dos cuadrados, y esto es lo que expondremos en el capítulo siguiente.

Capítulo 2

Suma de dos cuadrados

En el capítulo anterior nos adentramos en algunos problemas que nos muestran de qué manera se interesaron los matemáticos en los problemas que involucraron la suma de cuadrados. Desde la antigüedad hasta finales de la Edad Media este tipo de problemas se presentaban en un contexto de resolver principalmente situaciones mercantiles y de tierras. En el siglo XVII se empiezan a plantear problemas más de fondo, es decir, los interesados en las ciencias matemáticas voltearon al estudio de los números enteros, pero ya no desde la perspectiva de una aritmología Medioeval, y lo que ahora les interesaba era conocer la estructura aditiva subyacente a los enteros. Así, con estas nuevas interrogantes, surgió el interés por saber qué números enteros se pueden escribir como suma de dos cuadrados, y si había formas cerradas de representarlos o generarlos.

Seguramente en el entorno de Fermat sabían por – auscultación – que no era posible que todo entero fuera suma de dos cuadrados, pues es fácil ver que 3, 7, 11, 12, 14,…no pueden ser escritos como suma de dos cuadrados. Además parece que si el intervalo de medición es más grande los números que son representados como suma de dos cuadrados son aun más escasos. Por ejemplo, entre 100000 y 100030 hay sólo siete números que lo cumplen. También podemos decir que cada entero que es suma de dos cuadrados tampoco tiene muchas representaciones de esta forma; por ejemplo, entre 1 y 150000 sólo el 148625 es de los que más representaciones tiene como suma de dos cuadrados (ver la figura que sigue), y tiene sólo ocho, y en el caso de los primos que pueden ser representación de esta forma, sólo tendrán una (la demostración se presenta más adelante).

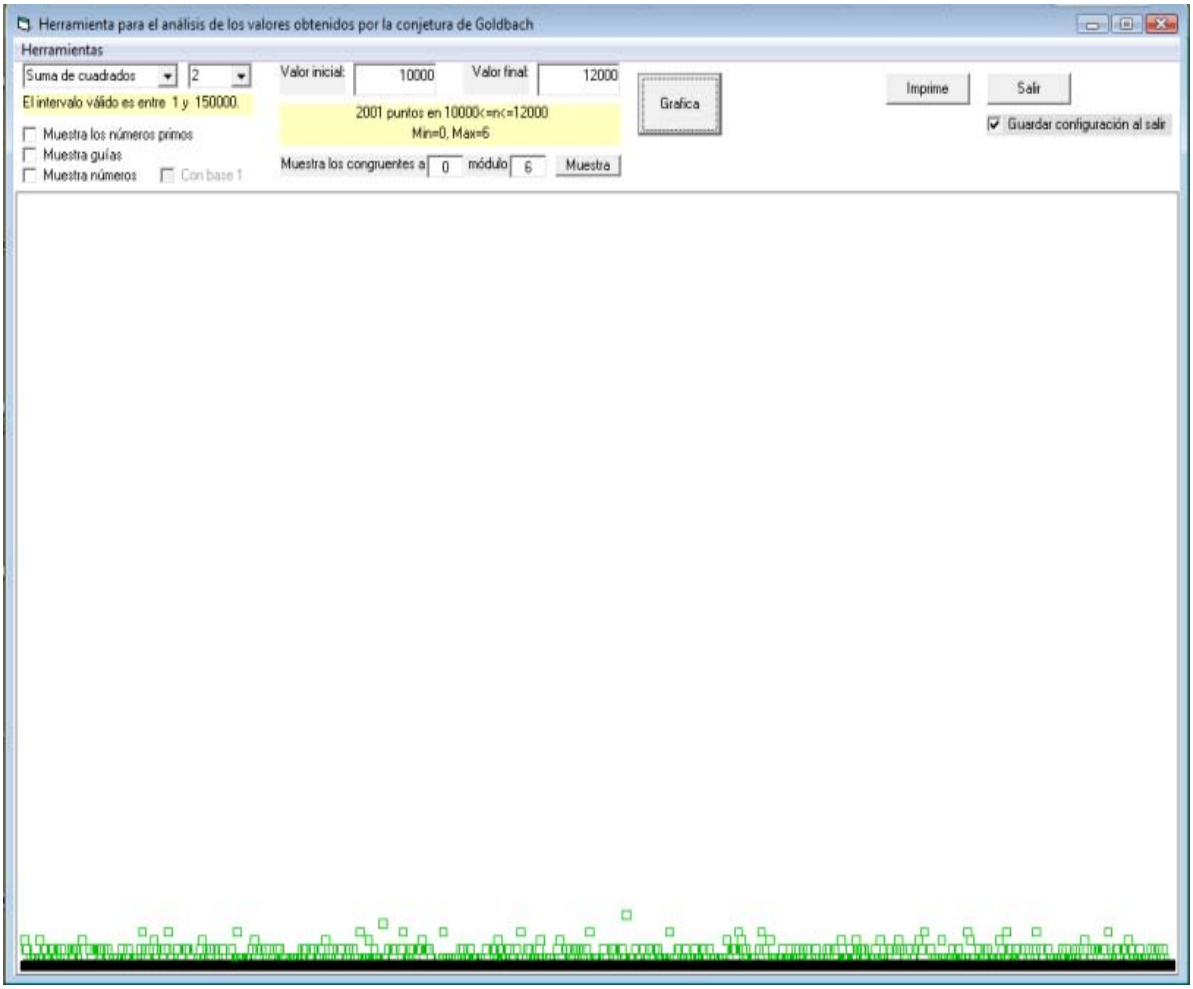


Figura 7: Gráfica de representaciones de enteros como suma de dos cuadrados

En la figura 7 se aprecia que los cuadrados verdes representan en su posición vertical la cantidad de representaciones como suma de cuadrados de los enteros, la franja negra son los enteros que no tienen representación como suma de dos cuadrados.[19]

Con la información mencionada pasemos a ver qué números se pueden representar de la forma señalada. Los primeros datos que tenemos sobre este problema los encontramos con el matemático francés Albert Girard (1595-1632); de él sabemos que sus planteamientos fueron conocidos algunos años antes que los resultados propuestos por Fermat. Se puede notar que los números 2, 4, 5, 8, 9, 10, 13, etc. sí se pueden expresar como suma de dos cuadrados, y a la vez algunos son de la forma $4k + 1$. De hecho este resultado fue propuesto

[19] El programa que se uso fue creado por José Antonio López Saucedo y no es un software comercial, éste fue creado exclusivamente para el uso del grupo de trabajo de teoría de números al que pertenezco.

por Fermat en 1646, pero demostrado por Euler hasta 1754.[20] Ahora demos lugar a un resultado que nos indica una clase de números que no pueden ser escritos como suma de dos cuadrados.

Teorema 2.1 Sea $n \in \mathbb{Z}$ tal que $n \equiv 3 \pmod 4$, entonces n no se puede expresar como suma de dos cuadrados.

Demostración. Supongamos que bajo la hipótesis que $n \equiv 3 \pmod 4$, $n = x^2 + y^2$ para $x, y \in \mathbb{Z}^+$. Por otro lado sabemos que el cuadrado de cualquier entero m módulo 4 cumple con $m^2 \equiv 0,1 \pmod 4$, y se debe a que si m es par, entonces m^2 es múltiplo de 4, y por tanto deja resto 0 módulo 4; si m es impar, entonces m^2 es impar y deja resto 1 módulo 4. Así, $n = x^2 + y^2 \equiv 0,1 \text{ ó } 2 \pmod 4$ pero nunca deja resto 3, es decir, $n \not\equiv 3 \pmod 4$, y esto contradice la hipótesis. ■

Con este teorema tenemos la clase residual que deja resto tres y donde ninguno de sus elementos se puede expresar como suma de dos cuadrados, y a partir de esto podemos encontrar otra clase residual módulo cuatro que contiene una infinidad de elementos que no pueden ser escritos como suma de dos cuadrados.

Teorema 2.2 Sea $n \in \mathbb{Z}$, si n no es expresable como suma de dos cuadrados, entonces su cuádruple tampoco es expresable como suma de dos cuadrados.

Demostración. Supongamos que $4n$ se puede expresar como la suma de dos cuadrados, entonces existen $x, y \in \mathbb{Z}^+$ tal que $4n = x^2 + y^2$. De esto se puede ver que tanto x como y deben de ser pares, pues si esto no se da, la igualdad no se da. Así, si $x = 2r$ y $y = 2s$, entonces $4n = 4r^2 + 4s^2$, y por lo tanto $n = r^2 + s^2$, pero esto contradice la hipótesis de que n no se puede expresar de esta forma. Finalmente, $4n$ no es expresable como suma de dos cuadrados. ■

Conocemos algunas clases residuales módulo cuatro que no son expresables totalmente como suma de dos cuadrados. Pasemos ahora a ver cuáles sí lo son, y para esto nece-

[20] Nótese que si un número es suma de dos cuadrados no significa que tenga que ser de la forma $4k + 1$; por ejemplo, $2^2 + 6^2 = 40$ y 40 no es de la forma $4k + 1$, pero si tendrán esta forma cuando a y b en $a^2 + b^2$ sean primos relativos.

sitamos previamente conocer algunos resultados a los que les daremos la categoría de lemas, ya que ayudarán a demostrar los teoremas posteriores.

El primer resultado está vinculado con el producto de dos enteros positivos, donde cada uno es suma de dos cuadrados, y a la vez este producto también es suma de dos cuadrados. Diofanto lo menciona implícitamente en su *Aritmética* y Fibonacci lo demuestra en su *Libro de los números cuadrados*.[21] La demostración que se presenta está fundamentada en la aplicación de áreas, de la misma manera como se utilizaba en la matemática griega.

Lema 2.3 (Diofanto) El producto de dos sumas de dos cuadrados, es también suma de dos cuadrados, y puede ser de dos maneras diferentes. Si $m = a^2 + b^2$ y $n = c^2 + d^2$, entonces

$$mn = (a^2 + b^2)(c^2 + d^2) = (ac + bd)^2 + (ad - bc)^2.$$[22]

$$\text{o puede ser } = (ac - bd)^2 + (ad + bc).$$

Se puede ver de manera conjunta como $mn = (a^2 + b^2)(c^2 + d^2) = (ac \pm bd)^2 + (ad \mp bc)$.

Así, si definimos a Q = $\{n | n = x_1^2 + x_2^2 \text{ con } x_1, x_2 \in \mathbb{Z}\}$,

entonces el lema nos indica que Q es cerrado bajo el producto, es decir, si $n_1,\ n_2 \in$ Q, entonces $n_1 \cdot n_2 \in$ Q.

Ejemplo 2.4 Si $n_1 = 5 = 2^2 + 1^2$ y $n_2 = 2 = 1^2 + 1^2$, entonces

$$10 = 5 \cdot 2 = (2^2 + 1^2)(1^2 + 1^2) = (2 \cdot 1 - 1 \cdot 1)^2 + (2 \cdot 1 - 1.1)^2$$

$$= 3^2 + 1^2.$$

En general, si $n_1, n_2, n_3, \ldots, n_r \in$ Q, entonces $n_1 \cdot n_2 \cdot n_3 \cdots n_r \in$ Q, $r \in \mathbb{Z}^+$. Ahora se demuestra el lema ya mencionado.

[21] Pisa, Leonardo de. *Libro de los números cuadrados* [1973], proposición IV.
[22] Diofanto usa implícitamente este resultado en la *Aritmética*, sin dar la demostración, esta puede ser observada geométricamente en Koshy, Thomas [2002].

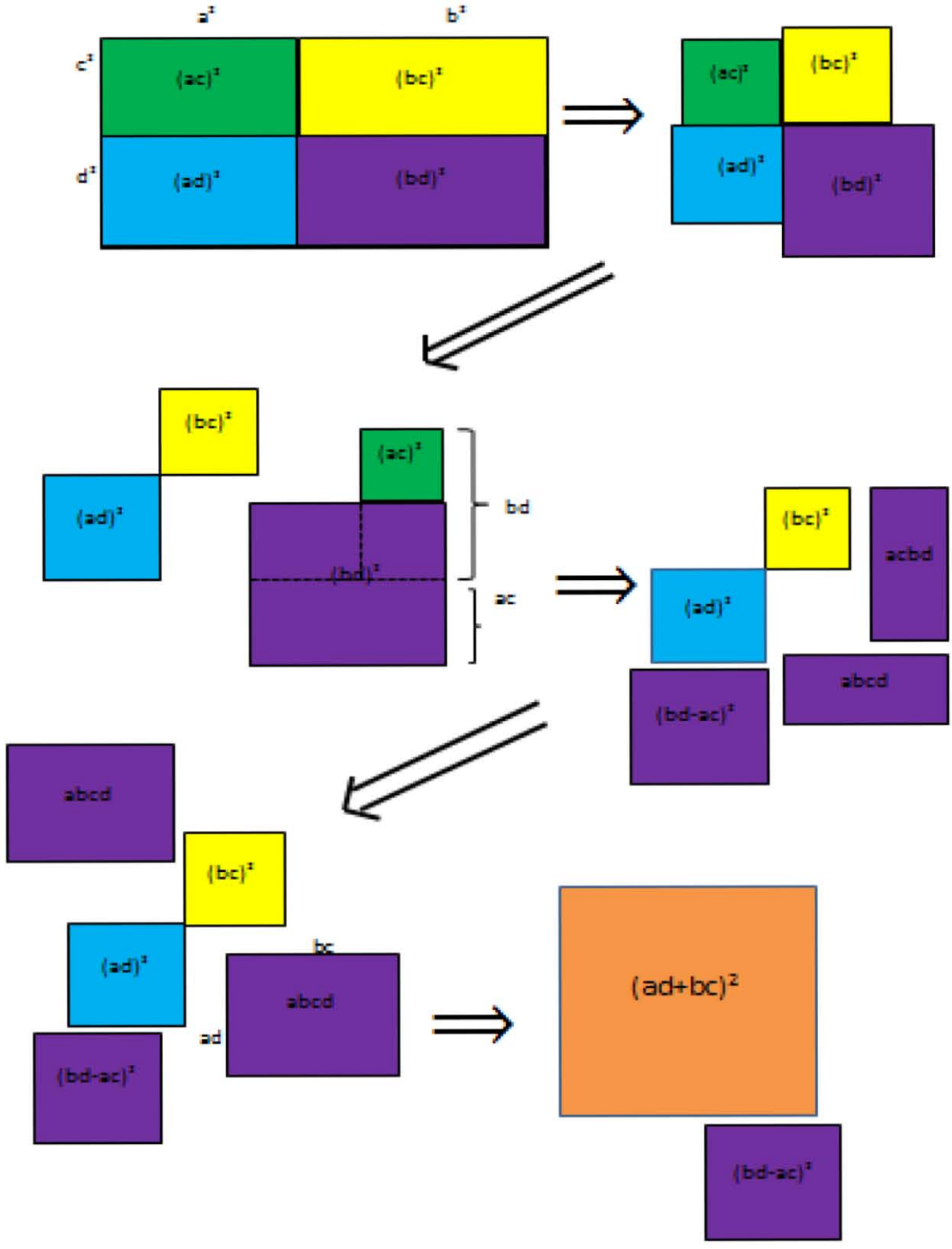


Figura 8: Lema 2.3

Pasamos ahora a identificar algunas características de los enteros positivos que sí pueden ser representados como suma de dos cuadrados.

Lema 2.5 Sea p un número primo tal que $p \equiv 1 \pmod 4$, entonces existen $x, y \in \mathbb{Z}^+$, tal que $x^2 + y^2 = mp$, para algún $m \in \mathbb{Z}^+$ y $m < p$.

Demostración. Por hipótesis p es primo y $p \equiv 1 \pmod 4$, entonces el símbolo de Legendre[23] nos indica que[24] $\left(\frac{-1}{p}\right) = 1$, es decir, -1 es residuo cuadrático modulo p. Entonces existe un entero positivo $\alpha < p$ tal que $\alpha^2 \equiv -1 \ (mod\ p)$, donde α es un elemento del sistema completo de residuos módulo p. Así, de la congruencia anterior se obtiene que $\alpha^2 + 1 = mp$, para $m \in \mathbb{Z}^+$; y si nombramos a $x = \alpha$ y $y = 1$, entonces $x^2 + y^2 = mp$.
Sólo falta ver que $m < p$, y para esto ya teníamos que $\alpha < p$ entonces $\alpha \leq p - 1$, y por otro lado $mp = \alpha^2 + 1 \leq (p-1)^2 + 1$, así $mp \leq (p-1)^2 + 1 = p^2 - 2(p-1) < p^2$, es decir, $mp < p^2$ por lo cual $m < p$. ■

Ejemplo 2.6 Si $p = 5 \equiv 1 \ (mod\ 4)$ entonces $2^2 \equiv -1 \ (mod\ 5)$, donde $\alpha = 2$ y $m = 1$.

El siguiente resultado muestra que se puede ir más lejos con m y que no sólo nos quedamos con que sea menor que p, ahora se demostrará que m es exactamente 1.

Lema 2.7 Si $p \equiv 1 \ (mod\ 4)$ y es primo, entonces p puede ser expresado como suma de dos cuadrados.

Demostración. Por el lema 2.5 y considerando el principio del buen orden, tenemos que existe un menor entero positivo m tal que $mp = x^2 + y^2$, para $x, y \in \mathbb{Z}^+$. Probaremos a través de una contradicción que $m = 1$.
Supongamos que $m > 1$, y considerando un sistema completo de residuos (nos referiremos al sistema como SCR) módulo m, entonces existen a, b en el SCR tal que

[23] Sea $a \in \mathbb{Z}$ y sea p un primo impar tal que $(a, p) = 1$. Se define al símbolo de Legendre igual a 1, y se denota como $\left(\frac{a}{p}\right)$ si a es residuo cuadrático módulo p, y se define igual a -1 en cualquier otro caso.
[24] Se usa el resultado que dice que si $p \equiv 1 \ (mod\ 4)$ entonces existe x tal que $x^2 \equiv -1 \ (mod\ p)$, y en consecuencia $\left(\frac{-1}{p}\right) = 1$.

$a \equiv x\ (mod\ m)$ y $b \equiv y\ (mod\ m)$……..……. (1),

donde $\frac{-m}{2} < a, b \leq \frac{m}{2}$……..……..(2).

Entonces

$$a^2 + b^2 \equiv x^2 + y^2 \equiv mp \equiv 0\ (mod\ m),$$

y en consecuencia $a^2 + b^2 \equiv 0\ (mod\ m)$, es decir, $a^2 + b^2 = mk$, para algún $k \in \mathbb{Z}^+$.

Ahora, por el lema 2.3, tenemos que

$(a^2 + b^2)(x^2 + y^2) = (ax + by)^2 + (ay - bx)^2$……..... (3)[25],

y esto nos lleva a que $(a^2 + b^2)(x^2 + y^2) = (mk)(mp) = m^2kp$……..…… (4).

A partir de (3) y (4) se tiene que $(ax + by)^2 + (ay - bx)^2 = m^2kp$.

Como $a \equiv x\ (mod\ m)$ entonces $ax \equiv x^2\ (mod\ m)$, por otro lado como $b \equiv y\ (mod\ m)$, por tanto $by \equiv y^2\ (mod\ m)$, entonces $ax + by \equiv x^2 + y^2 \equiv 0\ (mod\ m)$.

Nuevamente $a \equiv x\ (mod\ m)$, entonces $ay \equiv xy\ (mod\ m)$, y como $b \equiv y\ (mod\ m)$ entonces $bx \equiv xy\ (mod\ m)$, por lo tanto $ay - bx \equiv xy - xy \equiv 0\ (mod\ m)$. Con este resultado y el anterior tenemos que $(ax + by)$ y $(ay - bx)$ son múltiplos de *m*, y en consecuencia

$$\left(\frac{ax + by}{m}\right), \left(\frac{ay - bx}{m}\right) \in \mathbb{Z}.$$

De regreso a lo anterior, ya teníamos que $(ax + by)^2 + (ay - bx)^2 = m^2kp$, entonces $\left(\frac{ax+by}{m}\right)^2 + \left(\frac{ay-bx}{m}\right)^2 = kp$. Lo que obtenemos es que kp es suma de dos cuadrados enteros. Ya teníamos que m es el menor entero positivo tal que mp es suma de dos cuadrados y por (2) $a, b \leq \frac{m}{2}$. Luego $a^2 + b^2 \leq \frac{m^2}{4} + \frac{m^2}{4} = \frac{m^2}{2}$, y como $a^2 + b^2 = mk$, entonces se tiene que $mk \leq \frac{m^2}{2} < m^2$, por lo tanto $k < m$. Aquí ya estamos cerca de llegar a una contradicción sobre el hecho de que $m > 1$ y que a la vez es el mínimo entero positivo tal que mp es suma de dos cuadrados. Como llegamos a que $k < m$, entonces basta demostrar que $k > 0$ para terminar la contradicción.

[25] Tomamos una de las dos opciones en los signos de lo planteado en el lema 2.3.

Así, si $k = 0$, entonces $a^2 + b^2 = mk = 0$, y se tendría que $a = b = 0$, y por (1) $x \equiv y \equiv 0\ (mod\ m)$; de esta forma x, y serían divisibles por m y así $m^2 \mid x^2$ y $m^2 \mid y^2$, por lo tanto $m^2 \mid x^2 + y^2 = mp$, lo cual implica $m \mid p$, pero el lema 1.1.4 nos indica que $m < p$, entonces $m = 1$, y esto contradice nuestra hipótesis ($m > 1$). Por lo tanto $k > 0$ y cumple con que $1 \leq k < m$, y a la vez kp es suma de dos cuadrados, lo cual no puede suceder por la minimalidad de *m* y *mp* como suma de dos cuadrados. En conclusión, el entero *k* no puede existir y *m* tiene que ser 1, es decir, $mp = 1 \cdot p = p = x^2 + y^2$. ■

Con el teorema 2.7 y el teorema siguiente quedarán probados las condiciones necesarias y suficientes para que un entero positivo pueda ser expresado como suma de dos cuadrados.

Teorema 2.8 Sea $p = x^2 + y^2$ y p un primo impar, entonces $p \equiv 1\ (mod\ 4)$.

