UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE CIENCIAS

La conjetura de Goldbach en el contexto del intercambio matemático con Leonhard Euler

T E S I S

QUE PARA OBTENER EL TITULO DE:

Matemático

PRESENTA:

Ollin Tonatiuh Cortéz Gottwald

TUTOR

Mat. J. César Guevara Bravo

Ciudada Universitaria, Cd. Mx., 2023

Datos del alumno
Cortéz Gottwald Ollin Tonatiuh Universidad Nacional Autónoma de México Facultad de Ciencias Matemáticas 310013440
Datos del tutor
Mat. Julio César Guevara Bravo
Datos del sinodal 1
Dr. Carlos Álvarez Jiménez
Datos del sinodal 2
Dr. Leonardo Ignacio Martínez Sandoval
Datos del sinodal 3
M. en C. Israel Ramos García
Datos del sinodal 4
MCIC Ximena Estrada Zavaleta
Datos del trabajo escrito
La conjetura de Goldbach en el contexto del intercambio matemático con Leonhard Euler 91 pag 2023

Índice

Introducción

Este trabajo de tesis surgió a partir de estudiar la historia de las matemáticas y descubrir que nos ha proporcionado conocimientos apasionantes. La historia nos encaminó a conocer teorías que nos sorprenden por su perfección, y por sus vínculos inesperados de carácter interdisciplinario, como puede ser con la física, astronomía, biología o medicina. Notamos que todas las aportaciones de la ciencia llegan de la mano de grandes personajes, quienes han sido una inspiración para todos nosotros. Gracias a todos estos personajes que hemos estudiado en un periodo de más de dos mil años de historia de las matemáticas, hemos podido reconstruir una parte del desarrollo de las ideas científicas. Queremos hacer énfasis en que *es una parte lo que se ha podido reconstruir*, ya que existen muchos personajes y teorías que están en espera de ser estudiados, y no consideramos que por el hecho de que algo sucedió años o siglos atrás entonces ya no puede aportar nada a la teoría moderna de la ciencia.

En este trabajo queremos remarcar que aún tenemos mucho por aprender de los trabajos que se escribieron en los siglos pasados, principalmente a partir del siglo XVII, pues este siglo es donde se da un renacimiento de las matemáticas, es donde se inició el álgebra, la matematización de la física, el cálculo diferencial e integral, la astronomía matemática, etc. Durante los cursos que tomé del área de historia noté que aún existen innumerables trabajos en todo el mundo que se han estudiado poco y que están en espera de interpretación.

Para el siglo XVIII las matemáticas se presentan como una explosión de conocimientos, es decir, ya existían áreas de distinción, revistas especializadas, se imprimían muchos libros de temas matemáticos. Cada año de ese siglo se publicaron miles de trabajos altamente especializados en diversos idiomas regionales, y en latín que era la lengua de la cultura y la ciencia.

Uno de los elementos principales que motivó este trabajo de tesis fue descubrir que una de las vertientes que ha sido menos explorada en los documentos históricos de las matemáticas es el de la correspondencia. Desde el siglo XVII se formaron grupos de interés para cada tema por investigar en la física-matemática, y una manera directa para trabajar a distancia fue la correspondencia. Ésta fue muy nutrida, vigorosa y extensa, desde el siglo XVII hasta la primera mitad del siglo XX. En este tipo de comunicación quedó testimonio de la evolución de las ideas matemáticas, y es importante señalar que la mayor parte de esta correspondencia no fue publicada en sus épocas y, hasta la fecha, en muchos de los casos no se conoce mucho de su contenido. Pero lo que sí sabemos es que ahí se encuentran grandes aportaciones de la física-matemática, y cuando logremos comprender qué es lo que se encuentra en esas cartas entonces estaremos en mejores condiciones de entender muchos de los paradigmas de las matemáticas y de aportar nuevas teorías al respecto.

Correspondencia Euler-Goldbach

En el contexto de lo que se mencionó antes podemos decir que en el siglo XVIII se generó un intercambio epistolar de lo más vigoroso y trascendente. El intercambio de ideas entre los científicos desbordó la capacidad de cualquier persona para poder revisar y clasificar tanto material.

A través de mis cursos en la Facultad de teoría de números e historia de las matemáticas me interesé por los trabajos de Leonhard Euler y, junto con el profesor César Guevara me adentré en uno de los casos aún por estudiar, que es su correspondencia. Él sostuvo intercambio con diversos personajes del siglo XVIII, ésta es de gran importancia para entender el quehacer de la física-matemática de su época, y también es fundamental para que podamos avanzar más en la construcción del cuerpo matemático de sus aportaciones a la ciencia.

Para el trabajo de tesis centramos nuestra atención en mostrar que la carta donde se halla la famosa *conjetura de Goldbach* contenía temas verdaderamente trascendentes para la matemática y que la conjetura sólo fue una ocurrencia momentánea de Goldbach que no progresó entre ellos. La fama de la conjetura fue posterior. A partir de este señalamiento fue que consideramos que el tema de tesis sería mostrar que los temas matemáticos que contenía la famosa carta eran de gran importancia para ellos, que los estaban trabajando desde años antes y los siguieron posteriormente, y que el tema de la conjetura sólo ocupó dos cartas de las 196 que conocemos entre ellos.[1]

Consideramos que ha sido injusto que, de manera general, cuando se habla de la relación matemática entre Euler y Goldbach sea en torno de la conjetura cuando la realidad es otra.

Orden de la tesis

La tesis está dividida en siete capítulos, que a la vez son los temas que trata la carta 51, la que contiene la conjetura, fechada el 7 de junio de 1741. Cada tema de la carta lo trabajamos desde su origen en la correspondencia, hasta su término en ésta, entre los años 1729 y 1764, que es la correspondencia que se conoce. La finalidad, como ya lo mencionamos, es mostrar que los temas que trataron en esa carta ya tenían un pasado y transitaron también a los años que siguieron. Los capítulos son los siguientes:

1) Entorno histórico.
2) *Pequeño teorema de Fermat*, demostraciones del teorema.
3) La expresión polar del coseno, así como la gestación de algunos de los resultados sobre números complejos que posteriormente quedarían expuestos en *Introductio in analysin infinitorum* (1748).
4) Los números de la forma $4mn - m - n$, su posible representación como un cuadrado y otros números poligonales, así como su relación con los residuos cuadráticos.
5) Los primos de Fermat $2^{2^{n-1}} + 1$. Éste fue uno de los primeros temas en su correspondencia, se encuentra presente desde la segunda carta.
6) La famosa *conjetura de Goldbach*.
7) Problemas varios de polinomios con raíces vinculadas al número áureo. Series de logaritmos de funciones racionales. Sumas de cuadrados.

[1] Cabe señalar que el trabajo de investigación con las cartas lo realizamos directamente de los originales que están escritos en latín y alemán, pues no existe en la actualidad alguna traducción. Trabajamos directamente con la transcripción de [Juškevič & Winter 1965] y también con las cartas en su forma facsimilar que se encuentran en www.eulerarchive.maa.org.

I. Entorno histórico

Pocos personajes en la historia de las matemáticas han producido tantos trabajos y en tantas áreas de las ciencias exactas como lo hizo Leonhard Euler en el siglo XVIII. Nos dejó cerca de 800 trabajos publicados y muchos de ellos aún no los hemos estudiado con la profundidad adecuada.

Sabemos que Euler sostuvo intercambios con los personajes más destacados de su época, entre ellos estaban los hermanos Daniel y Johann Bernoulli, Christian Goldbach, Joseph Louis de Lagrange, Kirill Grigorevich Razumovskij, Grigorij Nikolajevich Teplov, Johann Kaspar Wettstein y se puede corroborar por la correspondencia que sostuvo con ellos —gran cantidad está a disposición de los investigadores—.[2]

Para estudiar las aportaciones de Euler lo primero que solemos hacer es recurrir a sus publicaciones, que ya se mencionó que son alrededor de 800, además, otra vía que no se puede pasar por alto es la de consultar la correspondencia que también es muy extensa, en ella se pueden encontrar procedimientos que no quedaron expuestos en sus trabajos publicados. A través de las cartas es posible conocer perfiles de Euler más cercanos a sus inquietudes personales, y éstas nos permiten esclarecer cuáles fueron sus prioridades en las diferentes etapas de su vida productiva.

La interpretación de la correspondencia no es fácil y si no se hace con el debido cuidado puede ser totalmente errónea e injusta. Pueden existir casos en los que nos podríamos quedar con una idea muy sesgada y limitada de lo que verdaderamente sucedió entre Euler y sus interlocutores. El personaje que más nos interesa en este trabajo, por su relación tan cercana con Euler y la teoría de los números, es Christian Goldbach.

Goldbach es conocido en cualquier libro de historia de las matemáticas; en la teoría de los números y hasta en novela histórica, por lo que hoy identificamos como la *conjetura de Goldbach*. Recordemos cuál es:

a) Todo entero par mayor de 2 se puede escribir como suma de dos primos.
b) Todo entero impar mayor que 5 se puede escribir como suma de tres primos.

Si bien no hay duda de que se le recuerda con mucha frecuencia, también es cierto que no se le identifica —salvo los especialistas— con otros temas de las matemáticas que no sea la conjetura. Es injusto para él que no se le recuerde por toda su trayectoria y que sólo quedó como un entusiasta al lado de Euler al que le propuso un resultado que ninguno de los dos pudo resolver. La relación entre ellos fue muy fructífera y su intercambio de ideas matemáticas fue de muchos años y la conjetura nunca fue un tema que les haya quitado atención a lo que verdaderamente los ocupaba. Pero, antes de seguir, primero contextualicemos su estrecha relación.

Euler-Goldbach

Christian Goldbach (1690-1764) fue un hombre que se identificó e intercambió opiniones con grandes personajes, por ejemplo, Leibniz en 1711, Nicolaus Bernoulli, A. de Moivre en 1712 y a Daniel Bernoulli en 1724, entre otros. Goldbach a través de Nicolás y Daniel Bernoulli logró que Euler aceptara formar parte de la *Academia de Ciencias de San Petersburgo*, y así fue que en 1727 llegó a la Academia y conoció a Goldbach. La afinidad de intereses dio lugar a una amistad casi inmediata y una relación matemática enriquecedora para el entorno de ambos. Dadas las circunstancias del momento, Goldbach tuvo que partir a Moscú en 1729 y Euler por su parte, —debido a la inestabilidad

---

[2] Sus trabajos en todas las áreas y la correspondencia con los personajes señalados se pueden consultar en: www.eulerarchive.maa.org. Para la correspondencia con Christian Goldbach además se tiene la edición de [Juškevič & Winter 1965] que es la que usamos principalmente para este trabajo.

de los Zares— tuvo que ocuparse en la marina rusa y posteriormente partió a Prusia. Fue por estas razones que iniciaron su intercambio epistolar desde 1729 hasta 1764.

De su intercambio se reconocen 196 cartas —las que se conocen—, que cubren temas como: teoría de los números, series, números complejos, teoría de funciones, cálculo, etc. Además, en estas cartas se puede encontrar el origen de muchos de los resultados que posteriormente publicaría Euler.

Los temas de su interés sobrepasan la posibilidad de que se pudiera pensar que la famosa conjetura ocupó un lugar medianamente importante en sus intercambios. Veamos cómo inicio la correspondencia entre ellos.

El 13 de octubre de 1729 Euler le escribió a Goldbach la primera carta, en ésta el tema principal es el comentario sobre una de las ideas que había trabajado para el cálculo de una función interpolante que permita obtener el factorial de valores fraccionarios o irracionales. La expresión convergente que propuso es

$$\frac{1\cdot 2^m}{1+m}\cdot\frac{2^{1-m}.3^m}{2+m}\cdot\frac{3^{1-m}\cdot 4^m}{3+m}\cdot\frac{4^{1-m}\cdot 5^m}{4+m}\cdot\ldots=\left[\left(\frac{2}{1}\right)^m\frac{1}{1+m}\right]\left[\left(\frac{3}{2}\right)^m\frac{2}{2+m}\right]\left[\left(\frac{4}{3}\right)^m\frac{3}{3+m}\right]\ldots=\ m!\ \ldots\ (1)$$

Enseguida calcula el caso $\frac{1}{2}$ y llega a que

$$\frac{1}{2}!=\frac{1}{2}\sqrt{\sqrt{-1}*\ln(-1)}=\frac{\sqrt{\pi}}{2}$$

Cabe mencionar que esta interpolación (1) generaba valores semejantes a otra que propuso Daniel Bernoulli a través de operar con una serie hipergeométrica.[3]

El primero de diciembre del mismo año Goldbach le respondió, y lo que predominó en la carta fueron los comentarios a la fórmula antes mencionada. Goldbach le señaló que sería conveniente explorar con una expresión equivalente pero que ésta ahora fuera de manera integral. Euler le respondió el 8 de enero de 1730 y deja ver que consideró los trabajos de Newton y Wallis, y en especial usó la integral de Wallis $\int_0^1 b^{\frac{p}{q}}(1-\mathrm{x})^{\mathrm{n}}dx$ como punto de partida para su estudio. En este intercambio de las primeras cartas podemos encontrar los orígenes de lo que después ya fue conocido como las funciones Gamma y Beta. Sin embargo, a las primeras cartas se les recuerda más por la posdata donde Goldbach le pregunta su opinión sobre los números de Fermat.[4]

---

[3] Se tiene registro de una carta del 6 de octubre de 1729 en la que Daniel Bernoulli propone a Goldbach que para una x positiva y A que tiende a infinito, el producto

$$\left(\mathrm{A}+\frac{\mathrm{x}}{2}\right)^{\mathrm{x}-1}\left(\frac{2}{1+\mathrm{x}}\frac{3}{2+\mathrm{x}}\frac{4}{3+\mathrm{x}}\cdots\frac{\mathrm{A}}{\mathrm{A}-1+\mathrm{x}}\right),$$

actúa como función interpolante para valores no necesariamente enteros. Así plantea que

$$\mathrm{x}!=\lim_{\mathrm{n}\to\infty}\left(\mathrm{A}+\frac{\mathrm{x}}{2}\right)^{\mathrm{x}-1}\prod_{\mathrm{i}=1}^{\mathrm{n}}\frac{\mathrm{i}+1}{\mathrm{i}+\mathrm{x}}.$$

Para ahondar más en este pasaje consúltese la carta original en [Juškevič y Winter] y para ejemplos de esta función en [Gronau, 2003].

Por otro lado, a través de la relación de amistad que tenían Daniel Bernoulli y Euler fue que él estaba al tanto de este problema de interpolación y después de tener una propuesta fue que Daniel le sugirió a Euler que le escribiera a Goldbach. Así se dio la carta del 13 de octubre de 1729.

[4] A pesar de que en este primer intercambio se muestra que se está gestando lo que hoy conocemos como las funciones *gamma* y *beta*, resulta que esta carta de Goldbach se recuerda más, pero por el último párrafo, éste menciona lo siguiente:

Por lo anterior, podemos testificar que la conjetura no figuró en sus primeros intercambios en 1729, la conjetura apareció hasta el 7 de junio de 1742, fue la carta 51 en la clasificación actual,[5] pero con esto bastó para que casi todo quedara opacado y que la conjetura permaneciera como lo único relevante en los 37 años de amistad. Bajo este cuestionamiento pasamos a mostrar la traducción de la carta 51 completa y los temas que ocupó.[6]

Carta 51

Goldbach a *Euler* — AAL: F. 136, Op. 2, No. 8

Moscú, 27 de mayo/7 de junio de 1742 — Hojas 43-45r

[…] Al último escrito de su excelencia del 8 de mayo por la presente le informo que, aunque no busqué ningún nuevo empleo, el Colegio del Reino, no obstante, en contra de mis sospechas, me ofreció el 19 de febrero un puesto de consejero de presupuesto, el cual acepté bajo ciertas condiciones. Ni precipitadamente, ni tímidamente.

Le deseo cordialmente que las múltiples promesas de su excelencia acerca de su pensión aquí pronto se hagan realidad. Pero pienso que el camino que le propuse después de su llegada a Berlín, en aquel tiempo habría sido el mejor y el más corto, si éste hubiese coincidido con el Sistema Mundial Óptimo.

A pesar de que en mi última carta me protegí con un *tal vez*, no habría creído que la fórmula $(a+b)^p - a^p - b^p$ no siempre es dividida por los divisores del número p, si su excelencia no lo hubiese mostrado claramente con su ejemplo citado.

Hasta donde recuerdo, en mi última carta imaginé la fórmula $2^{xp\sqrt{-1}} + 2^{-xp\sqrt{-1}}$, asumiendo $2^{p\sqrt{-1}} + 2^{-p\sqrt{-1}} = 0$, como las ordenadas de una curva serpentiforme, cuyas abscisas son x y cuyo eje es intersectado siempre que la fórmula sea $= 0$, de modo que cuando la misma fórmula es $= 2$, se obtiene la máxima ordenada abajo o arriba, y por consiguiente otras innumerables ordenadas que deben de ser iguales entre ellas. Sin embargo, se deslizó un error en mi expresión de aquel momento, el cual me marcó, su excelencia, con razón y que se puede corregir fácilmente declarando que, cuando q es un número cualquiera y estableciendo $2^{p\sqrt{-1}} + 2^{-p\sqrt{-1}} = 0$, entonces, asumiendo n como un número entero cualquiera, se tiene

$$2^{(8n-4-q)p\sqrt{-1}} + 2^{-(8n-4-q)p\sqrt{-1}} = 2^{qp\sqrt{-1}} + 2^{-qp\sqrt{-1}}.$$

Su excelencia encontró que todos los números que no pueden ser expresados como $4mn - m - n$, están comprendidos en la formula $v^2 + v + u^2$. Y creo que todo $4mn - m - n$ se puede llevar a la formula $y^2 + y - x^2$, de modo que cada número dado es igual a $p^2 + p \pm q^2$, donde p y q denotan números enteros, o bien alguna de las dos letras puede significar 0; de donde se observa que cualquier número está compuesto por un doble triangular $\pm$ un número cuadrado; como además todo número es igual a la formula $u^2 + v^2 + v + y^2 + y - x^2$, cuando se toma

$$u = \frac{z^2+z}{4} + 1,\ x = \frac{z^2+z}{4} - 1,\ u^2 - x^2 = z^2 + z$$

se sigue que el medio de un número dado se vuelve $\frac{n}{2} = \frac{v^2+v+y^2+y+z^2+z}{2}$, es decir, tres triangulares.

¿Ha advertido usted la observación de Fermat de que todos los números de la forma $2^{2^n} + 1$, es decir, 3, 5, 17, etc. son números primos? Pero él no afirma haberlo demostrado, ni siquiera, hasta donde sé existe alguna persona que haya sido capaz de demostrarlo.

Lo que tenemos aquí es el inicio de lo que hoy conocemos como primos de Fermat, y cabe mencionar que Euler no sólo le respondió la pregunta, posteriormente escribió varios artículos donde desarrolló el tema y que aún sigue vigente.

[5] La correspondencia completa de 196 cartas se puede consultar en www.eulerarchive.maa.org.

[6] Tratamos de conservar la redacción original.

Que en la formula poligonal $\frac{(p-2)x^2-(p-4)x}{2}$, cuando ésta se le iguala a $4mn - m - n$, p no pueda ser 5 ± 2 ni 5 ± 1, sino que se excluyen todos los trigonales, tetragonales, hexagonales y heptagonales, se sigue del mismo principio.

No considero inútil, que uno haga notar también aquellas proposiciones, las cuales son muy probables, a pesar de que falte una demostración real, pues cuando éstas posteriormente resultasen falsas, así se podría dar la oportunidad de encontrar una nueva verdad. La idea de *Fermat*, de que cada número $2^{2^{n-1}} + 1$ produce una serie de números primos, no se sostiene, como su excelencia ya ha mostrado, pero sería extraordinario que esta serie diera solo números que se pudiesen dividir de manera única en dos cuadrados. ***De este modo arriesgaré también una conjetura: Que todo número, que está compuesto por dos números primos, es un agregado [una suma] de tantos números primos que se quieran (incluida la unidad), hasta alcanzar un agregado [una suma] de unidades. [Anotado por Goldbach al margen: Después de haber vuelto a leer esto, veo que la conjetura se deja demostrar de manera rigurosa para el caso $\boldsymbol{n+1}$, si se cumple para $\boldsymbol{n}$ y $\boldsymbol{n+1}$ se puede dividir en dos números primos. La demostración es muy sencilla. Al menos parece que cada número que es mayor que $\mathbf{2}$ es un agregado [una suma] de tres números primos.] Por ejemplo:***

$$4 = \begin{cases} \mathbf{1+1+1+1} \\ \mathbf{1+1+2} \\ \mathbf{1+3} \end{cases} \qquad \mathbf{5} = \begin{cases} \mathbf{2+3} \\ \mathbf{1+1+3} \\ \mathbf{1+1+1+2} \\ \mathbf{1+1+1+1+1} \end{cases}$$

$$\mathbf{6} = \begin{cases} \mathbf{1+5} \\ \mathbf{1+2+3} \\ \mathbf{1+1+1+3} \\ \mathbf{1+1+1+1+2} \\ \mathbf{1+1+1+1+1+1} \end{cases} \qquad \textbf{etc.}$$

A continuación, siguen un par de observaciones, que pueden ser demostradas:

Si v es una función de x, tal que $v = c$ es un número cualquiera, se puede determinar a x de c y del resto de las constantes expresadas en la función. Entonces se puede determinar el valor de x en la ecuación $v^{2n+1} = (2v+1)(v+1)^{n-1}$.

Si se concibe la curva, cuya abscisa es x, con ordenada la suma de la serie $\frac{x^n}{n \cdot 2^{2n}}$, donde n representa el exponente del término, es decir, la ordenada $= \frac{x}{1 \cdot 2^2} + \frac{x^2}{2 \cdot 2^4} + \frac{x^3}{3 \cdot 2^6} + \frac{x^4}{4 \cdot 2^8}$ etc., esto es, si la abscisa fuera $= 1$, la ordenada sería $= \frac{1}{3}$

2. . . . . $l2$
3. . . . . $2l2$
4 o mayor . . . . infinito.

Quedo con todo respeto [...]

P. S. Ambas fórmulas de números no cuadrados, de las que usted hace mención, aún no las examino, creo sin embargo, que así mismo, cuando uno pone $a = hx + k$, $b = lx + m$, $c = nx + p$ bien pudiesen bajo la siguiente fórmula clasificarse, donde quiera que f, g, γ, δ son números enteros

$$\begin{matrix} (2f - 4\gamma\delta)x^2 + 4(f - 2\gamma\delta)(2g - \delta^2)x + (2g - \delta^2)^2 \\ -4\gamma^2 \qquad\qquad\qquad\qquad -2f \qquad\qquad -2g \end{matrix}$$

pues estos nunca pueden dar un cuadrado.

Independientemente de la exención del gasto de envío el cual su excelencia posee, aquí se incluye el gasto de envío de Berlín a Memel, y por cada carta se paga 65 copecas, entonces sólo pagaré por mis futuras cartas hasta Memel. En lo que respecta a los catálogos, éstos deberían de ser adjuntados siempre que otros envíos salgan de aquí a San Petersburgo para evitar algún peligro de demora. Mientras tanto, me gustaría saber si la más reciente edición del *Dictionaire* de Trevoux, publicado en este o en el anterior año, ya se vende en Berlín y cuál es su costo.

Si se toman m y p como números enteros positivos, la expresión $\frac{p+2\pm\sqrt{4p-m+3}}{m}$ no puede dar un número entero.

Si a su excelencia le sobraran algunos ejemplares del *Memoire de fluxu et fluxu maris*, me gustaría pedirle uno. ¿Ha terminado por completo su correspondencia con H. Chevalier *Mouhi*? La reseña que él llevará a cabo del Institutions Physiques de la Mad. la Marqu. *du Chatellet* valdrá la pena leerla. Mientras tanto, ¿no se habrá enterado, su eminencia, de cuál es el significado de la expresión *à la trancaise* que éste usó? Si algo curioso está contenido en la carta de H. *Poleni*, la cual envié desde San Petersburgo, me gustaría tener alguna noticia de ello. Además, ¿se debería de cambiar algo en la dirección de las cartas a su excelencia?

Goldbach

Podemos ver que la carta es extensa y que la conjetura (lo marcado con negritas) no fue un tema más sobresaliente que los otros. Por otro lado, ya estudiamos los contenidos de las cartas anteriores y la conjetura no era el resultado de un proceso de reflexión que se remontara al pasado, podemos afirmar que la conjetura apareció en esta carta y no tuvo un trabajo previo.

Se puede verificar que la carta 51 contiene 9 temas, uno es la conjetura, y cada uno de los otros 8 sí tiene un antecedente de trabajo previo, así como posterior, entonces podemos inferir que esos sí eran temas de su interés y algunos ya se habían reflexionado desde años atrás.

Los temas son estos:

1) El teorema que hoy conocemos como *pequeño teorema de Fermat*, del que Euler publicaría tres pruebas distintas, una de las cuales se encuentra en la correspondencia. La tercera demostración surge como un caso particular del *Teorema de Euler*, la cual hace uso de la función φ.

2) La expresión polar del coseno, así como la gestación de algunos de los resultados sobre números complejos que posteriormente quedarían bien expuestos en el *Introductio in analysin infinitorum* (1748), en el capítulo XXI (tomo II) *Sobre curvas trascendentes*, Euler define funciones algebraicas, trascendentes e intrascendentes.

3) Se trabaja con los números de la forma $4mn - m - n$, su posible representación como un cuadrado y otros números poligonales, así como su relación con los residuos cuadráticos. Este tipo de números es de los temas más tempranos en su correspondencia, así como de los que más perduraron en sus 37 años de intercambio.

4) Los legendarios primos de Fermat $2^{2^{n-1}} + 1$. Este fue uno de los primeros temas en su correspondencia, se encuentra presente desde la segunda carta. Se puede ver la evolución, que va desde de no tener una respuesta clara a la pregunta de si $2^{2^5} + 1$ es un número primo, hasta llegar a su refutación. De este tema Euler publicó posteriormente al menos dos artículos.

5) La famosa *conjetura de Goldbach*. Planteada como resultado de la pregunta del tema anterior, que, aunque falsa, da pie a encontrar nuevas verdades matemáticas. Aunque solo se encuentra en dos cartas, podemos leer la versión original de la conjetura y la posible razón de su reformulación.

6) Goldbach plantea un polinomio en el que aparentemente sólo pretende encontrar valores del dominio para ciertos valores de la imagen, pero en la respuesta de Euler queda de manifiesto que intrínsecamente lo que se intentaba era mostrar que ese polinomio tiene raíces vinculadas al número áureo.

7) Intercambian ideas sobre el desarrollo en series de logaritmos de funciones racionales.

8) Goldbach responde sobre expresiones de combinaciones de tres cuadrados donde la suma no puede ser un cuadrado, esto se lo mencionó Euler en la carta 50 en el contexto del problema de Fermat de que todo entero es suma de cuatro cuadrados.

9) La expresión $\frac{p+2\pm\sqrt{4p-m+3}}{m}$, la cual no puede expresarse en un número entero. A pesar de que este tema parece ser un tópico independiente, en realidad pertenece a la discusión de los números de la forma $4mn - m - n$.

Sin duda es injusto que la conjetura que ocupó sólo un comentario en la carta 51 y otro en la 52 le quitó la atención a toda la riqueza matemática de los otros temas que sí fueron de su verdadero interés y que muchos constituyeron la base para grandes aportaciones que posteriormente fueron reconocidas.

En los seis capítulos que siguen estudiaremos cada uno de los tópicos que se encuentran en la carta, y lo haremos en el contexto de las cartas anteriores y posteriores a la 51. Proponemos hacerlo así porque esta manera nos permitirá entender el contexto matemático entre ellos, cuando se cruzó la conjetura en sus vidas.

II. Pequeño Teorema de Fermat

El primer elemento matemático de la carta 51 que Goldbach escribió es el siguiente:

> A pesar de que en mi última carta me protegí con un *tal vez*, no habría creído que la fórmula $(a+b)^p - a^p - b^p$ no siempre es dividida por los divisores del número p, si su excelencia no lo hubiese mostrado claramente con su ejemplo citado.

Aquí se puede identificar lo que ahora es, dentro de la teoría de los números, un resultado fundamental para todos los que se inician en esta disciplina, y en particular cuando se estudia la aritmética modular. Nos referimos al que actualmente identificamos como *pequeño teorema de Fermat*, postulado por primera vez en el siglo XVII por Pierre de Fermat (1607-1665). Recordemos con un enunciado presentado con notación actual, el teorema mencionado:

***Teorema* 2.1** (*Pequeño teorema de Fermat*) Si p es un número primo, entonces para cualquier entero positivo a coprimo con p, se tiene que $a^{p-1} \equiv 1\ (mod\ p)$.

Como ya es sabido, a pesar de las múltiples contribuciones que Fermat realizó dentro de las matemáticas, se caracterizó por no presentar todas las pruebas a sus postulados, y este teorema es uno de ellos. Dada la falta de pruebas, muchos matemáticos se embarcaron en la tarea de demostrar los resultados de Fermat, y Euler fue uno de ellos.

El intercambio que se conoce en las cartas respecto a este resultado no fue muy extenso, comparado con los otros temas tratados en la misma, éste abarca alrededor de siete cartas, y entre ellas, la que más aborda el tema es la carta 47, del 6 de marzo del mismo año. En ésta, Euler le comunicó una demostración de este teorema a Goldbach.

El primer registro que tenemos de este resultado —correspondiente a las cartas entre ambos— se encuentra en la carta 15 escrita por Euler, el 25 de noviembre del 1731. Esta primera mención —lo subrayado en la cita que sigue—, se enmarca en la discusión acerca de un conjunto particular de números que conocemos como primos de Mersenne. La nota del 25 de noviembre es la siguiente:

> He sopesado también acerca de la fórmula $2^n - 1$ que no puede ser un número primo, a menos que n lo sea, y he investigado aquellos casos en que $2^n - 1$ no es un número primo y n sí lo es. Estas excepciones son: $n = 11$; $n = 23$; $n = 83$. Los números primos restantes menores a 100, al sustituirse por n, hacen a $2^n - 1$ un primo. En particular: $2^{11} - 1$ es dividido por 23; $2^{23} - 1$ por 47; y $2^{83} - 1$ por 167. <u>La razón de esto se encuentra en este elegante teorema: $2^n - 1$ siempre es divisible por $n + 1$, si efectivamente $n + 1$ fuera un número primo</u>. Así $2^{22} - 1$ es dividido por 23. Frecuentemente $2^{n/2} - 1$, así como $2^{n/4} - 1$, etc., pueden ser divididos por $n + 1$, y así investigando los casos en que $2^n - 1$ es un número primo, no es difícil.

Podemos observar que Euler plantea un caso particular del *pequeño teorema*, específicamente para $p = n + 1$ y $a = 2$.

No se puede dejar de mencionar que en 1732 Euler escribió el trabajo *Observationes de theoremata quodam Fermatiano aliisque ad números primos spectantibus*,[7] en él se encuentra el siguiente teorema:

$a^n - b^n$ siempre puede ser dividido por $n + 1$, si $n + 1$ es un primo que no divida ni a a ni a b.

---

[7] A partir de esta cita nos referiremos a los trabajos de Euler con base en el índice de creó Gustav Eneström, él listó todos los trabajos escritos por Euler con los números de E1 a E866. Para el caso del artículo señalado es el E26. Los contenidos completos se pueden consultar en: www.eulerarchive.maa.org

Euler comenta que cree que la prueba es difícil pues el teorema no es cierto a menos que $n+1$ sea primo. Después concluye que 2^n-1 podrá dividirse por $n+1$ siempre que $n+1$ sea un primo y siempre que $n+1$ no sea 2.

Es interesante notar que la carta del 25 de noviembre de 1731 registra lo que posteriormente se conocería en el artículo [Euler, Leonhard. 1738, E26].

Primera demostración

Después de la misiva del 25 de noviembre, no hay otra que haga referencia inmediata a este resultado hasta la carta 47, del 6 de marzo de 1742, donde aparece por segunda vez, y la cual resultaría ser la más importante, como se dijo anteriormente. En esta carta se prueba este teorema, pero es importante aclarar que ésta no sería la primera demostración desarrollada por Euler. A pesar de comunicarle su prueba a Goldbach en la carta 47, Euler ya había realizado otra demostración de éste. En 1736[8] presentó la prueba en el trabajo *Theorematum quorundam ad numeros primos spectantium demonstratio*, a través de una forma primigenia de lo que hoy conocemos como proceso de inducción. A continuación, desarrollaremos esta demostración la cual está dividida en tres teoremas. Los primeros, **2.2** y **2.3** equivalen —de alguna manera— a lo que actualmente entendemos como *base inductiva* y el **2.4** comprendería la *hipótesis* y *paso inductivo*.[9]

***Teorema* 2.2** Si p es un número primo impar, entonces la fórmula $2^{p-1}-1$ siempre puede ser dividida por p.

Demostración: Consideremos $1+1$ en lugar de 2, por lo que tendríamos $(1+1)^{p-1}$. Desarrollando mediante el *teorema del binomio* tenemos que

$$(1+1)^{p-1} = \binom{p-1}{0}\cdot 1^{p-1}\cdot 1^0 + \binom{p-1}{1}\cdot 1^{p-2}\cdot 1^1 + \binom{p-1}{2}\cdot 1^{p-3}\cdot 1^2 + \cdots$$

$$= \frac{(p-1)!}{0!\,(p-1)!} + \frac{(p-1)!}{1!\,(p-2)!} + \frac{(p-1)!}{2!\,(p-3)!} + \cdots$$

$$= 1 + \frac{p-1}{1} + \frac{p-1}{1}\frac{p-2}{2} + \frac{p-1}{1}\frac{p-2}{2}\frac{p-3}{3} + \cdots + \frac{p-1}{1} + 1$$

Notemos que el número de términos es igual a p y por lo tanto impar. Dado que cada término de esta suma proviene de un coeficiente binomial, por lo tanto, cada sumando es un número entero. Ahora bien, al restar 1 para eliminar el primer término de la secuencia obtenemos $(1+1)^{p-1}-1 = 2^{p-1}-1 = \frac{p-1}{1} + \frac{p-1}{1}\frac{p-2}{2} + \frac{p-1}{1}\frac{p-2}{2}\frac{p-3}{3} + \cdots \frac{p-1}{1} + 1$. Por lo tanto, la cantidad de términos de esta nueva sucesión es $p-1$, es decir, par.