Demostración. Sea p un primo impar, tal que $p = x^2 + y^2$, para algún $x, y \in \mathbb{Z}^+$, entonces x y y deben ser de distinta paridad, pues si son de la misma paridad entonces p sería par, lo cual contradice la hipótesis. De esta forma, sea $x = 2a$ y $y = 2b + 1$, por lo tanto $p = x^2 + y^2 = (2a)^2 + (2b + 1)^2 = 4a^2 + 4b^2 + 4b + 1 = 4(a^2 + b^2 + b) + 1$, es decir, $p = 4k + 1$ donde $k = a^2 + b^2 + b \in \mathbb{Z}$. Por tanto $p \equiv 1\ (mod\ 4)$. ■

El resultado que sigue, quizá sea *el más importante* respecto a la suma de dos cuadrados de un entero positivo *n*, ya que caracteriza a un número que es suma de dos cuadrados. Esto se hace a través de observar que los factores primos congruentes con 3 modulo 4 en la descomposición canónica de *n* tienen exponente par.

Teorema 2.9 Un entero positivo n se puede expresar como suma de dos cuadrados si y sólo si cualquier divisor primo $p \equiv 3\ (mod\ 4)$ de n tiene exponente par en la descomposición canónica de n.

Demostración. Primero supongamos que un entero positivo n es suma de dos cuadrados y que un primo p divide a $n = x^2 + y^2$, para x, y enteros positivos, por lo tanto $x^2 \equiv -y^2(mod\ p)$, es decir,$-y^2$ es un residuo cuadrático módulo p. Por el símbolo de Legendre se tiene que

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

y esto pasa si sólo si $p \equiv 1\ (mod\ 4)$.

Si se da el caso que un primo $p_1 = 4k + 3$ divida a *n*, entonces tendría que pasar que $x \equiv y \equiv 0\ (mod\ p_1)$, es decir, $x = p_1 a$ y $y = p_1 b$, con $a, b \in \mathbb{Z}^+$, entonces

$$\boldsymbol{n = x^2 + y^2 = p_1^2(a^2 + b^2) = p_1^2 m},\ \text{con}\ m = a^2 + b^2.$$

Ahora, sí *m* no es divisible por un primo de la forma $4k + 3$, entonces m tendría que serlo por un primo de la forma $4k + 1$, por lo que el resultado quedaría demostrado para el primo p_1, ya que éste sería el único primo de la forma $4k + 3$ con potencia par en la descomposición de *n*.

Por otro lado, si existe un primo $p_2 = 4r + 3$ tal que p_2 divide a *m*, entonces tiene que pasar –por el mismo análisis hecho con p_1– que $m = p_2^2 m_1$, con $m_1 = a_1^2 + b_1^2$, y por lo tanto $\boldsymbol{n = p_1^2 m = p_1^2(p_2^2 m_1)}$.[26] En general, si m_1 es divisible por un primo de la forma $4k + 1$, el resultado quedaría demostrado, con p_1 y p_2 primos de la forma $4k + 3$ con potencia par; por otra parte, si m_1 es divisible por un primo de la forma $4k + 3$, entonces ese primo también tendrá potencia par. En cualquiera de los casos los primos congruentes con 3 módulo 4 aparecerán con potencia par en la descomposición canónica de *n*.

Por último, falta mostrar el regreso, es decir, si cada factor primo $p \equiv 3(mod\ 4)$ de *n*, tiene exponente par, entonces n es expresable como suma de dos cuadrados.

Tómese a n como un producto de primos donde los $p_i \equiv 1\ mod\ (4)$ y los $q_i \equiv 3\ mod\ (4)$. Entonces

$$n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_r^{\alpha_r} \cdot q_1^{\beta_1} \cdot q_2^{\beta_2} \cdots q_s^{\beta_s} = \prod_{i=1}^{r} {p_i}^{\alpha_i} \cdot \prod_{i=1}^{s} q_i^{\beta_i}.$$

Como $p_i \equiv 1\ mod\ (4)$, entonces (por el lema 2.7) una parte del producto se puede expresar como suma de dos cuadrados, por lo tanto

$$p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_r^{\alpha_r} = \prod_{i=1}^{r} (x_i^2 + y_i^2),$$

[26] Puede suceder que $p_1 = p_2$.

y como el producto dos a dos de sumas de dos cuadrados es también suma de dos cuadrados, entonces

$$\prod_{i=1}^{r}(x_i^2 + y_i^2) = x^2 + y^2 \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (1).$$

Por hipótesis los $q_i \equiv 3\ (mod\ 4)$ tienen potencia par, así $(q_i)^{2\gamma_i} = ((4k+3)^{\gamma_i})^2 + 0^2$, donde $2\gamma_i = \beta_i$, para toda $i = 1,\ldots, s$. De esto se sigue que

$$q_1^{\beta_1} \cdot q_2^{\beta_2} \cdots q_s^{\beta_s} = \prod_{i=1}^{s} q_i^{2\gamma_i} = \prod_{i=1}^{s} \left(q_i^{\gamma_i}\right)^2 + 0^2.$$

Nuevamente por el lema 2.3 − el producto dos a dos de sumas de dos cuadrados es también suma de dos cuadrados−.

$$q_1^{\beta_1} \cdot q_2^{\beta_2} \cdots q_s^{\beta_s} = \prod_{i=1}^{s} \left(q_i^{\gamma_i}\right)^2 + 0^2 = z^2 + 0^2 \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (2).$$

De (1) y (2) se tiene

$$n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_r^{\alpha_r} \cdot q_1^{\beta_1} \cdot q_2^{\beta_2} \cdots q_s^{\beta_s} = (x^2 + y^2)(z^2 + 0^2) \ldots\ldots\ldots\ldots (3),$$

y por lo tanto

$$n = (x^2 + y^2)(z^2 + 0^2) = (xz)^2 + (yz)^2.$$

Así queda mostrado que n es suma de dos cuadrados, y la prueba está completa. ■

Demos lugar a otra propiedad que está en la misma categoría de las propiedades de los divisores de un número que es suma de dos cuadrados.

Teorema 2.1.0 Sean $x, y \in \mathbb{Z}^+$ y p un primo impar tal que $p \mid x^2 + y^2$ y $(x, y) = 1$. Entonces $p \equiv 1\ (mod\ 4)$.

Demostración. Sean *x, y* enteros positivos y p un primo impar tal que $p \mid x^2 + y^2$. Si suponemos que $p \mid x$, entonces $p \mid x^2$, por lo tanto $p \mid (x^2 + y^2) - x^2 = y^2$, es decir $p \mid y$, pero esto no puede suceder ya que $(x, y) = 1$, así ni x ni y son divisibles por p. mo $p \mid x^2 + y^2$, entonces $x^2 \equiv -y^2\ (mod\ p)$ y por tanto $(x^2)^{\frac{p-1}{2}} \equiv (-y^2)^{\frac{p-1}{2}} (mod\ p)$, así $(x^2)^{\frac{p-1}{2}} \equiv (-1)^{\frac{p-1}{2}} (y^2)^{\frac{p-1}{2}} (mod\ p)$ ..... (1).

Ya que $(p, x) = (p, y) = 1$, entonces por el Pequeño Teorema de Fermat [27] (PTF) se cumple que

$x^{p-1} \equiv y^{p-1} \equiv 1\ (mod\ p)$ ..... (2).

Así, por (2)

$$(x^2)^{\frac{p-1}{2}} = x^{p-1} \equiv y^{p-1} = (y^2)^{\frac{p-1}{2}} (mod\ p),$$

y de (1) y (2) tenemos que

$(-1)^{\frac{p-1}{2}} (y^2)^{\frac{p-1}{2}} \equiv (x^2)^{\frac{p-1}{2}} \equiv 1 \cdot (y^2)^{\frac{p-1}{2}} (mod\ p)$ ..... (3).

Se sabe que si $(p, y) = 1$, entonces $(y^n, p) = 1$. En particular $\left((y^2)^{\frac{p-1}{2}}, p\right) = 1$, de manera que la congruencia (3) se reduce a

$$(-1)^{\frac{p-1}{2}} \equiv 1 (mod\ p),$$

por lo tanto $1 = (-1)^{\frac{p-1}{2}}$, y al aplicar el Criterio de Euler[28] y el Símbolo de Legendre, vemos que

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} 1 \quad si\ p \equiv 1\ (mod\ 4) \\ -1\ si\ p \equiv 3\ (mod\ 4) \end{cases},$$

por lo tanto $p \equiv 1\ (mod\ 4)$. ■

Ejemplo 2.1.1 Si $p = 5$ es un primo impar, y por otro lado $85 = 2^2 + 9^2$ es divisible por 5, entonces nótese que 5 es de la forma $4k + 1$.

Sabemos que existen una infinidad de primos de la forma $4k + 1$, por lo tanto hay una infinidad de estos primos que se pueden expresar como suma de dos cuadrados, pero si no se toma en cuenta el orden y los signos de ellos, entonces demostraremos que la representación como suma de dos cuadrados es única.[29]

[27] Si p es un primo y a un número entero tal que $(p, a) = 1$, entonces $a^{p-1} \equiv 1\ (mod\ p)$.

[28] Sea $a \in \mathbb{Z}$ y p un primo impar tal que $(a, p) = 1$, entonces a es un residuo cuadrático de p si y sólo si $(a)^{\frac{p-1}{2}} \equiv 1\ (mod\ p)$.

[29] Es importante señalar que si estos números – los $4k + 1$ – no son primos, entonces pueden tener varias representaciones como suma de dos cuadrados o ninguna.

Teorema 2.1.2 (Teorema de Girand - Euler)

Todo primo de la forma $4k+1$ puede ser expresado de manera única como suma de dos cuadrados, salvo el orden y signos.

Demostración. Sea p un primo de la forma $4k+1$ y supongamos que tiene dos representaciones distintas como suma de dos cuadrados. Sea $p = x_1^2 + y_1^2 = x_2^2 + y_2^2$ con x_1, y_1, x_2 y y_2 enteros positivos, se demostrará que ambas representaciones son la misma. Como $p \equiv 1\ (mod\ 4)$ entonces -1 es residuo cuadrático, es decir, existe una $x \in \mathbb{Z}$ tal que $x^2 \equiv -1\ (mod\ p)$. Sea α la solución de la congruencia. Entonces

$$\alpha^2 \equiv -1\ (mod\ p)\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (1).$$

Por otra parte, de las representaciones de p como suma de dos cuadrados, se tiene que $p \mid x_1^2 + y_1^2$ y $p \mid x_2^2 + y_2^2$. Así

$$x_1^2 \equiv -y_1^2\ (mod\ p)\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (2)$$

$$x_2^2 \equiv -y_2^2\ (mod\ p)\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (3),$$

de $(1), (2)$ y (3) se obtiene

$$x_1^2 \equiv -y_1^2 \equiv y_1^2\alpha^2 (mod\ p)\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (4)$$

$$x_2^2 \equiv -y_2^2 \equiv y_2^2\alpha^2 (mod\ p)\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (5),$$

de (4) tenemos $x_1^2 - y_1^2\alpha^2 = tp$, con $t \in \mathbb{Z}$, así $\left(x_1 + (y_1\alpha)\right)\left(x_1 - (y_1\alpha)\right) = tp$, y como p es primo, entonces divide a alguno de los dos factores y sólo a uno,[30] por lo que

$$p \mid \left(x_1 + (y_1\alpha)\right) \Longrightarrow x_1 \equiv -y_1\alpha\ (mod\ p),$$

o bien

$$p \mid \left(x_1 - (y_1\alpha)\right) \Longrightarrow x_1 \equiv y_1\alpha\ (mod\ p).$$

Sin pérdida de generalidad supongamos que $x_1 \equiv y_1\alpha\ (mod\ p)$. Por (5) y haciendo un procedimiento análogo al que se hizo a partir de (4) se obtiene que $x_2 \equiv y_2\alpha\ (mod\ p)$. Por lo tanto [31]

$$x_1x_2 \equiv \alpha^2 y_1 y_2\ (mod\ p).$$

---

[30] Si divide a ambos entonces divide a la resta y se tendrá que $p \mid 2y_1\alpha$, pero $(p, \alpha) = 1$entonces $p \mid 2y_1$, pero p es impar, entonces $p \mid y_1$ y $p = x_1^2 + y_1^2$; por lo tanto $p = p^2(x_1^2 + y_1^2)$, y así $1 = p(x_1^2 + y_1^2)$, y esto es una contradicción.

[31] Si $x_1 \equiv -y_1\alpha\ (mod\ p)$ y $x_2 \equiv -y_2\alpha\ (mod\ p)$, entonces se haría un procedimiento análogo al que se hizo con la parte positiva.

De la congruencia anterior y por (1) se tiene que

$$x_1x_2 + y_1y_2 \equiv \alpha^2 y_1y_2 + y_1y_2 = (\alpha^2 + 1)y_1y_2 \equiv 0\ (mod\ p)\text{…….....……(6),}$$

como $x_1 \equiv y_1\alpha\ (mod\ p)$ y $x_2 \equiv y_2\alpha\ (mod\ p)$, entonces $x_1y_2 \equiv y_1y_2\alpha\ (mod\ p)$ y $y_1x_2 \equiv y_1y_2\alpha\ (mod\ p)$ respectivamente. Por lo tanto

$$x_1y_2 - y_1x_2 = \alpha(y_1y_2 - y_1y_2) \equiv 0\ (mod\ p)\text{…….....(7),}$$

de (6) y (7) se tiene que $x_1x_2 + y_1y_2 = rp$ y $x_1y_2 - y_1x_2 = sp$ respectivamente. Pero se había supuesto que $p = x_1^2 + y_1^2 = x_2^2 + y_2^2$, así que por el lema 2.3.

$$\begin{aligned} p^2 &= (x_1^2 + y_1^2)(x_2^2 + y_2^2) = (x_1x_2 + y_1y_2)^2 + (x_1y_2 - y_1x_2)^2 \\ &= r^2p^2 + s^2p^2 = p^2(r^2 + s^2). \end{aligned}$$

Por lo tanto

$$1 = (r^2 + s^2),$$

y esto es cierto si y sólo si $r = 0\ \ o\ \ s = 0$, es decir, $x_1x_2 + y_1y_2 = 0$ o $x_1y_2 - y_1x_2 = 0$. Ahora como $(x_1, y_1) = 1 = (x_2, y_2)$ entonces $x_1x_2 + y_1y_2 = 0$ o $x_1y_2 - y_1x_2 = 0$ si y sólo si $x_1 = \pm x_2$ y $y_1 = \pm y_2$ o $x_1 = \pm y_2$ y $y_1 = \pm x_2$, en cualquier caso, se tiene la misma representación. ■

Ahora presentamos una segunda demostración de la unicidad de la representación como suma de dos cuadrados que contiene más técnicas de geometría que de teoría de números, prácticamente sólo un lema de Euclides[32] extraído de sus libros aritméticos. Lo demás es operar con técnicas de geometría.

Consideremos un cuadrilátero convexo donde $a, b, c, d \in \mathbb{Z}^+$ son las longitudes de sus lados. Lo que se demostrará es que dicho cuadrilátero resulta ser cíclico[33] y además rectángulo, por lo que demostraremos que sus lados opuestos son iguales,[34] y así la representación de la suma de dos cuadrados será única. Ahora pasamos a demostrar que.

Todo primo de la forma $4k + 1$ *es representable como suma de dos cuadrados y de manera única.*

Demostración. Supongamos que la representación de p no es única. Sea

$$p = a^2 + b^2 = c^2 + d^2 \quad a, b, c, d \in \mathbb{Z}^+.$$

[32]Sea p un número primo tal que $p \mid ab$ entonces $p \mid a$ o $p \mid b$.
[33] Un cuadrilátero convexo es cíclico si y sólo si tiene dos ángulos opuestos suplementarios.
[34] Se probará que $a = c$, $b = d$ y por tanto las representaciones $a^2 + b^2$ y $c^2 + d^2$ serán iguales.

Lo que se probará es que ambas parejas $\{a, b\}, \{c, d\}$ representan el mismo primo p. Para esto, consideremos un cuadrilátero $ABCD$ tal que:

$AB = a, BC = b, CD = c, DA = d$ y $AC = \sqrt{p}$ – Véase la Figura 9–.

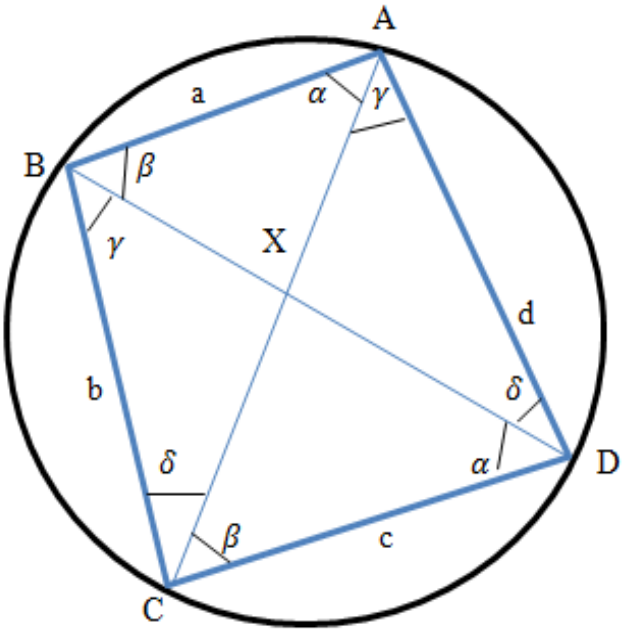


Figura 9: Cuadrilátero *ABCD*

Nótese que de cualquiera de las dos igualdades podemos extraer el inverso del Teorema de Pitágoras, por ejemplo de la primera igualdad $\left(\sqrt{p}\right)^2 = a^2 + b^2$, entonces tenemos triángulos rectángulos de lados $a, b, \sqrt{p}$ y $c, d, \sqrt{p}$, respectivamente.

Así podemos construir un cuadrilátero usando los triángulos que tendrían un lado en común $\sqrt{p}$, que a la vez es una diagonal del cuadrilátero, pero se deja claro – véase la Figura 10 – que las diagonales no tendrán por qué ser iguales.

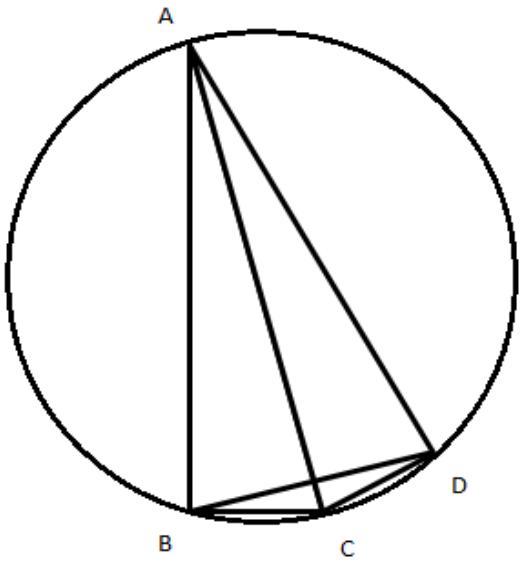


Figura 10

Nótese que precisamente lo que se quiere demostrar es que las diagonales deben tener la misma longitud, por lo que y al ser diámetros nos generarán en consecuencia un cuadrilátero cíclico, cuyos lados opuestos serán iguales y en consecuencia las representaciones de p como suma de cuadrados serán iguales. Ahora tómese a X como el punto de intersección de AC con BD y sea $AX = r, XC = \sqrt{p} - r, BX = u, XD = v$.

Se sabe que $a^2 + b^2 = p = \left(\sqrt{p}\right)^2$, es decir, que $(a, b, \sqrt{p})$ es una terna pitagórica, entonces el ΔABC es rectángulo. De la misma forma se tiene que el ΔADC es rectángulo, por lo cual $\measuredangle ABC \equiv \measuredangle ADC \equiv 90^{\circ}$, esto es, los triángulos rectángulos están inscritos en una semicircunferencia. Por lo tanto el cuadrilátero *ABCD* es cíclico, y en consecuencia se tienen las siguientes relaciones entre ángulos

$$\measuredangle BAC \equiv \measuredangle BDC \equiv \alpha,$$
$$\measuredangle ABD \equiv \measuredangle ACD \equiv \beta,$$
$$\measuredangle ADB \equiv \measuredangle ACB \equiv \delta,$$
$$\measuredangle CBD \equiv \measuredangle CAD \equiv \gamma.$$

Como el cuadrilátero es cíclico, entonces por el *Teorema de Ptolomeo*,[35] se sabe que

$$t\sqrt{p} = ac + bd, \text{ donde } t = BD = u + v. \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (1).$$

[35] Se dice que un cuadrilátero es cíclico si y sólo si $AC \cdot BD = AB \cdot CD + BC \cdot AD$

Aplicando la ley de los senos en el triángulo ΔBXC se tiene

$$\frac{Sin\ \delta}{Sin\,\gamma} = \frac{u}{\sqrt{p}-r},$$

y respectivamente para los triángulos ΔABC y ΔADC se obtiene

$$\frac{Sin\,\delta}{Sin\,\gamma} = \frac{\left(\frac{a}{\sqrt{p}}\right)}{\left(\frac{c}{\sqrt{p}}\right)} = \frac{a}{c}.$$

Así, de las igualdades anteriores

$$\frac{u}{\sqrt{p}-r} = \frac{a}{c} \implies u = \frac{a\left(\sqrt{p}-r\right)}{c} \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (2).$$

Análogamente para el ΔDXC se tiene que

$$\frac{Sin\,\beta}{Sin\,\alpha} = \frac{v}{\sqrt{p}-r},$$

pero de los triángulos ΔABC y ΔADC obtenemos

$$\frac{Sin\,\beta}{Sin\,\alpha} = \frac{\left(\frac{d}{\sqrt{p}}\right)}{\left(\frac{b}{\sqrt{p}}\right)} = \frac{d}{b},$$

por lo tanto

$$\frac{v}{\sqrt{p}-r} = \frac{d}{b} \implies v = \frac{d\left(\sqrt{p}-r\right)}{b} \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (3),$$

entonces

$$u+v = \frac{a\left(\sqrt{p}-r\right)}{c} + \frac{d\left(\sqrt{p}-r\right)}{b} = \left(\sqrt{p}-r\right)\left(\frac{a}{c}+\frac{d}{b}\right) = \left(\sqrt{p}-r\right)\left(\frac{ab+cd}{cb}\right) \ldots\ldots (4).$$

Se sabe que a partir del concepto de potencia de un punto,[36] y en particular para *X* en la circunferencia que circunscribe al cuadrilátero *ABCD* se llega a

$$u \cdot v = \frac{a\left(\sqrt{p}-r\right)}{c} \cdot \frac{d\left(\sqrt{p}-r\right)}{b} = \frac{ad\left(\sqrt{p}-r\right)^2}{cb} = r\left(\sqrt{p}-r\right),$$

por lo tanto

$$\frac{ad}{cb}\left(\sqrt{p}-r\right) = r \Leftrightarrow \frac{ad\sqrt{p}}{cb} - \frac{adr}{cb} = r \Leftrightarrow \frac{ad\sqrt{p}}{cb} = r\left(1+\frac{ad}{cb}\right) = r\left(\frac{cb+ad}{cb}\right)$$

[36] Si dos cuerdas AC y BD en una circunferencia se intersecan en un punto *X* entonces $XA \cdot XC = XB \cdot XD$

$$\frac{ad\sqrt{p}}{cb} = r\left(\frac{cb+ad}{cb}\right) \Leftrightarrow r = \frac{\frac{ad\sqrt{p}}{cb}}{\frac{cb+ad}{cb}} = \frac{ad\sqrt{p}}{cb+ad},$$

entonces

$$\frac{ad\sqrt{p}}{cb+ad} = r \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots.\ldots\ldots\ldots (5).$$

De (1), (4) y (5) se tiene

$$t = u + v = \left(\sqrt{p} - r\right)\left(\frac{ab+cd}{cb}\right) = \left(\sqrt{p} - \frac{ad\sqrt{p}}{cb+ad}\right)\left(\frac{ab+cd}{cb}\right)$$

$$= \left(\frac{(cb+ad)\sqrt{p} - ad\sqrt{p}}{cb+ad}\right)\left(\frac{ab+cd}{cb}\right) = \left(\frac{cb\sqrt{p}}{cb+ad}\right)\left(\frac{ab+cd}{cb}\right)$$

$$= \sqrt{p}\left(\frac{ab+cd}{cb+ad}\right),$$

por lo tanto

$$t = \sqrt{p}\left(\frac{ab+cd}{cb+ad}\right).$$

Ahora bien, recordando que $t\sqrt{p} = ac + bd$ de (1), se obtiene

$$ac + bd = t\sqrt{p} = \left[\sqrt{p}\left(\frac{ab+cd}{cb+ad}\right)\right]\sqrt{p} = p\left(\frac{ab+cd}{cb+ad}\right),$$

entonces

$$p = \frac{(ac+bd)(cb+ad)}{ab+cd},$$

y

$$ab + cd = \frac{(ac+bd)(cb+ad)}{p}.$$

Nuevamente, como p es primo entonces divide a $(ac+bd)$ o divide a $(cb+ad)$. Supongamos que $p \mid (ac+bd)$ entonces $p \leq ac + bd = t\sqrt{p}$; esto último por (1), así que

$$\sqrt{p}\sqrt{p} = p \leq t\sqrt{p} \Rightarrow \sqrt{p} \leq t \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots.\ldots (6).$$

Por otra parte, el diámetro de la circunferencia en el cuadrilátero ABCD es $\sqrt{P} = AC$,[37] y como el diámetro en cualquier circunferencia es mayor que cualquier longitud de cuerda en ella, en particular

[37] Pues se había concluido con anterioridad que el triangulo ACD era rectángulo, donde el $\measuredangle ADC = 90^\circ$, y por tanto la diagonal AC que es la hipotenusa del mismo triangulo tendría que ser el diámetro de la circunferencia.

Diámetro = $\sqrt{p} \geq BD = u + v = t \implies \sqrt{p} \geq t \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (7)$,

por (6) y (7) se tiene

$$\sqrt{p} \leq t \quad y \sqrt{p} \geq t,$$

por lo tanto

$$\sqrt{p} = t.$$

Así

$$AC = \sqrt{P} = t = BD.$$

En consecuencia las diagonales del cuadrilátero ABCD son iguales, y por ello el cuadrilátero resulta ser un *rectángulo,* por lo que $AB = CD$ y por ende $a = c$, $b = d$.

Finalmente llegamos a que

$$p = a^2 + b^2 = c^2 + d^2.$$

Con lo cual queda demostrada la unicidad de la representación de *p* como suma de dos cuadrados. ■

Queda así establecido que la descomposición de un número primo *p* como suma de dos cuadrados es única, salvo el orden y los signos. Para terminar mostraremos dos ejemplos en los cuales hay más de una representación como suma de dos cuadrados, donde si consideramos signos y orden:

Si $n = 2$ entonces $2 = 1^2 + 1^2 = 1^2 + (-1)^2 = (-1)^2 + 1^2 = (-1)^2 + (-1)^2$.

Si $n = 5$ entonces $5 = 2^2 + 1^2 = 2^2 + (-1)^2 = (-2)^2 + 1^2 = (-2)^2 + (-1)^2$

$$= 1^2 + 2^2 = (-1)^2 + 2^2 = 1^2 + (-2)^2 = (-1)^2 + (-2)^2.$$

Para finalizar esta parte sobre suma de dos cuadrados, vamos a explorar el caso donde sí cuentan los signos y el orden, y lo hacemos porque en el ámbito de la representación de coordenadas en el plano sí podemos tener estos casos. Denotemos a $f(n)$ como la función que expresa el número de representaciones de *n* como suma de dos cuadrados considerando el orden y signos. Así, tenemos que $f(2) = 4$ y $f(5) = 8$.[38] El siguiente resultado muestra el número de representaciones $f(n)$ utilizando la función $\tau(m, n)$, que hará explícito el hecho de que $f(n)$ siempre es un múltiplo de 4.

[38] Para tener una mejor idea en cuanto a esta función, ver el apéndice A.

Teorema 2.1.3 (Jacobi)

Sea $m, n \in \mathbb{Z}^+$ y sea $\boldsymbol{\tau(m,n)}$[39] que denota el numero de divisores positivos de *n*, que dejan el mismo residuo que *m* módulo 4. Entonces $f(n) = 4[\tau(1,n) - \tau(3,n)]$.[40]

Ya sabemos que hay una infinidad de enteros que no tienen una representación como suma de dos cuadrados. Cabe preguntarnos la posibilidad de que dado cualquier entero positivo siempre pudiéramos encontrar tres cuadrados que al ser sumados lo representen; un claro ejemplo nos muestra que no, pues el 7 no puede ser representado como suma de tres cuadrados. Con base en esto mostraremos que como no es posible con tres cuadrados representar a cualquier entero, entonces nos centraremos en exponer qué tipo de números son representados como suma de tres de ellos.

Suma de tres cuadrados

Sabemos por un resultado de Gauss - más adelante se anunciará- que existe una cantidad infinita de enteros que no se pueden escribir como suma de tres cuadrados. Como no todos los enteros se pueden expresar como suma de tres cuadrados, entonces ¿podemos saber cuáles son los enteros que sí son suma de tres cuadrados? Para adentrarnos en la ruta hacia la respuesta analizaremos diversas clases residuales, y para esto el teorema siguiente es fundamental.

Teorema 2.1.5 Si n es un entero positivo y $n \equiv 2(mod\ 4)$, *entonces n puede ser representado como suma de tres cuadrados.*

Para demostrar este teorema es necesario un lema previo (lema 2.1.4), y para probarlo será necesario disponer de algunos resultados de la teoría de *formas cuadráticas*, los cuales serán presentados al final de los capítulos en un apéndice,[41] no se incluyen las demostraciones de ellos, y el motivo de esta omisión radica en que dicha teoría es necesaria úni-

[39] Recordamos que la función tau (τ) está definida como el número de divisores de un entero positivo *n*; así se define a la función $\tau(m,n)$ que se menciona en el teorema, pero se deja claro que τ y $\tau(m,n)$ son dos representaciones distintas.
[40] La demostración detallada de éste resultado se encuentra en el apéndice A.
[41] Apéndice B.

camente para la demostración de este lema (2.1.4).[42] Con base en lo anterior pasemos a la demostración del lema en cuestión.

Lema 2.1.4 Sea $n \geq 2$. Si existe un entero positivo *d'* tal que *−d'* es un residuo cuadrático módulo *d'n – 1*, entonces *n* puede ser representado como la suma de tres cuadrados.

Demostración. Si $-d'$ es un residuo cuadrático módulo *d'n – 1*, entonces existen enteros a y b tales que

$$b^2 \equiv -d'(mod\ d'n - 1\ ),$$

y

$b^2 + d' = a(d'n - 1) = ac$, donde $c = d'n - 1$ ……. (1).

Por hipótesis, se tiene que $n \geq 2$ si y sólo si $d'n \geq 2d'$ si y sólo si $d'n - 1 \geq 2d' - 1$, pero se tiene que d' es un entero positivo, por lo que $d' \geq 1$ si y sólo si $2d' \geq 2$ si y sólo si $2d' - 1 \geq 1$.

Así

$$c = d'n - 1 \geq 2d' - 1 \geq 1.$$

Como $b^2 \geq 0$ y $d' \geq 1$ entonces $b^2 + d' \geq 1$. De la ecuación (1) y de las desigualdades anteriores se tiene que

$$ac = b^2 + d', \text{ entonces } a \geq 1,$$

ya que $c \geq 1$. Nuevamente de la ecuación (1) se deduce la equivalencia $d' = ac - b^2$. Ahora considérese a la matriz simétrica $A = \begin{pmatrix} a & b & 1 \\ b & c & 0 \\ 1 & 0 & n \end{pmatrix}$ y obtengamos su determinante

$$\det(A) = nac - nb^2 - c,$$

entonces

$$\det(A) = -c + n(ac - b^2) = d'n - c = 1.$$

Ya que de la ecuación (1) se tiene $c = d'n - 1$. De esta forma $a \geq 1$ y $\det(A) = 1$, entonces por el teorema (c) del apéndice B se tiene que la forma cuadrática F_A correspondiente a la matriz A es positiva-definida, donde $Dis(F_A) = |A| = 1$,[43] y $F_A(0,0,1) = n$, esto último se desprende de lo siguiente

[42] Para mayores detalles sobre estos resultados, se puede consultar Nathanson [1996], p.18.
[43] Definimos al discriminante de la forma cuadrática F_A como el determinante de la matriz simétrica A.

$$F_A(0,0,1) = (0,0,1)\begin{pmatrix} a & b & 1 \\ b & c & 0 \\ 1 & 0 & n \end{pmatrix}\begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} = n.$$

En otras palabras la forma F_A representa al entero n, y como $Dis(F_A) = 1$, entonces por el teorema (d) del apéndice B, la forma $x_1^2 + x_2^2 + x_3^2$ debe representar a $F_A = n$. ■

Anteriormente se analizaron las clases de números $4k, 4k+1, 4k+3$ que mostraban su relación con la suma de dos cuadrados. Ahora se pasará a demostrar que los números enteros de la forma $4k+2$ pueden expresarse como suma de tres cuadrados, que es el teorema señalado al inicio de esta sección.

Teorema 2.1.5 Si *n* es un entero positivo y $n \equiv 2(mod\ 4)$, entonces *n* puede ser representado como suma de tres cuadrados.

Demostración. Por hipótesis $n \equiv 2\ (mod\ 4)$, es decir, $n - 1 \equiv 1(mod\ 4)$. Nótese que $(n-1, 4) = (1,4) = 1$ y también que $(n, n-1) = 1$,[44] así que $(4n, n-1) = 1$.[45]

Por el teorema de *Dirichlet* [46] la progresión aritmética $\{4nj + (n-1) \mid j = 1, \dots n \dots\}$ contiene una infinidad de primos. Elegimos alguna $j \geq 1$ tal que para ese entero j, p es primo y $p = 4nj + (n-1) = (4j+1)n - 1 = d'n - 1$, donde $d' = 4j + 1$. Por otra parte como $n \equiv 2\ (mod\ 4)$, entonces $d'n \equiv n \equiv 2(mod\ 4)$.

Así

$$d'n - 1 \equiv 1(mod\ 4), \text{ y como } p = d'n - 1,$$

entonces

$$p \equiv 1(mod\ 4) \qquad \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots (1),$$

y por el Lema 2.1.4 basta probar que $-d'$ es un residuo cuadrático *módulo p*. Ahora bien, expresamos a d' como producto de primos impares, es decir, $d' = \prod_{q_i \mid d'} {q_i}^{k_i}$ donde los $q_{i's}$ son primos de la forma $4k+1$ y $4k+3$. Entonces $p = d'n - 1 \equiv -1\ (mod\ q_i)$, pues $d'n \equiv d' \equiv 0\ (mod\ q_i)$ para toda $i \in \mathbb{N}$.

[44] Esto es, ya que si $(n, n-1) = d \neq 1$ entonces por definición $d \mid n$ y $d \mid n-1$, y así *d* divide a la diferencia, es decir $d \mid n - (n-1) = 1$, y por lo tanto $d = 1$.

[45] Sean $a, b, c \in \mathbb{Z}$. Si $(a,b) = (a,c) = 1$ entonces $(a, bc) = 1$.

[46] Sean $a, b \in \mathbb{Z}$ tal que $(a,b) = 1$, entonces la progresión aritmética $\{a + bk \mid k \in \mathbb{Z}\}$ contiene una infinidad de números primos.

Si separamos a los primos $4k+1$ y $4k+3$ de la descomposición de d', se tiene que

$$d' = \prod_{q_i | d'} {q_i}^{k_i} = \prod_{\substack{q_i | d' \\ q_i \equiv 1 (mod\ 4)}} {q_i}^{k_i} \prod_{\substack{q_i | d' \\ q_i \equiv 3 (mod\ 4)}} {q_i}^{k_i}$$

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

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

Ahora, el producto anterior tomará únicamente los valores de 1 o -1 (mod 4), pero $d' = 4j+1$, así que $d' \equiv 1\ (mod\ 4)$.

Y como

$$d' \equiv \prod_{\substack{q_i | d' \\ q_i \equiv 3 (mod\ 4)}} (-1)^{k_i}\ \ (mod\ 4),$$

entonces

$$\prod_{\substack{q_i | d' \\ q_i \equiv 3 (mod\ 4)}} (-1)^{k_i} = 1 \dots \dots \dots \dots \dots \dots \dots \dots \dots \dots \dots \dots \dots \dots \dots \dots \dots \dots \dots \dots \dots (2).$$

Se tiene que $\left(\frac{-1}{p}\right) = 1$, ya que $p \equiv 1\ (mod\ 4)$. Falta mostrar que $\left(\frac{-d'}{p}\right) = 1$.

Sabemos $-$por propiedades del símbolo de Legendre[47] y aunado a que $p \equiv -1\ (mod\ q_i)$ $-$ que:

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

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

---

[47] Si p y q son primos impares distintos tal que $p \equiv 1\ (mod\ 4)$ o $q \equiv 1\ (mod\ 4)$, entonces $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$. Sea p un primo impar y a, b números enteros. Si $a \equiv b\ (mod\ p)$, entonces $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.

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

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

Luego de la igualdad (2) tenemos que

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

Por lo tanto *n* es suma de tres cuadrados. ■

Quedan así definidos los primeros resultados concernientes a la representación de la suma de tres cuadrados. Es de sorprender que previamente los números de la forma $4k + 2$ no tuvieran tanta importancia cuando se trabajaba con la representación de la suma de dos cuadrados, pero, como es el caso, hasta los resultados aparentemente relegados pueden ser finalmente trascendentes.

Y dentro del mismo contexto de los enteros que son suma de tres cuadrados, tenemos otro lema que a continuación se expondrá. La idea de la demostración de este resultado es encontrar un primo p en la progresión aritmética $A = \left\{4nj + \frac{cn-1}{2} \mid j \in \mathbb{Z}\right\}$ de tal manera que $2p = d'n - 1$, donde $d' = 8j + c$,[48] y mediante el lema 2.1.4 bastará probar que $-d'$ es un residuo cuadrático módulo $2p$; y haciendo un pequeño análisis resultará que es suficiente demostrar que $-d'$ es un residuo cuadrático modulo p y así n será suma de tres cuadrados.

Lema 2.1.6 Si *n* es un entero positivo tal que $n \equiv 1, 3\ o\ 5\ (mod\ 8)$, entonces *n* puede ser representado como la suma de tres cuadrados.

Demostración. Damos por entendido que 1 es suma de tres cuadrados no negativos. Es por ello que consideramos a $n \geq 2$.

[48] En la hipótesis del lema, *n* es un entero positivo de tal forma que $n \equiv 1,3\ o\ 5\ (mod\ 8)$ y al inicio se definirá a $c = \begin{cases} 3\ si\ \ n \equiv 1\ (mod\ 8) \\ 1\ si\ \ n \equiv 3\ (mod\ 8). \\ 3\ si\ \ n \equiv 5\ (mod\ 8) \end{cases}$

Definimos: $c = \begin{cases} 3\ si & n \equiv 1\ (mod\ 8) \\ 1\ si & n \equiv 3\ (mod\ 8) \\ 3\ si & n \equiv 5\ (mod\ 8) \end{cases}$

Analicemos esto. Si $n \equiv 1\ (mod\ 8)$, entonces $cn \equiv c\ (mod\ 8)$, pero $8 \equiv 0\ (mod\ 8)$ y $c \equiv c + 8\ (mod\ 8)$, por lo que $cn \equiv c + 8\ (mod\ 8)$. Ahora, como $c = 3$ se tiene que $cn - 1 \equiv c + 7 \equiv 2\ (mod\ 8)$; de esta forma $\frac{cn-1}{2} \equiv 1\ (mod\ 4)$,[49] y análogamente para $n \equiv 3\ (mod\ 8)$.

En cualquier caso se tiene que

$$\text{Si } n \equiv 1{,}3\ (mod\ 8), \text{ entonces } \frac{cn-1}{2} \equiv 1\ (mod\ 4).$$

Ahora, si $n \equiv 5\ (mod\ 8)$, entonces $cn \equiv 5c\ (mod\ 8)$, esto es $cn \equiv 15 \equiv 7\ (mod\ 8)$; de esta forma $cn - 1 \equiv 6\ (mod\ 8)$. Por lo tanto $\frac{cn-1}{2} \equiv 3\ (mod\ 4)$.

De $\frac{cn-1}{2} \equiv 1\ (mod\ 4)$ y también de $\frac{cn-1}{2} \equiv 3\ (mod\ 4)$ se tiene que $(1,4) = \left(\frac{cn-1}{2}, 4\right) = 1$ y $(3,4) = \left(\frac{cn-1}{2}, 4\right) = 1$, respectivamente.

En cualquiera de los casos $\left(\frac{cn-1}{2}, 4\right) = 1$ ……(1),

por otro lado también se tiene que $\left(\frac{cn-1}{2}, n\right) = 1$ ……(2).[50]

De (1) y (2), tenemos que $\left(\frac{cn-1}{2}, n\right) = \left(\frac{cn-1}{2}, 4\right) = 1$, por tanto $\left(\frac{cn-1}{2}, 4n\right) = 1$. Por el teorema de *Dirichlet* existe un primo $\boldsymbol{p}$ de la forma $\boldsymbol{p} = 4\text{nj} + \frac{cn-1}{2}$ perteneciente al conjunto $A = \left\{4nj + \frac{cn-1}{2} \mid j \in \mathbb{Z}\right\}$ para alguna $j \in \mathbb{Z}^+$. Entonces

$2p = 8nj + cn - 1 = n(8j + c) - 1 = d'n - 1,$ ……(3),

donde $d' = 8j + c$.

Gracias al Lema 2.1.4, bastaría probar que $-d'$es un residuo cuadrático modulo $2p$. Si $-d'$ es un residuo cuadrático modulo *p*, entonces existe un entero x_0 tal que

$$x_0^2 \equiv -d'(mod\ p),$$

además como $2px_0 + p^2 \equiv 0\ (mod\ p)$, entonces $(x_0 + p)^2 \equiv x_0^2\ (mod\ p)$; así

---

[49] Haciendo sustituciones correspondientes para este caso, se llega a que $cn - 1$ es par. Además $(cn\text{-}1,\ 8) = 2$, y $2 \mid 2$, entonces $\frac{cn-1}{2} \equiv \frac{2}{2}\ (mod\ \frac{8}{2})$.

[50] Afirmamos que $\left(\frac{cn-1}{2}, n\right) = 1$, pues si $\left(\frac{cn-1}{2}, n\right) = d$, entonces $d \mid n$ y $d \mid \frac{cn-1}{2}$, y así $d \mid 2d \mid cn - 1$, pero $d \mid cn$ entonces $d \mid 1$, y en consecuencia $d = 1$.

$(x_0 + p)^2 + d' \equiv x_0^2 + d' \equiv 0\ (mod\ p)$ ……. (4).

Sea $x = x_0$, si x_0 es impar, y sea $x = x_0 + p$, si x_0 es par, entonces x es impar y $x^2 + d'$ es par, por lo tanto $x^2 + d' \equiv 0\ (mod\ 2)$, y por (4) $x^2 + d' \equiv 0\ (mod\ p)$; de esta manera, como $(2, p) = 1$ y por lo anterior tenemos que $x^2 + d' \equiv 0\ (mod\ 2p)$, es decir, basta probar que $-d'$ es un residuo cuadrático módulo p. Ahora retomemos a d' y lo descomponemos en producto de potencias de primos impares, así

$$d' = \prod_{q_i \mid d'} {q_i}^{k_i} \qquad \text{……. (5).}$$

De lo anterior, se tiene que de (3) $2p = d'n - 1$, por lo que $2p \equiv -1\ (mod\ d')$, y de (5) $2p \equiv -1\ (mod\ \prod_{q_i \mid d'} {q_i}^{k_i})$, es decir, $2p \equiv -1\ (mod\ q_i)$ y $(p, q_i) = 1\ \ \forall i \in \mathbb{N}$.