Sumando cada par de términos de manera consecutiva nos arroja la siguiente fórmula $2^{p-1}-1 = \frac{p}{1}\frac{p-1}{2} + \frac{p}{1}\frac{p-1}{2}\frac{p-2}{3}\frac{p-3}{4} + \frac{p}{1}\frac{p-1}{2}\frac{p-2}{3}\frac{p-3}{4}\frac{p-4}{5}\frac{p-5}{6} + \cdots + p$, ya que para la primera suma se tiene que

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

[8] Apareció publicado posteriormente en 1741.

[9] [Euler 1741, E54].

$$= \frac{p-1}{1}\left(\frac{2}{2}+\frac{p-2}{2}\right)$$
$$= \frac{p-1}{1}\left(\frac{2+p-2}{2}\right)$$
$$= \frac{p}{1}\frac{p-1}{2}.$$

En general

$$\frac{p-1}{1}\frac{p-2}{2}\cdots\frac{p-(2k-2)}{2k-2}\frac{p-(2k-1)}{2k-1}+\frac{p-1}{1}\frac{p-2}{2}\cdots\frac{p-(2k-1)}{2k-1}\frac{p-2k}{2k}$$
$$= \frac{p-1}{1}\frac{p-2}{2}\cdots\frac{p-(2k-2)}{2k-2}\frac{p-(2k-1)}{2k-1}\left(1+\frac{p-2k}{2k}\right)$$
$$= \frac{p-1}{1}\frac{p-2}{2}\cdots\frac{p-(2k-2)}{2k-2}\frac{p-(2k-1)}{2k-1}\left(\frac{2k}{2k}+\frac{p-2k}{2k}\right)$$
$$= \frac{p-1}{1}\frac{p-2}{2}\cdots\frac{p-(2k-2)}{2k-2}\frac{p-(2k-1)}{2k-1}\left(\frac{2k+p-2k}{2k}\right)$$
$$= \frac{p}{1}\frac{p-1}{2}\frac{p-2}{3}\cdots\frac{p-(2k-2)}{2k-1}\frac{p-(2k-1)}{2k}$$

Observemos que nuestro último término es p, dado que $\frac{p-1}{1}+1=p$. Por lo tanto, en $2^{p-1}-1=\frac{p}{1}\frac{p-1}{2}+\frac{p}{1}\frac{p-1}{2}\frac{p-2}{3}\frac{p-3}{4}+\frac{p}{1}\frac{p-1}{2}\frac{p-2}{3}\frac{p-3}{4}\frac{p-4}{5}\frac{p-5}{6}+\cdots+p$ cada sumando tiene un número par de factores, y cada uno de los sumandos es divisible por p. Por lo que, si p es un número primo impar, entonces $2^{p-1}-1$ siempre es divisible por p.

Alternativamente, para el mismo número primo p, la expresión $2^{p-1}-1$, al ser multiplicada por 2, se puede llevar a la forma 2^p-2. Ahora bien, si se toma 2 como $1+1$ y aplicando el *teorema del binomio* tenemos

$$2^p=(1+1)^p=\binom{p}{0}\cdot 1^p\cdot 1^0+\binom{p}{1}\cdot 1^{p-1}\cdot 1^1+\binom{p}{2}\cdot 1^{p-2}\cdot 1^2+\cdots+1$$
$$=1+\frac{p}{1}+\frac{p}{1}\frac{p-1}{2}+\frac{p}{1}\frac{p-1}{2}\frac{p-2}{3}+\cdots+1$$

Al restar el primer y último término tenemos $2^p-2=\frac{p}{1}+\frac{p}{1}\frac{p-1}{2}+\frac{p}{1}\frac{p-1}{2}\frac{p-2}{3}+\cdots$. Podemos observar que esta suma es divisible por p, pues cada sumando lo es. Por lo que 2^p-2 es divisible por p. Por lo tanto, $2^{p-1}-1$ es divisible por p, si $p\neq 2$. ■

***Teorema* 2.3** Si p es un número primo distinto a 3, entonces $3^{p-1}-1$ siempre puede ser dividido por p.

Demostración: Consideremos la expresión $3^{p-1}-1$. Multiplicándola por 3 obtenemos 3^p-3. Consideremos a 3 como $1+2$, y usando el *teorema del binomio* para desarrollar $(1+2)^p$ obtenemos

$$3^p=(1+2)^p=\binom{p}{0}\cdot 1^p\cdot 2^0+\binom{p}{1}\cdot 1^{p-1}\cdot 2^1+\binom{p}{2}\cdot 1^{p-2}\cdot 2^2+\cdots+2^p$$
$$=1+\frac{p}{1}\cdot 2+\frac{p}{1}\frac{p-1}{2}\cdot 4+\frac{p}{1}\frac{p-1}{2}\frac{p-2}{3}\cdot 8+\cdots+2^p$$

Restamos el primer y último término de cada lado, pues estos no son divisibles por p, y obtenemos que

$$3^p - 2^p - 1 = \frac{p}{1} \cdot 2 + \frac{p}{1}\frac{p-1}{2} \cdot 4 + \frac{p}{1}\frac{p-1}{2}\frac{p-2}{3} \cdot 8 + \cdots.$$

Notemos que $3^p - 2^p - 1$ es divisible por p, pues cada sumando del lado derecho es divisible por p, por lo que la suma de la izquierda es divisible por p, y esta fórmula es equivalente a $3^p - 3 - 2^p + 2$, y por el teorema anterior $2^p - 2$ siempre es divisible por p, entonces tenemos que la expresión $3^p - 3$ es divisible por p, y consecuentemente $3^{p-1} - 1$ es divisible por p, si se tiene que $p \neq 3$. ■

***Teorema* 2.4** Sea p un número primo, si $a^p - a$ es divisible por p, entonces $(a+1)^p - (a+1)$ es divisible por el mismo número p.

Demostración: Supongamos que $a^p - a$ es divisible por p. Como hemos estado haciendo, usaremos el *teorema del binomio* para expandir $(1+a)^p$, así

$$\begin{aligned}(1+a)^p &= \binom{p}{0} \cdot 1^p \cdot a^0 + \binom{p}{1} \cdot 1^{p-1} \cdot a^1 + \binom{p}{2} \cdot 1^{p-2} \cdot a^2 + \cdots + a^p \\ &= 1 + \frac{p}{1} \cdot a + \frac{p}{1}\frac{p-1}{2} \cdot a^2 + \frac{p}{1}\frac{p-1}{2}\frac{p-2}{3} \cdot a^3 + \cdots + a^p\end{aligned}$$

Observemos que en esta expresión cada término es divisible por p, a excepción del primero y el último. Eliminándolos obtenemos $(1+a)^p - a^p - 1$, la cual es divisible por p. Esta expresión es equivalente a $(1+a)^p - a - 1 - a^p + a$. Por hipótesis tenemos que $a^p - a$ es divisible por p, por lo que $(1+a)^p - a - 1$ es divisible por p, y en consecuencia $(1+a)^{p-1} - 1$ también lo es, si $p \neq a+1$.

Por lo tanto, si p es un número primo, entonces la fórmula $a^{p-1} - 1$ es divisible por p, siempre que a y p sean coprimos. ■

Con esto se termina lo que se considera como la primera de tres pruebas hechas por Euler.

Como se señaló antes de la demostración, Euler recurrió a un proceso de inducción. Lo que actualmente plantearíamos como camino de la demostración, en este mismo contexto de la propuesta de Euler es que:

1) Si p es un número primo impar, entonces $2^p - 2$ siempre puede ser dividido por p, y en consecuencia también lo es $2^{p-1} - 1$.

2) Suponemos que p primo divide a $a^p - a$, con a en los naturales. Si $p \nmid a$, entonces también $a^{p-1} - 1$ es divisible por p.

3) Por demostrar que $(a+1)^p - (a+1)$ es divisible por el primo p

Como se mencionó, los teoremas **2.2** y **2.3** equivalen —de alguna manera— a lo que actualmente entendemos como *base inductiva*, lo que es 1), y el teorema **2.4** comprendería la *hipótesis* y *paso inductivo*, que es lo señalado en 2) y 3).

De ninguna manera se puede decir que Euler usó inadecuadamente el proceso inducción, pues se tiene que considerar que él estaba entre los primeros que estaban construyendo este modo de demostrar y a la vez presentaba las primeras demostraciones de este *teorema de Fermat*.

Segunda demostración

La segunda prueba corresponde a lo que se encuentra en la carta 47, la cual tiene similitudes con la desarrollada en el artículo *Theoremata circa divisores numerorum* de 1747, y que se dio a conocer en 1750.

Lo que le presenta a Goldbach en la carta 47 son dos proposiciones con sus respectivos corolarios. La primera proposición enuncia lo siguiente:

***Proposición* 2.5** La expresión $(a+b)^p - (a^p + b^p)$ siempre es divisible por p, si p es un número primo.

Demostración: Sea p un número primo. Se desarrollará la potencia $(a+b)^p$

$$(a+b)^p = \binom{p}{0} \cdot a^p \cdot b^0 + \binom{p}{1} \cdot a^{p-1} \cdot b^1 + \binom{p}{2} \cdot a^{p-2} \cdot b^2 + \cdots + b^p$$

$$= a^p + \frac{p}{1} \cdot a^{p-1} \cdot b^1 + \frac{p}{1}\frac{p-1}{2} \cdot a^{p-2} \cdot b^2 + \frac{p}{1}\frac{p-1}{2}\frac{p-2}{3} \cdot a^{p-3} \cdot b^3 + \cdots + \frac{p}{1} \cdot a^1 \cdot b^{p-1} + b^p$$

Nótese que cada término de la expresión es divisible por p, a excepción del primero y el último. Al restar a^p y b^p de ambos lados de la igualdad obtenemos $(a+b)^p - a^p - b^p$. Esta expresión es divisible por p, pues $\frac{p}{1} \cdot a^{p-1} \cdot b^1 + \frac{p}{1}\frac{p-1}{2} \cdot a^{p-2} \cdot b^2 + \frac{p}{1}\frac{p-1}{2}\frac{p-2}{3} \cdot a^{p-3} \cdot b^3 + \cdots + \frac{p}{1} \cdot a^1 \cdot b^{p-1}$ es divisible por p.

Por lo tanto, $(a+b)^p - (a^p + b^p)$ siempre es divisible por p, si p es un número primo. ■

***Corolario* 2.6** Si se propone $a = b = 1$, entonces $(a+b)^p - a^p - b^p = (1+1)^p - 1^p - 1^p = 2^p - 2$ es divisible por un número primo p. Por lo tanto, si $p \neq 2$ entonces $2^{p-1} - 1$ será divisible por p.

***Corolario* 2.7** Ahora bien, si $a = 2$ y $b = 1$, entonces $(a+b)^p - a^p - b^p = 3^p - 2^p - 1$ es divisible por p. Observemos que $3^p - 2^p - 1 = 3^p - 3 - 2^p + 2 = 3^p - 3 - (2^p - 2)$. Por **2.6** tenemos que $2^p - 2$ es divisible por p, por lo que $3^p - 3$ también será divisible por p. Por lo tanto, si $p \neq 3$, entonces $3^{p-1} - 1$ será divisible por p.

La segunda proposición enuncia lo siguiente:

***Proposición* 2.8** Si $a^p - a$ fuera divisible por p, también $(a+1)^p - (a+1)$ será dividido por p.

Demostración: Si en **2.5** consideramos que $b = 1$, entonces $(a+1)^p - a^p - 1$ será dividido por p. Por otro lado, por hipótesis $a^p - a$ es divisible por p. Sumando $(a+1)^p - a^p - 1$ y $a^p - a$ tenemos

$$(a+1)^p - a^p - 1 + a^p - a = (a+1)^p - a - 1$$

Por lo tanto, $(a+1)^p - (a+1)$ es divisible por p. ■

***Corolario* 2.9** Por lo tanto, $1^p - 1$ es divisible por p, de la misma manera $2^p - 2$ es divisible por p, y a partir de esto, $3^p - 3$, $4^p - 4$, $5^p - 5$, etc.

***Corolario* 2.10** De manera general, la expresión $a^p - a$ es divisible por un primo p, para cualquier entero a que se ponga. Por lo tanto, si $p \neq a$, entonces $a^{p-1} - 1$ también será divisible por p.

***Corolario* 2.11** De manera semejante, $b^{p-1} - 1$ es divisible por un número primo p, excepto si b es múltiplo de p. Se seguirá que $a^{p-1} - b^{p-1}$ será divisible por p, pues

$$a^{p-1} - 1 - (b^{p-1} - 1) = a^{p-1} - 1 - b^{p-1} + 1 = a^{p-1} - b^{p-1}.$$

La segunda demostración tiene elementos semejantes a la primera en el proceso de inducción, la diferencia es que ahora la Proposición **2.5** proporciona los elementos para la *base inductiva*, a través de los Corolarios **2.6** y **2.7**. Enseguida, la Proposición **2.8** —y de la misma forma que para la primera demostración— asume el papel de la *hipótesis* y *paso inductivo*. La diferencia entre las dos demostraciones es la manera en la que construye la base inductiva, mientras que en la primera demostración lo hace directamente, a través de los teoremas **2.3** y **2.4**; en la segunda, primero demuestra la Proposición **2.5** y posteriormente los casos particulares, Corolarios **2.6** y **2.7**, proporcionan los elementos para la la *base inductiva*.

En este trabajo de tesis no presentamos un estudio de la segunda demostración contenida en el *Theoremata circa divisores numerorum* de 1747, este trabajo se centró más en la carta de Euler a Goldbach. Para un estudio detallado de la segunda demostración contenida en el artículo señalado se 1747 se puede consultar a [Torres, 2012].

A continuación, presentamos una tabla mostrando las similitudes y diferencias en los enunciados de cada prueba:

Carta 47	*Theorematum quorundam ad numeros primos spectantium demonstratio* (Primera demostración)	*Theoremata circa divisores numerorum* (Segunda demostración)
Proposición 1: Si p es un número primo, entonces todo número de la forma $(a + b)^p - a^p - b^p$ es dividido por p.	-	*Teorema 1*: Si p es un número primo, entonces todo número de la forma $(a + b)^p - a^p - b^p$ es dividido por p.
Corolario 1: Evaluar $a = b = 1$ en *Teorema 1* para obtener $2^p - 2$, y luego $2^{p-1} - 1$.	*Teorema 1*: Si p es un número primo impar, entonces la fórmula $2^{p-1} - 1$ siempre puede ser dividida por p.	*Corolario 1*: Evaluar $a = b = 1$ en *Teorema 1* para obtener $2^p - 2$, y luego $2^{p-1} - 1$.
Corolario 2: Evaluar $a = 2$ y $b = 1$ en *Teorema 1* para obtener $3^p - 2^p - 1$, sumar $2^p - 2$ para obtener $3^p - 3$ y luego $3^{p-1} - 1$.	*Teorema 2*: Si p es un número primo distinto a 3, entonces $3^{p-1} - 1$ siempre puede ser dividido por p.	-

-	-	*Corolario 2*: Evaluar primos p sucesivos en $2^{p-1}-1$.
-	-	*Teorema 2*: Si p divide a^p-a y b^p-b, entonces $$(a+b)^p-a-b$$ es dividido por p.
-	-	*Corolario 1*: Evaluar $b=1$ en *Teorema 2*, para obtener $$(a+1)^p-a-1.$$
Proposición 2: Si a^p-a fuera divisible por p, también $$(a+1)^p-a-1$$ será dividido por p.	*Teorema 3:* Sea p un número primo, si a^p-a es divisible por p, entonces $(a+1)^p-a-1$ es divisible por el mismo número p.	*Corolario 2*: Si a^p-a es dividido por p, entonces también lo será $(a+1)^p-a-1$, y sucesivamente, es decir, en general c^p-c será dividido por p.
-	-	*Teorema 3*: Si p es un número primo, entonces c^p-c es dividido por p.
Corolario 1: Por tanto, 1^p-1 es divisible por p, de la misma manera 2^p-2 es divisible por p, y a partir de esto, 3^p-3, 4^p-4, 5^p-5, etc.	-	*Corolario 1*: Para cualquier número c, si p es primos, entonces c^p-c es dividido por p.
Corolario 2: De manera general, entonces la expresión a^p-a es divisible por un primo p, para cualquier entero a que se ponga. Por lo tanto, a menos que haya un divisor p de a, también $a^{p-1}-1$ será divisible por p.	-	-
-	-	*Corolario 2*: Si c^p-c es dividido por p, entonces $c^{p-1}-1$ es dividido por p, para $p\neq c$.
-	-	*Corolario 3*: Si p es primo, entonces $a^{p-1}-1$ es dividido por p, siempre que p no divida a a.

Corolario 3: De manera semejante, $b^{p-1} - 1$ es divisible por un número primo p, excepto si b es múltiplo de p. Se seguirá que $a^{p-1} - b^{p-1}$ será divisible por p.	-	*Teorema 4*: Si p no divide a a ni a b, entonces todo número de la forma $a^{p-1} - b^{p-1}$ es dividido por p.

La finalidad de la tabla es mostrar que la carta 47 tenía un antecedente y a la vez una extensión temática. Pero antes de regresar a la carta 51, que es nuestro eje central, veamos un bosquejo de lo que fue su tercera demostración del *pequeño teorema*. Lo hacemos con el fin de fortalecer la idea de que lo tratado en la carta 51 tuvo alcances notables.

Tercera demostración con teoría de residuos

La tercera demostración de Euler del *pequeño teorema* está en el artículo *Theoremata circa residua ex divisione potestatum relicta* (E262) (Teoremas sobre residuos obtenidos por divisiones de potencias) publicado en 1761. En este expone lo que ahora conocemos como teoría de los residuos, que es fundamental para la teoría de los números.

Euler trabajó con los residuos que deja cada una de las potencias de un número al ser dividida por un primo. En el artículo presenta algunas proposiciones básicas acerca de residuos, y éstas actualmente son parte de los teoremas fundamentales de las relaciones de congruencia. Euler utilizó todo esto para mostrar algunos teoremas con los que desarrolló el concepto actual de orden de un número módulo *n* (es decir, la mínima potencia m de a tal que $a^m \equiv 1\ (mod\ n)$). Así, planteó que si λ es el orden de a, entonces los residuos que deja dividir cada elemento de la serie $1, a^2, a^3, \ldots\ a^{\lambda-1}$ entre p (con $(a, p) = 1$) serán todos diferentes y de estos se derivan las clases residuales módulo p.

En el artículo desarrolla teoremas referentes al orden de a módulo p, que finalmente lo llevan al *pequeño teorema de Fermat*, que es necesario para demostrar teoremas sobre divisores de números de la forma $ax^n - y^n$. Estos resultados fueron la base para trabajar sobre cuerpos cuadráticos o para demostrar *leyes de reciprocidad cuadrática*, entre otros temas.

Es importante aclarar que este trabajo de Euler no pretendía presentar y demostrar el *pequeño teorema de Fermat*. Su interés estaba centrado en el estudio del comportamiento de los residuos de potencias, y el *pequeño teorema* sólo fue una consecuencia de otros resultados, que para él sí eran centrales en su artículo.

A continuación, se presenta la tercera demostración, pero se requieren teoremas previos que sólo serán enunciados. En este trabajo no se profundizará con las demostraciones[10] de ellos para no desviar el tema principal que está en torno a los antecedentes y continuidad de los temas de la carta 51 de la correspondencia.

[10] Para los interesados en ver las demostraciones completas se puede acudir al artículo original E262 o a la edición de Struik [1969].

***Teorema* 2.12** Si el número de los diferentes residuos resultantes de dividir las potencias $1, a, a^2, a^3, a^4, a^5$ ... entre el número primo p fuera menor que $p-1$,entonces se tendrán al menos tantos números que no son residuos como números que son residuos.

***Corolario* 2.13** Consecuentemente se tienen λ números que son residuos diferentes, y son tantos como diferentes números menores que p, entonces el número total de 2λ en conjunto no podrá ser mayor que $p-1$, porque no hay más números menores que p.

***Corolario* 2.14** Si a^λ es la mínima potencia que después de ser dividida por p deja como residuo 1, entonces se tendría que $\lambda < p-1$, y por lo tanto no se tendría que $\lambda > \frac{p-1}{2}$, en consecuencia, se tendría que $\lambda = \frac{p-1}{2}$ o $\lambda < \frac{p-1}{2}$.

***Corolario* 2.15** Si el exponente λ es el de la mínima potencia, éste es necesariamente menor que p; entonces será o bien $\lambda = p-1$ o $\lambda < p-1$; en el caso que $\lambda < p-1$, sabemos que será $\lambda = \frac{p-1}{2}$ o $\lambda < \frac{p-1}{2}$. Por lo tanto λ no podrá tomar como valor ningún número contenido más allá de los límites $p-1$ y $\frac{p-1}{2}$.

***Teorema* 2.16** Si p es un número primo, y a^λ la mínima potencia de a que deja la unidad cuando es dividida por p, y si $\lambda < \frac{p-1}{2}$; entonces no puede pasar que el exponente λ sea más grande que $\frac{p-1}{3}$: por lo tanto, será $\lambda = \frac{p-1}{3}$ o $\lambda < \frac{p-1}{3}$.

***Corolario* 2.17** Por lo tanto, si no se tiene que $\lambda < \frac{p-1}{3}$ se tendrá ciertamente que $\lambda = \frac{p-1}{3}$, y si suponemos que no pasa que $\lambda < \frac{p-1}{2}$, y que tampoco sucede que $\lambda < \frac{p-1}{3}$, entonces se sigue necesariamente que $\lambda = \frac{p-1}{3}$ o $\lambda = \frac{p-1}{2}$ o $\lambda = p-1$.

***Corolario* 2.18** Más aún, si $\lambda = \frac{p-1}{3}$ o $\lambda = \frac{p-1}{2}$, entonces la potencia a^{p-1} dividida por p dejaría como residuo la unidad. Pues como a^λ deja a la unidad como residuo, también lo harán $a^{2\lambda}$ y $a^{3\lambda}$.

***Teorema* 2.19** Si a^λ fuera la mínima potencia de a que deja la unidad cuando es dividida por un número primo p, y si fuera $\lambda < \frac{p-1}{3}$, entonces no puede pasar que $\lambda > \frac{p-1}{4}$ por lo tanto será $\lambda = \frac{p-1}{4}$ o $\lambda < \frac{p-1}{4}$.

***Corolario* 2.20** De manera similar se puede demostrar, que si $\lambda < \frac{p-1}{4}$ entonces es imposible que $\lambda > \frac{p-1}{5}$, y por lo tanto se tendría que $\lambda = \frac{p-1}{5}$ o $\lambda < \frac{p-1}{5}$.

***Corolario* 2.21** En general si se sabe que $\lambda < \frac{p-1}{n}$, se puede demostrar que no puede pasar que $\lambda > \frac{p-1}{n+1}$, por lo tanto $\lambda = \frac{p-1}{n+1}$ ó $\lambda < \frac{p-1}{n+1}$.

***Corolario* 2.22** De esto es claro que el número de todos los números que no son residuos tiene que ser 0 o λ o 2λ, o cualquier otro múltiplo de λ, pues si hubiera más números de este tipo que $n\lambda$, entonces como otros λ siguen se tiene que el número de no residuos serían $(n+1)\lambda$; y si estos no fueran los únicos números contenidos en los no residuos, entonces de nuevo se tendrían otros λ no residuos.

***Teorema* 2.23** Sea p un número primo y a^{λ} la mínima potencia de a que al ser dividida por p deja la unidad como residuo, entonces el exponente λ será un divisor del número $p-1$.

Con base en esta serie de teoremas y corolarios Euler llega al teorema esperado.

***Teorema* 2.24** (*Pequeño teorema de Fermat*) Si p es un número primo y a es primo con p entonces la potencia a^{p-1} dejará a la unidad como residuo cuando sea dividida por p.

Demostración: Sea a^{λ} la mínima potencia de a que deja a la unidad como residuo al ser dividida por p, entonces $\lambda < p$, pero del teorema anterior $\lambda = p-1$ o bien es un factor de $p-1$. Si pasa lo primero entonces el teorema queda demostrado. Pero si pasa que $p-1 = n\lambda$, y como a^{λ} deja como residuo 1 cuando es dividida por p, entonces también darán el mismo residuo $a^{2\lambda}$, $a^{3\lambda}$, etc., y así hasta que se llegue a $a^{n\lambda} = a^{p-1}$, que también dejará la unidad cuando sea dividida por p. ■

Esta demostración evidentemente es diferente a las otras dos. Ésta se fundamenta con residuos de potencias y un módulo primo. Euler compara su demostración con la que hizo en 1736, y comenta que difieren en que la primera dio inicio con el desarrollo del binomio $(a+b)^n$, y esto hace que el razonamiento parezca distante de lo que se quiere demostrar; pero en cambio, la última demostración se construye con base en residuos de potencias y estos hacen que la prueba parezca más natural, pues el *pequeño teorema de Fermat* queda en el contexto de residuos de potencias.

Ahora regresemos al origen de todo esto, que fue el primer pasaje de la carta 51:

> A pesar de que en mi última carta me protegí con un *tal vez*, no habría creído que la fórmula $(a+b)^p - a^p - b^p$ no siempre es dividida por los divisores del número p, si su excelencia no lo hubiese mostrado claramente con su ejemplo citado.

Lo que se puede detectar es que ambos están intercambiando ideas respecto de la carta 47 que trata la segunda demostración del *pequeño teorema*. En la carta 49 Goldbach le comenta que es posible que "se pueda decir de manera más general que $(a+b)^p - a^p - b^p$ siempre es divisible por algún divisor de p, de donde se sigue como caso particular que, cuando p es un número primo, la fórmula mencionada sería divisible por el mismo número p".

La respuesta de Euler en la carta 50 fue para corregir a Goldbach, le contesta esto:

> Por lo demás, que la demostración que recientemente le envié haya sido aprobada por su excelencia, me alegra mucho. Pero que la fórmula $(a+b)^p - a^p - b^p$, cuando p no es un número primo, debería de ser divisible por p o por algún divisor de p, exceptuando la unidad, no solamente no puede ser comprobado mediante mi demostración, sino que en muchos casos no se cumple. Como cuando $a=1$ y $b=1$, y $p=35$, entonces $2^{35}-2$ no puede ser divido ni por 5 ni por 7.

De manera clara Euler le muestra un contra ejemplo de que no siempre p o un divisor de p divide a $(a+b)^p - a^p - b^p$, y es en la carta 51 que Goldbach le reconoce a Euler su aclaración a través de un contraejemplo. Posteriormente en la carta 61 de enero de 1743 Euler le escribe otras propiedades de estas mismas expresiones.

No hay duda de que este tema de la carta 51 fue de gran importancia para ambos. Se puede ver que desde 1731 Euler ya le comunicaba algunas de sus reflexiones al respecto. Para 1736 ya había escrito la primera demostración del teorema y su interés se manifiesta aún en 1761 con la tercera demostración. Sin duda este primer elemento de la carta nos refleja un tema de gran interés para ambos.

III. Las raíces imaginarias $\sqrt{-1}$

En el segundo elemento matemático de la carta 51, Goldbach le expresa lo siguiente:

> Hasta donde recuerdo, en mi última carta imaginé la fórmula $2^{xp\sqrt{-1}} + 2^{-xp\sqrt{-1}}$, asumiendo $2^{p\sqrt{-1}} + 2^{-p\sqrt{-1}} = 0$, como las ordenadas de una curva serpentiforme, cuyas abscisas son x y cuyo eje es intersectado siempre que la fórmula sea $= 0$, de modo que cuando la misma fórmula es $= 2$, se obtiene la máxima ordenada abajo o arriba, y por consiguiente otras innumerables ordenadas que deben de ser iguales entre ellas. Sin embargo, se deslizó un error en mi expresión de aquel momento, el cual me marcó, su excelencia, con razón y que se puede corregir fácilmente declarando que, cuando q es un número cualquiera y estableciendo $2^{p\sqrt{-1}} + 2^{-p\sqrt{-1}} = 0$, entonces, asumiendo n como un número entero cualquiera, se tiene
>
> $$2^{(8n-4-q)p\sqrt{-1}} + 2^{-(8n-4-q)p\sqrt{-1}} = 2^{qp\sqrt{-1}} + 2^{-qp\sqrt{-1}}.$$

Se puede notar que esta comunicación la debemos de contextualizar y se debe a que este tema lo estaban reflexionando desde la carta 43, del 9 de diciembre de 1741. En ésta Euler le escribió lo siguiente:

> Recientemente encontré una paradoja curiosa, a saber, que el valor de esta expresión $\frac{2^{+\sqrt{-1}}+2^{-\sqrt{-1}}}{2}$ es aproximadamente igual a $\frac{10}{13}$, y esta fracción difiere de la verdad en solo una millonésima parte. El verdadero valor de esta expresión es el coseno del arco 0.693147180559, o bien el arco de $39°, 42', 51'', 52''', 9^{IV}$ de un círculo cuyo radio es $= 1$.

Para entender el contexto de lo que Euler le plantea a Goldbach, consideramos que es adecuado explorar los primeros pasos de Euler en el mundo de los ahora conocidos números complejos.

Euler y las raíces imaginarias

Es frecuente que al buscar sobre el origen de las raíces imaginarias nos encontremos primero con el trabajo de Caspar Wessel (1745-1818), pero esto es una imprecisión, pues la teoría de las raíces imaginarias ya contaba con múltiples propiedades para $\sqrt{-1}$, y fueron antes de Wessel. El que las planteó en diversos contextos, que van desde las ecuaciones diofantinas hasta las ecuaciones diferenciales fue Euler.

En una carta fechada el 18 de octubre de 1740 Euler le escribió a su maestro Johann Bernoulli y le compartió su análisis de que la solución de la siguiente ecuación diferencial:

$$\frac{d^2y}{dx^2} + y = 0, \text{ con } y(0) = 2 \text{ y } y'(0) = 2$$

se puede escribir de dos formas que son estas:

$$y(x) = 2\cos(x)$$
$$y(x) = e^{x\sqrt{-1}} + e^{-x\sqrt{-1}}$$

Independientemente de que el razonamiento de Euler es verdad para cada una de las funciones $y(x)$, lo más sobresaliente es que la igualdad entre ambas expresiones dio lugar a la expresión que sigue:

$$2\cos(x) = e^{x\sqrt{-1}} + e^{-x\sqrt{-1}}.$$

En la misma carta, aparte de las soluciones de la ecuación diferencial también presentó otra expresión trigonométrica en términos de las raíces imaginarias:

$$2i\sin(\mathrm{x}) = e^{x\sqrt{-1}} - e^{-x\sqrt{-1}}.$$ [11]

Un año después de su carta a Johann Bernoulli, Euler escribió a Goldbach (9 de diciembre de 1741, la carta citada arriba) y le plantea la siguiente aproximación

$$\frac{2^{+\sqrt{-1}} + 2^{-\sqrt{-1}}}{2} \approx \frac{10}{13}$$

El lado derecho es $\cos(ln2)$ y tiene una aproximación con $10/13$ de por lo menos hasta el sexto decimal. En 1748 Euler publicó en su libro *Introductio in analysin infinitorum* la fórmula que ahora vemos en todos los cursos de álgebra cuando estudiamos lo que ahora llamamos números complejos

$$e^{\pm i\alpha} = \cos(\alpha) \pm \sin(\alpha).$$

Para entender más el contexto del intercambio entre ellos sobre las raíces imaginarias consideramos que lo más adecuado es consultar su *Introductio in analysin infinitorum*, obra que publicó en 1748. Ésta recopila y nos lleva a entender de mejor manera el contexto de las cartas que analizaremos, correspondientes a este tema de las raíces imaginarias.

En este breve preámbulo de las raíces imaginarias presentes en el trabajo de Euler, no se puede dejar de mencionar que Nicolás Bernoulli tuvo un papel muy importante en él cuando construyó los paradigmas sobre las raíces imaginarias de polinomios, es más, se puede afirmar que en este tema Euler tuvo una influencia más tangible de parte de Nicolás que de Johann. Una lectura recomendada para entender esta influencia de Nicolás en Euler es la obra de Carlos Álvarez y Jean Dhombres [2011, pp. 183-191]. Esta obra nos permite entender cómo Nicolás le presenta ciertas observaciones a Euler respecto a las raíces de polinomios, pero además nos proporciona elementos para comprender de mejor manera la conformación de algunas partes del *Introductio*, por ejemplo, el Capítulo IX.

Introductio in analysin infinitorum

En el Tomo I §138, Euler desarrolla las expresiones polares para el seno y el coseno. Para entender cómo realizó esto, es conveniente regresar a §132. Primero retoma la identidad

$$\cos^2(x) + \sin^2(x) = 1$$

y observa que tiene los siguientes factores $[\cos(x) + i\sin(x)]\,[\cos(x) - i\sin(x)] = 1$. Después considera el siguiente producto

$$[\cos(z) + i\sin(z)][\cos(y) + i\sin(y)] \ldots (1).$$

Al desarrollar se obtiene

$$\cos(y)\cos(z) - \sin(y)\sin(z) + [\cos(y)\sin(z) + \sin(y)\cos(z)]i \ldots (2).$$

Dado que

$$\cos(y)\cos(z) - \sin(y)\sin(z) = \cos(y+z) \ldots (3)$$
$$\cos(y)\sin(z) + \sin(y)\cos(z) = \sin(y+z) \ldots (4),$$

sustituimos (3) y (4) en (2), por lo que podemos expresar el producto (1) como

[11] Para profundizar más en el contexto de las ecuaciones diferenciales y el lugar que ocuparon entre Johann Bernoulli y Euler se recomienda consultar [Álvarez, C. y Dhombres, J. 2011, pp. 176-182]. En la misma referencia se puede estudiar el antecedente de la correspondencia entre Johann Bernoulli y Leibniz correspondiente a las ecuaciones diferenciales, y esto es importante ya que posteriormente diversos elementos del intercambio entre ellos repercutirían en Euler, cuando él ya tenía una comunicación cercana con Johann Bernoulli.

$$[\cos(z) + i\sin(z)][\cos(y) + i\sin(y)] = \cos(y + z) + i\sin(y + z).$$

De igual manera, $[\cos(z) - i\sin(z)][\cos(y) - i\sin(y)] = \cos(y + x) - i\sin(y + z)$.