Retomando la parte inicial de la demostración, la cual se fragmentó en dos casos, vemos que:

Si $n \equiv 1\ o\ 3\ (mod\ 8)$, entonces $p \equiv 1\ (mod\ 4)$, y por consiguiente $\left(\frac{-1}{p}\right) = 1$, así

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

Aplicando el símbolo de Legendre al producto en (5) respecto a $\boldsymbol{p}$, tenemos que

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

Para el caso $n \equiv 5\ (mod\ 8)$, se tiene que $p \equiv 3\ (mod\ 4)$ y $d' \equiv 3\ (mod\ 8)$, ya que si $n \equiv 5\ (mod\ 8)$ entonces $c = 3$ y $d' = 8j + c = 8j + 3$.

Nuevamente, por (5) tenemos que

$$\begin{aligned} d' = \prod_{q_i \mid d'} {q_i}^{k_i} &= \prod_{\substack{q_i \mid d' \\ q_i \equiv 1 (mod\ 4)}} {q_i}^{k_i} \prod_{\substack{q_i \mid d' \\ q_i \equiv 3 (mod\ 4)}} {q_i}^{k_i} \\ &\equiv \prod_{\substack{q_i \mid d' \\ q_i \equiv 1 (mod\ 4)}} (1)^{k_i} \prod_{\substack{q_i \mid d' \\ q_i \equiv 3 (mod\ 4)}} (-1)^{k_i} \\ &\equiv \prod_{\substack{q_i \mid d' \\ q_i \equiv 3 (mod\ 4)}} (-1)^{k_i} \\ &\equiv 3\ (mod\ 4) \end{aligned}$$

$$\equiv -1\ (mod\ 4).$$

Así

$$\prod_{\substack{q_i \mid d' \\ q_i \equiv 3(mod\ 4)}} (-1)^{k_i} = -1 \qquad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (6).$$

Por reciprocidad cuadrática tenemos

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

ya que $p \equiv 3\ (mod\ 4)$ y por tanto $\left(\frac{-1}{p}\right) = -1$. Ahora, reanudando lo anterior

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

$$= -\prod_{\substack{q_i \mid d' \\ q_i \equiv 1(mod\ 4)}} \left(\frac{p}{q_i}\right)^{k_i} \prod_{\substack{q_i \mid d' \\ q_i \equiv 3(mod\ 4)}} \left(\frac{p}{q_i}\right)^{k_i} \prod_{\substack{q_i \mid d' \\ q_i \equiv 3(mod\ 4)}} (-1)^{k_i}\ ,^{51}$$

pero de (6)

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

Por lo tanto

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

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

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

Ahora bien, para cualquier primo $q_i \mid d'$, y tomando en cuenta que $2p \equiv -1(mod\ q_i)$, resulta lo siguiente

[51] Si p y q son primos impares distintos tal que $p \equiv q \equiv 3\ (mod\ 4)$. Entonces $\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$.

$$\left(\frac{-d'}{p}\right) = \prod_{q_i \mid d'} \left(\frac{p}{q_i}\right)^{k_i} = \prod_{q_i \mid d'} \left(\frac{2}{q_i}\right)^{k_i} \left(\frac{2p}{q_i}\right)^{k_i} = \prod_{q_i \mid d'} \left(\frac{2}{q_i}\right)^{k_i} \prod_{q_i \mid d'} \left(\frac{-1}{q_i}\right)^{k_i}.$$ [52]

De lo anterior nos importan los $q_{i's}$ donde $\left(\frac{2}{q_i}\right) = -1$, es decir, los $q_i \equiv \pm 3 \equiv 3{,}5\ (mod\ 8)$ y los $q_{i's}$ donde $\left(\frac{-1}{q_i}\right) = -1$, llevan a que $q_i = 4k + 3$. Ahora, de esta última igualdad multiplicando por dos ambos lados, se tiene que $2q_i = 8k + 6$, es decir,

$$2q_i \equiv 6\ (mod\ 8).$$

Retomando las congruencias lineales, basta con encontrar las soluciones de las q_i. Además, de la congruencia $2q_i \equiv 6\ (mod\ 8)$ tenemos que $(2, 8) = 2$ y como $2 \mid 6$, entonces dicha congruencia tiene exactamente dos soluciones módulo 8, a saber 3 y 7, ya que el conjunto $\left\{x_0 + \left(\frac{8}{2}\right) t \mid 0 \leq t < 2\right\}$, donde x_0 es una solución particular, contiene todas las soluciones. Si $x_0 = 3$ es una solución, entonces 7 = 3 + 4 (1) es la otra solución.

Así

$$q_i \equiv 3{,}7\ (mod\ 8).$$

Del producto anterior, se unificarán los productos donde $\left(\frac{2}{q_i}\right) = -1$, lo cual sucede cuando $q_i \equiv 3{,}5 (mod\ 8)$ y también los productos donde $\left(\frac{-1}{q_i}\right) = -1$, lo cual también sucede cuando $q_i \equiv 3{,}7 (mod\ 8)$. Así

$$\prod_{q_i \mid d'} \left(\frac{2}{q_i}\right)^{k_i} \prod_{q_i \mid d'} \left(\frac{-1}{q_i}\right)^{k_i} = \prod_{\substack{q_i \mid d' \\ q_i \equiv 3 (mod\ 8)}} (-1)^{k_i} \prod_{\substack{q_i \mid d' \\ q_i \equiv 5 (mod\ 8)}} (-1)^{k_i}$$

$$\prod_{\substack{q_i \mid d' \\ q_i \equiv 3 (mod\ 8)}} (-1)^{k_i} \prod_{\substack{q_i \mid d' \\ q_i \equiv 7 (mod\ 8)}} (-1)^{k_i}$$

[52] Se tiene que $(q_i, p) = 1\ \ \forall\ q_i \mid d'$, entonces $(q_i, 4p) = 1$ y también $\left(\frac{2^2}{q_i}\right) = 1$ para cualquier primo $q_i \mid d'$, así

$$1 = \left(\frac{2^2}{q_i}\right) \Rightarrow \left(\frac{p}{q_i}\right)\left(\frac{2^2}{q_i}\right) = \left(\frac{p}{q_i}\right),$$

por tanto

$$\left(\frac{p}{q_i}\right) = \left(\frac{p}{q_i}\right)\left(\frac{2^2}{q_i}\right) = \left(\frac{4p}{q_i}\right) = \left(\frac{2}{q_i}\right)\left(\frac{2p}{q_i}\right).$$

$$\equiv \prod_{\substack{q_i \mid d' \\ q_i \equiv 5 (mod\ 8)}} (-1)^{k_i} \prod_{\substack{q_i \mid d' \\ q_i \equiv 7 (mod\ 8)}} (-1)^{k_i}$$

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

por lo tanto

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

Así,$-d'$ es un residuo cuadrático módulo $2p = d'n - 1$ si

$$\sum_{\substack{q_i \mid d' \\ q_i \equiv 5,7}} k_i \equiv 0\ (mod\ 2),$$

que es lo que demostraremos a continuación. Nuevamente, tomemos a d' como descompuesto en primos de la siguiente manera

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

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

$$\equiv \prod_{\substack{q_i \mid d' \\ q_i \equiv 3,5 (mod\ 8)}} 3^{k_i} \prod_{\substack{q_i \mid d' \\ q_i \equiv 5,7 (mod\ 8)}} (-1)^{k_i}\ (mod\ 8).$$

En la factorización anterior se puede observar que d' queda expresado en potencias de tres y potencias de -1´s; en particular las potencias de este último son las que nos interesa tratar, pero para esto necesitamos retomar los dos casos que ya se habían mencionado. Las congruencias (7), (8), (9) y (10) se dan directamente, las pruebas se pueden observar en el apéndice C. Así que

si $n \equiv 1\ o\ 5\ (mod\ 8)$, entonces $c = 3$ y $d' = 8j + 3 \equiv 3\ (mod\ 8)$, y esto implica que

$$\sum_{\substack{q_i \mid d' \\ q_i \equiv 3,5 (mod\ 8)}} k_i \equiv 1\ (mod\ 2) \qquad \ldots\ldots\ldots\ldots\ldots\ldots (7),$$

y también

$$\sum_{\substack{q_i \mid d' \\ q_i \equiv 5,7 (mod\ 8)}} k_i \equiv 0\ (mod\ 2) \qquad \ldots\ldots\ldots\ldots\ldots\ldots\ldots (8).$$

Por otra parte, si $n \equiv 3\ (mod\ 8)$, entonces $c = 1$ y $d' = 8j + 1 \equiv 1\ (mod\ 8)$.

Y por tanto

$$\sum_{\substack{q_i \mid d' \\ q_i \equiv 3,5 (mod\ 8)}} k_i \equiv 0\ (mod\ 2) \qquad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (9),$$

y

$$\sum_{\substack{q_i \mid d' \\ q_i \equiv 5,7 (mod\ 8)}} k_i \equiv 0\ (mod\ 2) \qquad \ldots\ldots\ldots\ldots\ldots\ldots\ldots (10).$$

Entonces

$$\sum_{\substack{q_i \mid d' \\ q_i \equiv 5,7 (mod\ 8)}} k_i \equiv 0\ (mod\ 2),$$

en cualquiera de los dos casos. Así, $-d'$ es un residuo cuadrático módulo $2p = d'n - 1$, y de esta forma, por el lema 2.1.4, n es suma de tres cuadrados, que es lo que se quería demostrar. ■

El siguiente resultado, a diferencia de los anteriores, manifiesta qué números no pueden ser suma de tres cuadrados y se debe al gran genio de *Gauss*. Con esto ya nos acercamos a la necesidad de estudiar si cuatro cuadrados pueden representar a cualquier entero positivo, y esto quedará bien establecido con el teorema de Lagrange. Pero antes veamos el resultado de Gauss.

Teorema 2.1.7 Un entero positivo n se puede escribir como suma de tres cuadrados si y sólo si n no es de la forma $4^{\alpha}(8k+7)$, con α, k enteros no negativos.

Demostración. Sea $x \in \mathbb{Z}$ y $A = \{0,2,\dots,7\}$ un SCR módulo 8. Entonces existe $a \in A$ que es congruente con *x* tal que $x^2 \equiv a \ (mod\ 8)$, de esta forma, haciendo algunas operaciones, tenemos que

$$1^2 \equiv 1\ (mod\ 8), 2^2 \equiv 4\ (mod\ 8), 3^2 \equiv 1\ (mod\ 8), 4^2 \equiv 0\ (mod\ 8), 5^2 \equiv 1\ (mod\ 8), 6^2 \equiv 4\ (mod\ 8), 7^2 \equiv 1\ (mod\ 8).$$

Entonces para cualquier entero x tenemos que

$$x^2 \equiv 0{,}1\ o\ 4\ (mod\ 8).$$

Ahora, tomemos las diferentes combinaciones de un entero como suma de tres cuadrados. Así, si x, y, z son enteros, entonces

$$\begin{aligned} x^2 + y^2 + z^2 &\equiv 0+0+0 \equiv 0\ (mod\ 8) \\ &\equiv 0+0+1 \equiv 1\ (mod\ 8) \\ &\equiv 0+1+1 \equiv 2\ (mod\ 8) \\ &\equiv 1+1+1 \equiv 3\ (mod\ 8) \\ &\equiv 0+0+4 \equiv 4\ (mod\ 8) \\ &\equiv 0+1+4 \equiv 5\ (mod\ 8) \\ &\equiv 1+1+4 \equiv 6\ (mod\ 8) \\ &\equiv 0+4+4 \equiv 8\ (mod\ 8) \\ &\equiv 1+4+4 \equiv 9\ (mod\ 8) \\ &\equiv 4+4+4 \equiv 4\ (mod\ 8), \end{aligned}$$

pero $x^2 + y^2 + z^2 \not\equiv 7\ (mod\ 8)$. De aquí que la suma de tres cuadrados nunca puede ser congruente con 7 módulo 8, es decir, si $n \in \mathbb{Z}$ y *n* es suma de tres cuadrados entonces $n \not\equiv 7\ (mod\ 8)$. Ahora, si $4l = x^2 + y^2 + z^2$ con $x, y, z \in \mathbb{Z}$, entonces *x*, *y*, *z* deben de ser números enteros pares. Así

$$l = \left(\frac{x}{2}\right)^2 + \left(\frac{y}{2}\right)^2 + \left(\frac{z}{2}\right)^2.$$

Por lo tanto, $4^{\alpha}l$ es la suma de tres cuadrados si y sólo si l es la suma de tres cuadrados. Esto demuestra que cualquier entero que no se de la forma $4^{\alpha}(8k+7)$ puede ser expresado como suma de tres cuadrados.

Ahora, cualquier entero positivo *N* puede ser escrito de manera única en la forma $4^{\alpha}m$, donde $m \equiv 2\ (mod\ 4)$ ó $m \equiv 1,3, o\ 5\ (mod\ 8)$. Entonces por los lemas 2.1.5 y 2.1.6, el entero positivo *N* puede ser escrito como suma de tres cuadrados, excepto cuando *m* no es de la forma $8k + 7$. Por lo tanto si N no es de la forma $4^{\alpha}(8k + 7)$, entonces se puede escribir como suma de tres cuadrados. ■

El último teorema nos regresa al lema 2.1.6 para mostrarnos que unos de los casos también tienen elementos interesantes de paridad.

Teorema 2.1.8 Sea *n* un entero positivo tal que $n = 8k + 3$, entonces *n* es suma de tres cuadrados impares.

Demostración. En la demostración anterior teníamos que $x^2 \equiv 0,1\ o\ 4\ (mod\ 8)$, para cualquier entero *x*. Si *n* es suma de tres cuadrados entonces existen $x_1, x_2, x_3 \in \mathbb{Z}^+$ tal que $n = x_1^2 + x_2^2 + x_3^2$, y como $n \equiv 3\ (mod\ 8)$ por tanto $n = x_1^2 + x_2^2 + x_3^2 \equiv 3\ (mod\ 8)$, pero esto pasa si y sólo si $x_1^2 \equiv x_2^2 \equiv x_3^2 \equiv 1\ (mod\ 8)$ y por ende se tiene que cada cuadrado es impar. ■

Suma de cuatro cuadrados

Concluimos de lo anterior que no bastan tres cuadrados para poder expresar a cualquier entero positivo como suma de éstos. Viene entonces a la mente preguntarse si cuatro cuadrados serían suficientes para poder representar a todos los enteros positivos. Esto se demuestra en el teorema de Lagrange, que aunque Diofanto parece haberlo conjeturado, fue Claude Gaspard Bachet de Méziriac el primero en mencionarlo explícitamente en sus comentarios a la *Aritmética* de Diofanto; por su parte Fermat expresó que había descubierto una demostración, pero no la escribió; Euler trató de demostrar el resultado, pero no tuvo éxito alguno. Fue Lagrange el primero en demostrar y publicar su resultado en 1770.[53]

Al hablar del teorema de Lagrange nos referimos no sólo al problema de representar cualquier entero no negativo como suma de cuatro cuadrados, también nos acercamos a resultados importantes de la teoría aditiva de los números, como el que se refiere a conjuntos de enteros llamados *bases de algún orden k* para algún entero *k*. Pero es sin duda el teo-

[53] Véase Torrecillas, Blas [1999], pp. 39 – 40.

rema de Lagrange uno de los más importantes en esta rama de la matemática, ya que muchos resultados son una generalización de éste. En las páginas siguientes se demostrará dicho teorema, pero no sin antes probar algunos lemas que nos ayudarán a construir la demostración de Lagrange.

Lema 2.1.9 (Euler 1743) El producto de las sumas de cuatro cuadrados es suma de cuatro cuadrados.

Demostración.

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

Como en la identidad de Diofanto, el lema anterior muestra que el producto de las sumas de cuatro cuadrados es cerrado bajo el producto, mientras que el de tres cuadrados no lo es, es decir, el producto de las sumas de tres cuadrados no es suma de tres cuadrados; por ejemplo, 5 y 3 son cada uno suma de tres cuadrados, mientras que 15 no lo es.

Lema 2.2.0 (Euler 1751) Si p es un primo impar, entonces existen enteros x y y tales que $1+x^2+y^2 \equiv 0\ (mod\ p)$, donde $0 \leq x, y < \frac{p}{2}$.

Demostración. Sea p un primo impar y tomemos al conjunto $\{0,1,2,..,p-1\}$ como un SCR módulo p. Denotemos como A al siguiente conjunto

$$A = \left\{0^2, 1^2, 2^2, \dots, \left\{\frac{p-1}{2}\right\}^2\right\} = \left\{u^2 \middle| u = 0,1,2,3, \dots, \frac{p-1}{2}\right\},$$

que tiene $\frac{p+1}{2}$ distintas clases de congruencias módulo p. Por otra parte, tomemos a los inversos aditivos de los elementos de A y restémosle una unidad, dicho conjunto tiene, al igual que A, $\frac{p+1}{2}$ distintas clases de congruencias modulo p, es decir

$$B = \left\{-u^2 - 1 \middle| u = 0,1,2, \dots, \frac{p-1}{2}\right\}.$$

Afirmamos que no existen elementos de A que sean congruentes entre ellos, ya que suponiendo que existen dos elementos distintos u^2, v^2 en A tal que $u^2 \equiv v^2 (mod\ p)$, entonces

$u \equiv \pm v\ (mod\ p)$; teniendo como hipótesis que $u, v \leq \frac{p-1}{2}, u \neq v$ y $u \not\equiv v\ (mod\ p)$, si $u \equiv -v\ (mod\ p)$, entonces $p \mid u + v$, lo cual es imposible ya que

$$0 < u + v \leq \frac{p-1}{2} + \frac{p-1}{2} = p - 1 < p,$$

así, no existen $u^2, v^2 \in A$ tal que $u^2 \equiv v^2 (mod\ p)$. De la misma forma, no existen elementos distintos de *B* que sean congruentes. Ahora bien $\#(A \cup B) = p + 1$.[54] Entonces por el *principio del palomar*[55] tienen que existir $u^2 \in A$ y $-w^2 - 1 \in B$, tal que

$0 \leq u, w \leq \frac{p-1}{2} < \frac{p}{2}$, y además

$$u^2 \equiv -w^2 - 1\ (mod\ p),$$

es decir,

$$u^2 + w^2 + 1 \equiv 0\ (mod\ p).$$

Si $x = u$ y $y = w$, entonces $x^2 + y^2 + 1 \equiv 0\ (mod\ p)$. ■

El siguiente resultado forma parte de la demostración del teorema de Lagrange, y por ello pasamos a presentarlo con mayor detalle.

Corolario 2.2.1 Sea *p* un primo impar. Entonces existe un entero positivo $n < p$, tal que *np* se puede escribir como suma de cuatro cuadrados.

Demostración. Por 1.3.3, existen enteros *x, y* tales que $1 + x^2 + y^2 \equiv 0\ (mod\ p)$, donde $0 \leq x, y < \frac{p}{2}$, así $0^2 + 1^2 + x^2 + y^2 = np$ para algún $n \in \mathbb{N}$. Ahora,

$$np = 1 + x^2 + y^2 < \frac{p^2}{4} + \frac{p^2}{4} + 1 = \frac{p^2}{2} + 1 < p^2, \text{ entonces } n < p,$$

por lo que

$$np = 0^2 + 1^2 + x^2 + y^2, \text{ donde } n < p. \quad ■$$

El teorema fundamental de la Aritmética n os muestra que todo número natural puede ser expresado como producto de números primos, y como el siguiente lema nos mostrará que cualquier primo puede ser escrito como suma de cuatro cuadrados, y el lema 1.3.2 nos dice que el producto de ellos también es suma de cuatro cuadrados, entonces cualquier

[54] Denotamos al símbolo ♯ como la cardinalidad de un conjunto.
[55] Si *n+ 1* objetos se deben colocar en *n* casillas, entonces en alguna de las casillas hay más de un objeto.

natural será suma de cuatro cuadrados y por ende el *Teorema de Lagrange* quedaría así demostrado.

Lema 2.2.2 Todo número primo p puede ser escrito como suma de cuatro cuadrados.

Demostración. Asumimos que p es un primo impar, y para el caso de 2 ya sabemos que es suma de cuatro cuadrados. Apoyándonos en el Principio del Buen Orden y del corolario anterior, entonces asumimos que existe un mínimo entero positivo *m* tal que

$mp = w^2 + x^2 + y^2 + z^2$ ……(1),

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

Como *m* es un entero entonces puede ser tanto par como impar. Si *m* es par entonces *mp* es par, por lo cual w, x, y, z deben ser todos de la misma paridad o exactamente dos de ellos de la misma paridad, entonces sin pérdida de generalidad supongamos que

$$w \equiv x \ (mod\ 2) \ \text{ y } \ y \equiv z \ (mod\ 2),$$

y así $\frac{w \pm x}{2}, \frac{y \pm z}{2}$ son enteros, de esta forma

$$\left(\frac{w+x}{2}\right)^2 + \left(\frac{w-x}{2}\right)^2 + \left(\frac{y+z}{2}\right)^2 + \left(\frac{y-z}{2}\right)^2 = \frac{w^2 + x^2 + y^2 + z^2}{2} = \left(\frac{m}{2}\right)p.$$

Por tanto $\left(\frac{m}{2}\right)p$ puede ser expresado como suma de cuatro cuadrados, lo cual es una contradicción, pues m es el mínimo entero positivo tal que mp es suma de cuatro cuadrados. En conclusión, *m* tiene que ser impar y además veremos que tiene que ser exactamente 1.