Por lo tanto, $[\cos(z) \pm i\sin(z)][\cos(y) \pm i\sin(y)] = \cos(y + x) \pm i\sin(y + z)$.

En consecuencia, para §133, si los arcos son iguales, entonces

$$[\cos(z) \pm i\sin(z)]^2 = \cos(2z) \pm i\sin(2z),$$

y en general

$$[\cos(z) \pm i\sin(z)]^n = \cos(nz) \pm i\sin(nz).$$

Ahora bien, de esto podemos observar que

$$\cos(nz) = \frac{[\cos(z)+i\sin(z)]^n+[\cos(z)-i\sin(z)]^n}{2} \text{ y}$$

$$\sin(nz) = \frac{[\cos(z)+i\sin(z)]^n-[\cos(z)-i\sin(z)]^n}{2i}.$$

A continuación, en §134, Euler argumenta que si z es una cantidad (arco) infinitamente pequeña, entonces se tiene que $\sin(z) = z$ y $\cos(z) = 1$. Ahora, si se considera a n como un número infinitamente grande tal que nz resulte en una cantidad finita, es decir $nz = v$, entonces

$$\sin(z) = z = \frac{v}{n}.$$

Estos datos nos van a resultar de gran utilidad posteriormente.

Con esto se llega a §138. Se toma un arco z infinitamente pequeño y sea j un valor infinitamente grande tal que jz resulte en un valor finito v, así $jz = v$ y $z = \frac{v}{j}$, por lo que $\sin(z) = \frac{v}{j}$ y $\cos(z) = 1$. Entonces

$$\cos(v) = \cos(jz) = \frac{[\cos(z) + i\sin(z)]^j + [\cos(z) - i\sin(z)]^j}{2} = \frac{\left[1 + \frac{iv}{j}\right]^j + \left[1 - \frac{iv}{j}\right]^j}{2}$$

$$\sin(v) = \sin(jz) = \frac{[\cos(z) + i\sin(z)]^j - [\cos(z) - i\sin(z)]^j}{2i} = \frac{\left[1 + \frac{iv}{j}\right]^j - \left[1 - \frac{iv}{j}\right]^j}{2i}$$

Gracias a la construcción de la exponencial mediante series que aparece en el capítulo VII §125, sabemos que $e^x = \left[1 + \frac{x}{k}\right]^k$, para un número k infinitamente grande. Por lo tanto, si tomamos $x = iv, -x = -iv$ y $k = j$, obtenemos las expresiones polares para las funciones seno y coseno

$$\cos(v) = \frac{e^{iv} + e^{-iv}}{2}$$

$$\sin(v) = \frac{e^{iv} - e^{-iv}}{2i},$$

Además, las expresiones $e^{iv} = \cos(v) + i\sin(v)$ y $e^{-iv} = \cos(v) - i\sin(v)$.

Esto nos lleva al Tomo II §511. Se observa que las ecuaciones contienen exponentes del tipo imaginario, y Euler las clasifica en el “género” de trascendental. Comenta que es “bastante posible que una expresión que contiene exponentes imaginarios pueda dar un valor real definido.” Como ejemplo toma la siguiente ecuación

$$2y = x^i + x^{-i} \ldots ⑤$$

y resulta que la suma de cantidades de carácter imaginario genera un valor real. Además, dado que el logaritmo $\log(x) = v$ y que e es la base del logaritmo natural que resulta ser igual a 1, entonces tenemos que $x = e^v$. Se sustituye en ⑤ y tenemos

$$2y = e^{iv} + e^{-iv},$$

y para terminar resulta

$$y = \frac{e^{iv} + e^{-iv}}{2}.$$

Como se vio, en el Tomo I §138 Euler muestra que $\cos(v) = \frac{e^{iv}+e^{-iv}}{2}$. Por lo tanto, se tiene que $y = \cos(v) = \cos(\log(x))$. Si tomáramos un valor positivo para x, entonces la expresión $y = \cos(\log(x))$ nos dará el valor de la ordenada y. Como ejemplo se toma el valor $x = 2$, entonces $2y = 2^i + 2^{-i}$, por lo que

$$y = \cos(\log(2)) = \cos(0.6931471805599 \ldots).$$

Calculando el arco de $\log(2)$, observamos que éste equivale a $39°, 42', 51'', 52''', 9''''$, por lo que el coseno de dicho arco es igual a 0.76923890135408. Este valor corresponde a la abscisa $x = 2$. Aquí Euler remarca que las expresiones, como la anterior, las cuales involucran logaritmos y arcos circulares, se les puede denominar correctamente como trascendentes.

La correspondencia

Con lo expuesto en las dos secciones anteriores ahora podemos comprobar que Euler ya estaba trabajando en el tema de las raíces imaginarias por lo menos un año antes de que le comunicara por primera vez a Goldbach algunas reflexiones al respecto. Así, nos remontamos a la primera carta que trató este tema entre ellos, la carta 43, del 9 de diciembre de 1741. Para comodidad de la lectura enunciamos nuevamente el segmento de la carta de Euler a Goldbach:

> Recientemente encontré una paradoja curiosa, a saber, que el valor de esta expresión $\frac{2^{+\sqrt{-1}}+2^{-\sqrt{-1}}}{2}$ es aproximadamente igual a $\frac{10}{13}$, y esta fracción difiere de la verdad en solo una millonésima parte. El verdadero valor de esta expresión es el coseno del arco 0.693147180559, o bien el arco de $39°, 42', 51'', 52''', 9^{IV}$ de un círculo cuyo radio es $= 1$.

Sin el contexto del *Introductio* la expresión $\frac{2^{+\sqrt{-1}}+2^{-\sqrt{-1}}}{2}$ puede resultar confusa, pues en la correspondencia las primeras referencias a las raíces imaginarias se enmarcan en la discusión sobre la cuadratura de lúnulas[12] y esta fórmula no parece derivarse de ésto. Pero, gracias a lo expuesto anteriormente, podemos afirmar que Euler estaba desarrollando la relación entre las funciones exponenciales y las funciones trigonométricas dentro del campo de las raíces imaginarias, así como el estudio de curvas trascendentes. Para el 9 de diciembre de 1741 Euler ya tenía una comprensión profunda de este tema[13] y es posible argumentar que él llegó a la ecuación $\frac{2^{+\sqrt{-1}}+2^{-\sqrt{-1}}}{2}$ de la misma manera a la exhibida previamente.

La respuesta de Goldbach llegaría el 13 de febrero de 1742, en la carta 45

[12] Véase *Leonhard Euler und Christian Goldbach. Briefwechsel 1729-1764*, pp. 39-40.

[13] Ya se mencionó la correspondencia entre Euler y Johann I Bernoulli, específicamente la carta del 18 de octubre de 1740, además, véase *Eneström* E863c3.

> Observando lo que su excelencia me comunicó, que $\frac{2^{+\sqrt{-1}}+2^{-\sqrt{-1}}}{2}$ es aproximadamente igual a $\frac{10}{13}$, me vino a la mente que cuando se quisiese hacer $2^{p\sqrt{-1}} + 2^{-p\sqrt{-1}} = 0$, entonces p tendría que ser menor que 3 y mayor que 2. Reconozco que estos límites están dados grosso modo, pero no tuve la curiosidad de determinarlos más de cerca.

A partir de la observación planteada por Euler, que $\frac{2^{+\sqrt{-1}}+2^{-\sqrt{-1}}}{2} \approx \frac{10}{13}$, Goldbach deriva la ecuación $2^{p\sqrt{-1}} + 2^{-p\sqrt{-1}} = 0$ y muestra interés por encontrar el valor de p, el cual se encuentra acotado por 2 y 3, aunque no lo llega a determinar de manera exacta.

Goldbach escribió posteriormente dos cartas con especulaciones más que nada numéricas, que parecen estar al margen de lo que Euler le enunció en la primera carta, que es un resultado en términos de potencias de carácter imaginario y enfatiza su equivalencia con elementos de la trigonométrica, Euler dice que "el verdadero valor de esta expresión es el coseno del arco 0.693147180559, o bien el arco de $39°, 42', 51'', 52''', 9^{IV}$ de un círculo cuyo radio es $= 1$". Sin duda, el lado trigonométrico de la expresión de tipo imaginario es su verdadero interés en la carta —se pueden observar las ideas que desarrolló en su *Introductio*—. Otra evidencia que tenemos para argumentar de esta manera es lo que escribió al margen de la carta 45 de Goldbach. Euler escribió lo siguiente:

> En general, $2^{p\sqrt{-1}} + 2^{-p\sqrt{-1}} = 2\cos(p\log(2))$. Por lo tanto, si $2^{p\sqrt{-1}} + 2^{-p\sqrt{-1}} = 0$, entonces $p\log(2) = (2n+1)\frac{\pi}{2}$, donde $\frac{\pi}{2} = 1.5707963267$ .... Si $n = 0$, entonces $p\log(2) = \frac{\pi}{2}$, por lo que $p = \frac{\frac{\pi}{2}}{\log(2)} = \frac{1.5707963267\ldots}{0.6931471805\ldots} = \frac{34}{15} = 2.26618021$ ....

Aquí podemos encontrar el valor exacto de p, mismo que no fue determinado por Goldbach, pero aún más importante es la aparición de la expresión $2^{p\sqrt{-1}} + 2^{-p\sqrt{-1}} = 2\cos(p\log(2))$. Ésta nos remite nuevamente a lo desarrollado en el *Introductio* y no es la última vez que este tipo de expresión estará presente.

Para el 6 de marzo de 1742 Euler respondería lo siguiente en la carta 47:

> La curiosidad que su excelencia tuvo para investigar si la fórmula $2^{+p\sqrt{-1}} + 2^{-p\sqrt{-1}}$ pudiese ser igual a cero me dio motivos para notar que esto podría pasar en una infinidad de maneras: el primer valor para p, como observó su eminencia, se encuentra entre 2 y 3, a saber $p = 2.26618021$, pero el verdadero valor es $p = \frac{\pi}{2l2}$, donde $\pi = 3.14159265$ y $l2 = 1 - \frac{1}{2} + \frac{1}{3} - \frac{1}{4} +$ etc. $= 0.6931471805$. Todos los siguientes valores para p surgen de éste al multiplicarlo por 3, 5, 7, 9, etc.

Gracias a la nota de Euler en la carta 45, así como su énfasis en que "los siguientes valores para p surgen de éste al multiplicarlo por 3, 5, 7, 9, etc.", nos otorga otra prueba del interés trigonométrico que Euler tenía, además, estas dos referencias muestran que estaba pensando en la periodicidad de la función exponencial, de la cual Goldbach no se había percatado, es decir, parece que Goldbach no se enganchaba en el mismo contexto en el que Euler trataba de meterlo. Mientras que Euler quiere discutir de manera trigonométrica, Goldbach, al no entender el camino que éste primero está tomando –y quiere tomar–, recurre constantemente a argumentar de manera numérica. La incompatibilidad en cómo ver este problema será permanente durante la correspondencia que siguió.

En la carta 49, del 12 de abril de 1742, Goldbach respondería como sigue:

> Con motivo de lo que su excelencia escribió acerca de la fórmula $2^{p\sqrt{-1}} + 2^{-p\sqrt{-1}} = 0$, observé que cuando se coloca la variable n, entonces $2^{np\sqrt{-1}} + 2^{-np\sqrt{-1}} = 2$ siempre que n sea un número parmente par, y por otro lado será $= -2$ siempre que n sea un número impar. Y cuando n es un número entero, pero q es un número racional o irracional arbitrario, siempre sucederá que
>
> $$2^{(4n+q)p\sqrt{-1}} + 2^{-(4n+q)p\sqrt{-1}} = 2^{qp\sqrt{-1}} + 2^{-qp\sqrt{-1}}.$$

En mi opinión también es notable que cuando p es determinado por la ecuación $2^{p\sqrt{-1}} + 2^{-p\sqrt{-1}} = 3$, entonces $2^{xp\sqrt{-1}} + 2^{-xp\sqrt{-1}}$ será igual a

$$\left[\frac{(1+\sqrt{5})^{2x+1} - (-1+\sqrt{5})^{2x+1}}{2^{2x+1}}\right] - \left[\frac{\left(1+\sqrt{5}\right)^{2x-1} - \left(-1+\sqrt{5}\right)^{2x-1}}{2^{2x-1}}\right],$$

siempre que x sea un número entero.

Después de haber leído nuevamente esta observación, encuentro que ésta no es de importancia alguna, solo tomando $a = \frac{3\pm\sqrt{5}}{2}$, el término general es $a^x + a^{-x}$.

Como podemos observar, Goldbach muestra interés por encontrar soluciones para distintos tipos de ecuaciones que comparten estructura con la planteada originalmente por Euler. Hace notar lo siguiente: la ecuación $2^{np\sqrt{-1}} + 2^{-np\sqrt{-1}} = 2$, siempre que n sea el producto de dos números pares; $2^{np\sqrt{-1}} + 2^{-np\sqrt{-1}} = -2$, siempre que n sea el producto de números impares; la igualdad $2^{qp\sqrt{-1}} + 2^{-qp\sqrt{-1}} = 2^{(4n+q)p\sqrt{-1}} + 2^{-(4n+q)p\sqrt{-1}}$ se cumple si q es un número racional o irracional cualquiera; y finalmente, si p queda determinado por $2^{p\sqrt{-1}} + 2^{-p\sqrt{-1}} = 3$, entonces se cumple la igualdad

$$2^{xp\sqrt{-1}} + 2^{-xp\sqrt{-1}} = \left[\frac{(1+\sqrt{5})^{2x+1} - (-1+\sqrt{5})^{2x+1}}{2^{2x+1}}\right] - \left[\frac{\left(1+\sqrt{5}\right)^{2x-1} - \left(-1+\sqrt{5}\right)^{2x-1}}{2^{2x-1}}\right].$$

Éstas dos últimas serán corregidas por Euler en su siguiente carta.

Para el 8 de mayo de 1742, en la carta 50, Euler haría las siguientes observaciones:

En general cuando $a^{p\sqrt{-1}} + a^{-p\sqrt{-1}} = b$, se tiene que

$$a^{xp\sqrt{-1}} + a^{-xp\sqrt{-1}} = \left(\frac{b+\sqrt{(bb-4)}}{2}\right)^x + \left(\frac{b-\sqrt{(bb-4)}}{2}\right)^x,$$

y consecuentemente, cuando $2^{p\sqrt{-1}} + 2^{-p\sqrt{-1}} = 3$, se convierte en

$$2^{xp\sqrt{-1}} + 2^{-xp\sqrt{-1}} = \left(\frac{3+\sqrt{5}}{2}\right)^x + \left(\frac{3-\sqrt{5}}{2}\right)^x = \left(\frac{\sqrt{5}+1}{2}\right)^{2x} + \left(\frac{\sqrt{5}-1}{2}\right)^{2x}.$$

Por lo demás, las observaciones de su excelencia coinciden en mayor parte con mi teorema general, que $a^{+p\sqrt{-1}} + a^{-p\sqrt{-1}} = 2\cos(pla)$, solo que $2^{(4n+q)p\sqrt{-1}} + 2^{-(4n+q)p\sqrt{-1}}$ no es igual a $2^{qp\sqrt{-1}} + 2^{-qp\sqrt{-1}}$, a menos que $(2n+q)pl2$ o $2npl2$ sea igual a $m\pi$, donde $1:\pi$ denota el radio del diámetro de la circunferencia.

Como habíamos comentado anteriormente, Euler señala ciertos errores que Goldbach cometió al tratar de encontrar posibles soluciones a las ecuaciones arriba mencionadas. Euler muestra que en general, cuando se tiene una expresión del tipo $a^{p\sqrt{-1}} + a^{-p\sqrt{-1}} = b$, entonces $a^{xp\sqrt{-1}} + a^{-xp\sqrt{-1}} = \left(\frac{b+\sqrt{(bb-4)}}{2}\right)^x + \left(\frac{b-\sqrt{(bb-4)}}{2}\right)^x$. A continuación, nosotros demostraremos este hecho

***Afirmación* 3.1** Sea $a^{p\sqrt{-1}} + a^{-p\sqrt{-1}} = b$, entonces tenemos que $a^{xp\sqrt{-1}} + a^{-xp\sqrt{-1}} = \left(\frac{b+\sqrt{(bb-4)}}{2}\right)^x + \left(\frac{b-\sqrt{(bb-4)}}{2}\right)^x$.

Demostración: Sean $z = a^{p\sqrt{-1}}$ y $z^{-1} = a^{-p\sqrt{-1}}$. Si consideramos a z y z^{-1} como las raíces de una ecuación cuadrática, entonces

$$(x-z)(x-z^{-1}) = 0$$

$$\Rightarrow x^2 - (z + z^{-1})x + 1 = 0$$

Si sustituimos $b = z + z^{-1}$, entonces tenemos

$$x^2 - bx + 1 = 0$$

Entonces, gracias a la fórmula general, obtenemos que

$$z = \frac{b + \sqrt{b^2 - 4}}{2}$$

$$z^{-1} = \frac{b - \sqrt{b^2 - 4}}{2}$$

Por lo tanto, $z + z^{-1} = \frac{b+\sqrt{b^2-4}}{2} + \frac{b-\sqrt{b^2-4}}{2} = \frac{b+\sqrt{b^2-4}+b-\sqrt{b^2-4}}{2} = \frac{2b}{2} = b$.

Entonces

$$z^x = a^{xp\sqrt{-1}} = \left(\frac{b + \sqrt{b^2 - 4}}{2}\right)^x$$

$$z^{-x} = a^{-xp\sqrt{-1}} = \left(\frac{b - \sqrt{b^2 - 4}}{2}\right)^x$$

Por lo tanto, $a^{xp\sqrt{-1}} + a^{-xp\sqrt{-1}} = \left(\frac{b+\sqrt{b^2-4}}{2}\right)^x + \left(\frac{b-\sqrt{b^2-4}}{2}\right)^x$, obteniendo lo buscado. ■

Para el caso particular de Goldbach, si nuestra expresión es $2^{p\sqrt{-1}} + 2^{-p\sqrt{-1}} = 3$, entonces $2^{xp\sqrt{-1}} + 2^{-xp\sqrt{-1}} = \left(\frac{3+\sqrt{5}}{2}\right)^x + \left(\frac{3-\sqrt{5}}{2}\right)^x$. Por otro lado,

$$\left(\frac{3 + \sqrt{5}}{2}\right)^x = \left(\frac{5 + 2\sqrt{5} + 1}{4}\right)^x = \left(\left(\frac{\sqrt{5} + 1}{2}\right)^2\right)^x = \left(\frac{\sqrt{5} + 1}{2}\right)^{2x}$$

De manera análoga

$$\left(\frac{3 - \sqrt{5}}{2}\right)^x = \left(\frac{5 - 2\sqrt{5} + 1}{4}\right)^x = \left(\left(\frac{\sqrt{5} - 1}{2}\right)^2\right)^x = \left(\frac{\sqrt{5} - 1}{2}\right)^{2x}$$

Por lo tanto, $2^{xp\sqrt{-1}} + 2^{-xp\sqrt{-1}} = \left(\frac{3+\sqrt{5}}{2}\right)^x + \left(\frac{3-\sqrt{5}}{2}\right)^x = \left(\frac{\sqrt{5}+1}{2}\right)^{2x} + \left(\frac{\sqrt{5}-1}{2}\right)^{2x}$.

Ahora bien, al señalar el siguiente error cometido por Goldbach, Euler menciona un teorema general, el cual muestra que $a^{p\sqrt{-1}} + a^{-p\sqrt{-1}} = 2\cos(p \log(a))$, la igualdad que plantea, que

$$2^{qp\sqrt{-1}} + 2^{-qp\sqrt{-1}} = 2^{(4n+q)p\sqrt{-1}} + 2^{-(4n+q)p\sqrt{-1}},$$

se cumple sólo si $(2n + q)p \log(2)$ o $2np \log(2)$ es igual a $m\pi$.

Este resultado extiende lo planteado implícitamente en la carta 47 y de esta manera se retoma la discusión en el ámbito trigonométrico que Euler busca desarrollar en la correspondencia.

Con esto llegamos a la carta 51 (la de la conjetura), del 7 de junio de 1742. Goldbach comenta que:

> Hasta donde recuerdo, en mi última carta imaginé la fórmula $2^{xp\sqrt{-1}} + 2^{-xp\sqrt{-1}}$, asumiendo $2^{p\sqrt{-1}} + 2^{-p\sqrt{-1}} = 0$, como las ordenadas de una curva serpentiforme, cuyas abscisas son x y cuyo eje es intersectado siempre que la fórmula sea $= 0$, de modo que cuando la misma fórmula es $= 2$,

> se obtiene la máxima ordenada abajo o arriba, y por consiguiente otras innumerables ordenadas que deben de ser iguales entre ellas. Sin embargo, se deslizó un error en mi expresión de aquel momento, el cual me marcó, su excelencia, con razón y que se puede corregir fácilmente declarando que, cuando q es un número cualquiera y estableciendo $2^{p\sqrt{-1}} + 2^{-p\sqrt{-1}} = 0$, entonces, asumiendo n como un número entero cualquiera, se tiene
>
> $$2^{(8n-4-q)p\sqrt{-1}} + 2^{-(8n-4-q)p\sqrt{-1}} = 2^{qp\sqrt{-1}} + 2^{-qp\sqrt{-1}}.$$

Goldbach no se equivoca al considerar que la gráfica de $2^{xp\sqrt{-1}} + 2^{-xp\sqrt{-1}}$ es una curva 'serpentiforme', pues como hemos comentado, esta expresión está estrechamente ligada a la función coseno. Además, si se considera $2^{xp\sqrt{-1}} + 2^{-xp\sqrt{-1}} = 2$, se obtiene el máximo y el mínimo, pues el rango de esta función se encuentra en el intervalo $[-2, 2]$, y por lo tanto, tenemos una infinidad de máximos y mínimos, ya que estamos trabajando con una expresión de naturaleza periódica, como lo notó Euler anteriormente.

Por último, Goldbach señala, al tratar de corregir su error, que si q es un número cualquiera y se fija $2^{p\sqrt{-1}} + 2^{-p\sqrt{-1}} = 0$, entonces, si se considera n como un entero cualquiera obtenemos

$$2^{(8n-4-q)p\sqrt{-1}} + 2^{-(8n-4-q)p\sqrt{-1}} = 2^{qp\sqrt{-1}} + 2^{-qp\sqrt{-1}},$$

pero desafortunadamente, aquí volvería a cometer un error, el cual sería corregido, nuevamente, por Euler en su siguiente carta.

Como señala en el margen inferior de la carta 51, Euler desarrolla su respuesta. Primero recuerda que si $2^{p\sqrt{-1}} + 2^{-p\sqrt{-1}} = 0$, entonces $p\log(2) = \frac{(2n+1)\pi}{2}$, o bien, $p = \frac{(2n+1)\pi}{2\log(2)}$. Después sustituye el valor de p en $2^{xp\sqrt{-1}} + 2^{-xp\sqrt{-1}} = 2\cos(xp\log(2))$, para los casos $x = q$ y $x = r$, obteniendo así lo siguiente

$$2^{qp\sqrt{-1}} + 2^{-qp\sqrt{-1}} = 2\cos\left(\frac{(2n+1)q\pi}{2}\right)$$

$$2^{rp\sqrt{-1}} + 2^{-rp\sqrt{-1}} = 2\cos\left(\frac{(2n+1)r\pi}{2}\right)$$

Estas dos expresiones son iguales si y sólo si $\cos\left(\frac{(2n+1)q\pi}{2}\right) = \cos\left(\frac{(2n+1)r\pi}{2}\right)$, y a la vez para que esta igualdad se cumpla tiene que suceder que $\frac{(2n+1)q\pi}{2} = \frac{(2n+1)r\pi}{2}$, la cual depende del periodo.

Ahora bien, consideremos la siguiente identidad

$$\cos(s) = \cos(2m\pi \pm s) \ldots ⑥$$

Si $s = \frac{(2n+1)q\pi}{2}$, dado que $\frac{(2n+1)q\pi}{2} = \frac{(2n+1)r\pi}{2}$, por transitividad tenemos que $s = \frac{(2n+1)r\pi}{2}$. Sustituyendo $s = \frac{(2n+1)q\pi}{2}$ del lado izquierdo y $s = \frac{(2n+1)r\pi}{2}$ del lado derecho en ⑥ obtenemos

$$\cos\left(\frac{(2n+1)q\pi}{2}\right) = \cos\left(2m\pi \pm \frac{(2n+1)r\pi}{2}\right)$$

La igualdad se cumple si y solo si $\frac{(2n+1)q\pi}{2} = 2m\pi \pm \frac{(2n+1)r\pi}{2}$. Por lo tanto, tenemos que $\frac{(2n+1)q\pi}{2} \mp \frac{(2n+1)r\pi}{2} = 2m\pi$, por lo que $(2n+1)q\pi \mp (2n+1)r\pi = 4m\pi$. De manera que $q \mp r = \frac{4m}{2n+1}$.

Así, llegamos a la última carta en este intercambio. En la carta 52, del 30 de junio de 1742, Euler respondería precisamente con lo desarrollado como nota al margen en la carta 51

> En general $2^{p\sqrt{-1}}+2^{-p\sqrt{-1}}=2\cos(pl2)$. Así que cuando $2^{p\sqrt{-1}}+2^{-p\sqrt{-1}}=0$, $pl2$ tiene que ser igual a tal arco del círculo cuyo coseno sea $=0$. Pero esta propiedad la tienen todos los arcos contenidos en ésta fórmula $\frac{(2n+1)\pi}{2}$, y por consiguiente $p=\frac{(2n+1)\pi}{2l2}$. Por lo tanto, asumiendo que $p=\frac{(2n+1)\pi}{2l2}$ o que $2^{p\sqrt{-1}}+2^{-p\sqrt{-1}}=0$, tenemos que $2^{xp\sqrt{-1}}+2^{-xp\sqrt{-1}}=2\cos(xpl2)=2\cos\left(\frac{(2n+1)x\pi}{2}\right)$. Entonces, si se quiere que $2^{qp\sqrt{-1}}+2^{-qp\sqrt{-1}}=2^{rp\sqrt{-1}}+2^{-rp\sqrt{-1}}$, es necesario que $\cos\left(\frac{(2n+1)q\pi}{2}\right)=\cos\left(\frac{(2n+1)r\pi}{2}\right)$. Pero los cosenos de dos arcos distintos son iguales entre sí, si la suma o la diferencia de los arcos es igual a un múltiplo de la circunferencia 2π. Por lo tanto, $\frac{(2n+1)q\pi}{2}\pm\frac{(2n+1)r\pi}{2}=2m\pi$, y así $q\pm r=\frac{4m}{2n+1}$, por lo que $2^{\left(\frac{4m}{2n+1}-q\right)p\sqrt{-1}}+2^{-\left(\frac{4m}{2n+1}-q\right)p\sqrt{-1}}=2^{qp\sqrt{-1}}+2^{-qp\sqrt{-1}}$, en lo cual está contenido todo aquello que su excelencia me escribió sobre esta materia.

Sustituyendo $\frac{4m}{2n+1}$ con $q\pm r$ en la expresión $2^{\left(\frac{4m}{2n+1}-q\right)p\sqrt{-1}}+2^{-\left(\frac{4m}{2n+1}-q\right)p\sqrt{-1}}$, obtendríamos los siguientes dos casos

Caso 1 Si tenemos $q+r$, entonces

$$\begin{aligned}2^{\left(\frac{4m}{2n+1}-q\right)p\sqrt{-1}}+2^{-\left(\frac{4m}{2n+1}-q\right)p\sqrt{-1}}&=2^{(q+r-q)p\sqrt{-1}}+2^{-(q+r-q)p\sqrt{-1}}\\&=2^{rp\sqrt{-1}}+2^{-rp\sqrt{-1}}\end{aligned}$$

Caso 2 Si tenemos $q-r$, entonces

$$\begin{aligned}2^{\left(\frac{4m}{2n+1}-q\right)p\sqrt{-1}}+2^{-\left(\frac{4m}{2n+1}-q\right)p\sqrt{-1}}&=2^{(q-r-q)p\sqrt{-1}}+2^{-(q-r-q)p\sqrt{-1}}\\&=2^{-rp\sqrt{-1}}+2^{-(-r)p\sqrt{-1}}\\&=2^{rp\sqrt{-1}}+2^{-rp\sqrt{-1}}\end{aligned}$$

Por lo que tendríamos que $2^{qp\sqrt{-1}}+2^{-qp\sqrt{-1}}=2^{rp\sqrt{-1}}+2^{-rp\sqrt{-1}}$.

Como podemos observar, Euler regresa la discusión al dominio trigonométrico, haciendo hincapié nuevamente en las expresiones $2^{p\sqrt{-1}}+2^{-p\sqrt{-1}}=2\cos(pl2)$ y $2^{xp\sqrt{-1}}+2^{-xp\sqrt{-1}}=2\cos(xpl2)$, pero da por terminada la correspondencia de este tema de manera concluyente.

A manera de resumen, se percibe que este pasaje se puede considerar en la categoría de lo que ahora entendemos como números imaginarios, pero Goldbach no lo pudo comprender en su momento la manera como Euler se lo presentaba, es más, da la impresión de que Euler quería dirigir la discusión en un sentido de las representaciones polares y exponenciales de las raíces imaginarias, pero Goldbach una y otra vez lo interpreta desde un perfil de operaciones algebraicas elementales como cálculo de raíces, representaciones gráficas y cálculos numéricos. Finalmente, Euler da por terminado este tema en la correspondencia y siguen con los otros en que sí compartían puntos de vista.

Pero no podemos terminar el análisis de este pasaje sin considerar que Euler en estos años trabajaba la gestación de la teoría de los números imaginarios, entonces sería injusto juzgar a Goldbach por no haberse identificado con él en este tema, consideremos que estos temas aún no eran conocidos entre la comunidad y por lo tanto no era fácil meterse en el contexto de lo que estaba pensando Euler respecto de las raíces imaginarias.

IV. Números de la forma $4mn - m - n$

La discusión acerca de los números de la forma $4mn - m - n$ tiene una marcada importancia en la carta 51. A diferencia de los otros temas que encontramos en ella, que generalmente se examinan en un párrafo, éste se encuentra dividido en tres secciones. La relevancia de este tópico no se limitó a esta misiva, en la totalidad de la correspondencia se encuentra presente en 36 cartas, y por esta razón resulta ser uno de los temas más extensos en el intercambio entre Euler y Goldbach. A continuación, presentamos los pasajes de la carta 51 que corresponden a este tema:

> Su excelencia encontró que todos los números que no pueden ser expresados como $4mn - m - n$, están comprendidos en la formula $v^2 + v + u^2$. Y creo que todo $4mn - m - n$ se puede llevar a la formula $y^2 + y - x^2$, de modo que cada número dado es igual a $p^2 + p \pm q^2$, donde p y q denotan números enteros, o bien alguna de las dos letras puede significar 0; de donde se observa que cualquier número está compuesto por un doble triangular $\pm$ un número cuadrado; como además todo número es igual a la formula $u^2 + v^2 + v + y^2 + y - x^2$, cuando se toma
>
> $$u = \frac{z^2+z}{4} + 1, \quad x = \frac{z^2+z}{4} - 1, \quad u^2 - x^2 = z^2 + z$$
>
> se sigue que el medio de un número dado se vuelve $\frac{n}{2} = \frac{v^2+v+y^2+y+z^2+z}{2}$, es decir, tres triangulares.
>
> Que en la formula poligonal $\frac{(p-2)x^2-(p-4)x}{2}$, cuando ésta se le iguala a $4mn - m - n$, p no pueda ser 5 ± 2 ni 5 ± 1, sino que se excluyen todos los trigonales, tetragonales, hexagonales y heptagonales, se sigue del mismo principio.
>
> […]
>
> Si se toman m y p como números enteros positivos, la expresión $\frac{p+2\pm\sqrt{4p-m+3}}{m}$ no puede dar un número entero.

El intercambio para este tema registra su inicio en la carta 39, del 19 de agosto de 1741, un año antes de la famosa carta 51. En ésta, Goldbach plantea la pregunta que se vincula con proposiciones sobre números que no pueden ser cuadrados:

> Qué opina, su excelencia, de proposiciones tales como que $(3m + 2)n^2 + 3$ nunca puede ser un número cuadrado, para m y n números enteros positivos cualesquiera.

Esta pregunta no es fortuita, dado que Goldbach ya había trabajado este tipo de proposiciones. En su primer artículo matemático *Excerptae e litteris C. G. ad *** Regiomonte datis.*[14] publicado en 1717 observa que la diferencia del cuadrado de un número cualquiera y 2 nunca es divisible entre 3, en otras palabras[15], $x^2 \not\equiv 2\ (mod\ 3)$. Más aún, en otro artículo *Criteria quaedam aequationum quarum nulla radix rationalis est*,[16] publicado en 1738, Goldbach postula el siguiente teorema:

***Teorema* 4.1** Ningún número de la forma $3p + 2$ puede ser un cuadrado.

La respuesta a dicha pregunta llegaría con la carta 40, del 9 de septiembre de 1741. En ésta, Euler demuestra la proposición planteada por Goldbach y mencionó por primera vez a los números de la forma $4mn - m - n$ y similares:

> Su excelencia, el teorema, que ningún número de la forma $(3m + 2)n^2 + 3$ no puede ser cuadrado, es muy bueno, y puedo demostrar la veracidad del mismo de la siguiente manera: O bien n es divisib[le] entre 3 o bien no lo es. En el primer caso n^2 es divisib[le] entre 9 y la expresión $(3m + 2)n^2 + 3$ se vuelve una de la forma $9p + 3$, la cual, como ya es sabido, no puede ser un

[14] *Acta Eruditorum, Supplementa*, pp. 471-472.

[15] Esta notación no es de la época de Goldbach, la usamos para que la lectura de este trabajo sea más cómoda.

[16] *Commentarii Academiae Scientiarum Imperialis Petropolitanae*, pp. 98-102.

> cuadrado. En el otro caso, cuando n no es divisib[le] entre 3, entonces n^2 es un número de la forma $3p+1$, y $(3m+2)n^2+3$ se convierte a la forma $9mp+3m+6p+5$, que es $3q+2$, la cual, también es sabido, nunca puede ser un cuadrado. Hace largo tiempo encontré también teoremas similares, como que $4mn-m-1$ de ninguna manera puede ser un cuadrado. De la misma manera, $4mn-m-n$ tampoco puede ser un cuadrado, afirmando que m y n son números enteros positivos.