Para demostrar esto supongamos que $m > 1$. Tomemos a los enteros no negativos *a, b, c* y *d* del sistema completo de residuos módulo *m* entre $\frac{-m}{2}$ y $\frac{m}{2}$, tal que

$$w \equiv a \ (mod\ m), x \equiv b \ (mod\ m), y \equiv c \ (mod\ m), z \equiv d \ (mod\ m),$$

entonces

$$a^2 + b^2 + c^2 + d^2 \equiv w^2 + x^2 + y^2 + z^2 \equiv 0 \ (mod\ m).$$

Así, para algún $n \in \mathbb{N}$

$a^2 + b^2 + c^2 + d^2 = mn$ ……(2),

y como $\frac{-m}{2} < a, b, c, d < \frac{m}{2}$, tenemos que

$$0 \leq mn = a^2 + b^2 + c^2 + d^2 < 4\left(\frac{m}{2}\right)^2 = m^2,$$

por lo tanto

$$0 \leq n < m.$$

Pero n no será cero, ya que si $n = 0$, entonces $a = b = c = d = 0$, por lo que $w \equiv x \equiv y \equiv z \equiv 0(mod\ m)$; así $m^2 \mid w^2 + x^2 + y^2 + z^2$, lo que implica $m^2 \mid mp$ y $m \mid p$, lo cual no puede ser, pues $1 < m < p$. En conclusión

$$1 \leq n < m.$$

Por el lema 2.1.9

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

Por (1) y (2)

$(mp)(mn) = m^2np = r^2 + s^2 + t^2 + u^2$ ……(3),

donde

$$\begin{aligned}r &= wa + xb + yc + zd, \\ s &= wb - xa + yd - zc, \\ t &= wc - xd + ya - zb, \\ u &= wd + xc - yb - za.\end{aligned}$$

Como $w \equiv a\ (mod\ m)$, entonces $wa \equiv a^2 \equiv w^2(mod\ m)$, y lo mismo ocurre con las demás congruencias $x \equiv b\ (mod\ m),\ y \equiv c\ (mod\ m),\ z \equiv d\ (mod\ m)$, pues se obtiene que $xb \equiv x^2 \equiv b^2(mod\ m)$, $yc \equiv c^2 \equiv y^2(mod\ m)$ y $zd \equiv d^2 \equiv z^2(mod\ m)$, por lo que

$$r = wa + xb + yc + zd \equiv w^2 + x^2 + y^2 + z^2 \equiv 0\ (mod\ m).$$

Así $s \equiv t \equiv u \equiv 0\ (mod\ m)$, de esta manera *r, s, t* y *u* son divisibles por *m* y al dividir (3) entre m^2, se tiene

$$np = \left(\frac{r}{m}\right)^2 + \left(\frac{s}{m}\right)^2 + \left(\frac{t}{m}\right)^2 + \left(\frac{u}{m}\right)^2.$$

Donde $n < m$ y np es suma de cuatro cuadrados, lo cual es imposible, ya que *m* es el mínimo entero que cumple dicha propiedad. Por ello la condición $m > 1$ no es posible y no queda más que $m = 1$.

Por lo tanto

$$p = w^2 + x^2 + y^2 + z^2. \quad \blacksquare$$

Finalmente pasamos a demostrar el teorema de Lagrange, el cual prácticamente está hecho.

Teorema 2.2.3 (Lagrange 1770) Todo entero positivo *n* se puede escribir como suma de cuatro cuadrados.

***Demostración*.** El caso para $n = 1$ es directo, entonces consideremos a $n > 1$. Tomemos la descomposición canónica de *n* en potencias de primos, es decir

$$n = \prod_{i \in \mathbb{N}} p_i^{\alpha_i}.$$

Por el resultado anterior cada primo p_i, puede ser escrito como suma de cuatro cuadrados, por tanto cada potencia $p_i^{e_i}$ también, y por el lema 2.1.9 (Euler) el producto $\prod_{i \in \mathbb{N}} p_i^{\alpha_i}$ es suma de cuatro cuadrados, que es exactamente *n*. ■

Capítulo 3

Suma de cubos

Con el teorema de Lagrange demostramos que cualquier entero positivo se puede escribir como suma de cuatro cuadrados y ésta ya es la cantidad mínima de ellos que se requiere para que todo entero se pueda escribir como suma de cuatro de ellos. La pregunta inmediata que nos podríamos hacer estaría en torno a la posibilidad de tratar de generalizar la idea de la suma de cuadrados y con ello plantear que cualquier entero también se puede expresar como una suma de un número determinado de cubos. En este capítulo trabajaremos para encontrar cuántos cubos se necesitan para expresar a cualquier entero como suma de cubos. Pero antes abundaremos en torno del problema general.

Bajo el razonamiento anterior llegamos a una serie de preguntas cada vez más generales, y ya no sólo podríamos pensar que los enteros positivos se pueden expresar como suma de 4 cuadrados o un número determinado de cubos, sino también como una suma de cuartas potencias y, en general, como una suma de k-ésimas potencias para cualquier número natural k.

El primero en proponer estas representaciones de los enteros fue Edward Waring en su libro *Meditationes Algebraicae*, publicado en 1770, pero no pudo dar pasos definitivos para demostrar su propuesta. El primer avance definitivo lo dio Lagrange cuando demostró que todo entero positivo se puede escribir como una suma de cuadrados. Posteriormente Linnik probó que a partir de cierto entero todos los demás se puede escribir como una suma de siete cubos, o dicho de otro modo, salvo una cantidad finita de enteros, todos se pueden escribir como suma de siete cubos.[56]

Si quisiéramos saber para cualquier entero k positivo el menor número de k-ésimas potencias que se necesitarían para expresar a cualquier entero positivo, entonces sí estamos ante un gran problema pues hasta la fecha no se ha podido resolver esta cuestión para cual-

[56] Teorema 2.3, véase Melvyn B. Nathanson [1996], pp. 46-49.

quier *k*, más adelante se exponen algunos valores para *k* en los cuales el problema de Waring[57] ha quedado resuelto.

Hilbert nos brinda la demostración general de que cualquier entero positivo sí se puede expresar como la suma de *k-ésimas* potencias,[58] para cualquier *k* en los enteros positivos. Pero aún nos queda por saber explícitamente la cantidad mínima de potencias requeridas para cada *k*. En este capítulo sólo nos quedamos con algunos casos particulares de *k* en los que sí se ha logrado avanzar.

Antes de adentrarnos más en el tema damos unas definiciones.

Definición

Sea *A* un conjunto de números enteros. Se dice que el conjunto *A* es una **base de orden *k***, si cualquier entero puede ser escrito como suma de *k* enteros de *A* no necesariamente distintos. Se dice que *A* es una **base asintótica de orden *k***, si cualquier entero suficientemente grande puede ser escrito como suma de exactamente *k* elementos de *A*. Por ejemplo los cuadrados son una base de orden cuatro.

Definición

Sea $g(k)$ el mínimo número *s* de *k-ésimas* potencias necesarias para representar cualquier número entero positivo como suma de ellas, es decir, si $n \in \mathbb{N}$ y $x_i \in \mathbb{Z}^+$.

$$n = x_1^k + x_2^k + \cdots + x_{g(k)=s}^k .$$

El propósito de este capítulo es probar que los cubos son una base de orden 9, esto significa que para cualquier entero no negativo n, existen $x_1 \ldots x_9$, tal que

$$n = x_1^3 + x_2^3 + \cdots + x_9^3.$$

Para este propósito nos apegaremos a la demostración hecha por Wieferich y Kempner,[59] y para el desglose de ésta, probaremos previamente cuatro lemas que serán de ayuda para su mejor entendimiento.[60] Antes de ocuparnos con los detalles de la demostración de la suma de los nueve cubos, consideramos que es importante exponer los resultados

[57] Cada número entero es un cubo o la suma de 2, 3, 4,...,8 o 9 cubos; cada entero es o una cuarta potencia o la suma de 2, 3,..., 19 cuartas potencias de enteros no negativos y así sucesivamente.
[58] Publicado en *Göttingen Nachrichten* (*1909*) *17-36 y Math. Annalen 67* (*1909*)*, 281-305*.
[59] Véase B. Nathanson, Melvyn [1996], pp. 41-43.
[60] Lemas (3.1), (3.2), (3.3) y (3.4).

obtenidos en décadas pasadas para sí comprender por qué no se pudo llegar al resultado con seis, siete u ocho cubos, pero sí con nueve. Para esto recurrimos a unos trabajos de L.E. Dickson,[61] publicados en 1928 y 1935, y que están relacionados con los cuatro lemas antes señalados.

Trabajos previos de L. E. Dickson

En 1928 y 1939, L.E. Dickson publicó los artículos: *"Una demostración simple del teorema de Waring sobre cubos, con varias generalizaciones"*, y *"Todos los enteros excepto 23 y 239 son suma de ocho cubos"*. Cada uno contiene elementos vinculados con la suma de cubos para resolver el problema de Waring. Sobre los artículos mencionados sólo nos ocuparemos de los resultados vinculados con lo que atañe a Waring y las justificaciones se pueden ver en los artículos. Cabe mencionar que Dickson no expone las demostraciones de sus resultados; el motivo radica en que dichas pruebas en su gran mayoría son numéricas y además son el complemento (una extensión) de cálculos ya realizados.[62] Pasemos a enunciar los resultados requeridos.

Se tiene que cualquier entero N tal que $1 \leq N \leq 40000$, es suma de 6 cubos no negativos, y también que cualquier entero positivo $N \leq 40000$ es representable como suma de 7 cubos no negativos, excepto

15, 22, 56, 114, 167, 175, 186, 212, 231, 238, 303, 364, 420, 428 y 454.

Además, 23 y 239 son los únicos enteros que requieren 9 cubos.

De la lista de números antes expuestos se infiere que son necesarios más de 7 cubos para poder representarlos, y por lo tanto el mínimo número de cubos que posiblemente se requerirán serán 8, y precisamente sí son 8 cubos.

Entonces bastan 7 cubos para representar a todos los enteros positivos del mismo rango, salvo 23 y 239 [63] y los listados antes. Así, se puede observar que el entero 454 es el más grande que requiere 8 cubos. De los cálculos realizados por Dickson y Von Sterneck,

[61] L.E. Dickson [1928] y [1938], *Transactions of America Mathematical Society*.

[62] En 1903 Von Sterneck, por medio de una tabla numérica, mostró que cualquier entero N, tal que $8042 < N \leq 40000$, es suma de 6 cubos no negativos. Dickson amplió esa lista para cualquier $1 \leq N \leq 123000$ y posteriormente alcanzó hasta 560000.

[63] El teorema de Linnik [Nathanson, 1996].

se ve que solo 121 enteros requieren 7 cubos y el mayor de ellos es 8042; por tanto, si $N > 8042$ entonces *N* es suma de 6 cubos no negativos.

De esta forma, y de acuerdo con las dos definiciones que anteriormente mencionamos, el conjunto de los números cúbicos son una base asintótica de orden 6 para cualquier entero $8042 < N \leq 40000$. Linnik mostraría más adelante que si *N* es un entero suficientemente grande, entonces los cubos son una base asintótica de orden 7.

Uno los objetivos del primer artículo de Dickson [1928] es presentar algunos resultados generales para la representación de los números enteros como suma de cubos no negativos. Para esto define a C_n como la suma de *n* cubos no negativos, y además toma a $t \geq 0$. A partir de lo anterior ahora enunciamos sólo algunos de sus resultados

- La forma $f_t = tx^3 + C_8$ representa a todos los enteros positivos $\leq 40{,}000$ si y solo si $0 < t \leq 23$.

  Es claro aquí que si $t = 0$, entonces implicaría que $f_t = C_8$, pero esto no nos representa a todos los enteros menores que 40000, porque 23 y 239 ≤ 40,000 no se pueden representar – se mencionó antes - como suma de 8 cubos.

  En el caso más general, ya que $0 < t \leq 23$, entonces $0 \leq 23 - t < 23$ y también $23 < 239 - t < 239$; de esta forma $23 - t$ y $239 - t$ son suma de ocho cubos de acuerdo a lo que se escribió con anterioridad,[64] es decir, se cumple que $23 = C_8 + t$ y $239 = C_8 + t$, por lo cual $x = 1$ en la forma $f_t = tx^3 + C_8$.
- La forma $f_l = ly^3 + C_7$ representa a todos los enteros positivos $\leq 40{,}000$ si y solo si $l = 2 - 6{,}9 - 15$. f_7 representa todos $\leq 40{,}000$ excepto 22. f_8 representa todos excepto 23, 239 y 428.

Veamos el ejemplo para el caso del entero 15. Supongamos que 15 es de la forma descrita, es decir $f_l = 15$; de esta forma si $l > 15$ o si $l = 0$, entonces $f_l \neq 15$, ya que $15 = 2^3 + 7 \cdot 1^3$, o bien 15 cubos, donde dichos cubos son todos 1´s, entonces son necesarios al menos 8 cubos o bien 15 cubos para poder representarlos; en cualquier caso 15 no es representado por la forma $f_l = ly^3 + C_7$ fuera del rango mencionado.

[64] Los cálculos a los que Dickson hace referencia, y que no exhibe de manera explícita, pero que sí menciona nos permiten decir que por medio de esas cuentas los enteros 23 y 239 requieren 9 cubos, pues no bastan 8 para poder representarlos; de esta forma $23 - t$ y $239 - t$ requerirían ocho cubos para poder ser representados.

- Todo entero n es congruente módulo 96 a $N\gamma^3 + 6\mu$, para $0 \leq \gamma \leq 23$ y μ suma de tres cuadrados.

El punto de convergencia del segundo artículo (1939) es precisamente demostrar que todo entero positivo *N* es suma de ocho cubos, excepto 23 y 239. Para tal demostración el autor utiliza una serie de 5 lemas que a continuación se mencionarán, e insistimos en que las pruebas son totalmente numéricas y aquí no se presentan.

Lema I.- Todo entero $n \geq 233^6 D$ es una suma de 8 cubos si $D = 14.0029628$ o más generalmente si $D = d$, donde

$$d > 14 + \left(\frac{24}{167}\right)^3 \qquad d \leq 14.1.$$

Lema II.- Todo entero entre 8043 y 123,000 es suma de 6 cubos.
El siguiente lema es una extensión del lema II.

Lema III.- Todo entero entre 123,000 y 560,000 es suma de 6 cubos.

El siguiente lema es una consecuencia de los dos anteriores.

Lema IV.- Todo entero entre 8043 y 41623625 es una suma de 6 cubos.

Lema V.- Dados un entero positivo S y un número B, tales que $0 \leq B \leq S$, podemos encontrar un entero $i \geq 0$, tal que

$$B \leq S - i^3 < B + 3S^{\frac{2}{3}}.$$

De este último lema se puede concluir, mediante algunas sustituciones, que todo entero no menor que 455 es una suma de ocho cubos, y por debajo de 455, de acuerdo a los datos obtenidos por Dickson, 23 y 239 son los únicos enteros que requieren 9 cubos.[65]
Todo lo mencionado sobre representaciones de enteros positivos como suma de cubos es únicamente para cualquier entero N que se encuentra entre 1 y 40000.

Cuando se llegue al objetivo de este capítulo, que es el teorema de Wieferich – Kempner, únicamente mostraremos que cualquier entero $N > 40000$ es suma de nueve cubos, y de esta manera el problema de Waring respecto a cubos quedará probado.

[65] Para mayores detalles ver *All integers except 23 and 239 are sums of eight cubes.* L. E. Dickson [1939].

Con la información anterior, pasamos a detallar y a demostrar los primeros tres lemas (3.1, 3.2, 3.3) que ayudan a la prueba del teorema principal, que es el 3.5.

Todo entero es suma de nueve cubos

Como ya se mencionó al inicio del capítulo, nuestro objetivo es demostrar que todo entero se puede escribir como suma de nueve cubos, y mencionamos que se requieren cuatro lemas para la demostración hecha por Wieferich y Kempner. Ahora damos paso a los lemas correspondientes.

Lema 3.1 Sean *x*, *y* enteros no negativos, tales que $x \leq y^2$ y además *x* es suma de tres cuadrados. Entonces $6y(y^2 + x)$ es suma de 6 cubos no negativos.

Demostración. Por hipótesis sabemos que *x* es suma de tres cuadrados, entonces existen x_1, x_2, x_3 enteros no negativos, tales que $x = x_1^2 + x_2^2 + x_3^2$. Es claro que para cualquier $i = 1,2,3$ $0 \leq x_i^2 \leq x$, y como $x \leq y^2$, entonces $0 \leq x_i^2 \leq x \leq y^2$. Por lo tanto

$$0 \leq x_i \leq \sqrt{x} \leq y,$$

así

$$x_i \leq y \implies y - x_i \geq 0 \qquad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (1),$$

además

$$0 \leq x_i \leq 2x_i \leq y + x_i \implies y + x_i \geq 0 \qquad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (2).$$

Ahora damos lugar a la demostración de que $\boldsymbol{6y(y^2 + x)}$ es suma de 6 cubos no negativos.

$$\boldsymbol{6y(y^2 + x)} = 6y(y^2 + x_1^2 + x_2^2 + x_3^2) = 6y^3 + 6yx_1^2 + 6yx_2^2 + 6yx_3^2$$

$$= (2y^3 + 6yx_1^2) + (2y^3 + 6yx_2^2) + (2y^3 + 6yx_3^2) = \sum_{i=1}^{3} (2y^3 + 6yx_i^2)$$

$$= \sum_{i=1}^{3} y^3 + y^3 + 3yx_i^2 + 3yx_i^2$$

$$= \sum_{i=1}^{3} y^3 + y^3 + 3yx_i^2 + 3yx_i^2 + (3y^2x_i - 3y^2x_i) + (x_i^3 - x_i^3)$$

$$= \sum_{i=1}^{3} (y^3 + 3y^2x_i + 3yx_i^2 + x_i^3) + (y^3 - 3y^2x_i + 3yx_i^2 - x_i^3)$$

$$= \sum_{i=1}^{3} (y + x_i)^3 + (y - x_i)^3 \, .$$

De (1) y (2) los sumandos son no negativos, por lo tanto $\boldsymbol{6y(y^2 + x)}$ es una suma de seis cubos no negativos. ■

Lema 3.2 Para todo entero impar *b*, existe un entero impar a tal que

$$b \equiv a^3 (mod\ 2^t), \text{ con } t \geq 1.$$

Demostración. Sea $S = \{0,1,2,3, \dots, 2^t - 1\}$ un sistema completo de residuos módulo 2^t y de este conjunto considérese al subconjunto de los impares $S_2 = \{1,3, \dots, 2^t - 1\}$. El cubo de cada uno de los impares de S_2 es congruente a uno y solo uno de los impares del conjunto *S*.

Ahora veamos que el cubo de cualesquiera dos elementos de S_2, es decir, del conjunto $\{1^3, 3^3, 5^3, \dots (2^t - 1)^3\}$, no pueden ser congruentes módulo 2^t.

Tomemos dos impares a_1, a_2 de S_2 y sus cubos correspondientes a_1^3 y a_2^3, y supongamos que

$$a_1^3 \equiv a_2^3 (mod\ 2^t),$$

por lo tanto

$$2^t \mid a_2^3 - a_1^3 = (a_2 - a_1)(a_2^2 + a_2a_1 + a_1^2),$$

pero como $(a_2^2 + a_2a_1 + a_1^2)$ es impar, entonces

$$2^t \mid a_2 - a_1 \qquad \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots (1),$$

es decir

$$a_1 \equiv a_2 (mod\ 2^t),$$

pero $a_1,\ a_2$ son dos enteros impares de distintas clases de residuos, así $a_1 \not\equiv a_2 (mod\ 2^t)$, lo que contradice (1). Por lo tanto $a_1^3 \not\equiv a_2^3 (mod\ 2^t)$, es decir, cualesquiera dos cubos impares en $\{1^3, 3^3, 5^3, \dots (2^t - 1)^3\}$ caen en diferentes clases residuales de los impares módulo 2^t. Con esto podemos concluir que como cualquier impar es congruente a uno y solo uno de los impares en S_2, entonces para cualquier impar *b* existe un entero impar a tal que $b \equiv a^3 (mod\ 2^t)$.

Lema 3.3 Si $r \geq 22^3 = 10648$, 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*.** Para la construcción de r será necesario que m sea suma de tres cuadrados, pero primero analizaremos qué pasa cuando m no es suma de tres cuadrados. Del teorema 2.1.7 sabemos que si m *no es suma de tres* cuadrados, entonces $m = 4^{\alpha}(8k + 7)$ con α y k enteros no negativos; de esta forma

$$6m = 6 \cdot 4^{\alpha}(8k + 7).$$

Así,

♦ **si $\boldsymbol{\alpha \geq 2}$**, entonces

$$6m = 6 \cdot 4^{\alpha}(8k + 7) = 6 \cdot 4^{\alpha-2+2}(8k + 7) = 6 \cdot 4^2 \cdot 4^{\alpha-2}(8k + 7) = 96 \cdot 4^{\alpha-2}(8k + 7)$$
$$\equiv 0 \ (mod\ 96).$$

♦ **Si $\boldsymbol{\alpha = 1}$**, entonces

$$6m = 6 \cdot 4^{\alpha}(8k + 7) = 6 \cdot 4^{1}(8k + 7) = 24(8k + 7) = 24 \cdot 4(2t) + 168$$
$$= 96(2t) + 168 \equiv 168 \equiv 72 \ (mod\ 96).$$

♦ **Si $\boldsymbol{\alpha = 0}$ y $\boldsymbol{k}$ es un entero par** (sea $\boldsymbol{k = 2r}$, $\boldsymbol{r} \in \mathbb{Z}$)**,** entonces

$$6m = 6 \cdot 4^{\alpha}(8k + 7) = 6 \cdot 4^{0}(8(2r) + 7) = 96r + 42 \equiv 42 \ (mod\ 96).$$

♦ **Si $\boldsymbol{\alpha = 0}$ y $\boldsymbol{k}$ es un entero impar** (sea $\boldsymbol{k = 2r + 1}$, $\boldsymbol{r} \in \mathbb{Z}$), entonces

$$6m = 6 \cdot 4^{\alpha}(8k + 7) = 6 \cdot 4^{0}(8(2r + 1) + 7) = 96r + 90 \equiv 90 \ (mod\ 96).$$

De acuerdo con lo anterior si *m* no es suma de tres cuadrados entonces tenemos que

$$6m \equiv \begin{cases} 0 \pmod{96}, \ si\ \alpha \geq 2 \\ 72 \pmod{96}, \ si\ \alpha = 1 \\ 42 \pmod{96}, \ si\ \alpha = 0\ y\ k\ es\ par \\ 90 \pmod{96}, \ si\ \alpha = 0\ y\ k\ es\ impar. \end{cases}$$

Así, para este caso siempre existe un entero positivo g, que toma uno de los valores del conjunto $\{0, 72, 42, 90\}$, y que pertenecen a un SCR módulo 96,[66] tal que

$$6m \equiv g \ (mod\ 96).$$

Ahora, pasemos al caso en que *m* es suma de tres cuadrados. Suponemos que para cada número 6*m* existe un entero *h* que pertenece a un SCR módulo 96 tal que

[66] Consideremos al SCR módulo 96 como el conjunto $A = \{1,2, \ldots, 96\}$.

$$6m \equiv h \ (mod\ 96).$$

Como 6 divide a 96 y a $6m$, entonces h es un múltiplo de 6, por lo tanto h debe pertenecer al conjunto

$$B = \{6,12,18,24,30,36,48,54,60,66,78,84\}.$$[67]

Entonces podemos señalar que si m es un entero positivo que es suma de tres cuadrados, por lo tanto existe un entero h en un SCR módulo 96, tal que

$$6m \equiv h \ (mod\ 96),$$

donde $h \in B$.

Enseguida se mostrará una tabla (figura 11) en la se construyen los enteros $d^3 + h$ módulo 96, con $h \in B\ y\ d \in [0,22]$. La finalidad de construir esta tabla es para obtener un sistema completo de residuos módulo 96, con enteros de la forma $d^3 + h$, y cabe señalar que no es necesario considerar a todos los enteros del intervalo $[0,22]$, pues los cubos de algunos de ellos dejan el mismo resto módulo 96, como $12^3 \equiv 0^3, 16^3 \equiv 4^3, 20^3 \equiv 8^3\ (mod\ 96)$. De esta manera basta considerar a

$d \in D = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 13, 14, 15, 17, 18, 22\}$.

	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					

Figura 11: SCR módulo 96

[67] Este es un subconjunto de SCR denotado por A –ver nota a pie anterior-, y que además no contiene a los elementos $0, 72, 42, 90$, vinculados con el caso de m cuando no es suma de tres cuadrados.

Así, se muestra que los números enteros $d^3 + h$ forman un sistema completo de residuos módulo 96. Con este nuevo SCR tenemos que para $r \geq 22^3 \geq d^3 \geq 0$, entonces existe un entero del SCR tal que $r \equiv d^3 + h\ (mod\ 96)$, donde $h \in B$.

Como $r - d^3 \equiv h\ (mod\ 96)$ y h es múltiplo de seis, entonces $r - d^3 = 6m'$, pero si $6m' \equiv h\ (mod\ 96)$, y *h* pertenece al conjunto

$$B = \{6,12,18,24,30,36,48,54,60,66,78,84\},$$

entonces m' es suma de tres cuadrados. En otras palabras $r = d^3 + 6m'$, donde m' es suma de tres cuadrados y $d \in [0,22]$. Por lo tanto queda probado el lema. ■

Quedan mostrados también los primeros tres lemas de los cuatro que ya hemos citado y que son vitales para la demostración del teorema de Wieferich y Kempner. Ahora pasamos a enunciar el último lema, para después probar el teorema principal de nuestro capitulo. La demostración del cuarto lema (3.4) es de tipo numérico y corresponde básicamente a la conclusión de lo mencionado en los artículos de Dickson.

Lema 3.4 Si $1 \leq N \leq 40{,}000$, entonces

(i) *N* es una suma de nueve cubos no negativos.

(ii) $Si\ N \neq 23\ o\ 239$, entonces *N* es una suma de ocho cubos no negativos.

(iii) $Si\ N \neq 23\ o\ 239$ 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 suma de siete cubos no negativos.

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

Teorema 3.5 (Wieferich-Kempner) Todo entero no negativo es la suma de nueve cubos no negativos.

Demostración. Los cuatro lemas anteriores ahora serán usados para simplificar la demostración de este teorema. Anteriormente en el Lema 3.4, se mostró que todo *N* tal que $1 \leq N \leq 40{,}000$, puede ser escrito como suma de nueve cubos no negativos. Ahora bien, el problema se reduce a mostrar que todo entero $N > 40{,}000$ es suma de nueve cubos no negativos. Para esto, la prueba se dividirá en dos partes, en la primera veremos que se cumple para todo entero $N > 8^{10}$, y la segunda parte que lo hace para todos los enteros $40{,}000 < N \leq 8^{10}$.

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

Primera parte

Para esta parte consideremos que $n = \left[N^{\frac{1}{3}}\right]$. Por hipótesis $N > 8^{10}$, entonces $N^{\frac{1}{3}} > (8^{10})^{\frac{1}{3}} = \left(8^{\frac{1}{3}}\right)^{10} = 2^{10}$. De la parte entera de ambos lados de la desigualdad se tiene que $n > 2^{10}$.

Como $N > 8^{10}$, entonces el mínimo valor que puede tomar N es $8^{10} + 1 = 1{,}073{,}741{,}825$, y el mínimo para n es $n = \left[N^{\frac{1}{3}}\right] = [1024] = 1024 = 2 \cdot 8^3 = 2^{10}$.

Así, para cualquier $k \geq 2$, se tiene que $k + 1 \geq 3$. Entonces

$$8^{k+1} \geq 8^3, \text{ por tanto } 2 \cdot 8^{k+1} \geq 2 \cdot 8^3 = 2^{10} = n.$$

De esta forma

$$\mathbf{2^{10} \leq n \leq 2 \cdot 8^{k+1}} \quad \text{.....(1).}$$

Afirmamos que existe un entero $k \geq 3$, tal que

$$8 \cdot 8^{3k} < N \leq 8 \cdot 8^{3(k+1)},$$

y esto se obtiene al elevar al cubo las partes de (1).

Definamos a $N_i = N - i^3$ para $i = 1,2, \ldots, n$, y también a $d_i = N_{i-1} - N_i$. Entonces

$$d_i = N_{i-1} - N_i = N - (i-1)^3 - N + i^3 = 3i^2 - 3i + 1,$$

y como $i \geq 1$ se puede afirmar que $3i^2 - 3i + 1 < 3i^2$ si y sólo si $-3i + 1 < 0$, y esto pasa si y sólo si $3i > 1$.

Por lo tanto

$$d_i = 3i^2 - 3i + 1 = 3i^2 - (3i - 1) < 3i^2.$$

Además, $i \leq n = \left[N^{\frac{1}{3}}\right] \leq N^{\frac{1}{3}}$ por lo que $3i^2 \leq 3N^{\frac{2}{3}}$. Entonces

$$d_i = 3i^2 - 3i + 1 < 3i^2 \leq 3N^{\frac{2}{3}},$$

y esto puede quedar acotado por [68]

$$3N^{\frac{2}{3}} \leq \frac{3 \cdot 8^{2k+3}}{2}.$$

[68] Por la fórmula (1) $n \leq 2 \cdot 8^{k+1}$, entonces $N^{\frac{1}{3}} \leq 2^{3k+4}$ por lo cual $\left(N^{\frac{1}{3}}\right)^2 \leq \left(2^{k+1}\right)^2 \cdot \left(2^{2k+3}\right)^2$, y así $2N^{\frac{2}{3}} \leq 2^{2k+3} \cdot 4^{2k+3}$, de esta forma $2N^{\frac{2}{3}} \leq 8^{2k+3}$ y por tanto $3N^{\frac{2}{3}} \leq \frac{3 \cdot 8^{2k+3}}{2}$.

De esta manera

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

Elíjase algún $i \in \{1, 2, 3, \dots, n\}$ tal que

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

Ya que $i \geq 1$ y tomando a $k \geq 3$, entonces por definición de N_i tenemos que $N_n = N - n^3$.

Ahora bien, afirmamos que [69]

$$N_n = N - n^3 \leq (n+1)^3 - n^3 - 1 = 3n^2 + 3n < 6n^2,$$

y por (1) se tiene que $6n^2 \leq 3 \cdot 8^{2k+3}$.

Así, ya tenemos que

$$N_n = N - n^3 \leq 3n^2 + 3n < 6n^2 \leq 3 \cdot 8^{2k+3},$$

y como $k \geq 3$, entonces $3 \leq 8^{k-2}$ $3 \cdot 8^{2k} \cdot 8^3 \leq 8 \cdot 8^{3k}$ y así $3 \cdot 8^{2k+3} \leq 8 \cdot 8^{3k+1}$,

por lo tanto

$$\boldsymbol{N_n = N - n^3 \leq 3n^2 + 3n < 6n^2 \leq 3 \cdot 8^{2k+3} \leq 8^{3k+1} = 8 \cdot 8^{3k}} \quad \text{.....(3).}$$

Para terminar esta parte, de (2) se deduce que $i \leq n - 1$.

Por la definición de N_i es claro también que $N_i < N_{i-1}$. Por otra parte

$$N_{i-1} = N_{i-1} + [0 + 0] = N_{i-1} + [(N_i - N_i) + (N_{i+1} - N_{i+1})] = d_i + d_{i+1} + N_{i+1}.$$

Anteriormente, se tenía que

$$d_i < \frac{3 \cdot 8^{2k+3}}{2} \qquad \forall i = 1, \dots, n.$$

$$d_i + d_{i+1} + N_{i+1} < \frac{3 \cdot 8^{2k+3}}{2} + \frac{3 \cdot 8^{2k+3}}{2} + 8 \cdot 8^{3k} = 3 \cdot 8^{2k+3} + 8 \cdot 8^{3k},$$

y a la vez,[70] $3 \cdot 8^{2k+3} + 8 \cdot 8^{3k} \leq 11 \cdot 8^{3k}$.

En resumen, se tiene que

$$\boldsymbol{N_{i-1} < 3 \cdot 8^{2k+3} + 8 \cdot 8^{3k} \leq 11 \cdot 8^{3k}} \quad \text{.....(4).}$$

---

[69] Supongamos que la siguiente desigualdad es verdadera $N - n^3 \leq (n+1)^3 - n^3 - 1$, entonces $N \leq n^3 + 3n^2 + 3n + 1 - 1$ si y sólo si $N \leq \left[N^{\frac{1}{3}}\right]^3 + 3\left[N^{\frac{1}{3}}\right]^2 + 3\left[N^{\frac{1}{3}}\right]$ si y sólo si $N \leq N + 3n^2 + 3n$, si y sólo si $0 \leq 3n^2 + 3n$, como la última desigualdad es verdadera entonces la primera lo es.

[70] Por hipótesis $k \geq 3$, entonces $0 \geq 3 - k$ y así $8^{3-k} \leq 1$. Por tanto de la cadena siguiente de desigualdades se sigue $8^{3-k} \leq 1$, y así $3 \cdot 8^{3-k} \leq 3$, así $8^{3k}(3 \cdot 8^{2k+3-3k} + 8) \leq 11 \cdot 8^{3k}$ y de este modo $3 \cdot 8^{2k+3} + 8 \cdot 8^{3k} \leq 11 \cdot 8^{3k}$.

Como la igualdad $d_i = N_{i-1} - N_i$, es siempre impar, entonces uno de los enteros de la resta es impar. Ahora, elijase $a \in \{i, i-1\}$ de tal forma que $N_a = N - a^3$ sea un número impar. El lema 3.2 nos garantiza la existencia de un entero impar en el SCR modulo 8^k, es decir, existe un entero impar $b \in [1, 8^k - 1]$, tal que

$$N - a^3 \equiv b^3 (\, mod\ 8^k).$$

Como $b \in [1, 8^k - 1]$, entonces $1 \leq b < 8^k$, por lo tanto

$0 < b^3 < 8^{3k}$ .....(5).

También, como $a \in \{i, i-1\}$, entonces $N_i \leq N_a \leq N_{i-1}$, y por (2) tenemos $8 \cdot 8^{3k} \leq N_i$, de esta forma $8 \cdot 8^{3k} \leq N_a = N - a^3$, por lo cual

$8 \cdot 8^{3k} - 8^{3k} \leq (N - a^3) - 8^{3k}$ ..... (6).

Ahora de (5), $(N - a^3) - 8^{3k} < (N - a^3) - b^3 = N - a^3 - b^3$, y de esto último y también por (6) se tiene que $8 \cdot 8^{3k} - 8^{3k} < N - a^3 - b^3$. De esta forma

$$\mathbf{7 \cdot 8^{3k}} = 8 \cdot 8^{3k} - 8^{3k} < N - a^3 - b^3 < N - a^3 = N_a \leq N_{i-1} < \mathbf{11 \cdot 8^{3k}} \quad \text{.....(7).}$$

Como $N - a^3 \equiv b^3 (\, mod\ 8^k)$, entonces existe $q \in \mathbb{Z}$ tal que $N - a^3 - b^3 = 8^k q$. Por lo tanto, sustituyendo $8^k q$ por $N - a^3 - b^3$ en la desigualdad (7) nos da

$\mathbf{7 \cdot 8^{3k} < 8^k q} < 11 \cdot \mathbf{8^{3k}}$, y así $\mathbf{7 \cdot 8^{2k}} < q < 11 \cdot \mathbf{8^{2k}}$..... (8).

Tómese a $r = q - 6 \cdot 8^{2k}$. Es claro que $8^6 > 22^3$, y como $k \geq 3$, entonces $8^{2k} \geq 8^6$. Ahora, por (8) se tiene que $7 \cdot 8^{2k} < q$, por lo que $8^{2k} < q - 6 \cdot 8^{2k}$, es decir, $8^{2k} < r$. Por (8) se tiene que $q < 11 \cdot 8^{2k}$; entonces, de manera análoga a lo anterior

$$r = q - 6 \cdot 8^{2k} < 5 \cdot 8^{2k}.$$

Por lo tanto

$\mathbf{22^3 < 8^6 \leq 8^{2k}} < r < 5 \cdot \mathbf{8^{2k}}$ .....(9).

De (9) $r > 22^3$, y por el lema 3.3, *r* se expresa como $r = d^3 + 6m$, donde $0 \leq d \leq 22$ y *m* es suma de tres cuadrados. Sea $A = 8^k$ y como $r = d^3 + 6m$ y $d^3 \geq 0$, entonces $6m \leq r$ y por lo tanto $m \leq \frac{r}{6}$.

También por (9) se tiene que $r < 5 \cdot 8^{2k}$, entonces $\frac{r}{6} < \frac{5 \cdot 8^{2k}}{6}$, por lo tanto

$$\frac{5 \cdot 8^{2k}}{6} < 8^{2k} = A^2,$$

así

$\boldsymbol{m \leq \frac{r}{6} < \frac{5 \cdot 8^{2k}}{6} < A^2}$ .....(10).

Como $N - a^3 \equiv b^3 (\, mod\ 8^k)$, entonces

$N = a^3 + b^3 + 8^k \cdot q = a^3 + b^3 + 8^k(r + 6 \cdot 8^{2k})$

$= a^3 + b^3 + 8^k(d^3 + 6m + 6 \cdot 8^{2k})$

$= a^3 + b^3 + (2^k d)^3 + 8^k(6m + 6 \cdot 8^{2k})$

$= a^3 + b^3 + (2^k d)^3 + A(6m + 6A^2)$.

Si hacemos a $c = 2^k d$, se tiene que $N = a^3 + b^3 + c^3 + A(6m + 6A^2)$ ..... (11); por (10) se tiene que $m < A^2$, y m como suma de tres cuadrados; entonces, por el lema 3.1, tenemos que $A(6A^2 + 6m)$ es suma de seis cubos no negativos, y (11) queda como sigue.

$$N = a^3 + b^3 + c^3 + A(6m + 6A^2) = a^3 + b^3 + c^3 + \sum_{i=1}^{6} x_i^3.$$

Por lo tanto N es la suma de nueve cubos, y así la primera parte queda demostrada.

Segunda parte

Para terminar, ahora demostraremos la segunda parte, la que corresponde a demostrar que todo entero N tal que $40{,}000 < N \leq 8^{10}$, se puede escribir también como suma de nueve cubos. Para esto requerimos **c**onstruir al entero $a = \left[(N - 10{,}000)^{\frac{1}{3}}\right]$, y **c**omo $N > 40{,}000$ entonces $N - 10{,}000 > 30{,}000$. Por lo tanto

$$a = \left[(N - 10{,}000)^{\frac{1}{3}}\right] > (30{,}000)^{\frac{1}{3}},$$

y como $(30{,}000)^{\frac{1}{3}} = 31.07 > 31$, entonces

$$a = \left[(N - 10{,}000)^{\frac{1}{3}}\right] > (30{,}000)^{\frac{1}{3}} > 31.$$

Por otro lado, sea

$$d = (a + 1)^3 - a^3 = 3a^2 + 3a + 1,$$

y como $a > 31$, entonces $3a^2 + 3a + 1 < 4a^2$.

De la construcción de a se tienen la siguiente desigualdad $a < N^{\frac{1}{3}}$, entonces $4a^2 < 4N^{\frac{2}{3}}$. Por lo tanto $d = (a + 1)^3 - a^3 = 3a^2 + 3a + 1 < 4a^2 < 4N^{\frac{2}{3}}$.

Afirmamos que $N-(a+1)^3<10{,}000$ y también que $10{,}000\leq N-a^3$.[71]

Ahora bien

$$\begin{aligned} N-a^3 &= N-a^3+0 \\ &= N-a^3+[(a+1)^3-(a+1)^3] \\ &= N-(a+1)^3+[(a+1)^3-a^3] = N-(a+1)^3+d. \end{aligned}$$

Anteriormente teníamos que $d\leq 4N^{\frac{2}{3}}$ y $N-(a+1)^3<10{,}000$, por lo cual

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

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

Si $N-a^3\leq 40{,}000$, entonces por el lema 3.4 tenemos que $N-a^3$ es suma de 6 cubos y por tanto se llega al resultado.

Pero, si $N-a^3>40{,}000$, se construye otro entero $b=\left[(N-a^3-10{,}000)^{\frac{1}{3}}\right]>31$, tal que

$$N-a^3-(b+1)^3<10{,}000\leq N-a^3-b^3<10{,}000+4(N-a^3)^{\frac{2}{3}}.$$

Ahora, si $N-a^3-b^3\leq 40{,}000$, entonces por el lema 3.4 tenemos que $N-a^3-b^3$ es suma de seis cubos y así el resultado quedaría demostrado. Si $N-a^3-b^3>40{,}000$, se construye otro entero $c=\left[(N-a^3-b^3-10{,}000)^{\frac{1}{3}}\right]>31$, tales que

$$\begin{aligned} N-a^3-b^3-(c+1)^3<10{,}000 &\leq N-a^3-b^3-c^3 \\ &< 10{,}000+4(N-a^3-b^3)^{\frac{2}{3}} \\ &< 10{,}000+4\left(10{,}000+4\left(10{,}000+4N^{\frac{2}{3}}\right)^{\frac{2}{3}}\right)^{\frac{2}{3}} \\ &\leq 10{,}000+4\left(10{,}000+4\left(10{,}000+4(8^{10})^{\frac{2}{3}}\right)^{\frac{2}{3}}\right)^{\frac{2}{3}} \\ &= 10{,}000+4\left(10{,}000+4(10{,}000+4{,}194{,}304)^{\frac{2}{3}}\right)^{\frac{2}{3}} \\ &= 10{,}000+4\left(10{,}000+4(26049.301)\right)^{\frac{2}{3}} \end{aligned}$$

[71]Supongamos que la siguiente desigualdad es verdadera: $N-(a+1)^3<10{,}000$ por lo tanto $N-10{,}000<(a+1)^3$, entonces $(N-10{,}000)^{\frac{1}{3}}<(a+1)$, por tanto $\left[(N-10{,}000)^{\frac{1}{3}}\right]<[a+1]$ y así $a<a+1$ si y sólo si $0<1$; como esta última desigualdad es cierta, entonces la primera lo es. La desigualdad $10{,}000\leq N-a^3$ se da por la construcción de *a*.

$$= 10{,}000 + 4(2353.804 \ldots\ldots)$$
$$= 19{,}415.21637 \ldots\ldots < 20{,}000.$$

Por lo tanto, si $40{,}000 < N < 8^{10}$, entonces existen *a, b, c* enteros no negativos, tales que $10{,}000 < N - a^3 - b^3 - c^3 \leq 40{,}000$, y por el Lema 3.4 inciso (iv), $N - a^3 - b^3 - c^3$ puede ser escrito como suma de seis cubos no negativos, es decir, existen $x_i \in \mathbb{Z}^+$, con $i = 1,2, \ldots,6,$ tales que

$$N - a^3 - b^3 - c^3 = \sum_{i=1}^{6} x_i^3,$$

por lo tanto

$$N = a^3 + b^3 + c^3 + \sum_{i=1}^{6} x_i^3.$$

De esta forma *N* es la suma de nueve cubos, en cualquiera de los dos casos tomados. ■

Finalmente ya se demostró que todo entero no negativo se puede expresar como suma de 9 cubos no negativos, pero realmente 23 y 239, son los únicos enteros que necesitan de los nueve cubos, como lo muestra Dickson en 1939. En 1909 Landau muestra que todo entero suficientemente grande es suma de 8 cubos, aunque solo 15 enteros no negativos necesitan 8 cubos para ser representados. Linnik y Watson muestran independientemente que para cualquier entero suficientemente grande son necesarios siete cubos,[72] por tanto, se puede pensar que la representación de los enteros como suma de cubos se puede ir acotando, salvo para un numero finito de enteros.

Por otro lado se tiene que si $n \equiv \pm 4 \ (mod\ 9)$, entonces *n* no puede ser suma de tres cubos, por tanto existe un número infinito de enteros no negativos que necesitan más de tres cubos. De esta forma podemos inferir superficialmente que la representación de los enteros no negativos, como suma de cubos, está acotada inferiormente por 4 y superiormente por 9.

[72] Ya sabemos que todo entero no negativo es suma de nueve cubos, y si *n* es un número distinto de los siguientes valores y suficientemente grande,

15,22,23,56,114,167,175,186,212,231,238,239,303,364,420,428 *y* 454,

entonces *n* es suma de siete cubos.