Hay que observar que las afirmaciones de Euler no quedan demostradas formalmente, es decir, que las expresiones $9p+3$ y $3q+2$ no pueden ser un cuadrado. Esto se puede verificar fácilmente mediante las siguientes observaciones:

1. En el primer caso tenemos que los números mod 9 son de la forma $9k+s$, donde $s=0,1,2,\dots,8$. Al elevar a cada uno de estos números al cuadrado, obtenemos únicamente las siguientes expresiones: $9k'$; $9k'+1$; $9k'+4$; $9k'+7$. Por lo tanto, los números de la forma $9k+3$ nunca son un cuadrado.
2. En el segundo caso los números mod 3 son de la forma $3k+t$, donde $t=0,1,2$. Elevando al cuadrado a cada uno de éstos obtenemos únicamente lo siguiente: $3k'$; $3k'+1$. Por lo tanto, los números de la forma $3k+2$ nunca son un cuadrado.

Con la carta 45, del 13 de febrero de 1742, llegaría la respuesta de Goldbach, la cual es bastante positiva respecto a los teoremas planteados por Euler:

> El teorema, que $4mn-m-1$ no puede ser un cuadrado, me agrada bastante, y aunque de momento no lo pueda demostrar, he podido obtener estas consecuencias del mismo. Que no solo, como su excelencia ya había observado, $4mn-m-n$ tampoco puede ser cuadrado, sino en general la expresión $4mn-m-n^a$, donde a es un entero positivo cualquiera, nunca puede dar un cuadrado.

A pesar del pequeño inconveniente de no poder demostrar la proposición, Goldbach va más allá y generaliza el resultado de Euler. Con esto en mente, Euler escribiría el 6 de marzo de 1742, en la carta 47, el modo en que obtuvo sus teoremas:

> Que $4mn-m-1$ ó $4mn-m-n$ nunca pueden ser un cuadrado, no lo he podido demostrar rigurosamente hasta ahora, sino que los deduje de un teorema de *Fermat*, donde se afirma que la suma de dos cuadrados $aa+bb$ nunca es divisible por un número de la forma $4n-1$. Entonces si este teorema es verdadero, pasa que $aa+1\neq(4n-1)m$, donde yo, su excelencia, utilizo el signo $\neq$ para denotar una ecuación imposible. Por lo tanto, $aa\neq 4mn-m-1$. Más aún, es imposible que $\frac{aa+1}{4n-1}$ sea un número entero, o es $\frac{aa+1}{4n-1}\neq i$. Se sigue también que $\frac{aa+1}{4n-1}+1$ o $\frac{aa+4n}{4n-1}$ o $\frac{bb+4n}{4n-1}\neq i$. De igual manera $\frac{bb+4n}{4n-1}+n$ o $\frac{bb+4nn}{4n-1}$ o $\frac{cc+nn}{4n-1}$ no pueden ser número enteros. Y si se sigue de esta manera que $\frac{aa+n^\alpha}{4n-1}\neq m$ y también $aa\neq 4mn-m-n^\alpha$, la cual es la consecuencia, su excelencia, obtenida de estos teoremas. La verdad de esto depende de la veracidad del teorema, que una suma de dos cuadrados $aa+bb$ de ninguna manera es divisible entre $4n-1$ (si aa y bb no son por si solos divisibles por $4n-1$).

El resultado de Fermat al cual hace referencia Euler es fundamental para desarrollar toda la teoría que se desarrollará en este capítulo, el cual usaremos nuevamente más adelante. A continuación, probaremos este teorema que menciona.

***Teorema* 4.2** (*de Fermat*) Dados dos enteros a y b primos relativos entre sí, la suma a^2+b^2 no es divisible por $4n-1$.

Demostración: Sean a y b enteros, los cuales no son divididos por un número primo de la forma $4n-1$. Por **2.10** y **2.11** se tiene que $4n-1$ divide a $a^{4n-2}-b^{4n-2}$.

Por otro lado, si suponemos que $a^{4n-2}+b^{4n-2}$ es divisible por $4n-1$, entonces tendríamos que $4n-1$ divide a $(a^{4n-2}-b^{4n-2})+(a^{4n-2}+b^{4n-2})$, es decir, dividiría a $2a^{4n-2}$, y si divide a este producto que es un número par, pero como $4n-1$ es impar, entonces $4n-1$ tiene que dividir a

a^{4n-2}, por lo tanto dividiría a a, lo cual es una contradicción, pues por hipótesis $4n-1$ no divide a a.

Por lo tanto, $4n-1$ no divide a $a^{4n-2}+b^{4n-2}$.

Ahora bien, dado que $4n-2=2(2n-1)$, podemos reescribir $a^{4n-2}-b^{4n-2}$ como $(a^2)^{2n-1}-(b^2)^{2n-1}$. Entonces $(a^2)^{2n-1}+(b^2)^{2n-1}$ es igual a

$$(a^2+b^2)((a^2)^{2n-2}-(a^2)^{2n-3}b^2+\cdots-a^2(b^2)^{2n-3}+(b^2)^{2n-2})$$

Dado que $4n-1$ no divide a $a^{4n-2}+b^{4n-2}$, entonces tampoco divide a ninguno de los factores a^2+b^2 ni a $(a^2)^{2n-2}-(a^2)^{2n-3}b^2+\cdots-a^2(b^2)^{2n-3}+(b^2)^{2n-2}$.

Por lo tanto, a^2+b^2 nunca puede ser dividido por ningún primo de la forma $4n-1$, a menos que a y b sean divisibles por $4n-1$. ■

Gracias a este teorema Euler no sólo dedujo que $4mn-m-1$ y $4mn-m-n$ no pueden ser cuadrados, sino que logra deducir el resultado general planteado por Goldbach. A continuación, probaremos las afirmaciones de la carta:

Demostración: Por **4.2** tenemos que $\frac{a^2+b^2}{4n-1}$ no es un número entero. En particular, si tomamos a $b=1$, tenemos que $\frac{a^2+1}{4n-1}$ tampoco será un entero. Por lo tanto, $\frac{a^2+1}{4n-1}+1$ tampoco lo será.

De la última expresión $\frac{a^2+1}{4n-1}+1=\frac{a^2+1}{4n-1}+\frac{4n-1}{4n-1}=\frac{a^2+4n}{4n-1}$. Entonces $\frac{a^2+4n}{4n-1}$ no es un entero y, en consecuencia, $\frac{b^2+4n}{4n-1}$ tampoco lo será, así como no lo será $\frac{b^2+4n}{4n-1}+n$.

Por otro lado, al sumar lo anterior se tiene que $\frac{b^2+4n^2}{4n-1}$ no es un entero, pues Euler indica que la igualdad $\frac{b^2+4n^2}{4n-1}=\frac{b^2+(2n)^2}{4n-1}$, donde la expresión del lado derecho no puede ser entero, por la hipótesis de que $\frac{c^2+n^2}{4n-1}$ no es un entero. Esta clase de expresión de la suma de dos cuadrados la usará Euler posteriormente.

Por último, consideremos a $\frac{a^2+n^\alpha}{4n-1}$. Si $\alpha=2k$, entonces $\frac{a^2+n^{2k}}{4n-1}=\frac{a^2+(n^k)^2}{4n-1}$, por lo que $\frac{a^2+n^\alpha}{4n-1}$ no es un número entero.

Ahora bien, consideremos $\frac{a^2+(2n^{k+1})^2}{4n-1}$, que por hipótesis no es un entero. Escogemos esta expresión de esta forma ya que nos ayudará a mostrar qué sucede con el caso para $\alpha=2k+1$. Observemos lo siguiente:

$$\begin{aligned}\frac{a^2+(2n^{k+1})^2}{4n-1}&=\frac{a^2+4n^{2k+2}}{4n-1}\\&=\frac{a^2+4n^{2k+2}+n^{2k+1}-n^{2k+1}}{4n-1}\\&=\frac{a^2+n^{2k+1}}{4n-1}+\frac{4n^{2k+2}-n^{2k+1}}{4n-1}\\&=\frac{a^2+n^{2k+1}}{4n-1}+\frac{n^{2k+1}(4n-1)}{4n-1}\\&=\frac{a^2+n^{2k+1}}{4n-1}+n^{2k+1}\end{aligned}$$

Dado que n^{2k+1} es un entero, entonces tendremos que $\frac{a^2+n^{2k+1}}{4n-1}$ no es un entero, por lo tanto, si $\alpha=2k+1$, entonces $\frac{a^2+n^\alpha}{4n-1}$ no será un número entero.

Por lo tanto, $\frac{a^2+n^\alpha}{4n-1}$ no es un número entero, para todo entero α no negativo. ■

Con base en la misma carta desarrolla resultados correspondientes a lo que hoy conocemos como el *pequeño teorema de Fermat*. A partir de éstos, enuncia un teorema y corolarios que se vinculan con los divisores primos de la suma de dos cuadrados.

Ahora abriremos un paréntesis para comentar el artículo del estudiante Ph. Bédos titulado *Question 248 (Goldbach)*[17] de 1852. No sabemos mucho acerca de esta persona, pero la idea que desarrolló en este trabajo es algo que Goldbach intentó resolver y se verá más adelante en la correspondencia. Bédos quiere demostrar, sin usar el *teorema de Fermat*, que $4mn-m-n$ no es un cuadrado. El artículo comienza precisamente con una prueba de que $4mn-m-1$ no es un cuadrado. A continuación, presentamos la demostración de Bédos y queremos señalar que lo haremos a pesar de que detectamos inconsistencias en su exposición, pero la presentamos para completar el cuadro histórico.

Demostración: Sean $m,n\in\mathbb{Z}^+$. Supongamos que $4mn-m-1=a^2$. Si disminuyéramos m y n mediante m'' y n'' respectivamente, tendríamos lo siguiente:

$$\begin{aligned}4(m-m'')(n-n'')-(m-m'')-1 &= 4(mn-mn''-m''n+m''n'')-m+m''-1\\ &= 4mn-4mn''-4m''n+4m''n''-m+m''-1\\ &= (4mn-m-1)-(4mn''+4m''n-4m''n''-m''),\end{aligned}$$

y dado que $4(m-m'')(n-n'')-(m-m'')-1=4rs-r-1$, entonces por la suposición del inicio de la demostración tendríamos que[18] $4rs-r-1=b^2$, es decir, $4(m-m'')(n-n'')-(m-m'')-1=b^2$. Como $4mn-m-1=a^2$, entonces $4mn''+4m''n-4m''n''-m''=2a-1$, pues así obtendríamos que $b^2=a^2-2a+1=(a-1)^2$.

Ahora bien, tomando $4mn''+4m''n-4m''n''-m''=2a-1$ tenemos:

$$\begin{aligned}&4n''(m-m'')+(4n-1)m''=2a-1\\ &\Rightarrow 4n''(m''-m)-(4n-1)m''=-2a+1\\ &\Rightarrow 4n''=\frac{(4n-1)m''-2a+1}{m''-m}\\ &\Rightarrow 4n''=\frac{(4n-1)m''-2a+1+4mn-m-(4mn-m)}{m''-m}\\ &\Rightarrow 4n''=\frac{4m''n-4mn-(m''-m)+4mn-m-2a+1}{m''-m}\\ &\Rightarrow 4n''=\frac{4n(m''-m)-(m''-m)+4mn-m-2a+1}{m''-m}\\ &\Rightarrow 4n''=4n-1+\frac{4mn-m-2a+1}{m''-m}\end{aligned}$$

Dado que $\frac{4mn-m-2a+1}{m''-m}$ tiene que ser un número entero, obtenemos dos casos:

Caso 1: Si $4mn-2a+1=m''$, entonces:

$$4n''=4n-1+\frac{m''-m}{m''-m}$$

---

[17] *Nouvelles annales de mathématiques 1re série*, pp. 278-280.

[18] Es decir, Bédos supone al inicio que para $m,n\in\mathbb{Z}^+$, $4mn-m-1=a^2$, pero además, después supone que $4rs-r-1$ también es un cuadrado. Esta última suposición es fundamental para su demostración, pero a la vez es muy fuerte ya que da la impresión de suponer que la expresión $4mn-m-1$ siempre es un cuadrado para m y n enteros.

$$= 4n - 1 + 1$$
$$= 4n$$

Por lo tanto, $n'' = n$. Pero como $n - n'' = 0$, esto nos lleva a una contradicción, pues $n - n''$ es un entero positivo.

Caso 2: Si $4mn - m - 2a + 1 = t(m'' - m)$, entonces:

$$4n'' = 4n - 1 + \frac{t(m''-m)}{m''-m}$$
$$\Rightarrow 4n'' = 4n - 1 + t$$
$$\Rightarrow n'' = n + \frac{t-1}{4}$$

Como queremos que n'' sea un entero, $t - 1 = 4t'$, con t' un entero positivo. Entonces:

$$n'' = n + \frac{4t'}{4}$$
$$= n + t'$$

Por lo tanto, $n - n'' = -t'$, pero esto nos lleva a una contradicción, pues $n - n''$ es un entero positivo.

Por lo tanto, $4mn - m - 1$ no puede ser un cuadrado. ∎

Bédos continúa haciendo que $4mn - m - 1$ sea igual a 1 y argumenta de la siguiente manera:

$$4mn - m - 1 = 1$$
$$\Rightarrow (4n - 1)m - 1 = 1$$
$$\Rightarrow m = \frac{2}{4n-1}$$

Como quiere que m y n sean enteros, la única solución posible es $n = 0$ y $m = -2$. Pero Bédos olvida que por hipótesis m y n deben de ser enteros positivos, cometiendo así un error.

Después de esto iguala la fórmula a 4 y obtiene lo siguiente:

$$4mn - m - 1 = 4$$
$$\Rightarrow (4n - 1)m - 1 = 4$$
$$\Rightarrow m = \frac{5}{4n-1}$$

Aquí no comete el mismo error que en el caso anterior, pues argumenta que no existen soluciones en los enteros para esta expresión, haciendo referencia a los enteros positivos, pues la única solución posible es $n = 0$ y $m = -5$.

Finaliza esta parte de los números de la forma $4mn - m - 1$ diciendo que la fórmula tiene soluciones enteras para los cuadrados 0 y 1, pero a partir de 4 ésta no tiene soluciones en los enteros, cometiendo así el mismo error al igualar la fórmula a 0.

Concluye Bédos su artículo demostrando de manera parcial algunas de las expresiones que Euler planteó en la carta 47, él usa resultados como aquel de que $\frac{a^2+1}{4n-1}$ no es un entero, que es un resultado de Fermat, de que $4n - 1$ no divide a la suma de dos cuadrados. Para esta parte del artículo Bédos ya no tiene la intención de no usar el *teorema de Fermat*, éste ya se encuentra implícito en lo que está usando para sus pruebas finales.

Retomando la discusión principal del trabajo, Euler no agrega nada relevante al debate en la carta 48, del 13 de marzo de 1742, pero alienta a Goldbach a seguir trabajando este tema

> Su excelencia, la última vez tuve el honor de transcribir una demostración del teorema, que $4mn - m - n$ no puede ser un cuadrado. Del mismo se siguen muchas otras especulaciones interesantes en esta materia, y estoy seguro de que su excelencia podrá obtener aún más consecuencias maravillosas de esto.

Goldbach respondería en la carta 49, del 12 de abril de 1742. En esta carta plantearía una relación muy interesante entre los números de la forma $4mn - m - n$ y los números triangulares.

> Mi demostración de que cuando $4mn - m - n^{\alpha}$ no es un número cuadrado, así como $4mn - m - n^{\alpha+1} \neq a^2$, surge directamente de la única suposición, que $m = 4p - n^{\alpha}$, de donde se obtiene $4n(4p - n^{\alpha}) - 4p \neq 4b^2$. Esta ecuación dividida entre 4 da $4pn - p - n^{\alpha+1} \neq b^2$. Así, en la ecuación $x^{\alpha} = 4px - p - a^2$, x no puede tomar un valor entero positivo, donde α es un número entero cualquiera. Aún más, se sigue que, si bien $p^2 - p - e^2$ toma una infinidad de valores cuadrados en los enteros, no obstante $\frac{p \pm \sqrt{p^2 - p - e^2}}{2}$ no puede ser un número entero, además de que la primera fórmula mencionada $4mn - m - n^{\alpha}$ no da un número triangular, o que $x^{\alpha} = 4px - p - \frac{(b^2 - b)}{2}$ nunca tiene una raíz entera positiva.

Poco menos de un mes, en la carta 50, del 8 de mayo, Euler respondería a esto de la siguiente manera:

> Los corolarios que su excelencia derivó de mi teorema, que $4mn - m - n$ no puede ser un cuadrado, son bastante curiosos y exceden en importancia al teorema mismo. Pues que $4mn - m - n$ no puede ser un número triangular no lo había observado, pero además encontré de esto, que precisamente la fórmula $4mn - m - n$ tampoco puede ser un número heptagonal. En general encontré que todos los números, los cuales no pueden ser $= 4mn - m - n$ están comprendidos en esta fórmula: $xx + yy + y$. Por lo cual la expresión $4mn - m - n + xx + yy + y$ debe dar todos los números posibles.

Aquí la discusión se divide en dos vertientes. La primera se enfoca en la relación entre los números de la forma $4mn - m - n$ y los números poligonales. La segunda desarrolla la idea de que todo número que no es de la forma $4mn - m - n$ será de la forma $x^2 + x + y^2$. Habrá una tercera discusión, la cual está directamente relacionada con el último fragmento de la carta 51.

Números poligonales

Como podemos observar, en la primera sección de este fragmento, se hace referencia a los números triangulares y heptagonales, pero antes de continuar recordemos que estos números pertenecen a una familia que se conoce como *números poligonales* (los cuales, a su vez, pertenecen a una familia más grande denominada *números figurados*). Éstos llevan dicho nombre ya que pueden ser representados mediante puntos equidistantes, como polígonos regulares en dos dimensiones.

Consideremos la progresión de números $1, 2, 3, 4, 5, 6, 7, \ldots$. Ésta puede ser representada como $1 + 1m$, con $m \in \mathbb{Z}^+$. Agregar al 1 como factor nos va a resultar útil más adelante. Si sumamos números consecutivos de esta progresión obtenemos:

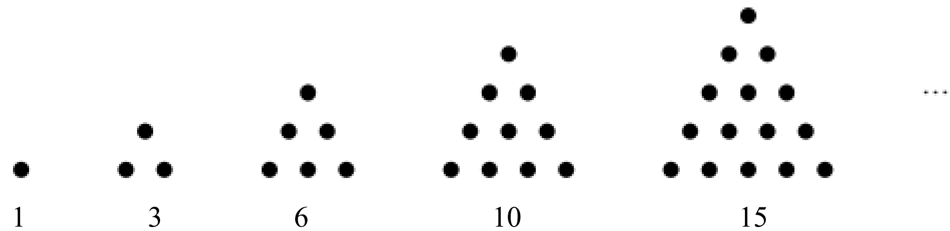
$$1 = 1$$

$$1 + 2 = 3$$

$$1 + 2 + 3 = 6$$

$$\vdots$$

Que a la vez son la representación aritmética del siguiente arreglo figurado:



Observemos que la suma de los primeros k elementos de la progresión nos genera:

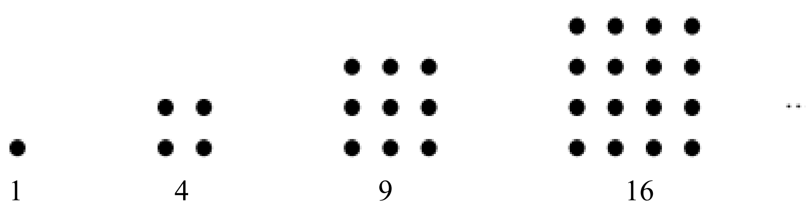
$$\begin{aligned}
1+2+\cdots+k &= (1+1(0))+(1+1(1))+\cdots+(1+1(k-1)) \\
&= 1+(1+1)+(1+2)+\cdots+(1+(k-1)) \\
&= k+1(1+2+3+\cdots+(k-1)) \\
&= k+1\cdot\tfrac{(k-1)k}{2} \\
&= \tfrac{k^2+k}{2}=\tfrac{k(k+1)}{2},
\end{aligned}$$

lo cual nos arroja el $k-$ésimo número triangular.[19]

Si tomamos la progresión $1, 3, 5, 7, 9, \ldots$, ésta se puede representar como $1+2m$, con $m \in \mathbb{Z}^{+}$. Al sumar números consecutivos de la progresión tenemos que:

$$1=1$$
$$1+3=4$$
$$1+3+5=9$$
$$\vdots$$

En este caso la representación aritmética tiene el siguiente arreglo figurado:



La suma de los k primeros elementos de la progresión es:

$$1+3+\cdots+(2k-1)=(1+2(0))+(1+2(1))+\cdots+(1+2(k-1))$$

[19] Es de notar que en el paso de sumar los elementos de la progresión se presenta un proceso de sumar los $(k-1)$ primeros enteros positivos. Queremos señalar que desde Diofanto ya se sumaban los enteros y se obtenía el resultado $\frac{k(k+1)}{2}$, y la justificación era con la prolongación de casos particulares. Actualmente percibimos la presencia de un proceso inductivo, el mismo que aún no se usaba a mediados del siglo XVIII con Euler y Goldbach, y la razón es que en esa época las demostraciones por inducción estaban aún en proceso de gestación.

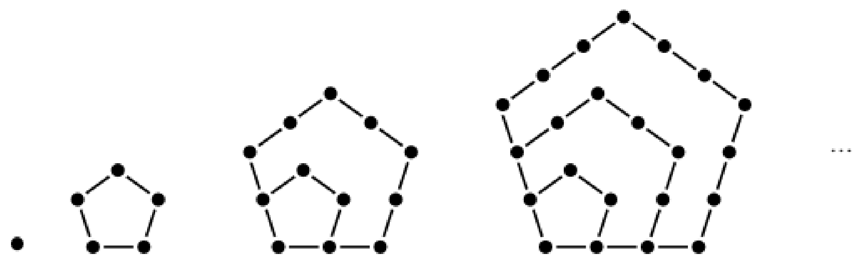
$$
\begin{aligned}
&= 1 + (1 + 2) + (1 + 4) + \cdots + (1 + (2k - 2)) \\
&= k + 2(1 + 2 + 3 + \cdots + (k - 1)) \\
&= k + 2 \cdot \tfrac{(k-1)k}{2} \\
&= k^2 ,
\end{aligned}
$$

lo cual es el k-ésimo cuadrado.

Para terminar los casos particulares tomando la progresión $1, 4, 7, 10, 13, \ldots$, la cual está representada por $1 + 3m$, con $m \in \mathbb{Z}^{+}$. Si tomamos la suma de números consecutivos de la misma tenemos:

$$
\begin{gathered}
1 = 1 \\
1 + 4 = 5 \\
1 + 4 + 7 = 12 \\
\vdots
\end{gathered}
$$

El arreglo figurado correspondiente es:



1 5 12 22

La suma de los k primeros elementos de la progresión son:

:

$$
\begin{aligned}
1 + 4 + \cdots + (3k - 2) &= (1 + 3(0)) + (1 + 3(1)) + \cdots + (1 + 3(k - 1)) \\
&= 1 + (1 + 3) + (1 + 6) + \cdots + (1 + (3k - 3)) \\
&= k + 3(1 + 2 + 3 + \cdots + (k - 1)) \\
&= k + 3 \cdot \tfrac{(k-1)k}{2} \\
&= \tfrac{3k^2 - k}{2},
\end{aligned}
$$

que resulta ser el k-ésimo número pentagonal.

En general, la fórmula $1 + lm$, con $l, m \in \mathbb{Z}^{+}$, genera la progresión 1, $1 + 1m$, $1 + 2m$, $1 + 3m$, …, $1 + (k - 1)m$. Sumando estos términos tenemos:

$$
\begin{aligned}
1 + (1 + 1m) + (1 + 2m) + \cdots + (1 + (k - 1)m) &= k + m(1 + 2 + \cdots + (k - 1)) \\
&= k + m \cdot \frac{(k - 1)k}{2}
\end{aligned}
$$

La última fórmula representa al k-ésimo poligonal de orden m, en otras palabras:

$$P_k(m) = k + m \cdot \frac{(k-1)k}{2}$$

Si desarrollamos esta fórmula obtenemos lo siguiente:

$$\begin{aligned} k + m \cdot \frac{(k-1)k}{2} &= \frac{2k + m(k-1)k}{2} \\ &= \frac{2k + mk^2 - mk}{2} \\ &= \frac{mk^2 - (m-2)k}{2}. \end{aligned}$$

Notemos que: si $m = 1$, tenemos un número triangular; si $m = 2$, obtenemos un número cuadrado; si $m = 3$, entonces tenemos un número pentagonal, etc. Así, podemos concluir que $m + 2 = p$, donde p representa el número de lados. Por lo tanto, $m = p - 2$. Sustituyendo m en $\frac{mk^2-(m-2)k}{2}$ tenemos $\frac{(p-2)k^2-(p-4)k}{2}$. Esta fórmula es la forma usual de los números poligonales, que representa al k-ésimo poligonal con p lados, es decir:

$$Q_k(p) = \frac{(p-2)k^2 - (p-4)k}{2}$$

Goldbach hará algunas observaciones de esta fórmula en la carta 51, las cuales mencionaremos más adelante.

Regresando a la discusión podemos observar que Euler, además de mostrar un gran interés por la relación planteada por Goldbach, asegura que ésta es mucho más significativa que el tema central de su discusión. Él, además de no haber notado la relación con los números triangulares, va más allá y plantea una nueva. Enuncia que los números de la forma $4mn - m - n$ no pueden ser números heptagonales.

Tenemos que ser cuidadosos, pues Euler no responde directamente a la formulación original, sino que se va a un caso particular, al de $\alpha = 1$. Es decir, en lugar de enunciar la relación para $4mn - m - n^\alpha$, enuncia ambas para $4mn - m - n$. A continuación, probaremos que $4mn - m - n$ no puede ser un número triangular ni un número heptagonal.

***Teorema* 4.4** Sean m, n, x enteros positivos, entonces $4mn - m - n \neq \frac{x^2+x}{2}$.

Demostración: Supongamos que $4mn - m - n = \frac{x^2+x}{2}$, entonces:

$$4mn - m - n = \frac{2x^2+2x}{4}$$

$$\Rightarrow 16mn - 4m - 4n = 2x^2 + 2x$$

$$\Rightarrow 16mn - 4m - 4n = 2x^2 + 2x + (1-1)$$

$$\Rightarrow 16mn - 4m - 4n + 1 = 2x^2 + 2x + 1$$

$$\Rightarrow 16mn - 4m - 4n + 1 = \frac{4x^2+4x+2}{2}$$

$$\Rightarrow 2(16mn - 4m - 4n + 1) = (4x^2 + 4x + 1) + 1$$

$$\Rightarrow 2(4m-1)(4n-1) = (2x+1)^2 + 1$$

$$\Rightarrow k(4n-1) = (2x+1)^2 + 1 \qquad \text{, donde } k = 2(4m-1)$$

$$\Rightarrow 4n-1 \mid (2x+1)^2+1$$

Pero esto último no puede suceder, pues contradice **4.2**.

Por lo tanto, $4mn-m-n \neq \frac{x^2+x}{2}$. ■

***Teorema* 4.5** Sean m, n, x enteros positivos, entonces $4mn-m-n \neq \frac{5x^2-3x}{2}$.

Demostración: Supongamos que $4mn-m-n = \frac{5x^2-3x}{2}$, entonces:

$$4mn-m-n = \frac{10x^2-6x}{4}$$

$$\Rightarrow 16mn-4m-4n = 10x^2-6x$$

$$\Rightarrow 16mn-4m-4n+1 = 10x^2-6x+1$$

$$\Rightarrow (4m-1)(4n-1) = (9x^2-6x+1)+x^2$$

$$\Rightarrow (4m-1)(4n-1) = (3x-1)^2+x^2$$

$$\Rightarrow k(4n-1) = (3x-1)^2+x^2 \qquad \text{, donde } k = 4m-1$$

$$\Rightarrow 4n-1 \mid (3x-1)^2+x^2$$

Pero esto último no puede suceder, pues contradice **4.2**.

Por lo tanto, $4mn-m-n \neq \frac{5x^2-3x}{2}$. ■

En este mismo contexto, en el caso de los números hexagonales también se pude demostrar que no pueden ser de la forma $4mn-m-n$, lo cual se puede realizar de dos maneras distintas. La primera será a través de mostrando que todo número hexagonal es un número triangular, pero para ello primero tendremos que hacer una observación. La segunda manera sigue el mismo argumento que hemos usado para los números triangulares y heptagonales.

Notemos que la fórmula $Q_k(p) = \frac{(p-2)k^2-(p-4)k}{2}$ es equivalente a $(p-2)\cdot\frac{k(k-1)}{2}+k$, pues:

$$\begin{aligned}(p-2)\cdot\frac{k(k-1)}{2}+k &= \frac{(p-2)k^2-(p-2)k}{2}+k\\ &= \frac{(p-2)k^2-(p-2)k+2k}{2}\\ &= \frac{(p-2)k^2-(p-2)k-(-2)k}{2}\\ &= \frac{(p-2)k^2-(p-2-2)k}{2}\\ &= \frac{(p-2)k^2-(p-4)k}{2}\end{aligned}$$

Ahora bien, mostraremos que todo número hexagonal es un número triangular:

***Lema* 4.6** Todo número hexagonal es un número triangular.

Demostración: Sea $Q_k(p) = (p-2)\cdot\frac{k(k-1)}{2}+k$. Para $p=6$ (un número hexagonal) tenemos que:

$$(6-2)\cdot\frac{k(k-1)}{2}+k = \frac{4k(k-1)}{2}+k$$

$$= \frac{4k(k-1)+2k}{2}$$
$$= \frac{2k(2k-2+1)}{2}$$
$$= \frac{2k(2k-1)}{2}$$

Dado que un número triangular puede ser de la forma $\frac{x(x-1)}{2}$, entonces tenemos que $\frac{2k(2k-1)}{2}$ es un número triangular para $x = 2k$.

Por lo tanto, todo número hexagonal es un número triangular. ■

Pasaremos a demostrar que un número hexagonal jamás es de la forma $4mn - m - n$.

***Teorema* 4.7** Sean m, n, x enteros positivos, entonces $4mn - m - n \neq 2x^2 - x$.

***Demostración* 1**: Por **4.6** sabemos que todo número hexagonal es un número triangular y como un número triangular no puede ser de la forma $4mn - m - n$, entonces se tiene que ningún número hexagonal es de la forma $4mn - m - n$. ■

***Demostración* 2**: Supongamos que $4mn - m - n = 2x^2 - x$, entonces:

$$4mn - m - n = \frac{8x^2 - 4x}{4}$$
$$\Rightarrow 16mn - 4m - 4n = 8x^2 - 4x$$
$$\Rightarrow 16mn - 4m - 4n + 1 = 8x^2 - 4x + 1$$
$$\Rightarrow (4m-1)(4n-1) = \frac{16x^2 - 8x + 2}{2}$$
$$\Rightarrow 2(4m-1)(4n-1) = (16x^2 - 8x + 1) + 1$$
$$\Rightarrow k(4n-1) = (4x-1)^2 + 1, \qquad \text{donde } k = 2(4m-1)$$
$$\Rightarrow 4n - 1 \mid (4x-1)^2 + 1$$

Pero esto no puede suceder, pues contradice **4.2**.

Por lo tanto, $4mn - m - n \neq 2x^2 - x$. ■

La comunicación entre ellos en lo que corresponde a este tema no tenía pérdida de interés, y así es que llegamos a la carta 51, la que contiene la conjetura. Por el momento nos enfocaremos en el segundo párrafo de este fragmento, ya regresaremos posteriormente a analizar los dos restantes. Goldbach le escribió lo siguiente:

> Su excelencia encontró que todos los números que no pueden ser expresados como $4mn - m - n$, están comprendidos en la fórmula $v^2 + v + u^2$. Y creo que todo $4mn - m - n$ se puede llevar a la formula $y^2 + y - x^2$, de modo que cada número dado es igual a $p^2 + p \pm q^2$, donde p y q denotan números enteros, o bien alguna de las dos letras puede significar 0; de donde se observa que cualquier número está compuesto por un doble triangular $\pm$ un número cuadrado; como además todo número es igual a la formula $u^2 + v^2 + v + y^2 + y - x^2$, cuando se toma
>
> $$u = \frac{z^2+z}{4} + 1,\ x = \frac{z^2+z}{4} - 1,\ u^2 - x^2 = z^2 + z$$
>
> se sigue que el medio de un número dado se vuelve $\frac{n}{2} = \frac{v^2+v+y^2+y+z^2+z}{2}$, es decir, tres triangulares.
>
> Que en la formula poligonal $\frac{(p-2)x^2-(p-4)x}{2}$, cuando ésta se le iguala a $4mn - m - n$, p no pueda ser 5 ± 2 ni 5 ± 1, sino que se excluyen todos los trigonales, tetragonales, hexagonales y heptagonales, se sigue del mismo principio.

[…]

Si se toman m y p como números enteros positivos, la expresión $\frac{p+2\pm\sqrt{4p-m+3}}{m}$ no puede dar un número entero.

Interpretemos lo señalado en este fragmento de la carta. Si en la fórmula $Q_k(p)=\frac{(p-2)k^2-(p-4)k}{2}$ se considera que $p=3,4,6,7$, o lo que es equivalente en números figurados a un triangular, un cuadrado, un hexagonal o un heptagonal respectivamente, entonces la formula $Q_k(p)$ nunca podrá ser de la forma $4mn-m-n$, lo cual probamos anteriormente en **4.4** hasta **4.7**.

Ahora bien, para completar la discusión acerca de los números de la forma $4mn-m-n$ y su relación con los números poligonales hablaremos de Galina Pavlovna Matvievskaya (1930). Ella encontró en un cuaderno de notas de Euler la siguiente pregunta:

¿Para qué enteros α y β la ecuación $4mn-m-n=\frac{(\alpha^2+\beta^2)x^2+(\alpha+\beta)x}{2}$ no es soluble?