Algunas líneas de trabajo actual

Ya sabemos que para representar a todo entero positivo como suma de cuadrados se requieren cuatro, pero si se usan dos o tres de ellos entonces existirán una infinidad de enteros que no pueden ser la suma de estas cantidades de cuadrados. Para el caso de la representación como suma de cubos son necesarios nueve para representar a cualquier entero positivo como suma de ellos, pero a partir de un número suficientemente grande todos pueden ser representados con una suma mayor o igual que cuatro cubos. Edward Waring fue más lejos y conjeturó que todo entero positivo se puede escribir como una suma de no más de 19 cuartas potencias. En 1964 Chen demostró que se requieren 37 quintas potencias para la representación correspondiente.

En el Capítulo 3 ya habíamos comentado lo que hoy se conoce como "Problemas de Waring", que era la representación de cualquier entero positivo como suma de *n*-ésimas potencias. Recordemos el gran problema que consiste en plantearse, dada una potencia *k*, entonces ¿cuál es el menor número requerido de estas potencias para representar a todo entero positivo? Ya habíamos definido a $g(k)$ como el menor número requerido de potencias de *k* para representar a todos los enteros positivos. Entonces la pregunta anterior se puede replantear como ¿cuál es valor de $g(k)$? A pesar de los esfuerzos para conocer cómo es $g(k)$ para cualquier *k* la siguiente tabla nos muestra lo poco que se sabe sobre el tamaño de $g(k)$.

- $g(2) = 4$ Conjetura de Fermat demostrada por Lagrange en 1770.
- $g(3) = 9$ Conjetura de Waring, demostrada por Wieferich en 1912.
- $g(4) = 19$ Conjetura de Waring, demostrada por el grupo de Balasubramanian, Dress y Deshouillers en 1986.
- $g(5) = 37$ Demostrada por Chen en 1964.
- $g(6) = 73$ Demostrada por Pillai en 1940.
- $g(7) = 143$ Demostrada por R.M. Stemmler en 1964.
- $g(8) = 279$ Demostrada por R.M. Stemmler en 1964.
- $g(9) = 548$ Demostrada por R.M. Stemmler en 1964.

♦ $g(10) = 1079$ Demostrada por R.M. Stemmler en 1964.

Podemos ver que solo se tiene certidumbre para *k* entre 2 y 6, para k entre 7 y 10 la información ya no es tan precisa, pero de once en adelante el camino ya es totalmente oscuro. Ya mencionamos que Hilbert demostró que todo entero se puede representar como suma de *k*-ésimas potencias, es decir, por Hilbert sabemos que $g(k)$ existe, pero el gran problema es conocer su valor exacto.

Otra vertiente que se generó a partir de este problema de Waring es conocer ¿Cuál es el menor número de potencias de *k* para el que existan sólo un número finito de fallas para representar a todo entero positivo? Por ejemplo, tenemos que para los cubos esa cantidad es mayor o igual que cuatro, es decir, a partir de un número suficientemente grande todo entero positivo puede ser escrito como suma mayor a tres cubos, lo que nos lleva a que la cantidad de fallas es finita.

Definamos a $G(k)$ como el menor número de potencias de *k* en el que existen solo un número finito de excepciones, es decir, si se quiere representar a los enteros positivos con menos potencias *k*, $G(k)$ tendrá sólo una cantidad finita de fallas. En este contexto sabemos que $G(2) = 4$ y $g(2) = 4$; para los cubos, $g(3) = 9$ y $4 \leq G(3) \leq 7$. Aquí estamos frente a $G(k)$ que es otro problema que aún está lleno de interrogantes, de $G(k)$ conocemos muy poco, y sólo podemos dar algunas aproximaciones en la tabla que sigue:

♦ $G(2) = 4$

♦ $4 \leq G(3) \leq 7$

♦ $G(4) = 16$

♦ $6 \leq G(5) \leq 17$ La cota superior R.C. Vaughan y T.D. Wooley [conjetura $G(5) = 6$].

♦ $9 \leq G(6) \leq 24$ La cota superior R.C. Vaughan y T.D. Wooley [conjetura $G(6) = 9$].

♦ $8 \leq G(7) \leq 33$ La cota superior R.C. Vaughan y T.D. Wooley [conjetura $G(7) = 8$].

♦ $32 \leq G(8) \leq 42$ Conjetura $G(8) = 32$.

♦ $13 \leq G(9) \leq 50$ Conjetura $G(9) = 13$.

♦ $12 \leq G(10) \leq 59$ Conjetura $G(8) = 12$.

Sólo conocemos con exactitud como es $G(k)$ para k = 2 y 4, para los restantes sólo se conocen rangos. En 1984 R. Balasubramanian y C. J. Mozzochi demostraron que

$$G(k) \leq \frac{-2\mathrm{Ln}(3k) - \mathrm{Ln}(6k)}{\mathrm{Ln}\frac{k-1}{k}} - 4,$$

esta cota superior es grande pero mejora un poco para k grande. R.C. Vaughan y T.D. Wooley obtienen (entre otras) las siguientes cotas para $10 \leq k \leq 20$.

$$G(k) \leq \left[\frac{157}{19}k - 23\right].$$

Además, I.M. Vinogradov obtuvo la cota $G(k) \leq 6k\log k + (4 + \log 216)k$, que mejoró con $G(k) < k(3\log k + 11)$. En 1959 demostró mediante su método de sumas trigonométricas que, para cualquier entero k suficientemente grande

$$G(k) < k(2\log k + 4\mathrm{loglog}\, k + 2\mathrm{logloglog}\, k + 13).$$

Y D.T. Wooley obtiene para valores grandes de k que

$$G(k) \leq k(\log k + \mathrm{loglog}\, k + O(1)).$$

Ésta es una muestra de los problemas que aún se tiene que resolver en la Teoría aditiva de los números, y con esto podemos tomar conciencia de que esta disciplina, la teoría de los números, mantiene un ritmo sorprendente de trabajo de investigación.

Apéndice A

La función $f(n)$

Ya se sabe que los números de la forma $4k+1$ se pueden representar como suma de dos cuadrados; además se demostró que si dichos números son primos entonces su representación es única. Si se deja de lado la propiedad de ser primo, entonces la representación como suma de dos cuadrados de dichos números no necesariamente es única, y si además consideramos orden y signos estos números tienen diferentes representaciones. Por lo anterior es preferible una notación que nos dé todas las representaciones de un número entero como suma de dos cuadrados; sea ésta $f(n)$. En seguida se describirán algunas consecuencias que se pueden extraer de la función mencionada.

Así, $f(n)$ se define como el número de representaciones de n en términos de una suma de dos cuadrados, considerando orden y signos, es decir, si

$$A = \{(x,y) \mid x^2 + y^2 = n, n \in \mathbb{N}, x, y \in \mathbb{Z}\}.$$

Entonces $f(n) = \#A$.[73]

Ejemplo. Si $n = 160$ entonces $f(n) = 8$ y las representaciones son éstas:

$$160 = (12)^2 + (4)^2 = (4)^2 + (12)^2 = (-12)^2 + (-4)^2 = (-4)^2 + (-12)^2$$
$$= (-4)^2 + (12)^2 = (12)^2 + (-4)^2 = (-12)^2 + (4)^2 = (4)^2 + (-12)^2.$$

En general, si un número n tiene como representación de suma de dos cuadrados al par (b,c), entonces n tendrá 8 representaciones, a saber

$$(b,c)\ (-b,c)\ (b,-c)\ (-c,-b)$$
$$(c,b)\ (c,-b)\ (-c,b)\ (-b,-c)'$$

y si la representación como suma de dos cuadrados es $(a,0)$ o (a,a), entonces $f(n)$ tendrá 4 representaciones en ambos casos, a saber

$$(a,0)\ (-a,0) \quad (a,a) \quad (-a,a)$$
$$(0,a)\ (0,-a) \quad (-a,-a)\ (a,-a).$$

[73] Denotamos $\#A$, como la cardinalidad del conjunto A.

Un ejemplo peculiar es cuando n es una potencia de 2, es decir, si $n = 2^m, m \in \mathbb{N}$. *Una potencia de dos se puede expresar como suma de dos cuadrados y además de 4 formas.* Así

$$f(2^m) = 4 \quad \forall m \in \mathbb{N}.$$

Para verificar lo anterior basta con expresar a $n = 2^m$ de la siguiente manera:

Si m es par, entonces $n = 2^m = \left(2^{\frac{m}{2}}\right)^2 + 0^2$, cuya representación se denotaría con el par $(a, 0)$, donde $a = 2^{\frac{m}{2}}$ y se obvia la segunda entrada del par ordenado.

Si $m = 2k + 1$ es impar, entonces $n = 2^m = 2^{2k+1} = (2^k)^2 \cdot 2 = (2^k)^2 + (2^k)^2$, cuya representación se denotaría con el par (a, a), donde $a = 2^k$.

En cualquiera de los dos casos se tendrían 4 formas de representación para una potencia de 2, ya que se mencionó que cualquier entero positivo que tenga a los pares $(a, 0)$ y (a, a) como representaciones en suma de dos cuadrados, tendrán 4 formas. Por otro lado aplicando el teorema de Jacobi[74] se llega al mismo resultado

$$f(2^m) = 4[\tau(1, 2^m) - \tau(3, 2^m)].$$

Los divisores de 2^m son 1, 2,…,$2^{m-1}, 2^m$, y queda claro que en dichos divisores sólo el 1 es impar, y por tanto $\tau(1, 2^m) = 1$, y como los divisores restantes son pares entonces $\tau(3, 2^m) = 0$. Por lo tanto

$$f(2^m) = 4\,[\tau(1, 2^m) - \tau(3, 2^m)] = 4[1 - 0] = 4.$$

En general, la función $f(n)$ hace explícita la cantidad de representaciones de *n* como suma de dos cuadrados, pero no dice quiénes son o cómo encontrar a cada una de ellas. Ahora bien, en matemáticas en ocasiones es importante, más no indispensable, saber que más allá de lo analítico se encuentran las interpretaciones geométricas, y en especial la de las funciones. Entonces es indiscutible pensar que existen interpretaciones geométricas que involucran la función $f(n)$; un ejemplo de ello es la suma $\sum_{i=1}^{n} f(i)$. Veámoslo de la siguiente manera

$$f(1) = \#\{(x, y) \mid x, y \in \mathbb{Z}, x^2 + y^2 = 1\}$$
$$f(2) = \#\{(x, y) \mid x, y \in \mathbb{Z}, x^2 + y^2 = 2\}$$

[74] Para tono número natural *n* se tiene que $f(n) = 4[\tau(1, n) - \tau(3, n)]$. En la parte final de suma de dos cuadrados mencionamos este teorema.

⋮

$$f(n) = \#\{(x,y) \mid x,y \in \mathbb{Z}, x^2 + y^2 = n\}.$$

Así, la suma $\sum_{i=1}^{n} f(i)$ representa geométricamente a todos los puntos reticulares del plano cartesiano que cumplen la ecuación $x^2 + y^2 \leq n$, donde $x, y \in \mathbb{Z}$.

Ejemplo. Si $n = 5$ entonces $\sum_{i=1}^{5} f(i) = 20$, es decir, existen 20 puntos en el plano que cumplen que $x^2 + y^2 \leq 5$ y $x, y \in \mathbb{Z}$. Haciendo algunas cuentas queda claro que tanto *x* como *y* no deben exceder de $\sqrt{5}$. En general, de la ecuación $x^2 + y^2 \leq n$ queda claro también que tanto *x* como *y* no deben exceder de $\sqrt{n}$.

Nuevamente, si tomamos a todos los puntos $P = (x, y)$ tales que $x^2 + y^2 \leq n$, de modo que sean el centro de cuadrados unitarios, entonces el área de la región formada por todos los cuadrados unitarios – *llamamos R a esa región* – también representa a $\sum_{i=1}^{n} f(i)$. La figura A muestra la región de dicha suma.

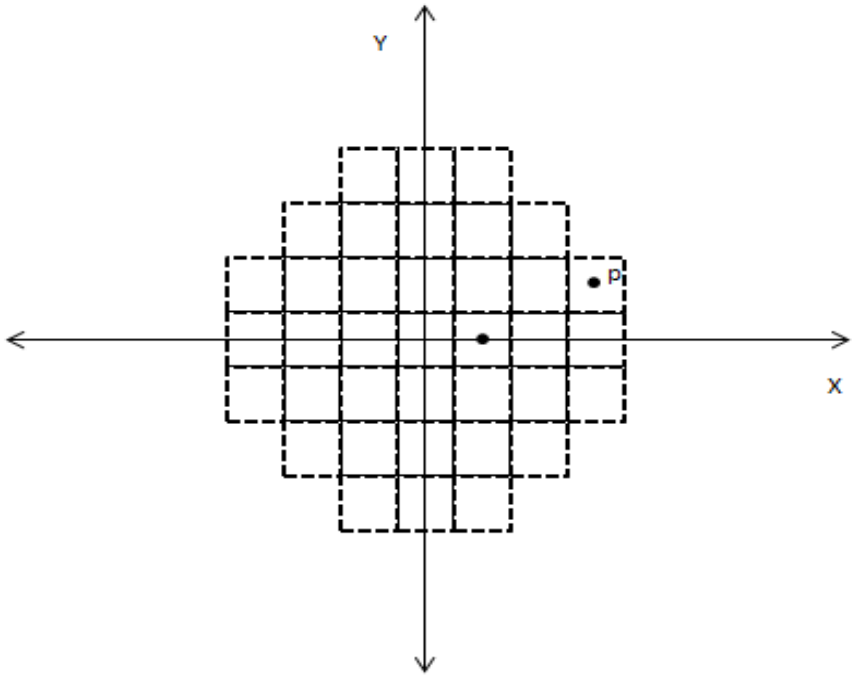


Figura A.

Si tomamos todos los puntos en el plano cartesiano que cumplen la ecuación $x^2 + y^2 \leq n$, y dejamos a un lado la propiedad de que $x, y \in \mathbb{Z}$, entonces la suma $\sum_{i=1}^{n} f(i)$ representará a todos los puntos (x, y) que viven en el interior y en el círculo $x^2 + y^2 = n$,

y que son exactamente los puntos que están dentro de la región R, y así dicha región queda como una aproximación al círculo de radio $\sqrt{n}$.

Es lógico encontrarse en algunas ocasiones con resultados que más allá de cumplir con cierta propiedad, traen consigo algunas características importantes, y esta función de representación es uno de esos resultados. Anteriormente se vio que $f(n)$ es siempre un múltiplo de 4, y mediante cálculos sencillos, nos encontraremos que el número de dichas representaciones no es totalmente creciente, más bien en algunos números dicha función suele ser repetitiva; entonces para una cantidad de representaciones de ciertos enteros hay un promedio, y por lo tanto vale la pena pensar en el valor característico de una serie de datos que en este caso son el número de representaciones de los números naturales. Se demostrará que cuando la cantidad de enteros *n* va creciendo indefinidamente dicho valor característico es siempre muy cercano a π.

Así, si denotamos a $F(n)$ como el valor promedio de $f(n)$, entonces

$$F(n) = \frac{1}{n+1}\sum_{i=1}^{n} f(i) = \frac{1}{n+1} \cdot (\text{Área de R}) \ldots\ldots (1),$$

y se demostrará que

$$\lim_{n\to\infty} f(n) = \pi.$$

Para la prueba se tomará y analizará desde un punto *(x, y)* de la región R, y después sólo se generalizará para el conjunto de cuadrados unitarios que será exactamente la región descrita. Sea $P = (x, y)$ tal que $x^2 + y^2 = n = \left(\sqrt{n}\right)^2$ – *obsérvese la figura B* - Es claro que la distancia del origen al punto P es exactamente $\sqrt{n}$; ahora, por la desigualdad del triángulo, tenemos que – tomando a P'como un vértice del cuadrado unitario de P-.

$$d(0, P') \leq d(0, P) + d(P, P').$$

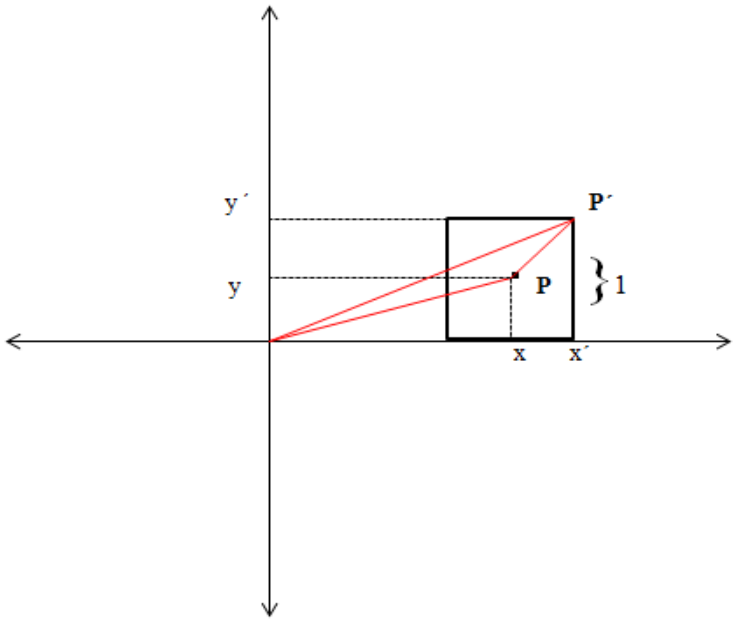


Figura B.

Pero como $d(0,P)=\sqrt{n}$, $d(P,P')=\frac{\sqrt{2}}{2}$ - esta última igualdad se desprende de la diagonal del cuadrado unitario -, entonces

$$\sqrt{n} < d(0,P') \leq \sqrt{n}+\frac{\sqrt{2}}{2} \ldots\ldots (2).$$

Se había mencionado que la región R está formada por todos los cuadrados unitarios con centro (x,y) y que viven en el círculo $x^2+y^2=n=\left(\sqrt{n}\right)^2$ y en el interior de el. Entonces dicha región está contenida en el círculo concéntrico al origen y de radio $d(0,P')$ y por lo tanto R también está contenida en el círculo concéntrico al origen y con radio $\sqrt{n}+\frac{\sqrt{2}}{2}$; esto último se cumple por (2).

Por otra parte es claro que la desigualdad $\sqrt{n}-\frac{\sqrt{2}}{2}<\sqrt{n}=d(0,P)<\sqrt{n}+\frac{\sqrt{2}}{2}$ se cumple; así, en términos de áreas, se tiene que la región R contiene al círculo con centro en el origen y radio $\sqrt{n}-\frac{\sqrt{2}}{2}$. También es bien sabido que el área de un círculo se obtiene de la fórmula $A=\pi r^2$, y por tanto la desigualdad anterior queda expresada de la siguiente forma

$$\pi\left(\sqrt{n}-\frac{\sqrt{2}}{2}\right)^2 < A(R) < \pi\left(\sqrt{n}+\frac{\sqrt{2}}{2}\right)^2,$$

pero

$$A(R) = \sum_{i=1}^{n} f(i),$$

entonces

$$\pi\left(\sqrt{n} - \frac{\sqrt{2}}{2}\right)^2 < \sum_{i=1}^{n} f(i) < \pi\left(\sqrt{n} + \frac{\sqrt{2}}{2}\right)^2,$$

y dividiendo toda la desigualdad entre $n + 1$, se tiene que

$$\frac{\pi\left(\sqrt{n} - \frac{\sqrt{2}}{2}\right)^2}{n+1} < \frac{\sum_{i=1}^{n} f(i)}{n+1} < \frac{\pi\left(\sqrt{n} + \frac{\sqrt{2}}{2}\right)^2}{n+1}.$$

Por último, se denotó anteriormente que $F(n) = \frac{1}{n+1}\sum_{i=1}^{n} f(i)$,

entonces

$$\frac{\pi\left(\sqrt{n} - \frac{\sqrt{2}}{2}\right)^2}{n+1} < F(n) < \frac{\pi\left(\sqrt{n} + \frac{\sqrt{2}}{2}\right)^2}{n+1}.$$

Si *n* va creciendo indefinidamente, entonces el límite de las ecuaciones de los extremos convergerá a π, y $F(n)$ convergerá también a π.

Así

$$\lim_{n\to\infty} F(n) = \pi.$$

Éste es un resultado elegante establecido por Gauss y que fue descubierto después de su muerte en una de sus publicaciones.

Demostración del teorema de Jacobi

Para demostrar el teorema de Jacobi primero se analizará la función $\tau(m, n)$[75] en términos del símbolo de Legendre cuando $m = 1, 3$ y el módulo es 4, y veremos que

$$\sum_{d \mid n} \left(\frac{-1}{d}\right) = [\tau(1, n) - \tau(3, n)].$$

[75] Sean $m, n \in \mathbb{N}$. Denotamos a $\tau(m, n)$ como el número de divisores de *n* que dejan el mismo residuo que *m* módulo 4.

Después relacionamos a $\tau(m,n)$ con $R(n)$[76] a través de los divisores de *n*. El motivo de esta relación es que *f(n)* también se puede definir en términos de $R(n)$ a través de los divisores de la forma *4k+1* y *4k+3* de *n*, y por último se pasa a demostrar el teorema de Jacobi – cita 74 –.

Sea $m,n \in \mathbb{Z}^+$. Definimos a $\boldsymbol{\tau(m,n)}$ como el número de divisores positivos de *n*, que dejan el mismo residuo que *m* módulo 4.

Es claro, tal como se ha definido a la función τ, que $\tau(1,n)$ representa a todos los divisores de la forma 4k+1 y que $\tau(3,n)$ a todos los divisores de la forma 4k+3.[77] Por otra parte recordemos que por el símbolo de Legendre

$$\left(\frac{-1}{d}\right) = \begin{cases} -1 \ \ si\ d \equiv 3 (mod\ 4) \\ \ \ 1\ si\ d \equiv 1\ (mod\ 4) \end{cases},$$

entonces la siguiente suma representa al número de divisores de la forma 4k+1 de un número natural *n*

$$\sum_{\substack{d \mid n \\ d \equiv 1 (mod\ 4)}} \left(\frac{-1}{d}\right).$$

Análogamente, la siguiente suma representa al número de divisores de la forma $4k+3$ de *n*

$$\sum_{\substack{d \mid n \\ d \equiv 3 (mod\ 4)}} \left(\frac{-1}{d}\right),$$

antes de continuar, expresamos a *n* mediante la factorización con primos de la forma $4k+1$ y $4k+3$.