La respuesta a esta pregunta se puede obtener de la demostración del teorema[20] que sigue:

***Teorema* 4.8** La ecuación $4mn-m-n=\frac{(\alpha^2+\beta^2)x^2+(\alpha+\beta)x}{2}$ es soluble si y sólo si existe un primo p tal, que $\alpha\equiv\beta\not\equiv 0\ (mod\ p)$, con $p\equiv -1\ (mod\ 4)$.

Demostración:

⇒] Consideremos la ecuación $4mn-m-n=\frac{(\alpha^2+\beta^2)x^2+(\alpha+\beta)x}{2}$ y supongamos que es soluble. Desarrollando obtenemos lo siguiente:

$$4mn-m-n=\frac{2(\alpha^2+\beta^2)x^2+2(\alpha+\beta)x}{4}\ \ldots (1)$$

$$\Rightarrow 16mn-4m-4n=2(\alpha^2+\beta^2)x^2+2(\alpha+\beta)x$$

$$\Rightarrow 16mn-4m-4n+1=2(\alpha^2+\beta^2)x^2+2(\alpha+\beta)x+1$$

$$\Rightarrow 16mn-4m-4n+1=\frac{4(\alpha^2+\beta^2)x^2+4(\alpha+\beta)x+2}{2}$$

$$\Rightarrow 2(4m-1)(4n-1)=4(\alpha^2+\beta^2)x^2+4(\alpha+\beta)x+2$$

$$\Rightarrow 2(4m-1)(4n-1)=4\alpha^2x^2+4\beta^2x^2+4\alpha x+4\beta x+2$$

$$\Rightarrow 2(4m-1)(4n-1)=4\alpha^2x^2+4\alpha x+1+4\beta^2x^2+4\beta x+1$$

$$\Rightarrow 2(4m-1)(4n-1)=(2\alpha x+1)^2+(2\beta x+1)^2\ \ldots (2)$$

Por lo tanto, la ecuación (1) es equivalente a (2).

Ahora bien, observemos que del número $4m-1$ tenemos dos casos:

Caso 1: Si $4m-1$ es primo, entonces $4m-1$ divide a $(2\alpha x+1)^2+(2\beta x+1)^2$ si y sólo si divide a $(2\alpha x+1)^2$ así como a $(2\beta x+1)^2$.

Caso 2: Si $4m-1$ no es primo, sería un número compuesto, teniendo así factores primos. Entonces sus factores primos podrían ser de la forma $4k+1$ o $4k-1$. Pero como nuestro número es de la forma $4m-1$, entonces no puede tener sólo factores de la forma $4k+1$, debe tener por lo menos uno de la forma $4k-1$, o estar formado por una cantidad impar de factores de la forma $4k-1$. De cualquier de las dos formas, necesariamente tiene un factor es de la forma $4k-1$. Así, sea $p=4k-$

[20] *Leonhard Euler und Christian Goldbach. Briefwechsel 1729-1764*, pág. 105.

1 un factor primo, entonces p divide a $(2\alpha x+1)^2+(2\beta x+1)^2$ si y sólo si divide a $(2\alpha x+1)^2$ y a $(2\beta x+1)^2$.

Por lo tanto, p divide a $2\alpha x+1$ y a $2\beta x+1$ respectivamente, en otras palabras, tenemos que $2\alpha x+1 \equiv 2\beta x+1 \equiv 0\ (mod\ p)$. Así, p divide a la diferencia de $2\alpha x+1$ y $2\beta x+1$, es decir, $p \mid 2x(\alpha-\beta)$. Observemos que $p \nmid \alpha\beta x$, pues si p dividiera a alguno, en particular a α, entonces $p \mid 2\alpha x$, lo cual no puede suceder. Esto es análogo en el caso de β y x. Como p es un primo impar, entonces, dado que $p \mid 2x(\alpha-\beta)$, por lo tanto, $p \mid \alpha-\beta$, en otras palabras, $\alpha \equiv \beta \not\equiv 0\ (mod\ p)$.

Por lo tanto, si la ecuación $4mn-m-n=\frac{(\alpha^2+\beta^2)x^2+(\alpha+\beta)x}{2}$ es soluble, entonces existe un primo p tal, que $\alpha \equiv \beta \not\equiv 0\ (mod\ p)$, con $p \equiv -1\ (mod\ 4)$.

$\Leftarrow$] A la inversa, sea $2(4m-1)(4n-1)=(2\alpha x+1)^2+(2\beta x+1)^2$ y supongamos que existe un primo p tal, que $\alpha \equiv \beta \not\equiv 0\ (mod\ p)$, con $p \equiv -1\ (mod\ 4)$. Tenemos dos casos:

Caso 1: Si $4m-1$ es primo, entonces $4m-1$ divide a $(2\alpha x+1)^2+(2\beta x+1)^2$ si y sólo si divide a $(2\alpha x+1)^2$ y a $(2\beta x+1)^2$.

Caso 2: Si $4m-1$ no es primo, entonces tiene como factor primo a $p=4k-1$,[21] por lo que p divide a $(2\alpha x+1)^2+(2\beta x+1)^2$ si y sólo si divide a $(2\alpha x+1)^2$ y a $(2\beta x+1)^2$.

Así, p divide a $2\alpha x+1$ y a $2\beta x+1$ respectivamente. Entonces, fijando x en la congruencia $2\alpha x+1 \equiv 0\ (mod\ p)$ nos arroja una solución entera para 2.

Por lo tanto, si existe un primo p tal, que $\alpha \equiv \beta \not\equiv 0\ (mod\ p)$, con $p \equiv -1\ (mod\ 4)$, entonces la ecuación $4mn-m-n=\frac{(\alpha^2+\beta^2)x^2+(\alpha+\beta)x}{2}$ es soluble.

Por lo tanto, la ecuación $4mn-m-n=\frac{(\alpha^2+\beta^2)x^2+(\alpha+\beta)x}{2}$ es soluble si y sólo si existe un primo p tal, que $\alpha \equiv \beta \not\equiv 0\ (mod\ p)$, con $p \equiv -1\ (mod\ 4)$. ■

Alternativamente, podemos demostrar la imposibilidad de dicha ecuación de la misma manera que hemos actuado en los teoremas anteriores.

***Teorema* 4.9** Sean $m,n,x \in \mathbb{Z}^+$ y sean $\alpha,\beta \in \mathbb{Z}$, entonces $4mn-m-n \neq \frac{(\alpha^2+\beta^2)x^2+(\alpha+\beta)x}{2}$.

Demostración: Supongamos que $4mn-m-n=\frac{(\alpha^2+\beta^2)x^2+(\alpha+\beta)x}{2}$, entonces:

$$4mn-m-n=\frac{2(\alpha^2+\beta^2)x^2+2(\alpha+\beta)x}{4}$$
$$\Rightarrow 16mn-4m-4n=2(\alpha^2+\beta^2)x^2+2(\alpha+\beta)x$$
$$\Rightarrow 16mn-4m-4n+1=2(\alpha^2+\beta^2)x^2+2(\alpha+\beta)x+1$$
$$\Rightarrow 16mn-4m-4n+1=\frac{4(\alpha^2+\beta^2)x^2+4(\alpha+\beta)x+2}{2}$$
$$\Rightarrow 2(4m-1)(4n-1)=4(\alpha^2+\beta^2)x^2+4(\alpha+\beta)x+2$$
$$\Rightarrow 2(4m-1)(4n-1)=4\alpha^2x^2+4\beta^2x^2+4\alpha x+4\beta x+2$$
$$\Rightarrow 2(4m-1)(4n-1)=4\alpha^2x^2+4\alpha x+1+4\beta^2x^2+4\beta x+1$$
$$\Rightarrow k(4n-1)=(2\alpha x+1)^2+(2\beta x+1)^2$$

[21] Esto se justifica como en el *caso 2* de $\Rightarrow$].

$$\Rightarrow 4n-1 \mid (2\alpha x+1)^2+(2\beta x+1)^2$$

donde $k=2(4m-1)$.

Pero lo último no puede suceder en general, por un lado, contradice lo que enuncia **4.2** y por otra parte sí puede suceder bajo las condiciones que nos indica **4.8**.

Por lo tanto, $4mn-m-n \neq \frac{(\alpha^2+\beta^2)x^2+(\alpha+\beta)x}{2}$. ■

Aquí surge la pregunta acerca de cuándo las fórmulas $\frac{(\alpha^2+\beta^2)x^2+(\alpha+\beta)x}{2}$ y $\frac{(p-2)x^2-(p-4)x}{2}$ son iguales. Notemos que en la fórmula $\frac{(p-2)x^2-(p-4)x}{2}$, la suma de los coeficientes es dos, es decir, $(p-2)-(p-4)=2$. Entonces, de manera análoga, queremos encontrar los valores para los cuales se cumple que $(\alpha^2+\beta^2)+(\alpha+\beta)=2$. Ésta última expresión nos arroja la ecuación de la circunferencia $\left(\alpha+\frac{1}{2}\right)^2+\left(\beta+\frac{1}{2}\right)^2=\frac{5}{2}$, pues:

$$(\alpha^2+\beta^2)+(\alpha+\beta)=2$$
$$\Rightarrow (\alpha^2+\alpha)+(\beta^2+\beta)=2$$
$$\Rightarrow \left(\alpha^2+\alpha+\frac{1}{4}+\frac{1}{4}\right)+\left(\beta^2+\beta+\frac{1}{4}+\frac{1}{4}\right)=2$$
$$\Rightarrow \left(\alpha+\frac{1}{2}\right)^2+\left(\beta+\frac{1}{2}\right)^2=\frac{5}{2}$$

Por lo tanto, sólo necesitamos encontrar las raíces enteras de dicha circunferencia, las cuales son: $(-2,0)$, $(-2,-1)$, $(-1,-2)$, $(0,-2)$, $(-1,1)$, $(1,0)$, $(0,1)$, $(1,-1)$. Así, tenemos que $\frac{(\alpha^2+\beta^2)x^2+(\alpha+\beta)x}{2}=\frac{(p-2)x^2-(p-4)x}{2}$ cuando (α,β) es alguna de las raíces antes mencionadas.

Sustituyendo cada raíz en nuestra fórmula podemos observar que

- Cuando $(\alpha,\beta)=(1,0)$ o $(\alpha,\beta)=(0,1)$, entonces:

  $\frac{(\alpha^2+\beta^2)x^2+(\alpha+\beta)x}{2}=\frac{x^2+x}{2}$, un número triangular.

- Si $(\alpha,\beta)=(-1,1)$ o $(\alpha,\beta)=(1,-1)$, entonces:

  $\frac{(\alpha^2+\beta^2)x^2+(\alpha+\beta)x}{2}=\frac{2x^2}{2}=x^2$, un número cuadrado.

- Cuando $(\alpha,\beta)=(-2,0)$ o $(\alpha,\beta)=(0,-2)$, entonces:

  $\frac{(\alpha^2+\beta^2)x^2+(\alpha+\beta)x}{2}=\frac{4x^2-2x}{2}=2x^2-x$, un número hexagonal.

- Si $(\alpha,\beta)=(-2,-1)$ o $(\alpha,\beta)=(-1,-2)$, entonces:

  $\frac{(\alpha^2+\beta^2)x^2+(\alpha+\beta)x}{2}=\frac{5x^2-3x}{2}$, un número heptagonal.

Fuera de éstos no es posible encontrar otro número poligonal a partir de la fórmula $\frac{(\alpha^2+\beta^2)x^2+(\alpha+\beta)x}{2}$.

Números de la forma x^2+x+y^2

Ahora regresaremos a la carta 50, la cual citaremos nuevamente a continuación

> Los corolarios que su excelencia derivó de mi teorema, que $4mn - m - n$ no puede ser un cuadrado, son bastante curiosos y exceden en importancia al teorema mismo. Pues que $4mn - m - n$ no puede ser un número triangular no lo había observado, pero además encontré de esto, que precisamente la fórmula $4mn - m - n$ tampoco puede ser un número heptagonal. En general encontré que todos los números, los cuales no pueden ser $= 4mn - m - n$ están comprendidos en ésta fórmula $xx + yy + y$. Por lo cual la expresión $4mn - m - n + xx + yy + y$ debe dar todos los números posibles.

Euler enuncia en la segunda parte de este fragmento que todo número que no es de la forma $4mn - m - n$ debe de estar comprendido en la fórmula $x^2 + y^2 + y$. Angelo Genocchi (1817-1889) demostró esta afirmación en su artículo de 1853, *Demonstration d'un théorème d'Euler*[22]. A continuación, desarrollaremos dicha prueba.

***Teorema* 4.10** Todo número entero que no es de la forma $4mn - m - n$ será necesariamente de la forma $x^2 + y^2 + y$.

Demostración: Sean $m, n, x, y \in \mathbb{Z}$ y sea N un entero tal que $N \neq 4mn - m - n$. Ahora bien, sea $4N + 1$. Observemos que este número no tiene divisores de la forma $4m - 1$, pues si los tuviera el cociente sería de la forma $4n - 1$ y esto llevaría a que $N = 4mn - m - n$, lo que es una contradicción con la hipótesis, es decir, se tendría que:

$$4N + 1 = (4m - 1)(4n - 1)$$
$$\Rightarrow 4N + 1 = 16mn - 4m - 4n + 1$$
$$\Rightarrow 4N = 16mn - 4m - 4n$$
$$\Rightarrow N = 4mn - m - n$$

Por lo tanto, el número $4N + 1$ solo tiene divisores de la forma $4k + 1$, con $k \in \mathbb{Z}$. A su vez, los divisores primos impares de $4N + 1$ son de la misma forma, $4k + 1$, por lo dicho antes.

Ahora, por el *teorema de la suma de dos cuadrados de Fermat* sabemos que un primo p es expresable como suma de dos cuadrados si y sólo si $p = 2$ o $p \equiv 1 \ (mod\ 4)$.[23]

También sabemos que el producto de dos sumas de dos cuadrados también es suma de dos cuadrados[24], entonces por el *teorema fundamental de la aritmética* $4N + 1$ es una suma de dos cuadrados.

Entonces, $4N + 1 = d^2 + e^2$, donde d y e son de paridad diferente, es decir,

$$4N + 1 = (2x)^2 + (2y + 1)^2$$
$$\Rightarrow 4N + 1 = 4x^2 + 4y^2 + 4y + 1$$
$$\Rightarrow 4N = 4x^2 + 4y^2 + 4y$$
$$\Rightarrow N = x^2 + y^2 + y$$

Por lo tanto, todo número entero que no es de la forma $4mn - m - n$ será necesariamente de la forma $x^2 + y^2 + y$. ■

Dado que todo número entero es o bien de la forma $4mn - m - n$ o bien $x^2 + y^2 + y$, Euler concluye que todo número entero será de la forma $4mn - m - n + x^2 + y^2 + y$.

Goldbach respondería lo siguiente en la carta 51

[22] *Nouvelles annales de mathématiques 1re série*, pp. 235-236.

[23] La demostración de este teorema se expone en el Apéndice A.

[24] Esta propiedad se expone en el Apéndice A.

Su excelencia encontró que todos los números que no pueden ser expresados como $4mn - m - n$, están comprendidos en la formula $v^2 + v + u^2$. Y creo que todo $4mn - m - n$ se puede llevar a la formula $y^2 + y - x^2$, de modo que cada número dado es igual a $p^2 + p \pm q^2$, donde p y q denotan números enteros, o bien alguna de las dos letras puede significar 0; de donde se observa que cualquier número está compuesto por un doble triangular $\pm$ un número cuadrado; como además todo número es igual a la formula $u^2 + v^2 + v + y^2 + y - x^2$, cuando se toma

$$u = \frac{z^2+z}{4} + 1,\ x = \frac{z^2+z}{4} - 1,\ u^2 - x^2 = z^2 + z$$

se sigue que el medio de un número dado se vuelve $\frac{n}{2} = \frac{v^2+v+y^2+y+z^2+z}{2}$, es decir, tres triangulares.

Que en la formula poligonal $\frac{(p-2)x^2-(p-4)x}{2}$, cuando ésta se le iguala a $4mn - m - n$, p no pueda ser 5 ± 2 ni 5 ± 1, sino que se excluyen todos los trigonales, tetragonales, hexagonales y heptagonales, se sigue del mismo principio.

[…]

Si se toman m y p como números enteros positivos, la expresión $\frac{p+2\pm\sqrt{4p-m+3}}{m}$ no puede dar un número entero.

Aquí Goldbach demuestra un resultado ligeramente distinto al planteado por Euler en **4.10**.

***Proposición* 4.11** Todo número entero de la forma $4mn - m - n$ puede ser llevado a uno de la forma $y^2 + y - x^2$.

Demostración: Tomando la expresión $(m+n-1)^2 + (m+n-1) - (m-n)^2$ y desarrollando obtenemos:

$$\begin{aligned}(m+n-1)^2 + (m+n-1) - (m-n)^2 \\ = (m^2+n^2+2mn-2m-2n+1) + (m+n-1) - (m^2-2mn+n^2) \\ = m^2 - m^2 + n^2 - n^2 + 2mn + 2mn - 2m + m - 2n + n + 1 - 1 \\ = 4mn - m - n\end{aligned}$$

Por lo tanto, $4mn - m - n = (m+n-1)^2 + (m+n-1) - (m-n)^2$, es decir, es de la forma $y^2 + y - x^2$. ■

A partir de esto concluye que todo número entero puede ser llevado a uno de la forma $y^2 + y \pm x^2$, es decir, el doble de un número triangular, esto es un número rectangular, más/menos un número cuadrado. Además, al sumar las fórmulas anteriores, obtenemos que todo número entero será de la forma $u^2 + v^2 + v + y^2 + y - x^2$. Aquí Goldbach escoge valores muy particulares para las variables u y x, pues quiere obtener un resultado más general. La elección para dichas variables es $u = \frac{z^2+z}{4} + 1$ y $x = \frac{z^2+z}{4} - 1$, pues:

$$\begin{aligned}u^2 - x^2 = \left(\frac{z^2+z}{4}+1\right)^2 - \left(\frac{z^2+z}{4}-1\right)^2 \\ = \left(\frac{z^4+2z^2z+z^2}{16} + \frac{z^2+z}{2} + 1\right) - \left(\frac{z^4+2z^2z+z^2}{16} - \frac{z^2+z}{2} + 1\right) \\ = \frac{z^4+2z^2z+z^2}{16} - \frac{z^4+2z^2z+z^2}{16} + \frac{z^2+z}{2} + \frac{z^2+z}{2} + 1 - 1\end{aligned}$$

$$= z^2 + z$$

Por lo tanto, $u^2 - x^2 = z^2 + z$.

Ahora, sustituyendo $u^2 - x^2$ en $u^2 + v^2 + v + y^2 + y - x^2$ obtenemos la nueva fórmula $v^2 + v + y^2 + y + z^2 + z$. En otras palabras, Goldbach muestra que todo número entero es la suma de tres dobles triangulares, es decir, un número rectangular, o bien que la mitad de todo entero es la suma de tres triangulares, es decir, $\frac{n}{2} = \frac{v^2+v+y^2+y+z^2+z}{2}$. Este teorema se parece en cierta medida al siguiente teorema de Fermat:

***Teorema* 4.12** (*del número poligonal de Fermat*) Todo número natural es la suma de a lo más n números poligonales.

En su artículo *Demonstratio theorematis Fermatiani omnem numerum sive integrum sive fractum esse summam quatuor pauciorumve quadratorum*[25] de 1754/5, Euler demuestra el caso particular para $n = 4$ del *Teorema del número poligonal de Fermat*, además de generalizarlo para números racionales, es decir, prueba el siguiente resultado:

***Teorema* 4.13** Todo número racional es la suma de a lo más cuatro números cuadrados.

Sin embargo, el procedimiento de Goldbach para llegar a esta conclusión contiene un error, el cual Euler le hace notar en la carta 52, del 30 de junio. Desde un principio, la elección de las variables era arbitraria, es decir, para cualquier número entero, por lo que no es posible tomarse $u = \frac{z^2+z}{4} + 1$ y $x = \frac{z^2+z}{4} - 1$, ya que estas expresiones no arrojan todos los posibles números. Algunos de los números que no están representados en estas fórmulas son 3, 5, 7, entre otros. Por lo tanto, es imposible llegar al resultado general planteado por Goldbach si uno toma como hipótesis que las variables sean números enteros arbitrarios. Es decir, en términos modernos tenemos que para los valores de z no se pueden tener como imágenes en las x e u a todos los enteros, esto es, la función no es suprayectiva bajo z, hacia los enteros.

A pesar de los comentarios de Euler, Goldbach concluirá esta discusión en la carta 53, del 30 de julio, argumentando de la siguiente manera:

> Que todos los números están comprendidos en la fórmula $y^2 + y - x^2$ es algo ya sabido, pero esto no habría impedido mis intenciones, si tan solo las suposiciones $u = \frac{z^2+z}{4} + 1$ y $x = \frac{z^2+z}{4} - 1$ hubieran sido derivadas de fundamentos adecuados, pues como en ésta proposición: Cualquier número es igual a tres trigonales, uno positivo y dos negativos, no importa que en la fórmula $\frac{x^2+x-y^2-y-z^2-z}{2}$, x, y y z representen todos los números posibles, sino que también es posible sustituir x por $2u^2$, si tan solo se prueba que ésta sustitución, para cualquier número dado, no afecta el resultado de la fórmula antes mencionada. Así mismo, el caso, que todo número está compuesto por tres trigonales, tendría una explicación parecida, si la suposición $x = \frac{z^2+z}{4} + 1$ estuviese fundamentada adecuadamente.

El último fragmento

En la carta 51, casi al final aparece un pequeño comentario que a simple vista no tiene relación alguna con los temas discutidos en esta sección, y aunque este sólo se desarrollará en tres cartas y pareciera que no tendrá mayor relevancia para el cuerpo de su correspondencia, consideramos que esto no quita que sí sea importante mencionarlo y darle un espacio en este trabajo.

Goldbach transmitiría este comentario a Euler en la misma carta 51

[25] *Novi Commentarii Academiae Scientiarum Imperialis Petropolitanae*, pp. 13-58.

Si se toman m y p como números enteros positivos, la expresión $\frac{p+2\pm\sqrt{4p-m+3}}{m}$ no puede dar un número entero.

Con una mirada más cuidadosa podemos observar que la expresión $\frac{p+2\pm\sqrt{4p-m+3}}{m}$ se encuentra relacionada con la discusión de este capítulo. Notemos lo siguiente:

Sea $n = \frac{p+2\pm\sqrt{4p-m+3}}{m}$, entonces

$$mn = p + 2 \pm \sqrt{4p - m + 3}$$

$$\Rightarrow mn - p - 2 = \pm\sqrt{4p - m + 3}$$

$$\Rightarrow (mn - p - 2)^2 = 4p - m + 3$$

$$\Rightarrow m^2n^2 - mnp - 2mn - mnp + p^2 + 2p - 2mn + 2p + 4 = 4p - m + 3$$

$$\Rightarrow (m^2n^2 - 2mnp + p^2) - 4mn + 4p + 4 = 4p - m + 3$$

$$\Rightarrow (mn - p)^2 = 4p - m + 3 + 4mn - 4p - 4$$

$$\Rightarrow (mn - p)^2 = 4mn - m - 1$$

Por lo tanto, si $n = \frac{p+2\pm\sqrt{4p-m+3}}{m}$, entonces $4mn - m - 1 = (mn - p)^2$, pero esto contradice a **4.2**.

Por lo tanto, $\frac{p+2\pm\sqrt{4p-m+3}}{m}$ no puede ser un número entero.

Así, si se iguala la expresión $\frac{p+2\pm\sqrt{4p-m+3}}{m}$ con un entero n y desarrollamos de manera inversa, logramos ver que el último comentario de Goldbach está enmarcado en la discusión de los números de la forma $4mn - m - n$.

En la carta 52 Euler respondería lo siguiente

> Que $\frac{p+2\pm\sqrt{(4p-m+3)}}{m}$ nunca pueda ser un entero queda aclarado cuando se iguala esta fórmula a un número entero n, pues mientras que $p = mn \pm \sqrt{(4mn-1)}$, $4mn - 1$ no puede ser un cuadrado.

Para entender el argumento de Euler partiremos de nuevamente de igualar $\frac{p+2\pm\sqrt{4p-m+3}}{m}$ a un entero y expandiendo la misma:

$$n = \frac{p + 2 \pm \sqrt{4p - m + 3}}{m}$$

$$\Rightarrow mn = p + 2 \pm \sqrt{4p - m + 3}$$

$$\Rightarrow mn - p - 2 = \pm\sqrt{4p - m + 3}$$

$$\Rightarrow (mn - p - 2)^2 = 4p - m + 3$$

$$\Rightarrow m^2n^2 - mnp - 2mn - mnp + p^2 + 2p - 2mn + 2p + 4 = 4p - m + 3$$

A partir de este punto agruparemos todos los términos al lado izquierdo de la igualdad para poder construir una ecuación cuadrática en términos de p, para ello llevaremos a cabo las simplificaciones vistas anteriormente en el análisis del fragmento de Goldbach de la carta 51:

$$\Rightarrow p^2 - 2mnp + [(mn)^2 - 4mn + m + 1] = 0$$

Usando la fórmula general para encontrar las raíces de esta ecuación tenemos lo siguiente:

$$p = \frac{2mn \pm \sqrt{(-2mn)^2 - 4((mn)^2 - 4mn + m + 1)}}{2}$$

$$\Rightarrow p = \frac{2mn \pm \sqrt{4(mn)^2 - 4(mn)^2 - 4(-4mn + m + 1)}}{2}$$

$$\Rightarrow p = \frac{2mn \pm \sqrt{-4(-4mn + m + 1)}}{2}$$

$$\Rightarrow p = \frac{2mn \pm 2\sqrt{4mn - m - 1}}{2}$$

$$\Rightarrow p = mn \pm \sqrt{4mn - m - 1}$$

Claramente la expresión a la que llegamos difiere significativamente de la original, mientras que en el fragmento de la carta tenemos que $p = mn \pm \sqrt{4mn - 1}$, nuestro análisis nos muestra que la raíces de la ecuación son de la forma $p = mn \pm \sqrt{4mn - m - 1}$. Llevando a cabo una revisión bibliográfica sobre este aspecto, encontramos que tanto P.H. Fuss [1843, 135] como A. P. Juškevič y E. Winter [1965, 111] representan las raíces como $p = mn \pm \sqrt{4mn - 1}$, faltando un $-m$ dentro de la raíz cuadrada. Esto nos hace pensar que más que un error de dedo por parte de los compiladores, la equivocación viene por parte de Euler, pues no sólo escribe que $p = mn \pm \sqrt{4mn - 1}$, si no que $4mn - 1$ nunca puede ser un cuadrado, afirmando en dos ocasiones con una expresión que no contiene un $-m$. Solo quedaría revisar los manuscritos originales de la correspondencia para aclarar este asunto, lo cual queda más allá de nuestro trabajo.

Se llegará así a la conclusión de esta discusión con Goldbach, que dirá lo siguiente en la carta 53, del 30 de julio de 1742

> Poco después de escribir mi carta, noté que la observación $\frac{p+2\pm\sqrt{4p-m+3}}{m} \neq$ número entero no es de importancia alguna.

A pesar de que éste último fragmento resultó no ser de "importancia alguna", se encuentra enmarcado dentro de la discusión sobre los números de la forma $4mn - m - n$. Creemos que su inclusión hace más rico el análisis de la correspondencia, dándole el lugar que merece, a pesar de que teóricamente no agrega nada relevante al debate entre Goldbach y Euler.

Residuos cuadráticos

Finalmente, y para dar una perspectiva más grande a esta discusión, comentaremos sobre el artículo *Demonstratio theorematis Fermatiani omnem numerum sive integrum sive fractum esse summam quatuor pauciorumve Quadratorum*[26]. En éste Euler presenta resultados acerca de la *teoría de residuos cuadráticos*, la cual está construyendo en este trabajo, de la que se desprenderá una manera alternativa para probar que $4mn - m - n$ no es un cuadrado, lo cual se inscribe en las discusiones que hemos presentando. Para entender la prueba hay que definir lo que es el *complemento de un residuo* y demostrar un teorema previo:

***Definición* 4.14** Dado el residuo r de un divisor p, el *complemento de un residuo* se define como la diferencia $p - r$.

Ahora, una vez definido el complemento, podemos proceder con la demostración.

[26] Véase *Novi Commentarii academiae scientiarum Petropolitanae*, Tomus 5, pp. 13-58.

***Teorema* 4.15** Si todos los cuadrados son divididos por el primo $p = 4n - 1$ y de éstos surgen los residuos $1, \alpha, \beta, \gamma, \delta, \dots, \upsilon$, entonces el complemento de cualquier residuo no será uno de los residuos.

Demostración: Supongamos que r es un residuo $mod\ p$, y que $p - r$ es el complemento, y a la vez residuo $mod\ p$. Dado que $p - r \equiv -r\ (mod\ p)$, tenemos que $-r$ también es residuo $mod\ p$.

Puesto que r y $-r$ son residuos cuadráticos $mod\ p$, entonces existen enteros s y t tales, que se cumple que $s^2 \equiv r\ (mod\ 4n - 1)$ y $t^2 \equiv -r\ (mod\ 4n - 1)$.

Sumando ambas congruencias tenemos que

$$s^2 + t^2 \equiv r - r\ (mod\ 4n - 1)$$

$$\Rightarrow s^2 + t^2 \equiv 0\ (mod\ 4n - 1)$$

Pero esto no puede suceder, pues contradice **4.2**.

Por lo tanto, $-r$ no es un residuo cuadrático $mod\ p$, por lo que el complemento de r no es un residuo cuadrático $mod\ 4n - 1$. ■

Con estas herramientas a nuestra disposición pasaremos a demostrar lo siguiente:

***Teorema* 4.16** $4mn - m - n$ no es un cuadrado.

Demostración: Con base en lo demostrado anteriormente tenemos los residuos $1, \alpha, \beta, \gamma, \delta, \dots, \upsilon$ correspondientes con los cuadrados $1, 2^2, 3^2, 4^2, \dots, (2n - 1)^2$, el último residuo υ corresponde a la división de $(2n - 1)^2$ entre $4n - 1$. Al dividir $(2n - 1)^2 = 4n^2 - 4n + 1$ entre $4n - 1$ obtenemos el residuo $\upsilon = -3n + 1$, pero como $-3n + 1 \equiv n\ (mod\ 4n - 1)$, tenemos que n también es residuo cuadrático.

Por otro lado, el complemento del residuo $\upsilon = -3n + 1$ es $p - \upsilon$, es decir

$$4n - 1 - (-3n + 1) = 7n - 2$$

Pero notemos que $7n - 2 \equiv -n\ (mod\ 4n - 1)$. Por lo tanto $-n$ es complemento del residuo. Pero de **4.15** tenemos que el complemento de cualquier residuo no puede ser residuo de un cuadrado. Por lo tanto $-n$ no es residuo de un cuadrado.

Ahora bien, observemos que los números de la forma $mp - n = m(4n - 1) - n$, al ser divididos por $(4n - 1)$, dejan residuo $-n$, es decir, $m(4n - 1) - n \equiv -n\ (mod\ 4n - 1)$. Sin embargo, de lo antes mencionado, $-n$ no puede ser residuo de ningún cuadrado, y dado que $-n$ es residuo de $m(4n - 1) - n$, tenemos que $m(4n - 1) - n = 4mn - m - n$ no puede ser un cuadrado. ■

Aquí terminamos esta sección del análisis de la correspondencia que involucra la expresión $4mn - m - n$ y como se pudo notar es el tema de mayor interés entre ellos, hasta donde hemos avanzado en la correspondencia que se desprende de la carta 51. Podríamos seguir con el análisis de la expresión señalada, pero hemos decidido detenernos hasta aquí para dar paso a los otros pasajes de la carta 51, que es el objetivo principal de nuestro estudio.

V. Primos de Fermat

Goldbach, en la carta 51 presenta —la ahora reconocida— *conjetura de Fermat* como ejemplo de una proposición que, si bien es falsa, puede dar luz a nuevas verdades. Es aquí donde los *primos de Fermat* entran en escena. Argumenta que 'sería extraordinario' que la serie $2^{2^{n-1}}+1$ produjera números que se pudieran dividir de manera única en dos cuadrados. A continuación, exhibimos el fragmento de la carta:

> No lo considero inútil, que uno haga notar también aquellas proposiciones, las cuales son muy probables, a pesar de que falte una demostración real, pues cuando éstas posteriormente resultasen falsas, así se podría dar la oportunidad de encontrar una nueva verdad. La idea de *Fermat*, que cada número $2^{2^{n-1}}+1$ produce una serie de números primos, no se sostiene, como su excelencia ya ha mostrado, pero sería extraordinario que ésta serie diera solo números que se pudiesen dividir de manera única en dos cuadrados.

Este tema fue de interés mutuo para estos dos matemáticos y se remonta a la segunda carta de su correspondencia, la del 1 de diciembre de 1729. A pesar de que la correspondencia alrededor de esta materia solo cuenta con once cartas, ésta llegó a ser de tal interés para Euler, que publicó dos artículos sobre este tópico: *Observationes de Theoremata Quodam Fermatiano, Aliique ad Numeros Primos Spectantibus*, un breve artículo enfocado únicamente en la *conjetura de Fermat*; además del *Theoremata Circa Divisores Numerorum*, un trabajo más extenso donde expone formalmente su refutación de la conjetura. Antes de estudiar estos dos trabajos, haremos un análisis de sus primeros intercambios sobre este tópico.

Como ya mencionamos, la primera aparición sobre los *primos de Fermat* se encuentra en la carta 2 de su correspondencia, del 1 de diciembre de 1729, donde Goldbach lanza la siguiente pregunta, en su postdata:

> ¿Conoce la observación de Fermat, que todos los números en la fórmula $2^{2^{x-1}}+1$, a saber $3, 5, 17$, etc., son primos? El mismo confesó, sin embargo, que no pudo demostrar esto, y hasta donde sé, nadie más lo ha podido demostrar.

El 8 de enero de 1730, en la carta 3, Euler respondería lo siguiente

> No he podido descubrir nada respecto a la observación de Fermat. Sin embargo, no estoy totalmente convencido de que él lo haya podido inferir legítimamente por inducción, al sustituir x en la fórmula 2^{2^x}, ciertamente no logró llegar al número [potencia] seis.

A pesar de que Euler no ha logrado descubrir algo respecto a esta petición de Goldbach, no se encuentra del todo convencido de que Fermat haya logrado inferir que $2^{2^5}+1$ es un número primo.

El 22 de mayo de 1730, en la carta 4, llegaría la respuesta de Goldbach, en ella se aprecia que se adentró más en la materia:

> Respecto a la observación de Fermat, concuerdo con usted que no parece creíble que él haya expresado seis términos de la progresión, pero no es necesario realizar tanto trabajo acerca de la posibilidad de la observación, pues es fácil notar que los restos de los términos ordenados, respecto a un divisor, se repiten circularmente [cíclicamente]. Por ejemplo, $2^{2^x}+1$, donde $x=2$, será dividido por 7 dejando como resto 3, por lo que el siguiente término dejaría el mismo resto como $(3-1)^2+1$ al ser dividido por 7, a saber 5. Así, $(5-1)^2+1$ dividido por 7 dejará resto 3. Por lo tanto, todos los posibles restos de todos los términos al ser divididos por 7 (donde naturalmente el cociente es >0), serán únicamente 3 y 5. Por el mismo razonamiento, es fácil de observar que ningún término de la serie de Fermat será dividido por algún número <100. Pero sea como haya sido la observación de Fermat, es cierto que todo número 2^p+1, donde p no es $=$ a algún 2^n (donde n es un entero positivo), no es primo, pues sus divisores pueden ser determinados fácilmente. Así el número $2^{84}+1$ tiene como divisor a 17, el número $2^{1736}+1$ a 257, etc.

En la respuesta de Goldbach se puede extraer la idea (en notación de congruencias) de que

$$(3-1)^2+1=2^{2^1}+1\equiv 5\ (mod\ 7)$$

$$(5-1)^2+1=2^{2^2}+1\equiv 3\ (mod\ 7)$$

$$(9-1)^2+1=2^{2^3}+1\equiv 5\ (mod\ 7)$$

De manera equivalente

$$2^{2^1}\equiv 4\ (mod\ 7)$$

$$2^{2^2}\equiv 2\ (mod\ 7)$$

$$2^{2^3}\equiv 4\ (mod\ 7)$$

Lo que propone Goldbach es que los residuos de los números de Fermat módulo 7 siempre serán 5 o 3, y sí tenía razón. Lo podemos justificar de la manera que sigue

$$2^{2^1}\equiv 2^2=4\ (mod\ 7) \qquad\qquad 2^{2^1}\equiv 4\ (mod\ 7)$$

$$\left(2^{2^1}\right)^2\equiv (2^2)^2\ (mod\ 7)$$

$$2^{2^2}\equiv (2^2)^2\equiv 2\ (mod\ 7) \qquad\qquad 2^{2^2}\equiv 2\ (mod\ 7)$$

$$2^{2^3}=\left(2^{2^2}\right)^2\equiv (2)^2\ (mod\ 7) \qquad\qquad 2^{2^3}\equiv 4\ (mod\ 7)$$

$$\left(2^{2^3}\right)^2\equiv (2^2)^2\ (mod\ 7)$$

$$2^{2^4}\equiv 2\ (mod\ 7) \qquad\qquad 2^{2^4}\equiv 2\ (mod\ 7)$$

De esta manera se llega a un proceso cíclico de los residuos que sólo se queda con la repetición de 2 y 4.

El 4 de junio de 1730, en la carta 5, Euler respondió

> En la expresión 2^n+1 no todas las n de la progresión geométrica dan lugar a que el número tenga divisores. [...] si n es un número impar, el binomio 2^n+1 generado por a^n+b^n tendrá a $a+b$ como divisor. Si n fuera múltiplo de un numero impar, como $n=ki$ donde i es el impar, entonces el divisor será a^k+b^k. Pero si la potencia solo tiene factores de dos, entonces en número a^n+b^n no tiene factores como los anteriores para la potencia impar, pero no es suficiente para decir que no tiene ningún factor.

Euler le está reiterando que las expresiones de la forma a^n+b^n sin duda son factorizables cuando n es impar o tiene un factor par, es decir,

$$(a+b)(a^{n-1}-a^{n-2}b+a^{n-3}b^2-\cdots-ab^{n-2}+b^{n-1})=a^n+b^n.$$

Los comentarios que encontramos en esta carta serán afinados y consolidados en su artículo de 1732 *Observationes de Theoremata Quodam Fermatiano, Aliique ad Numeros Primos Spectantibus*, que contextualizamos más adelante, en esta misma sección. Y deja muy claro que para las potencias n que son potencias de 2 no hay factorización de la clase como la que se presentó antes, pero esto no implica que sólo puedan tener factorización de esta forma. En su momento Fermat planteó la posibilidad de que las potencias para n con sólo factores 2 podrían dar lugar sólo a primos, los que se conocen como los primos de Fermat.

En la carta 6, del 26 de junio, Goldbach respondió

> Incluso aunque no sea verdad la proposición de Fermat es digna de elogio. Tengo esta observación.

> Es probable que el divisor mínimo del número $a^{2^x}+1$ sea de la forma $n^{2^x}+1$, pero esto aún no es examinado, solo para $x=1$ se demuestra fácilmente.

Pero, después Goldbach desarrolla algunos ejemplos y plantea que $2^{2^x}+1$ no tendría divisores de la forma $n^{2^x}+1$.

El 25 de junio, en la carta 7, Euler respondió a Goldbach

> Del teorema de Fermat, parece verdad, pero demostración de ello, sin embargo, todavía no la he conseguido. Se han descubierto que algunas de sus propiedades parecen útiles y deben de ser consideradas. La serie 3, 5, 17, 257, etc. cuyos términos generales son $2^{2^{x-1}}+1$, según Fermat son números primos.

Euler después comenta que posiblemente se puede demostrar, pero que no puedo hacerlo.

El 31 de julio Goldbach respondería lo siguiente en la carta 8:

> Se ha observado que en todo número $2^{2^{x+p}}+1$ cuando x y p son números enteros, la división entre $2^{2^x}+1$ deja resto 2 . Debido a esto, $\left(2^{2^x}+1\right)\left(2^{2^x}-1\right)=\left(2^{2^{x+1}}-1\right)$, de nuevo $\left(2^{2^{x+1}}+1\right)\left(2^{2^{x+1}}-1\right)=\left(2^{2^{x+2}}-1\right)$, y así sucesivamente, hasta que lleguemos a $\left(2^{2^{x+p}}-1\right)$, cuyo número es menor que $\left(2^{2^{x+p}}+1\right)$ [en dos unidades]; De esto se sigue, en todo caso, que en todos los números de la serie de Fermat existen primos. Y usted dice, sin embargo, ¿cómo se va a demostrar que todos estos números son primos?

Lo que le comunica Goldbach es que todo número de Fermat de la forma $2^{2^{x+p}}+1$, con $x,p\in\mathbb{Z}$, no tiene divisores de la forma $2^{2^x}+1$ ya que la división deja resto 2, y esto parece que lleva a Goldbach a proponer que si los números $2^{2^x}+1$ no dividen a $2^{2^{x+p}}+1$ entones ya no existirán otros posibles divisores, entonces los $2^{2^{x+p}}+1$ podrían ser primos. Para ver que $2^{2^{x+p}}+1$ deja residuo 2 cuando es dividido por $2^{2^x}+1$ Goldbach deja ver un proceso de inductivo.

Plantea que $\left(2^{2^x}+1\right)\left(2^{2^x}-1\ \right)=2^{2^{x+1}}-1$, al sumar 2 entonces $\left(2^{2^x}+1\right)\left(2^{2^x}-1\ \right)+2=2^{2^{x+1}}+1$, entonces al dividir $2^{2^{x+1}}+1$ entre $2^{2^x}+1$ deja residuo 2.

Para el caso $2^{2^{x+2}}+1$ se tiene que

$$2^{2^{x+2}}-1=\left(2^{2^{x+1}}+1\right)\left(2^{2^{x+1}}-1\right)$$

$$\Rightarrow 2^{2^{x+2}}+1=\left(2^{2^{x+1}}+1\right)\left(2^{2^{x+1}}-1\right)+2$$

$$\Rightarrow 2^{2^{x+1}}+1 \text{ no divide a } 2^{2^{x+2}}+1$$

Y así para el caso $2^{2^{x+p}}+1$

$$2^{2^{x+p}}-1=(2^{2^{x+p-1}}+1)(2^{2^{x+p-1}}-1)$$

$$\Rightarrow 2^{2^{x+p}}+1=\left(2^{2^{x+p-1}}+1\right)\left(2^{2^{x+p-1}}-1\right)+2$$

$$\Rightarrow 2^{2^{x+p-1}}+1 \text{ no divide a } 2^{2^{x+p}}+1$$

Además, en cada factorización de $2^{2^{x+p}}-1$, con $p=1,2,\dots$, podemos sustituir a varios factores hasta llegar a que $2^{2^x}+1$ divide a $2^{2^{x+p}}-1$, pero no dividirá a $2^{2^{x+p}}+1$, y así con $2^{2^{x+i}}$, con $i=1,2,\dots,p-1$.

Por ejemplo, $2^{2^{x+3}}-1=\left(2^{2^{x+2}}+1\right)\left(2^{2^{x+2}}-1\right)$, de lo anterior sustituimos $2^{2^{x+2}}-1$ y se tiene que $2^{2^{x+3}}-1=\left(2^{2^{x+2}}+1\right)\left(2^{2^{x+1}}+1\right)\left(2^{2^{x+1}}-1\right)$.

Ahora sustituimos $2^{2^{x+1}}-1$ y se tiene

$$2^{2^{x+3}}-1=\left(2^{2^{x+2}}+1\right)\left(2^{2^{x+1}}+1\right)\left(2^{2^{x}}+1\right)\left(2^{2^{x}}-1\right)$$

$$\Rightarrow 2^{2^{x+3}}+1=\left(2^{2^{x+2}}+1\right)\left(2^{2^{x+1}}+1\right)\left(2^{2^{x}}+1\right)\left(2^{2^{x}}-1\right)+2$$

$$\Rightarrow 2^{2^{x+i}}+1, \text{ con } i=1,2,\dots,p-1, \text{ no divide a } 2^{2^{x+3}}+1$$

Y es de esta manera en que Goldbach le enuncia a Euler que ningún número de la forma $2^{2^{x+i}}+1$ divide a otro de la forma $2^{2^{x+p}}+1$ y que por lo tanto podrían ser primos al no tener divisores que no sea el mismo número. Pero ahora ya sabemos que sí tienen otros divisores que son de otra forma.

Con esto llegamos a la carta 51, del 7 de junio de 1742. Volveremos a citar el fragmento para mantener la continuidad de la discusión y tener el panorama completo de la correspondencia sobre este tema.

> No lo considero inútil, que uno haga notar también aquellas proposiciones, las cuales son muy probables, a pesar de que falte una demostración real, pues cuando éstas posteriormente resultasen falsas, así se podría dar la oportunidad de encontrar una nueva verdad. La idea de *Fermat*, que cada número $2^{2^{n-1}}+1$ produce una serie de números primos, no se sostiene, como su excelencia ya ha mostrado, pero sería extraordinario que esta serie diera solo números que se pudiesen dividir de manera única en dos cuadrados.

Llegado este punto, ya sabemos que no todos los números de la forma $2^{2^{n-1}}+1$ producen primos, pues Euler dio un primer argumento en 1732 refutando esta idea, pero Goldbach se aventura a formular que "sería extraordinario" que dicha fórmula produjera números que se pudiesen descomponer de manera única en dos cuadrados, como ya comentamos al inicio del capítulo.

Euler le respondió en la carta 52, del 30 de junio de 1742.

> Si todos los números comprendidos en la fórmula $2^{2^{n-1}}+1$ se pudiesen dividir de manera única en dos cuadrados, entonces todos estos números serían necesariamente primos, lo cual no sucede. Pues todos estos números están contenidos en esta fórmula $4m+1$, la cual, siempre que sea un número primo, se puede resolver de manera única en dos cuadrados sin ninguna falla. Sin embrago, siempre que $4n+1$ no sea un número primo, entonces éste no sería resoluble en dos cuadrados, o bien lo será en más de un modo. Pero que $2^{32}+1$, el cual no es un número primo, se pueda dividir en dos cuadrados en al menos dos maneras, lo puedo demostrar: I. Si a y b son resolubles en dos cuadrados, entonces su producto ab también será resoluble en dos cuadrados; II. Si el producto ab y el factor a fuesen resolubles en dos cuadrados, de igual manera el otro factor b será resoluble en dos cuadrados. Estos teoremas se pueden demostrar de manera rigurosa. Ahora $2^{32}+1$, un número que es resoluble en dos cuadrados, a saber $2^{32}+1$, es divisible por $641=25^2+4^2$. Por lo tanto, el otro factor, el cual llamaré b con el fin de la brevedad, ciertamente será también una suma de dos cuadrados. Si $b=pp+qq$, entonces $2^{32}+1=(25^2+4^2)(pp+qq)=(25p+4q)^2+(25q-4p)^2$ y simultáneamente $2^{32}+1=(25p-4q)^2+(25q+4p)^2$, y por lo tanto, $[2^{32}+1]$ es una suma de dos cuadrados en al menos dos maneras. De esto se puede encontrar la doble resolución *a priori*. Así obtendremos $p=2556$ y $q=409$, y por lo tanto $2^{32}+1=65536^2+1^2=62264^2+20449^2$.

Euler en primer lugar le recuerda a Goldbach que el número de Fermat $2^{2^5}+1$ no es primo y además este número lo usará de contraejemplo para mostrarle que no todos los números de la forma $4k+1$ tienen representación única como suma de dos cuadrados, sólo pasará con los primos de esta forma. Actualmente reconocemos el *teorema de Girard–Euler* que enuncia lo siguiente:

***Teorema* 5.1** (*Girard–Euler*) Todo primo de la forma $4k+1$ puede ser expresado de manera única como suma de dos cuadrados, salvo el orden y signos.

Este enunciado redondea la respuesta de Euler de que no todos los números de la forma $2^{2^m}+1$ pueden ser representados de manera única como suma de dos cuadrados, a no ser que el número sea primo.

En 1732 Euler presentaba a la Academia de San Petersburgo el artículo *Observationes de Theoremata Quodam Fermatiano, Aliique ad Numeros Primos Spectantibus*, pero publicado por primera vez hasta 1738. Éste será el primer trabajo en el que Euler refuta la *conjetura de Fermat*. Comienza con la siguiente afirmación:

***Afirmación* 5.2** a^n+1 tiene divisores siempre que n sea un número impar o sea dividido por un número impar distinto a la unidad.

Euler no probó esta afirmación, pero se puede demostrar de la siguiente manera[27]:

Demostración: Primero observemos que a^n+b^n, con n impar o divisible por un número impar distinto a la unidad, se puede factorizar como

$$(a+b)(a^{n-1}-a^{n-2}b+a^{n-3}b^2-\cdots-ab^{n-2}+b^{n-1}).$$

Para esto desarrollaremos el producto, así

$$\begin{aligned}&(a+b)(a^{n-1}-a^{n-2}b+a^{n-3}b^2-\cdots-ab^{n-2}+b^{n-1})\\ &=(a^n-a^{n-1}b+a^{n-2}b^2-\cdots-a^2b^{n-2}+ab^{n-1})\\ &\quad+(a^{n-1}b-a^{n-2}b^2+a^{n-3}b^3-\cdots-ab^{n-1}+b^n)\end{aligned}$$

Observemos que, si n es impar, tenemos un número par de sumandos que se repiten, pero cada uno con un signo distinto, por lo que éstos se van a eliminar entre sí, y lo anterior es igual a:

$$\begin{aligned}a^n+[(a^{n-1}b-a^{n-1}b)+(a^{n-2}b^2-a^{n-2}b^2)+\cdots+(ab^{n-1}-ab^{n-1})]+b^n&\\ =a^n+[0+0+\cdots+0]+b^n&\\ =a^n+b^n.&\end{aligned}$$

Por lo tanto, $(a+b)(a^{n-1}-a^{n-2}b+a^{n-3}b^2-\cdots-ab^{n-2}+b^{n-1})=a^n+b^n$, por lo que $a+b\mid a^n+b^n$.

Por otro lado, si n es dividido por un número impar, entonces $n=rs$, donde r o s es impar. Sin pérdida de generalidad supongamos que s es impar, por lo que $a^n+b^n=a^{rs}+b^{rs}=(a^r)^s+(b^r)^s$. Dado que s es impar, tenemos el proceso análogo al anterior.

Por lo tanto, $(a^r+b^r)((a^r)^{s-1}-(a^r)^{s-2}b^r+(a^r)^{s-3}(b^r)^2-\cdots-(a^r)(b^r)^{s-2}+(b^r)^{s-1})=a^n+b^n$, por lo que $a^r+b^r\mid a^n+b^n$.

Ahora bien, si se sustituye $b=1$ tenemos que $a^r+1\mid a^n+1$.

Por lo tanto, a^n+1 tiene divisores siempre que n sea un número impar o sea dividido por un número impar distinto a la unidad. ■

Euler observa que si n es un número que no puede ser dividido por un número impar, excepto la unidad, y si además n es una potencia de 2, entonces para la expresión a^n+1 llega a la siguiente afirmación:

[27] Esta demostración se desarrolló en *Los primeros trabajos de Euler sobre algunos teoremas de Fermat y otros acerca de la teoría de números*, pp. 14-15.

***Afirmación* 5.3** Si $a^n + 1$ es primo, entonces será necesariamente de la forma $a^{2^m} + 1$, pero el recíproco no siempre se cumple, pues si a es impar, entonces $a^{2^m} + 1$ siempre es dividido por 2.

De igual manera, Euler no demostró esta afirmación.

Ahora bien, si se tomara a como un número primo, Euler argumenta que existirían una infinidad de casos en los que se obtiene un número compuesto. Pone como primer ejemplo que $a^2 + 1$ es divisible por 5 si $a = 5b \pm 3$, pues

$$\begin{aligned} a^2 + 1 &= (5b \pm 3)^2 + 1 \\ &= (25b^2 \pm 15b \pm 15b + 9) + 1 \\ &= 25b^2 \pm 30b + 10. \end{aligned}$$

Como podemos observar, 5 divide a cada término de la expresión, por lo que 5 divide a $a^2 + 1$, si $a = 5b \pm 3$.

Los otros ejemplos listados son: $30^2 + 1$ es dividido por 17; $50^2 + 1$ es dividido por 41; $10^4 + 1$ lo es por 73; $63^8 + 1$ por 17; y $6^{128} + 1$ es dividido por 257.

Después de esto Euler hace notar algo muy importante, el estudio de los números de la forma $2^{2^m} + 1$ solo se había llevado a cabo a partir de una tabla de números primos que no excedía a $100{,}000$, y en ninguno de ellos se había encontrado alguno que tuviera divisores distintos a él mismo y a la unidad. Este punto es crucial, pues resultaría que el siguiente número de Fermat, $2^{2^5} + 1$, al cual no logró llegar, consta de diez cifras.

El hecho de que sólo se usaran número primos menores a $100{,}000$, entre otras razones que no son especificadas, llevaron a Fermat a afirmar que $2^{2^m} + 1$ siempre resultaba en un número primo, resultado que posteriormente fue propuesto a John Wallis (1616-1703) y a otros matemáticos de la época como un "teorema distinguido" a probar. Al menos confesó no tener una prueba de este problema, pero no dudaba de su veracidad.

Para Fermat este resultado sería de gran utilidad para poder exhibir un número primo mayor que cualquier número dado, lo cual sería una hazaña complicada de lograr sin un "teorema universal" como el que postulara su afirmación.

Euler continúa declarando que si bien la validez de este problema es clara para $m = 1, 2, 3, 4$, en $2^{2^m} + 1$, pues los números 5, 17, 257 y $65{,}537$, son primos, el teorema falla para el caso $2^{2^5} + 1$, pues $2^{2^5} + 1 = 2^{32} + 1 = 4{,}294{,}967{,}297$, y este número puede ser dividido por 641. Con esto por fin se logra dar una respuesta a la *conjetura de Fermat*, mostrando que la fórmula $2^{2^m} + 1$ no siempre arroja números primos. Si bien Euler escribe que no sabe "por qué destino" se volvió claro el hecho de que $2^{2^5} + 1$ no es un primo, comenta que llegó a esta conclusión después de haber trabajo este problema por varios días.

Concluye la discusión sobre los números de Fermat manifestando que, gracias a la refutación antes expuesta, el problema de encontrar un primo mayor que un número dado sigue sin poder resolverse.

Finalmente, el 2 de septiembre de 1748, Euler presentaba a la Academia de San Petersburgo el artículo *Theoremata Circa Divisores Numerorum*, que sería publicado por primera vez en 1750. En este trabajo Euler muestra formalmente que $2^{2^5} + 1$ no es un número primo. Para probar esto tenemos que demostrar algunos resultados previos. Uno de ellos se deduce a partir del *pequeño teorema de Fermat*[28]:

---

[28] Véase capítulo *Pequeño Teorema de Fermat.*

***Teorema* 5.4** Si a y b no son divididos por un número primo p, entonces todo número de la forma $a^{p-1} - b^{p-1}$ es divisible por p.

Demostración: Sean a y b enteros, los cuales no son divisibles por p un número primo. Por el *pequeño teorema de Fermat* tenemos que $a^{p-1} - 1$ y $b^{p-1} - 1$ son divisibles por p. Si tomamos la diferencia de éstos obtenemos

$$\begin{aligned} a^{p-1} - 1 - (b^{p-1} - 1) &= a^{p-1} - 1 - b^{p-1} + 1 \\ &= a^{p-1} - b^{p-1} \end{aligned}$$

Por lo tanto, $a^{p-1} - b^{p-1}$ es divisible por p, pues $a^{p-1} - 1$ y $b^{p-1} - 1$ son divisibles por p.

Por lo tanto, si a y b no son divididos por un número primo p, entonces todo número de la forma $a^{p-1} - b^{p-1}$ es divisible por p. ■

Teniendo este resultado a la mano, Euler demuestra lo siguiente:

***Teorema* 5.5** La suma de dos cuadrados $a^2 + b^2$ nunca puede ser dividida por ningún primo de la forma $4n - 1$, a menos que a y b sean divisibles por $4n - 1$.

Demostración: La demostración es semejante al Teorema 4.2 del capítulo IV. ■

Euler observa que, dado que todos los números primos pueden escribirse como $4n + 1$ o $4n - 1$, entonces si $4n - 1$ no es un primo, es un compuesto que tendrá un divisor de la forma $4k - 1$, ya que de lo contrario si no tiene un factor de la forma $4k - 1$, no es posible que el producto de los factores de lugar a la forma $4n - 1$. Así, dado que la suma de dos cuadrados no puede ser dividida por un primo de la forma $4n - 1$, entonces no será divisible por ningún número de la forma $4n - 1$.

Por lo tanto, $a^2 + b^2$ no será divisible por ningún número de la serie

$$3, 7, 11, 15, 23, 27, 31, 35, \ldots,$$

por lo que todos los divisores primos de esta suma, a excepción del 2, serán de la forma $4n + 1$, siempre y cuando a y b sean primos relativos. Así, los números

$$2, 5, 13, 17, 29, 37, 41, 53, 61, 73, 89, 97, \ldots$$

dividirían a la suma.

Ahora bien, Euler comenta que es fácil observar que los números de la forma $4n - 1$ no pueden ser suma de dos cuadrados, pues estos cuadrados solo pueden ser pares o impares, y serán de la forma $4a$ y $4b + 1$ respectivamente. Gracias a estos detalles, si la suma de dos cuadrados es impar, entonces necesariamente un sumando es par y el otro impar, de donde tendríamos $4a + 4b + 1$, pero este número es de la forma $4n + 1$. Por lo tanto, ningún número de la forma $4n - 1$ puede ser suma de dos cuadrados.

Después de esto hace notar que a pesar de que este teorema siempre fue afirmado [aceptado] por todos los autores del método *diofantino*, ninguno, hasta donde Euler tiene conocimiento, lo ha demostrado. La única excepción sería Fermat, pero él jamás publicó su prueba, por lo que, hasta donde a Euler concierne, él es el primero en publicar finalmente esta prueba.

Por lo tanto, de todo lo anterior se deriva que toda suma $a^2 + b^2$, donde a y b son primos relativos entre sí, es un primo o no tiene divisores salvo el 2, a menos que estos sean de la forma $4n + 1$.

A continuación, demuestra el siguiente teorema:

***Teorema* 5.6** La suma de dos bicuadráticos $a^4 + b^4$, donde a y b son primos relativos, tiene como divisores a 2 o a números de la forma $8n + 1$.

Demostración: Sea a^4+b^4, donde a y b son primos relativos. Entonces o ambos son impares, o uno es par y el otro impar. En el primer caso 2 divide a la suma y se puede simplificar, en el otro caso los divisores impares, si existieran, serían de la forma $4n+1$. Esto último sucede dado que $a^4+b^4=(a^2)^2+(b^2)^2$, y por el teorema anterior ningún número de la forma $4n-1$ divide a la suma de dos cuadrados, o bien, solo los números de la forma $4n+1$ dividen a dicha suma.

Por otro lado, todo número de la forma $4n+1$ puede expresarse como $8n+1$ u $8n-3$. Sin embargo, ningún número de la forma $8n-3$ puede dividir a la suma de dos bicuadráticos. Primero supongamos que $8n-3$ es un número primo, entonces $a^{8n-4}-b^{8n-4}$ es divisible por $8n-3$.[29] Por lo tanto, $8n-3$ no puede dividir a $a^{8n-4}+b^{8n-4}$, pues si lo hiciera, entonces dividiría a a y a b, pero por hipótesis éstos son primos relativos.

Ahora bien, dado que $8n-4=4(2n-1)$, podemos reescribir $a^{8n-4}+b^{8n-4}$ como $(a^4)^{2n-1}+(b^4)^{2n-1}$. Entonces $(a^4)^{2n-1}+(b^4)^{2n-1}$ es igual a

$$(a^4+b^4)((a^4)^{2n-2}-(a^4)^{2n-3}b^4+\cdots-a^4(b^4)^{2n-3}+(b^4)^{2n-2})$$

Dado que $8n-3$ no divide a $a^{8n-4}+b^{8n-4}$, entonces tampoco divide a ninguno de los factores a^4+b^4 ni a $(a^4)^{2n-2}-(a^4)^{2n-3}b^4+\cdots-a^4(b^4)^{2n-3}+(b^4)^{2n-2}$.

Para el caso en que $8n-3$ no es un número primo, entonces es compuesto, por lo tanto, tiene un factor primo y puede ser de la forma $8k+1, 8k+3, 8k+5$ o $8k+7$. Para el caso $8k+5$, éste es equivalente a $8k-3$ que es el caso anterior que se vio que no es posible que divida a a^4+b^4. Para los casos $8k+3$ y $8k+7$ se procede de manera semejante como lo fue con el primo $8n-3$. Para $8k+3$ y con el *pequeño teorema* se tendrá que $a^{8n+2}\equiv 1(mod\ 8n+3)$, y al elevar al cuadrado las partes de la congruencia se tendrá que $a^{4(4n+1)}\equiv 1(mod\ 8n+3)$. Se hace algo semejante con b, y por un proceso semejante para el primo $8n-3$ se tiene que $8k+3$ no divide a a^4+b^4.

Para $8k+7$ se toma su equivalencia $8k-1$, pero este es un número de la forma $4k'-1$ y éstos no pueden dividir a a^4+b^4. Por último, el producto de factores que son sólo de la forma $8k+1$ no pueden generar uno de la forma $8n-3$, entonces $8n-3$ no puede tener un factor primo $8k+1$.

Por lo tanto, a^4+b^4 no puede ser dividido por ningún número de la forma $8n-3$, a menos que a y b sean divisibles por $8n-3$.

Entonces, la suma de dos bicuadráticos a^4+b^4, donde a y b son primos relativos, tiene como divisores a 2 o a números de la forma $8n+1$. ■

Continúa observando que todo número impar se puede escribir como $8n\pm 1$ y $8n\pm 3$, y del teorema anterior, repite que la suma de dos cuartas potencias solo puede ser divisible por $8n+1$. Por lo tanto, todos los divisores primos de a^4+b^4, donde a y b son primos relativos, son $2, 17, 41, 73, 89, 97, 113, 137, 193$, etc. De esta manera, si cualquier número n es de la forma a^4+b^4, entonces tendríamos que n es primo o bien sus únicos divisores son de la forma $8n+1$ o 2. Así, ningún número que tiene como divisor uno de la forma $8n+1$ es la suma de dos cuartas potencias, a menos que éste tenga cuatro divisores iguales, los cuales son descartados generalmente al considerar cuartas potencias.

El artículo prosigue con el siguiente teorema:

***Teorema* 5.7** La suma a^8+b^8, donde a y b son primos relativos, tiene como divisores a 2 o a números de la forma $16n+1$.

---

[29] Suponemos que el primo $8n-3$ y a son primos relativos, entonces por el *pequeño teorema de Fermat* $a^{8n-4}\equiv 1(mod\ 8n-3)$, y lo mismo con b. Por lo tanto, se restan las congruencias y $a^{8n-4}-b^{8n-4}$ es divisible por $8n-3$.

Demostración: Sea a^8+b^8, donde a y b son primos relativos. Notemos que, puesto que $a^8+b^8=(a^2)^4+(b^2)^4$, por el teorema anterior, a^8+b^8 solo admite divisores de la forma $8n+1$. Ahora bien, $8n+1$ puede ser reescrito como $16n+1$ o como $16n-7$, pues si tomamos $n=2k$, entonces $8n+1=8(2k)+1=16k+1$, mientras que si tomamos a $n=2k+1$, entonces $8n+1=8(2k+1)+1=16k+9$, pero $9\equiv -7\ (mod\ 16)$, por lo que $8n+1$ se puede reescribir como $16k-7$.

Si suponemos que $16n-7$ es un número primo, entonces $a^{16n-8}-b^{16n-8}$ es divisible por $16n-7$ y por un proceso semejante al del Teorema 5.6 se tiene que $a^{16n-8}+b^{16n-8}$ no es divisible por $16n-7$. Ahora, como $16n-8=8(2n-1)$, entonces podemos reescribir $a^{16n-8}+b^{16n-8}$ como $(a^8)^{2n-1}+(b^8)^{2n-1}$. Así, $(a^8)^{2n-1}+(b^8)^{2n-1}$ es igual a

$$(a^8+b^8)((a^8)^{2n-2}-(a^8)^{2n-3}b^{48}+\cdots-a^8(b^8)^{2n-3}+(b^8)^{2n-2})$$

Dado que $16n-7$ no divide a $a^{16n-8}+b^{16n-8}$, tampoco divide a los factores (a^8+b^8) ni a $((a^8)^{2n-2}-(a^8)^{2n-3}b^{48}+\cdots-a^8(b^8)^{2n-3}+(b^8)^{2n-2})$.

En el caso cuando $16n-7$ es compuesto se desarrolla un proceso semejante a **5.6** y se concluye que $16n-7$ no puede ser factor de (a^8+b^8).

Por lo tanto, a^8+b^8 nunca puede ser dividido por ningún número de la forma $16n-7$, a menos que a y b sean divisibles por $16n-7$.

Por lo tanto, la suma a^8+b^8, donde a y b son primos relativos, tiene como divisores a 2 o a números de la forma $16n+1$. ■

Notemos que para la suma a^2+b^2 sus divisores son 2 o números de la forma $4n+1$, para a^4+b^4 también tenemos a 2 o a $8n+1$, y para a^8+b^8 tenemos como divisores a 2 o a $16n+1$. Todos estos divisores, a excepción del 2, son de la forma $2^{m+1}n+1$, pues si $m=1$ obtenemos $2^{1+1}n+1=2^2n+1=4n+1$, para $m=2$ tenemos $2^{2+1}n+1=2^3n+1=8n+1$ y para $m=3$ tenemos $2^{3+1}n+1=2^4n+1=16n+1$. Gracias a esto, Euler llega al siguiente teorema general:

***Teorema* 5.8** La suma $a^{2^m}+b^{2^m}$, donde a y b son primos relativos, tiene como divisores a 2 o a números de la forma $2^{m+1}n+1$.

Demostración: Como observamos, los divisores de a^2+b^2 son de la forma 2^2n+1, por **5.6** los divisores de a^4+b^4 son de la forma 2^3n+1 y por **5.7** los divisores de a^8+b^8 son de la forma 2^4n+1. La demostración para $a^{16}+b^{16}$ utiliza un método análogo al de los teoremas anteriores, por lo que sus divisores son de la forma 2^5n+1. De aquí en adelante se entiende que $a^{32}+b^{32}$, $a^{64}+b^{64}$, etc. tiene como divisores a 2^6n+1, 2^7n+1, etc. respectivamente.

Por lo tanto, en general, tenemos que la suma $a^{2^m}+b^{2^m}$ tiene como divisores a números de la forma $2^{m+1}n+1$, o bien a 2. ■

Euler deduce de esto que si $a^{2^m}+b^{2^m}$ tuviese divisores primos, estos serían 2 o números de la forma $2^{m+1}n+1$.

Gracias a este último resultado, Euler por fin logra dar un argumento sólido del por qué el número de Fermat $2^{32}+1$ no es un número primo. Dado que $2^{32}+1=2^{2^5}+1^{2^5}$, sabemos que sus divisores serán de la forma 2^6n+1, o bien, $64n+1$, por lo que solo es necesario buscar números primos que tengan esta forma. Tomando $n=10$ obtenemos 641, y este número resulta ser un divisor de $2^{32}+1$.

Fermariales

Las últimas apariciones de los *números de Fermat* en la correspondencia entre ellos se encuentran en las cartas 101 y 102, del 26 de febrero y el 5 de abril de 1746 respectivamente. En estas cartas, los *números de Fermat* se ubican dentro de una discusión sobre series, y con esto se distancian temáticamente de las primeras cartas que giraban en torno a si el número $2^{32}+1$ era o no primo. Además de que la conversación se desvincula de la materia antes mencionada, también se encuentran alejadas temporalmente por poco más de tres años, pues la última carta que trata la primalidad de $2^{32}+1$ es del 30 de junio de 1742, mientras que la primera misiva sobre series es del 26 de febrero de 1746, como habíamos comentado.