Así

$$n = \prod_{i=1}^{r} p_i^{\alpha_i} \prod_{j=1}^{s} q_j^{\beta_j}.$$

Se sabe que el producto de dos números de la forma 4k+1 es de la misma forma, y en general el producto de un número finito de primos de la forma 4k+1 también es de la forma $4k+1$.

[76] R(n): el número de pares ordenados (x,y) de enteros tal que $x^2 + y^2 = n$.

[77] Si suponemos que existen r divisores de la forma 4k+1 y s divisores de la forma 4k+3, entonces $f(n) = 4[r-s]$.

Es decir

$$(4k_1+1)(4k_2+1)\cdots(4k_n+1)=4k+1,$$

en particular, $\underbrace{(4k+1)(4k+1)\cdots(4k+1)}_{n-veces}=(4k+1)^n$.

Así, si p_i es un primo de la forma $4k+1$, entonces $p_i^{\alpha_i}=(4k+1)^{\alpha_i}$.

Si tomamos en cuenta a todos los divisores de *n* entonces se tendrán $\prod_{i=1}^{r}(\alpha_i+1)\cdot\prod_{j=1}^{s}(\beta_j+1)$; sin embargo sólo algunos son de la forma $4k+1$ y $4k+3$. De la factorización de *n* podemos observar que el producto $\prod_{i=1}^{r}(\alpha_I+1)$ representa a los divisores de la forma $4k+1$, pero no a todos.

De igual modo, si $q_1^{\beta_1},\ldots,q_s^{\beta_s}$ son primos de la forma $4k+3$, entonces sólo los primos con potencia impar representan a los divisores de la misma forma, y los que tienen potencia par representan a los divisores de la forma $4k+1$también; así el número de divisores de la forma $4k+1$ aumenta en $\prod_{i=1}^{r}(\alpha_I+1)$ más los primos de la forma $4k+3$ con potencia par. Pero aún con todo esto, no se puede decir que se han encontrado todos los divisores de las dos formas descritas, ya que los siguientes productos también representan a los divisores de ambas formas.

Si $q\equiv 3(mod\ 4)$ entonces $q^{2k}\equiv(3)^{2k}\equiv 1\ (mod\ 4)$ y $q^{2k+1}\equiv(3)^{2k}\cdot 3\equiv 3(mod\ 4)$, de esta manera

$$p\cdot q^{2k}\equiv p\equiv 1(mod\ 4)$$
$$p\cdot q^{2k+1}\equiv 3p\equiv 3(mod\ 4)$$
$$q^{2k}\cdot q^{2k+1}\equiv 1\cdot 3\equiv 3(mod\ 4)$$
$$q^{2k}\cdot q^{2k}\equiv 1(mod\ 4)$$
$$q^{2k+1}\cdot q^{2k+1}\equiv 3\cdot 3\equiv 1(mod\ 4).$$

Entonces quisiéramos una fórmula explícita que nos dé directamente a todos los divisores primos de la forma $4k+1$, y todos los de la forma $4k+3$. Sin embargo nos es difícil tener dicha fórmula, si es que la hubiera, así que daremos por hecho que existen números específicos de divisores de las dos formas, a saber *r* y *s*. Por tanto

$$\sum_{d\mid n}\left(\frac{-1}{d}\right)=\sum_{\substack{d\mid n\\ d\equiv 1(mod\ 4)}}\left(\frac{-1}{d}\right)+\sum_{\substack{d\mid n\\ d\equiv 3(mod\ 4)}}\left(\frac{-1}{d}\right)\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots(1).$$

Explícitamente

$$\sum_{d|n}\left(\frac{-1}{d}\right) = \underbrace{1+1+\cdots+1}_{r\ divisores\ (4k+1)} + \underbrace{(-1)+(-1)+\cdots+(-1)}_{s\ divisores\ (4k+3)}$$

$$= r\cdot(1) + s(-1) = r - s.$$

Así

$$\sum_{d|n}\left(\frac{-1}{d}\right) = r - s = \tau(1,n) - \tau(3,n) \qquad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots.\ldots.(2).$$

En otras palabras, si queremos mostrar que $f(n) = 4[\tau(1,n) - \tau(3,n)]$, entonces será equivalente a mostrar que

$$f(n) = 4\sum_{d|n}\left(\frac{-1}{d}\right) = R(n).$$

Esto es claro desde un principio, ya que cada uno de los sumandos del segundo miembro de la igualdad (1) se han definido de la misma manera que las representaciones con la función tau de (2), pero se quería hacer énfasis en que las representaciones de divisores de un número *n* mediante distintas formas denotan exactamente las mismas cantidades, sólo que en algunas ocasiones resulta más fácil trabajar con alguna de ellas. Dada la explicación anterior, se prueba finalmente el teorema de Jacobi de la siguiente manera.

Teorema (Jacobi)

Si *n* es un número natural, entonces el número de representaciones de *n* como suma de dos cuadrados es $R(n)$, donde

$$R(n) = 4\sum_{d|n}\left(\frac{-1}{d}\right).$$

Demostración. Sea *n* un número natural y que se expresa como producto de primos, donde $p_i = 4k+1$ y $q_j = 4k+3$, de la siguiente manera:

$$n = 2^{\alpha}\prod_{i=1}^{r} p_i^{\alpha_i}\prod_{j=1}^{s} q_j^{\beta_j}.$$

Es claro que al tomar divisores de *n* de la forma $4k+1$ y $4k+3$, las potencias de dos no entran en ningún divisor de dichas formas. Entonces podemos tomar a *n* simplemente como

$$n = \prod_{i=1}^{r} p_i^{\alpha_i} \prod_{j=1}^{s} q_j^{\beta_j} = a \cdot b\,,$$

donde *a* es el primer producto de primos y *b* es el segundo producto de primos respectivamente, es claro que *a* y *b* no necesariamente son números primos, pero sí que $(a, b) = 1$.

Es fácil ver que cualquier divisor *d* de *n* puede ser un producto de primos de la forma $4k + 1$, y también un producto de primos de la forma $4k + 3$ o bien un producto de ambos primos.

Sea $n = a \cdot b$ y $d \mid n$, entonces existen d_1 y d_2 tales que $d_1 \mid a$, $d_2 \mid b$ y $d = d_1 \cdot d_2$, donde d, d_1, d_2 son divisores impares. Por tal motivo podemos aplicar el símbolo de Jacobi y se tiene que

$$\left(\frac{-1}{d}\right) = \left(\frac{-1}{d_1}\right)\left(\frac{-1}{d_2}\right).$$

Entonces

$$\sum \left(\frac{-1}{d}\right) = \left[\sum \left(\frac{-1}{d_1}\right)\right]\left[\left(\frac{-1}{d_2}\right)\right] \ldots\ldots\ldots (1).$$

Y haciendo lo anterior repetidamente generalizamos a potencias de primos. Ahora bien, si el número en general es una potencia de 2, entonces entre sus divisores $1, 2, 2^2, \ldots, 2^k$, el único termino no cero, se obtiene tomando $d = 1$, pues es de la forma 4k+1.

En el caso de un primo $p \equiv 1(mod\ 4)$, entonces $\left(\frac{-1}{p}\right) = 1$, y si se tiene p^{α_i} entonces cada uno de los $\alpha_i + 1$ sumandos serán 1; así

$$\sum_{d \mid \prod_{i=1}^{r} p_i^{\alpha_i}} \left(\frac{-1}{\prod_{i=1}^{r} p_i^{\alpha_i}}\right) = \prod_{i=1}^{r} (\alpha_i + 1)\,.$$

En el caso de que un primo $q \equiv 3(mod\ 4)$, los sumandos se alternan entre 1 y -1, y entonces

$$\sum_{d \mid q^{\beta}} \left(\frac{-1}{d}\right) = \sum_{j=0}^{\beta} \left(\frac{-1}{q^j}\right) = \sum_{j=0}^{\beta} \left(\frac{-1}{q}\right)^j = \sum_{j=0}^{\beta} (-1)^j = \begin{cases} 1 \ \ si\ \beta\ es\ par \\ 0 \ \ si\ \beta\ es\ impar. \end{cases}$$

De esta manera se tenía que

$$n = \prod_{i=1}^{r} p_i^{\alpha_i} \prod_{j=1}^{s} q_j^{\beta_j},$$

y tomando $p_{i's} = d_1$ y $q_{j's} = d_2$, junto con (1), llegamos a que

$$\sum \left(\frac{-1}{d}\right) = \left[\prod_{i=1}^{r} (\alpha_i + 1)\right](1) = \prod_{i=1}^{r} (\alpha_i + 1), \qquad si\ \beta\ es\ par.$$

De la misma manera

$$\sum \left(\frac{-1}{d}\right) = \left[\prod_{i=1}^{r} (\alpha_i + 1)\right] \cdot 0 = 0, \quad si\ \beta\ es\ impar.$$

Así

$$\sum \left(\frac{-1}{d}\right) = \prod_{i=1}^{r} (\alpha_i + 1).$$

De esta manera tenemos que [78]

$$R(n) = 4\prod_{i=1}^{r} (\alpha_i + 1) = 4\sum \left(\frac{-1}{d}\right) = 4[\tau(1,n) - \tau(3,n)] = f(n),$$

que es lo que se quería demostrar. ■

[78] **Teorema.** Sea n un entero positivo y $n = 2^k \prod_p p^{\alpha} \prod_q q^{\beta}$, donde p representa los divisores de la forma 4k+1 y q representa a los primos de la forma 4k+3. Si $k = 0\ o\ 1$ y todos los β son 0, entonces $r(n) = 2^{t+2}$, donde t es el número de primos p de la forma 4k+1 que divide a n, de otra manera $r(n) = 0$. Si todos los β son pares, entonces $R(n) = 4\prod_{i=1}^{r} (\alpha_i + 1)$, de otra manera $R(n) = 0$.
Denotamos a $r(n)$ como el número de pares ordenados *(x, y)* de enteros tales que *(x, y)=1* y $x^2 + y^2 = n$, que es el número de representaciones de *n.* Véase Niven, Zuckerman, Montgomery [1991], pp. 163-168.

Apéndice B

Al inicio del capítulo 2 se mencionó que para la suma de tres cuadrados se hace uso de un resultado propio de formas cuadráticas. Sin embargo no profundizaríamos en dicha teoría −en el capítulo se explicó el motivo−, así que únicamente se pasarán a exponer algunos resultados de esta teoría sin ninguna demostración.

A la expresión siguiente (1) se le denomina *función homogénea en n-variables de segundo grado*. Un caso especial de estas funciones es cuando *n = 2*, y dicha función se le denomina *forma cuadrática*.

$$F_A(x) = x^t Ax = \sum_{i=1}^{n}\sum_{j=1}^{n} a_{ij}x_i x_j \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (1).$$

Donde *A* es una matriz simétrica asociada a la forma y x es un elemento de un espacio vectorial *V*. La expresión (1) también se puede ver así

$$F_A(x) = \sum_{i=1}^{n}\sum_{j=1}^{n} a_{ij}x_i x_j = \sum_{i=1}^{n}\sum_{j=1}^{n} a_{ji}x_i x_j = \sum_{i=1}^{n} a_{ii}x_i^2 + 2\sum_{i<j}^{n} a_{ij}x_i x_j.$$

Ejemplo.

Tómese la matriz identidad I_n de tamaño $n \times n$. Entonces la forma cuadrática asociada es

$$F_{I_n}(x_1, \ldots, x_n) = \sum_{i=1}^{n}\sum_{j=1}^{n} a_{ij}x_i x_j = a_{11}x_1^2 + a_{22}x_2^2 + \cdots + a_{nn}x_n^2 = x_1^2 + x_2^2 \ldots + x_n^2,$$

pues

$$I_n = \begin{pmatrix} 1 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & 1 \end{pmatrix} = \begin{cases} a_{ij} = 0 \;\; si \;\; i \neq j \\ a_{ij} = 1 \;\; si \;\; i = j \end{cases}.$$

Una forma cuadrática $F: V = \mathbb{R}^n \to \mathbb{R} = K,\ [F_A(x) = x^t Ax]$, se dice que es *positiva-definida* si $F_A(x) = x^t Ax > 0 \ \ \forall\, 0 \neq x \in V$.

Además, se dice que una forma cuadrática es binaria, si está expresada con dos variables y ternaria si tiene tres variables. Así, se pasa a describir los resultados que ayudarán para la solución del lema 2.1.4, primero se mencionan dos resultados respecto a formas cuadráticas binarias.

Lema (a) Sea la matriz simétrica $A = \begin{pmatrix} a & b \\ b & c \end{pmatrix}$, y sea $F_A(x_1, x_2) = ax_1^2 + 2bx_1x_2 + cx_2^2$ la forma cuadrática asociada a la matriz A. Se tiene que la forma cuadrática binaria F_A es positiva definida si y sólo si $a \geq 1$ y el discriminante *d* satisface $d = \det(A) = ac - b^2 \geq 1$.

Una característica para que cualquier entero positivo representado por una forma cuadrática sea suma de dos cuadrados, es que sea una forma positiva-definida y con discriminante 1.

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

Generalizando las formas cuadráticas binarias, se llega a las formas cuadráticas ternarias, que a continuación se pasan a mencionar y que son en realidad una generalización de las formas vistas anteriormente.[79]

Formas Cuadráticas Ternarias

Lema (c) Sea $B = \begin{pmatrix} b_{11} & b_{12} & b_{13} \\ b_{12} & b_{22} & b_{23} \\ b_{13} & b_{23} & b_{33} \end{pmatrix}$ una matriz simétrica de tamaño 3×3 y F_B su correspondiente forma cuadrática ternaria con determinante d. Entonces

$$b_{11}F_B(x_1, x_2, x_3) = (b_{11}x_1 + b_{12}x_2 + b_{13}x_3)^2 + G_{B^*}(x_2, x_3).$$

Donde G_{B^*} es la forma cuadrática binaria asociada a la matriz

$$B^* = \begin{pmatrix} b_{11}b_{22} - b_{12}^2 & b_{11}b_{23} - b_{12}b_{13} \\ b_{11}b_{23} - b_{12}b_{13} & b_{11}b_{33} - b_{13}^2 \end{pmatrix},$$

y G_{B^*} tiene discriminante $b_{11}d$. Si F_B *es positiva-definida* entonces G_{B^*}*es positiva-definida*, en cambio la F_B es *positiva definida* si y solo si los siguientes tres determinantes son positivos

$$b_{11} = \det(b_{11}) \geq 1, d' = det\begin{pmatrix} b_{11} & b_{12} \\ b_{12} & b_{22} \end{pmatrix} \geq 1 \text{ y } d = \det(B) \geq 1.$$

Teorema (d) Toda forma cuadrática ternaria *positiva-definida* con discriminante 1 es equivalente a la forma $x_1^2 + x_2^2 + x_3^2$.

[79] Todas las pruebas de estos resultados tanto de formas binarias como de ternarias, pueden verse en Nathanson [1996], pp. 9-17.

Apéndice C

Se llegó a que para probar que $-d'$ sea un residuo cuadrático módulo $2p = d'n - 1$, tenemos que probar que

$$\sum_{\substack{q_i \mid d' \\ q_i \equiv 5,7}} k_i \equiv 0 \ (mod\ 2),$$

de esta manera, nos basaremos en la prueba por contradicción tomando como ciertas nuestras hipótesis del problema en cuestión. Como se puede observar,[80] en ambos casos la suma (8) que es la misma que (10) queda expresada como se quería mostrar, pero veamos por qué (7), (8), (9), y (10) se cumplen, verificándolos mediante una prueba por contradicción.
Se tiene que

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

Del primer caso del cual se concluyen (7) y (8), supongamos que (8) no se cumple, por tanto se tiene que

$$\sum_{\substack{q_i \mid d' \\ q_i \equiv 5,7 (mod\ 8)}} k_i \equiv 1 \equiv (mod\ 2),$$

entonces

$$\sum_{\substack{q_i \mid d' \\ q_i \equiv 5,7 (mod\ 8)}} (-1)^{k_i} = -1.$$

Ahora bien, se tiene que toda potencia de 3 deja como resto 1 o 3 módulo 8, ya que para cualquier entero positivo *k*.

$(3)^{2k} = (3^2)^k = 9^k \equiv 1^k \equiv 1\ (mod\ 8)$,

$(3)^{2k+1} = 3(3^2)^k = 3(9^k) \equiv 3(1^k) \equiv 3\ (mod\ 8)$.

[80] Las congruencias (7), (8), (9), y (10) que se demuestran en este apéndice están escritas de manera ordenada al final de la prueba del lema 2.1.6.

Por tanto, sí $d' \equiv 3\ (mod\ 8)$, entonces

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

pero

$$\prod_{\substack{q_i \mid d' \\ q_i \equiv 3,5(mod\ 8)}} 3^{k_i} \equiv 3^{\alpha_j} \equiv 3\ o\ 1\ (mod\ 8),$$

para alguna $\alpha_j \in \mathbb{Z}^+$; así

$$d' \equiv 3 \equiv -3, -1\ (mod\ 8),$$

de esta manera, $3 \equiv -3\ (mod\ 8)$ y $3 \equiv -1\ (mod\ 8)$, lo que es una contradicción.

Por lo tanto

$$\sum_{\substack{\boldsymbol{q_i \mid d'} \\ \boldsymbol{q_i \equiv 5,7(mod\ 8)}}} \boldsymbol{k_i \equiv 0\ (mod\ 2)}.$$

Falta mostrar (7). Para probarlo supongamos que no se cumple, es decir, que

$$\sum_{\substack{q_i \mid d' \\ q_i \equiv 3,5(mod\ 8)}} k_i \equiv 0\ (mod\ 2),$$

y como

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

entonces

$$\prod_{\substack{q_i \mid d' \\ q_i \equiv 3,5(mod\ 8)}} 3^{k_i} \equiv 3\ (mod\ 8) \qquad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (11),$$

pero

$$\sum_{\substack{q_i \mid d' \\ q_i \equiv 3,5(mod\ 8)}} k_i \equiv 0\ (mod\ 2).$$

De esta forma existen k_i pares y un número par de $k_{i's}$ impares.

Por lo tanto

$$\prod_{\substack{q_i \mid d' \\ q_i \equiv 3,5 (mod\ 8)}} 3^{k_i} \equiv 1\ (mod\ 8) \qquad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (12),$$

por (11) y (12), tenemos que $3 \equiv 1\ (mod\ 8)$, lo que es un absurdo. Así:

$$\sum_{\substack{\boldsymbol{q_i \mid d'} \\ \boldsymbol{q_i \equiv 3,5 (mod\ 8)}}} \boldsymbol{k_i \equiv 1\ (mod\ 2)}.$$

Para el caso en que $n \equiv 3\ (mod\ 8)$, $c = 1$ y $d \equiv 1\ (mod\ 8)$ se sigue un procedimiento análogo al anterior, y así se obtiene la veracidad de (9) y (10); de esta forma $-d'$ es un residuo cuadrático módulo $2p = d'n - 1$, y por lo tanto n es suma de tres cuadrados, que es lo que se quería demostrar. ■

Bibliografía

Carrera, I Pla, Josep. 2009. Liu Hui, *Nueve capítulos de la matemática china*. Primera edición. Colección nivola.

Cossali, Pietro. 1799. *Origine, trasporto in Italia, primi progressi in essa dell'algebra. Storia critica di nuove disquisizioni analitiche e metafisiche* . Dos volúmenes. Parma 1797 e 1799.

Dickson, L.E. *Simpler proofs of Waring´s theorem on cubes with various generalizations.* Transactions of the American Mathematical Society, Vol. 30, No. 1, Jan. 1928, pp. 1-18.

Dickson, L.E. *All integers except 23 and 239 are sums of eight cubes.* Transactions of the American Mathematical Society, August 1939, pp. 588-591.

Díez Freyle, Juan. 2008. *Sumario compendioso de las cuentas de plata y oro.* Primera edición. UNAM.

Hilbert, David. 1909. *"Beweis für die Darstellbarkeit der ganzen zahlen durch eine feste Anzahl n-ter Potenzen (Waringsches Problem)"* Göttinger Nachrichten.), 17-36. *Mathematische Annalen* 67, pp. 281-305.

Koshy, Thomas. 2002. *Elementary Number Theory with Applications,* Harcourt, Academic Press.

Nathanson, Melvyn. 1996. *Additive Number Theory, the Classical Bases*. New York: Springer- Verlag.

Niven, I., Zuckerman, H.S., Montgomery, H.L. 1991. *An Introduction to the Theory of Numbers*. USA: John Wiley & Sons, Inc.

Pacioli, Luca. 1494. *Summa de Arithmetica Geometría Proportioni et Proportionalitá*. Venecia: Paganino de Paganini. Edición facsimilar proveniente de la Biblioteca de la Universidad de Sevilla. Consultado en la Biblioteca virtual Miguel de Cervantes.

Pisa, Leonardo de. 1973. *El Libro de los Números Cuadrados*, traducción de la versión francesa de Paul Ver Eecke. Buenos Aires: Eudeba.

Pisa, Leonardo de. 2002. *Fibonacci´s Líber Abaci*. Traducción de L.E. Singler. Nueva York: Springer-Verlag.

Shively, Levi. 1984. *Introducción a la Geometría Moderna*, traducido por Andrés Palacios Priego. México: Continental, UNAM.

Suter, H. 1892. Das Mathematik Verzeichnis im Fihrist des Ibn Ab-Ja-An-Nadim, zum ernten Mal vollständing ins Deustsche übersetzt mit Anmerkungen versehen. (Abhandlung zur Geschichte der Mathematik). T.G. Leipzig.

Suter, H. 1890. Die Mathematiker und Astronomen der Araben und ihre Werke. (Abhandlung zur Geschichte der Mathematischen Wissenschaften). Leipzig.

Tattersall, James. 2005. *Elementary Number Theory in Nine Chapters*. New York: Cambridge University Press.

Torrecillas, Jover, Blas. 1999. Fermat, *El mago de los números*. Tercera edición. Colección nivola.