Dentro de este contexto, entramos en materia y presentamos la carta 101. En ésta Goldbach le escribe como postdata lo siguiente:

> P.S. Desde hace tiempo he observado que la serie cuya ley de progresión es $A^2+4A=B$, donde A denota un término cualquiera y B el término que le sigue [subsecuente], tiene este término general $a^{-2^x}-2+a^{2^x}$, y de esto se puede encontrar el término general de esta serie $1+1\cdot 3+1\cdot 3\cdot 5+1\cdot 3\cdot 5\cdot 17+1\cdot 3\cdot 5\cdot 17\cdot 257$ +etc., de la cual todos los factores de los términos son números que Fermat sostuvo eran números primos.

Goldbach comenta que si se tiene una serie $\sum_{n=0}^{\infty} a_n$, cuya ley de progresión es $A^2+4A=B$, donde A denota un término cualquiera a_n y B representa el término subsiguiente a_{n+1}, entonces la expresión $a^{-2^x}-2+a^{2^x}$ describirá al término general de dicha serie. Así, a partir de esto, expresa que es posible encontrar el término general de la serie

$$1+1\cdot 3+1\cdot 3\cdot 5+1\cdot 3\cdot 5\cdot 17+1\cdot 3\cdot 5\cdot 17\cdot 257+\cdots$$

donde cada factor representa productos de *números de Fermat*.

Euler respondería a esto en la carta 102 de la siguiente manera:

> Inicialmente quedé asombrado por la serie $1+1\cdot 3+1\cdot 3\cdot 5+1\cdot 3\cdot 5\cdot 17$ +etc., pero cuando observé la misma más minuciosamente, en breve noté que hace tiempo expresé el término general de esta bajo otras circunstancias. Encontré que cuando
>
> $$(1+a)(1+a^2)(1+a^4)(1+a^8)(1+a^{16})\cdots\left(1+a^{2^n}\right)=s$$
>
> entonces $(1-a)s=1-a^{2^{n+1}}$, y así $s=\frac{a^{2^{n+1}}-1}{a-1}$.
>
> Por lo tanto, cuando $a=2$, tenemos $1\cdot 3\cdot 5\cdot 17\cdots\left(2^{2^n}+1\right)=2^{2^{n+1}}-1$.

Si bien Euler se sorprendió al leer la serie presentada por Goldbach, notó que él mismo ya había descrito el término general de dicha serie bajo circunstancias distintas. Estos serían sus trabajos sobre funciones *generadoras* y *particiones*.

Por un lado, Euler presenta la expresión para $F_n=2^{2^n}+1$, con $n=0,1,2,\ldots$, donde el producto de números de Fermat indica que $F_0\cdot F_1\cdot F_2\cdot\ldots\cdot F_n=F_{n+1}-2$. Cabe señalar que la expresión puede ser no solo para primos.

Euler nos da el caso para $a=2$, en la expresión de las particiones y por lo tanto $F_0\cdot F_1\cdot F_2\cdot\ldots\cdot F_n=F_{n+1}-2$. Una demostración en términos actuales, pero no tan alejada de Euler, se desarrolla por inducción de la siguiente manera:

***Proposición* 5.9** Sea $F_n=2^{2^k}+1$, el cual denota al k-ésimo número de Fermat, donde k es un entero no negativo. Entonces para todo entero positivo n se cumple que

$$F_0\cdot F_1\cdot F_2\cdot\ldots\cdot F_n=F_{n+1}-2.$$

Demostración: Por inducción sobre n

Base Para $n = 1$ tenemos que $F_0 = F_1 - 2$, lo cual se cumple, pues $F_0 = 3$ y $F_1 = 5$.

Hipótesis de inducción Supongamos que la afirmación se cumple para n, es decir, se cumple que $F_0 \cdot F_1 \cdot F_2 \cdot \ldots \cdot F_{n-1} = F_n - 2$.

Paso inductivo Sea $F_0 \cdot F_1 \cdot F_2 \cdot \ldots \cdot F_{n-1} \cdot F_n$, por la *hipótesis de inducción* tenemos que

$$\begin{aligned} F_0 \cdot F_1 \cdot F_2 \cdot \ldots \cdot F_{n-1} \cdot F_n &= (F_0 \cdot F_1 \cdot F_2 \cdot \ldots \cdot F_{n-1})F_n \\ &= (F_n - 2)F_n \\ &= (2^{2^n} - 1)(2^{2^n} + 1) \\ &= (2^{2^n})^2 - 1 \\ &= 2^{2^{n+1}} - 1 \\ &= F_{n+1} - 2 \end{aligned}$$

Por lo tanto, para todo entero positivo n se cumple que $F_0 \cdot F_1 \cdot F_2 \cdot \ldots \cdot F_n = F_{n+1} - 2$. ■

Por otro lado, Euler presenta el producto $(1 + a)(1 + a^2)(1 + a^4)(1 + a^8)(1 + a^{16}) \cdots \left(1 + a^{2^n}\right)$ y en estos años él trabajaba con funciones generadoras para obtener las particiones de un número entero. Este producto cuadra totalmente con una función generadora para obtener la partición de un entero con sumandos diferentes de la forma 2^n, es decir, se pueden generar las formas de escribir a m de la forma $m = 2^{\lambda_1} + 2^{\lambda_2} + \cdots + 2^{\lambda_t}$, con $\lambda_i \neq \lambda_j$, $i \neq j$, $a = 2$, $\lambda_i = 2^r$, y además saber de cuantas formas se puede encontrar esta suma.

A la vez se tiene que cada factor $1 + a^{2^n}$ de la función generadora, para $a = 2$, es un número de Fermat, y esto hace que la relación particiones producto de primos o número de Fermat sea más interesante. Por esta razón a estos productos le llamaremos *fermariales*, y es por los *primoriales*.

VI. La conjetura de Goldbach

En este capítulo llegamos a la esperada *conjetura de Goldbach*, recordemos que esta es la columna vertebral de la tesis, todo el análisis de los capítulos anteriores es para exhibir que la conjetura no fue la pieza central de su correspondencia, y tampoco lo fue de la carta 51. Ahora confirmaremos que Goldbach no estaba pensando con mucha antelación en lo que propuso como conjetura, y se puede ver en que su propuesta final de conjetura para Euler quedó en el margen de la carta. Sin embargo, sabemos que actualmente es un problema famoso del que se han realizado numerosos avances, aunque hasta el día de hoy se mantienen firmes varios pendientes, y esto de alguna manera acaparó la atención de toda la correspondencia entre ellos.

Con base en lo anterior vamos a la carta 51. Nuestro problema en cuestión se encuentra acoplado con los *primos de Fermat*, los cuales analizamos en el capítulo anterior con más profundidad. El vínculo entre estos dos tópicos no recae en que compartan necesariamente la temática, más bien su relación se concentra en que Goldbach plantea en ambas partes proposiciones que posiblemente puedan ser verdaderas. Pero si éstas son demostradas eventualmente como falsas, es posible, aun así, obtener de ellas nuevas verdades. Esto es el núcleo de lo que a Goldbach le interesa, conjeturar problemas que ayuden a desarrollar la matemática. A continuación, mostramos el fragmento de la carta 51, del 7 de junio de 1742, donde observamos lo argumentado anteriormente[30]

> No lo considero inútil, que uno haga notar también aquellas proposiciones, las cuales son muy probables, a pesar de que falte una demostración real, pues cuando éstas posteriormente resultasen falsas, así se podría dar la oportunidad de encontrar una nueva verdad. La idea de *Fermat*, que cada número $2^{2^{n-1}}+1$ produce una serie de números primos, no se sostiene, como su excelencia ya ha mostrado, pero sería extraordinario que ésta serie diera solo números que se pudiesen dividir de manera única en dos cuadrados. **De este modo arriesgaré también una conjetura: Que todo número, que está compuesto por dos números primos, es un agregado [una suma] de tantos números primos como que se quieran (incluida la unidad), hasta alcanzar un agregado [una suma] de unidades. [*Anotado por Goldbach al margen*: Después de haber vuelto a leer esto, veo que la conjetura se deja demostrar de manera rigurosa para el caso $\boldsymbol{n+1}$, si se cumple para $\boldsymbol{n}$ y $\boldsymbol{n+1}$ se puede dividir en dos números primos. La demostración es muy sencilla. Al menos parece que cada número que es mayor que 2 es un agregado [una suma] de tres números primos.] Por ejemplo:**
>
> $$4=\begin{cases}1+1+1+1\\1+1+2\\1+3\end{cases}\qquad 5=\begin{cases}2+3\\1+1+3\\1+1+1+2\\1+1+1+1+1\end{cases}$$
>
> $$6=\begin{cases}1+5\\1+2+3\\1+1+1+3\\1+1+1+1+2\\1+1+1+1+1+1\end{cases}\qquad \text{etc.}$$

En la Figura 1 se observa que Goldbach reflexionó sobre el problema que le señalo a Euler después de terminar la carta, pues es notorio que escribió la nota marginal que marcamos en el rectángulo vertical.

[30] A partir de esto arroja la ahora famosa *conjetura de Goldbach*, la cual no es enteramente equivalente con su versión actual. La conjetura la marcamos en **negritas**.

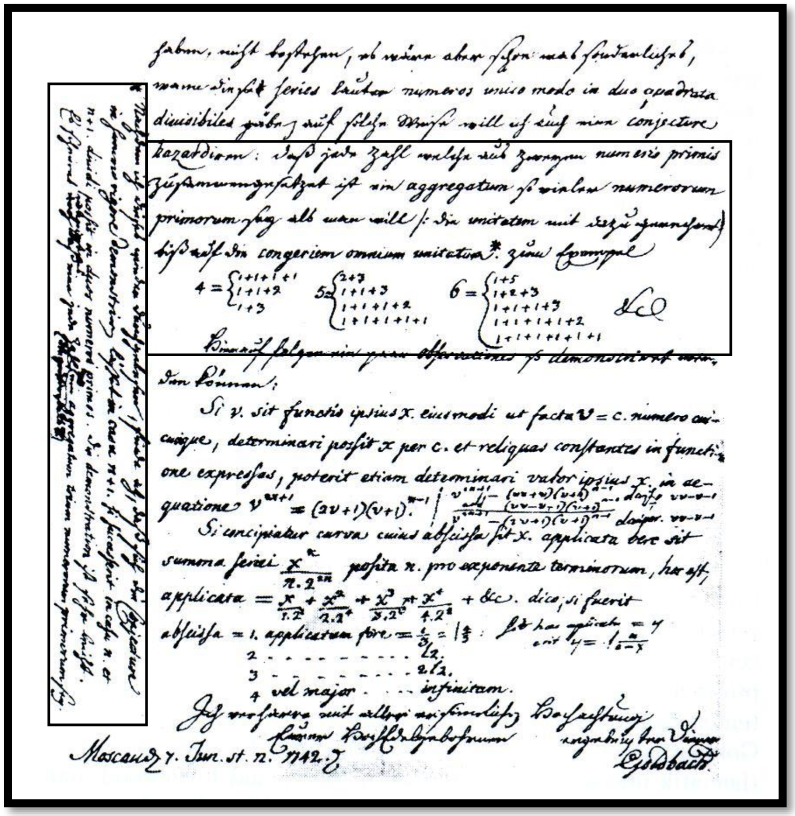


Figura 1. Manuscrito original de la carta 51

Análisis de la conjetura

Para comenzar con nuestro análisis es importante recalcar que Goldbach enuncia su conjetura entorno a los problemas cuya verdad no está garantizada, pues a pesar de que eventualmente sean demostrados como falsos, estos problemas nos guiarán a nuevas verdades matemáticas. En una primera lectura de la carta 51 salta a la vista que la conjetura actual difiere en gran medida a la planteada por Goldbach en su misiva. Actualmente este problema se divide en dos conjeturas, conocidas como *binaria* y *terciaria*, las cuales enunciamos a continuación.

***Conjetura* 6.1** (*Binaria*): Todo entero par mayor que 2 puede ser escrito como suma de dos primos.

***Conjetura* 6.2** (*Terciaria*): Todo entero impar mayor que 7 puede ser escrito como suma de tres primos.

A continuación, mostramos la conjetura original para que el lector pueda realizar una comparación entre el postulado original y la versión actual.

> Que todo número, que está compuesto por dos números primos, es un agregado [una suma] de tantos números primos que se quieran (incluida la unidad), hasta alcanzar un agregado [una suma] de unidades. Por ejemplo:

$$4 = \begin{cases} 1+1+1+1 \\ 1+1+2 \\ 1+3 \end{cases} \qquad 5 = \begin{cases} 2+3 \\ 1+1+3 \\ 1+1+1+2 \\ 1+1+1+1+1 \end{cases}$$

$$6 = \begin{cases} 1+5 \\ 1+2+3 \\ 1+1+1+3 \\ 1+1+1+1+2 \\ 1+1+1+1+1+1 \end{cases} \qquad \text{etc.}$$

[Anotado por Goldbach al margen: Después de haber vuelto a leer esto, veo que la conjetura se deja demostrar de manera rigurosa para el caso $n+1$, si se cumple para n y $n+1$ se puede dividir en dos números primos. La demostración es muy sencilla. Al menos parece que cada número que es mayor que 2 es un agregado [una suma] de tres números primos.]

Como podemos observar, la versión original de la conjetura nos dice que, "*si un número está compuesto por dos primos, entonces éste se puede descomponer en tantos números primos como se quiera, incluida la unidad, hasta llegar a una suma de unidades*". Aquí hacemos hincapié en que es importante notar que en la época de Euler y Goldbach la unidad, era considerada como un número primo, bajo ciertas circunstancias, no en todas las ocasiones. De regreso al análisis, Goldbach muestra algunos ejemplos de descomposiciones en sumas de primos, en particular usa a los números 4, 5 y 6, como suma de dos primos. Esto nos lleva a pensar que el verdadero interés de Goldbach va más allá de lo que actualmente postulan las conjeturas *binaria* y *terciaria* (**6.1** y **6.2** respectivamente), pues en esencia las afirmaciones de Goldbach van más de la mano sobre la posibilidad de poder descomponer un número en cuantos sumandos de números primos se quiera, siempre y cuando nuestro valor inicial esté compuesto por dos números primos.

Aun así, es posible entender el por qué la conjetura original quedó reducida a lo que hoy entendemos por la *conjetura de Goldbach*, pero para ello tenemos que analizar primero el comentario marginal de Goldbach.

Al terminar su misiva, es posible notar que Goldbach reflexionó más sobre la conjetura que aventuró en su carta, pues agrega una observación al margen del escrito[31], ya que no le quedaba espacio suficiente en el manuscrito original para añadir su comentario. A continuación, mostramos su nota marginal:

> Después de haber vuelto a leer esto, veo que la conjetura se puede demostrar de manera rigurosa para el caso $n+1$, si se cumple para n y $n+1$ se puede dividir en dos números primos. La demostración es muy sencilla. Al menos parece que cada número que es mayor que 2 es un agregado [una suma] de tres números primos.

Como podemos observar, Goldbach intenta dar un bosquejo de la demostración de su conjetura. Argumenta que si un número cualquiera n cumple con el enunciado, entonces también lo hará $n+1$, pues si n es suma de dos primos, entonces por hipótesis será suma de cuantos primos uno quiera, por lo que $n+1$ será suma de tres, cuatro, … primos. Aquí es importante notar que la descomposición de $n+1$ depende directamente de la descomposición de n. Por otro lado, si n cumple con la conjetura y $n+1$ también es suma de dos primos, comenta que "la demostración es muy sencilla", pues cumple directamente con la hipótesis de la conjetura, por lo que $n+1$ podrá ser escrito como suma de cuantos primos se quiera. Para este caso, la descomposición de $n+1$ no depende de la descomposición de n.

Ahora bien, otro detalle importante a notar aquí es la conclusión a la que Goldbach llega al final de su comentario, a saber, que "al menos parece que cada número que es mayor que 2 es un agregado

[31] Véase el recuadro vertical de la Figura 1.

de tres números primos". Cabe la posibilidad que **6.2** haya surgido de esta conclusión, pero es relevante distinguir las diferencias entre ambos enunciados. Nótese que **6.2** habla estrictamente de número impares y su descomposición en tres primos, mientras que Goldbach arroja una conjetura más general, pues nos dice que todo número mayor que 2 es suma de tres primos. A comparación con el enunciado actual, la formulación de Goldbach no se ve restringida con la paridad del número.

Antes de continuar con un análisis más detallado de la nota marginal nos surge la pregunta: ¿Qué pasó después de que Goldbach leyera su conjetura? Pudo haber sucedido que, al considerar la descomposición en dos primos, se haya dado cuenta que se encontraba en un terreno inestable, pues si tomamos un número muy grande, su descomposición como suma de dos primos resultará en números muy grandes, por ejemplo $163186 = 71993 + 91193$. Así pues, realizar ahora la descomposición en 3 o más primos se vuelve una tarea mucho más complicada, pues los números resultantes ya no se pueden manipular de manera tan sencilla, comparado con los ejemplos mencionados en su carta. Así, el comentario marginal surge como un replanteamiento de su conjetura con el fin de encontrar descomposiciones de números en sumandos primos, eliminando por completo la hipótesis de que n inicialmente sea suma de dos primos. Pero, finalmente este párrafo no es más que una especulación.

Con lo comentado anteriormente, y gracias a un rápido análisis de la nota marginal, creemos apropiado proponer los siguientes puntos:

a) La descomposición de un número n en 3, 4, 5, o más primos no requiere *a priori* de que n sea suma de dos primos, basta que los número pares lo sean.

b) Es posible extraer de las ideas de Goldbach el siguiente enunciado (en adelante *Enunciado de la Descomposición en Primos* o *EDP*): todo número es la suma de tres o más primos hasta alcanzar puras unidades.

c) La *conjetura de Goldbach* y *EDP*, aunque están íntimamente relacionadas, no son equivalentes.

El comentario al margen

Regresando a la nota marginal, continuaremos con un análisis más detallado de lo que Goldbach nos dice, para ello recurriremos a un lenguaje matemático más actualizado. Recordemos lo que nos dice el enunciado de Goldbach:

Si se cumple la conjetura para n, es decir, si existen q_1, q_2 primos tales que $n = q_1 + q_2$, para $n \geq 2$, entonces $\sum_{i=1}^{j} p_i = n$, para toda j, con $2 \leq j \leq n$. Entonces $\left(\sum_{i=1}^{j} p_i\right) + 1 = n + 1$, para toda j, con $2 \leq j \leq n$ (nótese que $n + 1$ será suma de 3, 4, 5,... , n primos, pero no necesariamente de 2).

Por lo tanto, $\sum_{t=1}^{k} p_t = n + 1$, para toda k, con $2 \leq k \leq n + 1$. Y si $n + 1$ es suma de dos primos, entonces por lo anterior lo es de 3, 4, 5, ..., n, y en consecuencia la conjetura se cumple para $n + 1$.

Veamos un ejemplo de esta afirmación:

$n = 9$	$n + 1 = (9) + 1 = 10 = 5 + 5$
$n = 7 + 2$	$n + 1 = (7 + 2) + 1$
$n = 7 + 1 + 1$	$n + 1 = (7 + 1 + 1) + 1$
$n = 5 + 2 + 1 + 1$	$n + 1 = (5 + 2 + 1 + 1) + 1$
$n = 5 + 1 + 1 + 1 + 1$	$n + 1 = (5 + 1 + 1 + 1 + 1) + 1$
$n = 3 + 2 + 1 + 1 + 1 + 1$	$n + 1 = (3 + 2 + 1 + 1 + 1 + 1) + 1$
$n = 3 + 1 + 1 + 1 + 1 + 1 + 1$	$n + 1 = (3 + 1 + 1 + 1 + 1 + 1 + 1) + 1$

$n = 2 + 1 + 1 + 1 + 1 + 1 + 1 + 1$ $\quad n + 1 = (2 + 1 + 1 + 1 + 1 + 1 + 1 + 1) + 1$

$n = 1 + 1 + 1 + 1 + 1 + 1 + 1 + 1 + 1$ $\quad n + 1 = (1 + 1 + 1 + 1 + 1 + 1 + 1 + 1 + 1) + 1$

Aquí utilizamos el caso $n = 9$ para demostrar el caso $n + 1 = 10$. Es importante observar que las descomposiciones para el caso 10 no dependen en nada de su descomposición inicial en dos primos (incluso puede ser que no exista), que para este caso pueden ser $5 + 5$ o $7 + 3$.

Ahora veamos que sucede para el caso del número 11:

$n = 10$ $\quad n + 1 = (10) + 1 = 11$

$n = 7 + 3$ $\quad n + 1 = (7 + 3) + 1$

$n = 7 + 2 + 1$ $\quad n + 1 = (7 + 2 + 1) + 1$

$n = 7 + 1 + 1 + 1$ $\quad n + 1 = (7 + 1 + 1 + 1) + 1$

$n = 5 + 2 + 1 + 1 + 1$ $\quad n + 1 = (5 + 2 + 1 + 1 + 1) + 1$

$n = 5 + 1 + 1 + 1 + 1 + 1$ $\quad n + 1 = (5 + 1 + 1 + 1 + 1 + 1) + 1$

$n = 3 + 2 + 1 + 1 + 1 + 1 + 1$ $\quad n + 1 = (3 + 2 + 1 + 1 + 1 + 1 + 1) + 1$

$n = 3 + 1 + 1 + 1 + 1 + 1 + 1 + 1$ $\quad n + 1 = (3 + 1 + 1 + 1 + 1 + 1 + 1 + 1) + 1$

$n = 2 + 1 + 1 + 1 + 1 + 1 + 1 + 1 + 1$ $\quad n + 1 = (2 + 1 + 1 + 1 + 1 + 1 + 1 + 1 + 1) + 1$

$n = 1 + 1 + 1 + 1 + 1 + 1 + 1 + 1 + 1 + 1$ $\quad n + 1 = (1 + 1 + 1 + 1 + 1 + 1 + 1 + 1 + 1 + 1) + 1$

Aunque es posible descomponer 11 en tres o más primos, no es posible descomponerlo en dos (incluyendo la unidad). Por lo tanto, la conjetura no se cumple para $n = 11$ (pero sí se cumple *EDP*). Asimismo, se puede identificar rápidamente que 17 y 23, entre otros, tampoco cumplen con la conjetura, por no poder ser representados como suma de dos primos.

Esto nos lleva a la parte final de la carta:

> Al menos parece que cada número que es mayor que 2 es un agregado de tres números primos.

No sería difícil entender el origen de este enunciado si tratáramos de imaginar el proceso lógico que Goldbach siguió al estructurar su conjetura. Después de un pequeño examen, podremos ver que por lo menos hasta el número 25, todos los números pares sí pueden ser escritos como suma de dos primos, pero esto no sucede con los impares, ya que no todos cumplen con la conjetura, esto es, no pueden ser expresados como suma de dos primos.

Sin embargo, como en general el caso inmediato anterior a los casos fallidos sí cumple con ser suma de dos primos, entonces sabemos que, al menos, los casos fallidos se pueden expresar como suma de tres primos. Esto es, si n, que sería nuestro caso anterior, es suma de dos primos, entonces $n + 1$, nuestro casi fallido, lo será de tres, sin importar si $n + 1$ puede ser expresado como suma de dos. Entonces, en principio, podemos suponer que todo número mayor a dos se puede expresar como suma de tres primos, llegando así al enunciado final de su conjetura.

Comentamos anteriormente que este enunciado es muy parecido a lo que hoy conocemos como la conjetura *terciaria* (**6.2**) de Goldbach. La diferencia radica en que Goldbach escribió en su carta un enunciado aún más general que dice: "*cada número que es mayor que* 2", y la conjetura *terciaria* solamente hace referencia a los números impares.

Es importante notar que, después de leer la carta y, en particular, los párrafos donde Goldbach hace referencia a la suma de números primos, no se encuentra mención alguna de la multicitada conjetura *binaria* (**6.1**). No hay que confundir cuando Goldbach escribe que "*todo número, que está compuesto* *por dos números primos*” con la conjetura *binaria*, pues lo que él propuso fundamentalmente fue una serie de implicaciones para aquellos números que se pueden descomponer como suma de dos primos. Además, Goldbach en ninguna parte de la misiva menciona los números pares, siempre se refiere a “*todo número*”, o bien a “*cada número*”. La conjetura y, sobre todo, las implicaciones propuestas en la carta, aunque cercanas, requerían de un mayor análisis —o de mayor intuición— para acercarse a la conjetura *binaria*.

La respuesta de Euler

La respuesta de Euler llegaría en la carta 52, del 30 de junio de 1742. En ella encontramos lo siguiente:

> Que todo número que es resoluble como [suma] de dos primos, puede [a su vez] ser representado como [suma] de tantos primos como se quiera, puede ser ilustrado y confirmado por una observación, misma que usted me comunicó formalmente, concretamente, que todos los números pares son suma de dos primos. Supongamos que el número propuesto n sea par, por lo tanto, es una suma de dos números primos, y entonces $n-2$ también es una suma de dos números primos, por lo que n también es una de tres, y también cuatro, y así sucesivamente. Pero si n es un número impar, entonces es una suma de tres números primos, ya que $n-1$ es la suma de dos, y se puede seguir resolviendo las demás sumas. Sin embargo, que todo número par sea la suma de dos números primos, lo que considero un teorema correcto, es algo que no puedo demostrar.

La respuesta se puede dividir en dos secciones: la primera, donde menciona que si consideramos que todos los pares son suma de dos primos, entonces los pares y los impares (en los casos donde es posible representarlos como suma de dos primos) pueden ser descompuestos como suma de tantos primos como queramos; y la segunda, donde da el esbozo de una construcción de la descomposición para tres o más primos.

Análisis de la primera sección

Aquí Euler nos lleva a seguir sosteniendo que la conjetura inicial que planteó Goldbach —en la carta 51— fue la descomposición de todos los enteros positivos mayores que tres en 3, 4 o tantos primos como queramos. Pero es de gran importancia señalar que, para darle viabilidad a la conjetura, Euler supone valido el enunciado que dice “[...] concretamente, que todos los números pares son suma de dos números primos [...]”

Este párrafo sería el inicio de los miles de referencias que durante los siglos XVIII al XXI se han dado a la hoy conocida *conjetura de Goldbach*. Miles de artículos han mencionado la famosa conjetura *binaria* que actualmente dice que *todo entero par mayor o igual que cuatro es la suma de dos primos*. Pero hagamos una escala en el camino y veamos —nuevamente— que, hasta este momento, en la correspondencia que conocemos entre el día 7 y el 30 de junio, Goldbach no había mencionado algo parecido a una conjetura *binaria* para los pares. El primero que menciona la conjetura *binaria* fue Euler, precisamente en esta carta del 30 de junio, y recordemos lo que dice: “[...] *una observación, misma que usted me comunicó formalmente, concretamente, que todos los números pares son suma de dos números primos* [...]”. Aquí, tenemos la afirmación de Euler de que Goldbach le había comunicado formalmente la relación *binaria*, pero, por otro lado, la falta de información donde veamos que verdaderamente Goldbach lo hizo, nos lleva a proponer más de una interpretación.

> *) Por un lado, después de que Euler estudiara lo que Goldbach le envía el día 7, piensa que es natural, así como necesario, completar la conjetura, y lo hizo mencionando la representación binaria de los pares. Esto es, al leer la conjetura *terciaria* de Goldbach, se percata que detrás está la posibilidad de que los pares sean suma de dos primos. Al ver la nota al margen comprendió que el razonamiento de Goldbach se basaba en que la descomposición en tres primos o más se apoyaba

en los números que sí cumplían la binaria, de tal forma que los que no la cumplían, por lo menos cumplieran la terciaria.

Además, sabemos —por sus cartas— que Euler se daba tiempo para hacer las pruebas numéricas que fueran necesarias para convencerse de los resultados que proponía, por lo que no era difícil que se diera cuenta que la representación binaria erraba rápidamente en impares muy pequeños, pero no así para los pares[32]. Así, Euler le da el crédito a Goldbach, reconociendo que él fue el de la iniciativa que dio lugar al problema.

A pesar de lo escrito en la carta del día 30 se tendría que reconocer que de acuerdo con la información que se conoce, el primero que mencionó la famosa *conjetura de Goldbach* fue realmente Euler[33].

*) Una segunda vía es que exista una carta intermedia o anterior entre la del día 7 y la del 30, donde Goldbach sí hubiera propuesto la relación binaria para los pares, y con ello se justificaría el que Euler le diera el crédito a Goldbach. Esta posibilidad es incierta ya que Goldbach estaba en Moscú y Euler en Prusia, y el periodo entre las dos cartas conocidas fue de tres semanas. Además, casi todos los temas de la carta del 7 son respondidos en la del 30, con lo que se detecta una continuidad entre ambas. La realidad es que tampoco podemos negar totalmente la existencia de otra carta, ya que es posible que, en caso de haber existido, simplemente no ha llegado a nuestras manos, y sólo contamos con lo escrito por Euler en su respuesta.

En conclusión, con lo que se tiene desde que se publicó por primera vez la correspondencia entre ellos[34] no se puede decir que la conjetura *binaria* fue propuesta por Goldbach, pero lo que sí podemos decir es que el primero que la menciona —sin demostrar— fue Euler en la carta del 30 de junio de 1742.

Como ya se mencionó, a Goldbach se le puede reconocer el haber enunciado algo parecido a lo que hoy conocemos como conjetura *terciaria* (**6.2**). Pero las alteraciones históricas han perdurado. Es decir, actualmente **6.2** nos dice *que todo número impar mayor que 6 es la suma de tres primos*, pero Goldbach escribió que *todo número mayor que 2 es suma de tres primos* y, otra vez, resulta que la *terciaria* actual no la propusieron ni Euler ni Goldbach.

---

[32] Los cálculos computacionales en la actualidad nos muestran que cualquier prueba numérica que ellos hubieran hecho para los pares, hubiera resultado exitosa.

[33] No es raro encontrar en trabajos de ciencia frases de personajes célebres que al ser sometidos a un análisis histórico más serio resulta que nunca las dijo nadie. Así mismo encontramos autorías dudosas o incluso erradas. Como ejemplo de lo indicado se puede mencionar que Euler en su artículo de 1732-1733 analiza las ecuaciones del tipo $x^2 - Ay^2 = 1$ (con números enteros), pero se conserva una duda, parece que Euler erróneamente la llama *ecuación de Pell*; posteriormente la historia la consolido como una aportación de John Pell, y si Euler se equivocó o no, ya no es tan importante para algunos, finalmente para muchos será la *ecuación de Pell.*
Otro ejemplo es la prueba de primalidad de Wilson que dice:
Si un entero n es primo, entonces $(n-1)! \equiv -1 \ (mod\ n)$ (que actualmente es un sí y sólo si)
Aquí la duda está en que quien enunció el teorema fue Edward Waring [1991, 363] y se lo atribuyó a John Wilson (ya Gauss [1965, 50] lo mencionó en *Disquisitiones Arithmeticae*), la duda que persiste es que no se tiene ninguna referencia de que Wilson hubiera trabajado sobre el problema más allá de haber hecho pruebas numéricas, la primera demostración que se conoció fue hasta 1773 con Lagrange. Sabemos que Wilson fue alumno sobresaliente y amigo de Waring, en el siguiente pasaje de sus *Meditationes Algebraicae* encontramos el aprecio que le tenía Waring [1991, 363] (con lo cual la duda persiste): "This truly elegant property of prime number was discovered by a most excellent man, master of all matters mathematical, John Wilson, Esq". Pero nuevamente las inercias de la costumbre hicieron que toda obra que hace referencia al teorema se le mencione como *teorema de Wilson*, siendo que podría ser el *teorema de Wilson-Waring-Lagrange*.

[34] Véase [Fuss, P. H. 1843].

Análisis de la segunda sección

La segunda sección de la carta, Euler la utiliza para comentar lo que podrían ser algunos elementos útiles que ayuden a demostrar la viabilidad de la conjetura. No demostrará que la descomposición se vale para aquellos que son suma de dos primos, sino que supondrá que todos los números pares cumplen con ser suma de dos primos y, en consecuencia, la descomposición se cumplirá para 3, 4, 5, o tantos primos como se quiera para todos los enteros. Recordemos lo que se mencionó en el inicio de la sección en cuestión:

> Supongamos que el número propuesto n sea par, por lo tanto, es una suma de dos números primos, y entonces $n-2$ también es una suma de dos números primos, por lo que n también es una de tres, y también cuatro, y así sucesivamente.

Lo que plantea Euler es que la veracidad de la relación binaria implica la descomposición de cualquier par en tantos primos como queramos. Ahora trataremos de reproducir el razonamiento de Euler:

Sea n un entero positivo par, como se asumió verdadera la relación binaria, entonces $n-2$ es suma de dos primos, esto es, $n-2 = p_1 + p_2$ y de aquí $n = 2 + p_1 + p_2$, entonces n es suma de tres primos. También lo es de cuatro, es decir, si n es par, entonces $n - 4$ es suma de dos primos, y por tanto $n - 4 = p_3 + p_4$ y en consecuencia $n = 4 + p_3 + p_4 = 2 + 2 + p_3 + p_4$ es suma de cuatro primos. Lo mismo sucede para cinco primos considerando que $n - 6$ es par. En general si n es par tenemos que $n-2r$ es par, por lo que $n-2r = p_i + p_j$, entonces $n = 2r + p_i + p_j$, por lo que $n = 2 + 2 + \cdots + 2 + p_i + p_j$, resultando en que n es suma de $r+2$ primos.

En la segunda parte de esta sección escribe:

> Pero si n es un número impar, entonces es una suma de tres números primos, ya que $n-1$ es la suma de dos, y se puede seguir resolviendo las demás sumas. Sin embargo, que todo número par sea la suma de dos números primos, lo que considero un teorema correcto, es algo que no puedo demostrar.

Aquí lo que Euler quiere es hacer notar que los impares también pueden ser escritos como suma de 3, 4, 5 o tantos primos como queramos, a partir de que los pares anteriores sean suma de dos primos. La justificación es semejante a la anterior: sea n entero positivo impar, por tanto $n - 1$ es suma de dos primos, es decir, $n - 1 = P_1 + P_2$, entonces $n = 1 + P_1 + P_2$.[35] También lo es de cuatro, esto es, $n-3$ es par, por tanto es suma de dos primos $n-3 = P_s + P_t$, entonces $n = 3 + P_s + P_t = 1 + 2 + P_s + P_t$. De la misma forma lo será de 5 primos, esto es, $n-5$ es par, por tanto es suma de dos primos $n - 5 = P_u + P_v$, entonces $n = 5 + P_u + P_v = 1 + 2 + 2 + P_u + P_v$. En general si n es impar, $n-2r+1$ es par, por lo que $n-2r+1 = p_x + p_y$, entonces $n = 2r+1+p_x + p_y$, por lo que $n = 1+2+2+\cdots+2+p_i + p_j$, resultando en que n es suma de $r+3$ primos.

Así, tenemos —por los dos últimos resultados— que todos los enteros positivos podrían ser escritos como suma de tres primos o más, siempre que los enteros pares pudieran ser escritos como suma de dos primos[36].

---

[35] Para este caso podríamos tomar cualquier primo impar P_r y restarlo a n, con lo cual obtenemos que $n - P_r$ es par, por tanto, $n = P_r + P_w + P_z$ es suma de tres primos.

[36] Aunque Euler ya no lo menciona, pero con un argumento semejante podríamos decir que si suponemos verdadera la terciaria para los pares entonces tenemos la representación binaria para ellos. La demostración es la siguiente:
Sea n par, y como Goldbach propone que todos los enteros son suma de tres primos entonces

$$n+2 = p + p_1 + p_2,$$

Con estos dos resultados se puede observar que, como ya lo dijimos, la verdadera *conjetura de Goldbach* nunca fue la representación binaria, pues se observa claramente que Euler le está contestando sobre la viabilidad de la descomposición sucesiva en primos. La representación binaria de los pares es un resultado que Euler supone verdadero y necesario para llevar a cabo su análisis, reconoce la complejidad de esta última suposición, ya que al final del párrafo escribe: "sin embargo, que todo número par es suma de dos primos, considero que es un teorema verdadero, aunque no puedo demostrarlo".[37]

Después de la respuesta de Euler no volvieron a tratar el tema después de junio de 1742 (de acuerdo con la información que se tiene hoy en día). Un problema parecido se vuelve a mencionar hasta la carta 165, del 16 de diciembre de 1752, cuando Euler le escribe a Goldbach lo siguiente:

> Encontré en mis papeles todavía otro teorema, el cual su excelencia me comunicó con anterioridad [en alguna ocasión]. A saber, que cualquier número imparmente par $4a + 2$ siempre será igual a una suma de 2 números primos de la forma $4n + 1$, como $6 = 1 + 5$, $10 = 5 + 5$, $14 = 1 + 13$, $18 = 1 + 17 = 5 + 13$, $22 = 5 + 17$, $26 = 13 + 13$, $30 = 1 + 29 = 13 + 17$, $34 = 5 + 29 = 17 + 17$, con lo cual observo que no solo ninguna excepción ocurre para números pequeños, si no que para números grandes se espera mucho menos alguna. Pues los números, en los cuales tal descomposición [disección] es posible de una sola manera, son: 2, 6, 10, 14, 22, 26, 38, 50, 62, 86 y a partir de aquí hasta 150 no hay ninguna más, tampoco hasta 230. De allí que para los que le siguen se espera mucho menos alguna, pues la cantidad de soluciones siempre aumenta, por lo que 210 se deja resolver de 9 formas.[38]

---

pero para que esta suma de tres primos genere un número par entonces uno de ellos tendría que ser par, por tanto, $p = 2$, y obtenemos que $n = p_1 + p_2$.

Que actualmente la que nos interesaría es que los impares en la *terciaria* implicara los pares en la *binaria*, pero hoy sólo contemplamos la *terciaria* para los impares, entonces, necesitaríamos que la *terciaria* en los impares implicara la *binaria* en los pares.

[37] Dass aber ein jeder numerus par eine Summa duorum primorun sei, halte ich für ein ganz gewisses Theorema, ungeacht ich dasselbe nicht demonstrieren kann.

[38] Este postulado es una versión más específica de la *conjetura de Goldbach*, esto es, que todos los números pares son suma de dos primos. Recordemos que esta versión de la conjetura es postulada por Euler en su carta del 30 de junio de 1742. Para este nuevo postulado ya no nos interesa cualquier número par, sino todo aquel parmente par que sea de la forma $4a + 2$, y por el lado de su representación en suma de primos, ya no nos interesa que sean dos primos cualesquiera, sino que ahora queremos que sean específicamente de la forma $4n + 1$. Notemos que Euler sigue considerando a la unidad como un número primo, pues en algunos de sus ejemplos el número uno es parte de la descomposición en primos, lo cual es consistente con esta nueva conjetura, pues la unidad cumple con ser de la forma $4n + 1$, a saber $4(0) + 1 = 1$.

Continúa observando que los números 2, 6, 10, 14, 22, 26, 38, 50, 62, 86 tienen una única representación como suma de primos de la forma $4n + 1$, pero después del 86 todo número imparmente par tiene al menos dos representaciones, aunque Euler solo llegó hasta el número 230. A continuación, hace notar que 210 tiene nueve representaciones distintas. Es importante notar que 210 se puede descomponer de diecinueve maneras distintas como suma de dos primos, pero solo nueve de ellas cumplen con la conjetura planteada, las otras diez resultan ser sumas de primos de la forma $4n + 3$. A continuación, dejaremos una tabla con las descomposiciones y las formas respectivas de sus primos:

Descomposición de 210 como suma de dos primos	**Forma de los primos en la descomposición**
$11 + 199$	$4n + 3$
$13 + 197$	$4n + 1$
$17 + 193$	$4n + 1$
$19 + 191$	$4n + 3$
$29 + 181$	$4n + 1$
$31 + 179$	$4n + 3$

Antes de terminar el análisis de esta parte de la carta 51, no podemos dejar de mencionar, atendiendo a un mayor rigor histórico, que antes de Goldbach, quien abordó el tema fue Descartes, al enunciar que todo número par es la suma de uno, dos o tres primos.

En 1770, Edward Waring publica sus *Meditationes Algebraicae*. En el problema 63, [Waring 1991, 362] habla de la representación de un número en diferentes formas, ya sea como un producto o como una suma de enteros. Después de dar algunos ejemplos, escribe: "Aquí es apropiado mencionar algunas propiedades de los enteros y de los números primos, 1) todo número par es suma de dos primos, y todo número impar es primo o suma de tres primos, [...]".

Desde luego, Waring no tenía por qué conocer el enunciado de Descartes, ni el contenido de las cartas entre Goldbach y Euler. En el primer caso, los manuscritos fueron publicados hasta 1908 y, en el segundo caso, las cartas se publicaron por primera vez en 1843. Lo mismo podríamos decir de Goldbach y Euler respecto a lo escrito por Descartes.[39]

Por lo tanto, continuando con el mismo rigor, quizá la *conjetura de Goldbach* debería llamarse la *conjetura de Descartes-Goldbach-Euler-Waring*.

Interpretaciones confusas

Desde principios del siglo XIX, las citas referentes a la conjetura han sido numerosas, y es sorprendente ver que la gran mayoría de los libros y artículos que mencionan la carta del 7 de junio de 1742, lo hacen alterando su contenido, y pocos mencionan y analizan la respuesta de Euler del día 30 del mismo mes. Ejemplo de ello son historiadores como Michael S. Mahoney [1981, 450], Günther Frei [1994, 825], Carl Boyer [1991, 457], entre otros; y matemáticos como Tom Apostol [1998, 9], Melvyn Nathanson [1996, 177] o Wang Yuan [1984, 1], entre otros.

En general, se menciona la *conjetura de Goldbach*, en sus modalidades *binaria* y *terciaria*, pero de una forma simplista y sacada del contexto de lo que verdaderamente pensaban Euler y Goldbach. Es decir, la manera como la formulan no corresponde a como fue pensada originalmente.

$37 + 173$	$4n + 1$
$43 + 167$	$4n + 3$
$47 + 163$	$4n + 3$
$53 + 157$	$4n + 1$
$59 + 151$	$4n + 3$
$61 + 149$	$4n + 1$
$71 + 139$	$4n + 3$
$73 + 137$	$4n + 1$
$79 + 131$	$4n + 3$
$83 + 127$	$4n + 3$
$97 + 113$	$4n + 1$
$101 + 109$	$4n + 1$
$103 + 107$	$4n + 3$

Euler desarrolla de manera más exhaustiva esta conjetura en su artículo *De inductione ad plenam certitudinem evehenda* publicado en 1784 (E556 en el índice *Eneström*).

[39] No se tiene exactamente una fecha de cuando Descartes comentó este resultado, se tiene que consultar la correspondencia que es donde se puede encontrar su observación. La correspondencia y este comentario de la conjetura se pueden estudiar en [Tannery 1996, 298].

Luego entonces, ¿Qué ha sucedido? ¿La inercia de repetir verdades a medias hace que con los años se arraiguen a tal grado que después ya se toman como verdades incuestionables? La alteración no está en haber modificado solamente la cota inferior de validación de la conjetura, pues el uno ya no es considerado como primo, ésta va más allá como ya se expuso en las secciones anteriores.

Pretextar que la información ha sido de difícil acceso no es justificación suficiente, pues la primera edición de las cartas se publicó en 1843 y la edición alemana en 1965. Además, desde los años 30 ya se contaba con el artículo de Ralph Archibald [1935], en el que se reproducen las citas textuales de la conjetura y de la respuesta de Euler, a partir de la edición de 1843. Por otro lado, en 1969, D. Struik [1969] publicó su *Source Book*[40]. Por todo lo anterior, se hace evidente la total indiferencia hacia la lectura de las cartas originales o de los artículos como los de Archibald, que, si bien pueden ser cuestionables, también son útiles para conocer la fuente original y así entender cuál fue la verdadera conjetura.

[40] Adicionalmente podemos mencionar otros ejemplos donde el manejo de la información se triangula a tal grado que los errores ya ni siquiera se perciben, por ejemplo: en el artículo de Archibald se encuentra la trascripción original —en la mezcla de latín-alemán— de la edición francesa de 1843, así como su traducción al inglés; Struik en su libro parece que ya no recurrió totalmente a los originales por sus mismas referencias a las citas —entre ellas a Archibald—, aquí al final podemos encontrar un error de la cita de Struik a la carta de Euler del 30 de junio, cuando Struik se refirió a la conjetura mencionó "However, that every number is a sum of two primes, [...]", cuando debe de decir "However, that every even number is a sum of two primes, [...]".

VII. Los últimos fragmentos

Después del pasaje de la conjetura que se expuso en el Capítulo VI, Goldbach termina su carta con tres elementos matemáticos que fueron de breve trascendencia entre ellos, en el momento que se escribió la carta. Posiblemente, los problemas planteados a continuación formaban parte de algunos paradigmas que no quedaron explícitos en la carta de Goldbach. A continuación, presentamos cada uno de los problemas.

Primer fragmento

El primer elemento se enuncia en la carta 51 de esta manera:

> Si v es una función de x, tal que $v = c$ es un número cualquiera, se puede determinar a x de c y del resto de las constantes expresadas en la función. Entonces se puede determinar el valor de x en la ecuación $v^{2n+1} = (2v+1)(v+1)^{n-1}$.

El planteamiento de Goldbach no es del todo claro, parece que se refiere a encontrar valores de v para que se cumpla la igualdad $v^{2n+1} = (2v+1)(v+1)^{n-1}$ o, dicho de otra manera, encontrar raíces del polinomio $v^{2n+1} - (2v+1)(v+1)^{n-1} = 0$. Esto lo podemos deducir por la respuesta de Euler en la carta 52:

> El teorema de su excelencia, que si es posible encontrar la raíz x de la ecuación $v = c$, para una función v de x, entonces también es posible determinar el valor de x en la ecuación $v^{2n+1} = (2v+1)(v+1)^{n-1}$. Me costó mucho esfuerzo averiguar, hasta que finalmente me di cuenta, que esta ecuación $v^{2n+1} - (2v+1)(v+1)^{n-1} = 0$ es divisible por $vv - v - 1$. Entonces se tiene que $v^{2n+1} - (2v+1)(v+1)^{n-1} = v(v^{2n} - (v+1)^n) + (vv - v - 1)(v+1)^{n-1}$, y $v^{2n} - (v+1)^n$ es divisible por $vv - v - 1$. Por lo tanto, para cualquier n la ecuación $v^{2n+1} = (2v+1)(v+1)^{n-1}$ es satisfecha por $vv = v + 1$, y también por $v = \frac{1 \pm \sqrt{5}}{2}$, así es posible encontrar la raíz x de esta ecuación por hipótesis.

Después de analizar la carta de la respuesta de Euler podemos interpretar y complementar el contenido, y ahora lo presentamos.

Como ya se mencionó, se quiere encontrar raíces del polinomio

$$v^{2n+1} - (2v+1)(v+1)^{n-1} = 0 \ldots (1)$$

Primero se toma el segundo sumando y se reescribe de esta manera:

$$\begin{aligned} -(2v+1)(v+1)^{n-1} &= -(-v^2 + v^2 + v + v + 1)(v+1)^{n-1} \\ &= -(-v^2 + (v+1) + v(v+1))(v+1)^{n-1} \\ &= (v^2 - (v+1) - v(v+1))\,(v+1)^{n-1} \\ &= (v^2 - v - 1)(v+1)^{n-1} - v(v+1)(v+1)^{n-1} \end{aligned}$$

Se sustituye en (1) y se tiene que:

$$\begin{aligned} v^{2n+1} - (2v+1)(v+1)^{n-1} &= v^{2n+1} + (v^2 - v - 1)(v+1)^{n-1} - v(v+1)(v+1)^{n-1} \\ &= v^{2n+1} + (v^2 - v - 1)(v+1)^{n-1} - v(v+1)^n \\ &= v(v^{2n} - (v+1)^n) + (v^2 - v - 1)(v+1)^{n-1} \\ &= 0 \end{aligned}$$

Por otro lado, el segundo factor del primer sumando $v^{2n}-(v+1)^n=(v^2)^n-(v+1)^n$ es divisible por $v^2-(v+1)=v^2-v-1$, pues en general se cumple que $x-y|x^n-y^n$, para toda $n\in\mathbb{Z}^+$. Entonces

$$v^2-(v+1)|(v^{2n}-(v+1)^n)$$

Por lo tanto, la ecuación original $v^{2n+1}-(2v+1)(v+1)^{n-1}$ es divisible por v^2-v-1, entonces

$$v^{2n+1}-(2v+1)(v+1)^{n-1}=(v^2-v-1)g(v),$$

para una $g(v)$ que es el otro polinomio de la factorización.

Lo que llama la atención y, Euler lo señala, es que las raíces de v^2-v-1 están vinculadas a φ, el número áureo, es decir, $\varphi=\frac{1\pm\sqrt{5}}{2}$.

Finalmente, en la carta 53, del 30 de julio de 1742, Goldbach respondería con un pequeño comentario sobre lo desarrollado por Euler, pero éste no agregaría más detalles relevantes a la discusión:

> Lo que había escrito sobre $v^{2n+1}=(2v+1)(v+1)^{n-1}$ fue solamente basado al considerar al número $\frac{1\pm\sqrt{5}}{2}$, sin sospechar que la ecuación podría ser dividida, lo cual, como ahora veo, es indispensable en casos semejantes.

Con esto termina el intercambio de ideas para este problema, no tenemos más información, por el momento, para saber dónde encaja esta reflexión de Goldbach y la respuesta de Euler.

Segundo fragmento

El problema que Goldbach le comunica a Euler es sobre la serie

$$\sum_{i=1}^{\infty}\frac{x^n}{x\cdot 2^{2n}}$$

El fragmento original de la carta 51 es el siguiente:

> Si se concibe la curva, cuya abscisa es x, con ordenada la suma de la serie $\frac{x^n}{n\cdot 2^{2n}}$, donde n representa el exponente del término, es decir, la ordenada $=\frac{x}{1\cdot 2^2}+\frac{x^2}{2\cdot 2^4}+\frac{x^3}{3\cdot 2^6}+\frac{x^4}{4\cdot 2^8}$ etc., esto es, si la abscisa fuera $=1$, la ordenada sería $=\frac{1}{3}$
>
> 2. …………………… $l2$
>
> 3. …………………… $2l2$
>
> 4 o mayor ………… infinito.

Lo que Goldbach muestra es que comienza a darle valores a la abscisa x, argumentando que: si $x=1$, entonces la ordenada sería igual a $y=\log\left(\frac{4}{3}\right)=\frac{1}{3}$; si $x=2$, entonces $y=\log(2)$; si $x=3$, $y=2\log(2)$; y por último, si $x\geq 4$, entonces se indefine nuestra serie.

Es de notar que Euler escribe un pequeño comentario al margen de la carta respecto al caso de $x = 1$, es el siguiente:

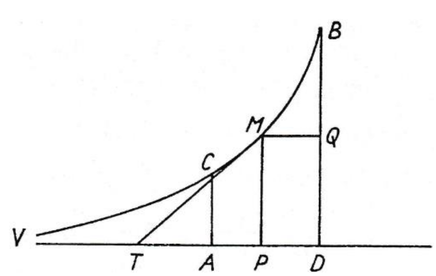
> [si la abscisa fuera $= 1$, la ordenada sería $= \frac{1}{3}$]$= l\left(\frac{4}{3}\right)$. Si la ordenada $= y$ se tiene que $y = l\left(\frac{4}{4-x}\right)$.

Con esto podemos observar que los valores que Goldbach obtiene provienen de la expresión $y = \log\left(\frac{4}{4-x}\right)$, pues si verificamos para cada caso tendremos lo siguiente:

- Si $x = 1$, entonces $y = \log\left(\frac{4}{4-x}\right) = \log\left(\frac{4}{4-1}\right) = \log\left(\frac{4}{3}\right)$.
- Si $x = 2$, entonces $y = \log\left(\frac{4}{4-x}\right) = \log\left(\frac{4}{4-2}\right) = \log\left(\frac{4}{2}\right) = \log(2)$.
- Si $x = 3$, entonces $y = \log\left(\frac{4}{4-x}\right) = \log\left(\frac{4}{4-3}\right) = \log\left(\frac{4}{1}\right) = \log(4) = \log(2^2)$ $= 2\log(2)$.
- Si $x = 4$, entonces $y = \log\left(\frac{4}{4-x}\right) = \log\left(\frac{4}{4-4}\right) = \log\left(\frac{4}{0}\right)$, lo cual no está definido.

Aquí parece haber un problema, pues si observamos lo comunicado por Goldbach y lo comparamos con la nota de Euler podemos encontrar una discrepancia en el caso de $x = 1$. Verificando el valor de esta expresión podemos notar que éste vale 0.287682 ... y no $\frac{1}{3}$ como afirma Goldbach. Esto podemos verificarlo en la carta 52, donde Euler construye la curva logarítmica $y = \log\left(\frac{4}{4-x}\right)$ geométricamente y corrigiendo a Goldbach de su error al final del fragmento:

> Si se concibe [la curva], cuya abscisa $= x$, con ordenada $y = \frac{x}{1\cdot 2^2} + \frac{x^2}{2\cdot 2^4} + \frac{x^3}{3\cdot 2^6} + \frac{x^4}{4\cdot 2^8}$ +etc, que en general es $y = l\frac{4}{4-x}$, por lo que la curva es logarítmica, en donde la ordenada se vuelve la asíntota, cuando $x = 4$. Sea VCB una logarítmica ordinaria que tiene asíntota VD, cuya subtangente constante es $AT = 1$. Tomando la ordenada $AC = 1$, y cualquier otra PM, sea $AP = t$ y $PM = u$, se tiene $t = lu$ o bien $udt = du$. Ahora considere la ordenada $DB = 4AC = 4$, se tiene $AD = l4$, y juntando MQ se tiene $BQ = x$ y $QM = y$ para el caso propuesto. En efecto $AP = t = l4 - y$ y $PM = u = 4 - x$, y como $t = lu$, entonces $l4 - y = l(4 - x)$ y $y = l\frac{4}{4-x}$. Por otra parte, su excelencia escribió $\frac{1}{3}$ para la suma de la serie que es igual a y, para el caso $x = 1$, pero esta suma es $= l\frac{4}{3}$.



Parece que lo importante de este problema es que ambos estaban en el canal del estudio de las series y en particular la que representa a $y = \log\left(\frac{4}{4-x}\right)$ que es

$$= \frac{x}{1 \cdot 2^2} + \frac{x^2}{2 \cdot 2^4} + \frac{x^3}{3 \cdot 2^6} + \frac{x^4}{4 \cdot 2^8} + \cdots + \frac{x^n}{4 \cdot (2^2)^n} + \cdots.$$

Sabemos del gran trabajo de Euler en el tema de las series, pero este problema no lo tocó nuevamente con Goldbach en la correspondencia que se conoce.

Tercer fragmento

El último problema de la carta ya no es un planteamiento, es más bien un comentario de Goldbach sobre dos proposiciones que Euler escribió el 8 de mayo de 1742, en la carta 50. En ella Euler enuncia que $3a^2 + 3b^2 + 7c^2$ y $2a^2 + 6b^2 + 21c^2$ no pueden ser cuadrados. A continuación, dejaremos el fragmento original

> Este teorema se parece en cierto modo al de *Fermat*[41], que $pp + qq + rr + ss$ produce todos los números posibles. Tengo muchos más teoremas similares, como que $3aa + 3bb + 7cc$ nunca puede ser un cuadrado. Además $2aa + 6bb + 21cc$ no puede ser un cuadrado, y parecidos. Más no he podido encontrar ninguna fórmula similar que contenga 4 letras independientes la una de la otra.

Cabe señalar que Euler no proporciona más comentarios ni elementos de una demostración. Goldbach en la carta sólo le comenta que no ha podido explorar adecuadamente este problema y le escribe lo siguiente:

> P. S. Ambas fórmulas de números no cuadrados, de las que usted hace mención, aún no las examino, creo sin embargo, que así mismo, cuando uno pone $a = hx + k$, $b = lx + m$, $c = nx + p$ bien pudiesen bajo la siguiente fórmula clasificarse, donde quiera que f, g, γ, δ son números enteros
>
> $$\begin{array}{lll}(2f - 4\gamma\delta)x^2 + 4(f - 2\gamma\delta)(2g - \delta^2)x + (2g - \delta^2)^2 \\ \quad -4\gamma^2 \qquad\qquad\qquad\qquad -2f \qquad\qquad -2g\end{array}$$
>
> pues estos nunca pueden dar un cuadrado.

Este comentario de Goldbach no da elementos para comprender qué es lo que le quiso trasmitir. Para este comentario de Goldbach no se encuentra una respuesta de Euler, posiblemente él tampoco captó el fondo del comentario y ya no le contesto más al respecto.

[41] Euler hace referencia al problema que propone Fermat de que todo entero es una suma de cuatro cuadrados, resultado que posteriormente Lagrange demostrará con toda la formalidad.

Conclusión

El objetivo de este trabajo de tesis fue el de analizar qué significó para Euler y Goldbach el problema que hoy conocemos como *conjetura de Goldbach*. Estudiamos la carta del 7 de junio de 1742 que contiene la mencionada conjetura. Mostramos que dicha carta está repartida en seis pasajes matemáticos. Después de hacer una detallada revisión de cada uno de los seis elementos matemáticos, encontramos que la mayoría tenían un antecedente que incluso se remonta a varios años atrás e incluso varios hacia delante de la famosa conjetura. Encontramos que la carta tiene elementos que se relacionan con el *pequeño teorema de Fermat*, Números Complejos, Funciones Trascendentes, Sumas de Cuadrados, entre otros temas.

La mayoría de los pasajes estudiados de la carta llegaron a resultados explícitos que se publicaron en artículos y algunos terminaron en los libros que Euler publicó, entre ellos, el *Introductio in analysin infinitorum*.

Por otro lado, el pasaje donde reside la conjetura no tenía un antecedente al 7 de junio de 1742. Lo que propuso Goldbach fue una idea totalmente nueva, obteniendo la respuesta de Euler en la carta siguiente, del 30 de junio de 1742. En la respuesta básicamente le señala que la parte de la conjetura que hoy conocemos como *binaria*, es un resultado que parece ser verdadero pero que no le es posible demostrar en ese momento. Esto fue todo lo que se intercambió entre ellos respecto al pasaje de la conjetura, no encontramos una carta más, excepto éstas dos.

Ahora, podemos concluir que la conjetura no significo prácticamente nada entre ellos, fue un problema más, como los hubo otros, que no trascendieron en sus intereses. Los que le dieron la relevancia para que poco a poco se convirtiera en un problema de mayor interés fueron otros, entre ellos Edward Waring en la *Miscellanea Analytica*.

Actualmente se percibe de manera imprecisa que la conjetura fue el gran producto de la larga comunicación en Euler y Goldbach, pero gracias al estudio realizado podemos concluir en la tesis que esto no es así. El intercambio entre ellos fue de una riqueza matemática enorme que aún merece seguir siendo estudiada.

Apéndice A[42]

Demostración del *teorema de la suma de dos cuadrados de Fermat* de que todo primo de la forma $4k + 1$ es una suma de dos cuadrados.

***Lema* A.1** (*de Diofanto*) El producto de dos sumas de dos cuadrados cada una es también suma de dos cuadrados, y puede ser de dos maneras diferentes.

Demostración: Si $m = a^2 + b^2$ y $n = c^2 + d^2$, entonces

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

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

Se puede ver de manera conjunta como

$$mn = (a^2 + b^2)(c^2 + d^2) = (ac \pm bd)^2 + (ad \mp bc)^2. \blacksquare$$

***Lema* A.2** 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*[43] nos indica que[44] $\left(\frac{-1}{p}\right) = 1$, es decir, -1 es residuo cuadrático módulo 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 (nos referiremos al sistema como SCR de ahora en adelante). 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 efectivamente $m < p$, 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 $m < p$. $\blacksquare$

***Teorema* A.3** (*de la suma de dos cuadrados de Fermat*) Si $p \equiv 1\ (mod\ 4)$ y es primo, entonces p puede ser expresado como suma de dos cuadrados.

Demostración: Por **A.2** 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 SCR módulo m, entonces existen a, b en el SCR tal que

$$a \equiv x\ (mod\ m) \text{ y } b \equiv y\ (mod\ m) \ldots (1)$$

donde

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

[42] Las demostraciones de este apéndice están escritas con base en el trabajo de [Ramírez. 2015].
[43] 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.
[44] Se usa el resultado el cual postula que si $p \equiv 1\ (mod\ 4)$, entonces existe x tal, que $x^2 \equiv -1\ (mod\ p)$, y en consecuencia $\left(\frac{-1}{p}\right) = 1$.

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 **A.1**, tenemos que

$$(a^2 + b^2)(x^2 + y^2) = (ax + by)^2 + (ay - bx)^2 \ldots ③^{45},$$

y esto nos lleva a que

$$(a^2 + b^2)(x^2 + y^2) = (mk)(mp) = m^2kp \ldots ④.$$

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 $b \equiv y\ (mod\ m)$, tenemos de igual manera que $by \equiv y^2\ (mod\ m)$, entonces

$$ax + by \equiv x^2 + y^2 \equiv 0\ (mod\ m) \ldots ⑤.$$

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

$$ay - bx \equiv xy - xy \equiv 0\ (mod\ m) \ldots ⑥.$$

De ⑤ y ⑥ 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 sabemos que $a, b \leq \frac{m}{2}$. 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 $mk \leq \frac{m^2}{2} < m^2$, 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.

Así, si $k = 0$, entonces $a^2 + b^2 = mk = 0$, y se tendría que $a = b = 0$, y por ① tenemos que $x \equiv y \equiv 0\ (mod\ m)$; 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 **A.2** 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, $mp = 1 \cdot p = p = x^2 + y^2$. ■

[45] Tomamos una de las dos opciones en los signos de lo planteado en **A.1**.

Bibliografía

Álvarez, Carlos y Dhombres, Jean. 2011. *Une histoire de l'imaginaire mathématique. Vers le théorème fondamental de l'algèbre et sa démonstration par Laplace en 1795*. Ed. Hermann. Francia.

Apostol, Tom. 1998. *Introduction to Analytic Number Theory*. New York: Springer-Verlag.

Archibald, Ralph. 1935. "Goldbach's Theorem". *Scripta Mathematica*. **3**: 44-50, 153-161.

Bedós, Ph. 1852. "Question 248 (Goldbach)". *Nouvelles annales de mathématiques 1re série*, Tome 11, pp. 278-280.

Boyer, Carl. 1991. *A History of Mathematics.* NJ: John Wiley & Sons.

Dickson, Leonard. 1919. *History of the Theory of Numbers*. Washington: Carnegie Institution of Washington.

Euler, Leonhard. 1738, E26 "Observationes de theoremate quodam Fermatiano aliisque ad numeros primos spentactibus". *Commentarii academiae scientiarum Petropolitanae*, Tomus 6, pp. 103-107. (Traducción de David Zhao).

Euler, Leonhard. 1740, E863c3. "Seventeen letters from Euler to Johann I Bernoulli, 1727-1740". *Euler Archive - All Works*, pp. 73-77.

Euler, Leonhard. 1741, E54 "Theorematum quorundam ad numeros primos spectantium demonstration". *Commentarii academiae scientiarum Petropolitanae*, Tomus 8, pp. 141-146. (Traducción de David Zhao).

Euler, Leonhard. 1748, E101. *Introductio in analysin infinitorum*, Tomus Primus. Lausana: Marcum-Michaelem Bousquet & Socios. (Traducción de John D. Blanton).

Euler, Leonhard. 1748, E102. *Introductio in analysin infinitorum*, Tomus Secundus. Lausana: Marcum-Michaelem Bousquet & Socios. (Traducción de John D. Blanton).

Euler, Leonhard. 1750, E134 "Theoremata circa divisores numerorum". *Novi Commentarii academiae scientiarum Petropolitanae*, Tomus 1, pp. 20-48. (Traducción de David Zhao).

Euler, Leonhard. 1760, E242. "Demonstratio theorematis Fermatiani omnem numerum sive integrum sive fractum esse summam quatuor pauciorumve Quadratorum". *Novi Commentarii academiae scientiarum Petropolitanae*, Tomus 5, pp. 13-58.

Euler, Leonhard. 1761, E262. "Theoremata circa residua ex divisione potestatum relicta". *Novi Commentarii academiae scientiarum Petropolitanae*, Tomus 7, pp. 49-82. (Traducción de Jordan Bell).

Euler, Leonhard. 1784, E556 "De inductione ad plenam certitudinem evehenda". *Acta Academiae Scientiarum Imperialis Petropolitanae*, Tomus 2, pp. 38-48.

Frei, Günther. 1994. "Number Theory. Contenido en: Grattan-Guinness, I. (Edt). *Companion Encyclopaedia of the History and Philosophy of the Mathematical Sciences*. 2 Vols. London: Routledge, 1st ed.

Fuss, P. H. 1843. *Correspondance mathématique et physique de quelques célèbres géometrès du XVIIIème siècle*, Tome I. St. Pétersbourg.

Fuss, P. H. 1843. *Correspondance mathématique et physique de quelques célèbres géometrès du XVIIIème siècle*, Tome II. St. Pétersbourg.

Gauss, Carl F. 1965. *Disquisitiones Arithmeticae*. Yale University Press-New Haven and London.

Genocchi, Angelo. 1853. "Demonstration d'un théorème d'Euler (voir t. XI, p. 327)". *Nouvelles annales de mathématiques 1re série*, Tome 12, pp. 235-236.

Goldbach, Christian. 1717. "Excerptae e litteris C. G. ad *** Regiomonte datis". *Acta Eruditorum, Supplementa*, Tomus 6, pp. 471-472.

Goldbach, Christian. 1738. "Criteria quaedam aequationum quarum nulla radix rationalis est". *Commentarii Academiae Scientiarum Imperialis Petropolitanae*, Tomus 6, pp. 98-102.

Gronau, Detlef. 2003. "Why is the gamma function so as it is." *Teaching Mathematics and Cumputer Science*. Vol.1 #1, pag 43-53.

Guevara Bravo, J. César y Ojeda Uresti, Juan. 2006. "¿Formuló Goldbach la conjetura de Goldbach? ". *Ciencias* 81, enero-marzo, pp. 72-79.

Juškevič, A. P. & Kopelevič, J. Kh. 1994. *Chrisitan Goldbach 1690-1764*. Vita mathematica, Band 8. Berlin: Birkhäuser Verlag.

Juškevič, A. P. & Winter, E. 1965. *Leonhard Euler und Christian Goldbach. Briefwechsel 1729-1764*. Berlin: Akademie-Verlag.

Koch, Helmut. 2007. "Der Briefwechsel von Leonhard Euler und Christian Goldbach". *Elemente der Mathematik*, Band 62. ETH Zürich.

Mahoney, Michael. 1981. "Christian Goldbach". Contenido en: Dictionary of Scientific Biography. Vol. 5. C. Gillispie (Editor). New York: Charles Scribner´s Sons.

Nathanson, Melvyn B. 1996. *Additive Number Theory The Classical Bases*. New York: Springer Verlag.

Richstein, J. 2001 "Verifying the Goldbach Conjecture up to 4×10^{14}". Math. Comput. 70: 1745-1750.

Ramírez A., José Luis. 2015. *Origen y primeros problemas de la teoría aditiva de los números*. Tesis de Licenciatura, Universidad Nacional Autónoma de México, TESIUNAM.

Sobrevilla Moreno, Pedro José. 2012. *Los primeros trabajos de Euler sobre algunos teoremas de Fermat y otros acerca de la teoría de números*. Tesis de Licenciatura, Universidad Nacional Autónoma de México, TESIUNAM.

Struik, Dirk. 1969. *A Source Book of Mathematics, 1200-1800*. Cambridge, Massachusetts: Harvard University Press.

Tannery, Adam y Tannery, Paul. 1996. *Oeuvres de Descartes*. Tomo X. Pag. 298. París: Librairie Philosophique J. Vrin.

Torres Villa, Mauricio. 2012. *El fundamento inductivo de la aritmética*. Tesis para obtener el doctorado en filosofía de la ciencia. Director: Carlos Álvarez Jiménez. Universidad Nacional Autónoma de México.

Wang Yuan (Edt). 1984. *Goldbach Conjecture*. Singapore**:** World Scientific Pub.

Waring, Edward. 1991. *Meditationes Algebraicae*. Rhode Island: American Mathematical Society.

Zaldívar, Felipe. 2007. *Fundamentos de Álgebra*. México: Fondo de Cultura Económica.

Zaldívar, Felipe. 2012. *Introducción a la teoría de números*. México: Fondo de Cultura Económica.