UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE CIENCIAS

Los primeros trabajos de Euler sobre algunos teoremas de Fermat y otros acerca de la teoría de números.

T E S I S

QUE PARA OBTENER EL TÍTULO DE:

Matemático

P R E S E N T A :

Pedro José Sobrevilla Moreno

DIRECTOR DE TESIS:
Mat. Julio César Guevara Bravo
2012

Índice General

INTRODUCCIÓN

Cuando se revisan de manera superficial las aportaciones culturales de los individuos de una comunidad, es frecuente que no se perciba lo importantes y fructíferas que éstas fueron. En ocasiones se identifican sólo algunos pasajes de sus contribuciones, y si bien pueden ser importantes, tampoco implica que sean los únicos o los más trascendentes. El riesgo que se corre cuando sólo se popularizan algunas aportaciones en la vida de las personas, es perder partes importantes que pueden proporcionar datos fundamentales para comprender mejor cómo se desarrollaron las vidas de los individuos, tanto en el ámbito personal como en el académico.

En el caso de la ciencia pasa algo semejante, y nos referimos a que el desarrollo de las teorías científicas generalmente no se gesta de manera aislada o casi espontánea.[1] Los practicantes de estas disciplinas por lo menos intercambian comentarios con algunos de sus colegas y escriben versiones preliminares de sus resultados.

Pero si se da el caso de que en alguna investigación histórica no se recurre a la mayoría de las fuentes aportadas por algún autor, entonces puede pasar que sólo algunos de sus resultados científicos alcancen cierta popularidad en tanto que otros no. Una consecuencia de lo señalado es que se empieza a crear una imagen de que lo importante en el trabajo intelectual de ciertos autores se restringe sólo a eso resultados famosos. Y más aún, cuando

[1] Por ejemplo, tenemos el caso de Galois, de cuya vida existen múltiples versiones que están a nivel de entretenidas narraciones noveladas, en las que se menciona que escribió todas sus ideas referentes a las matemáticas durante la noche previa al duelo en el que perdió la vida.

vemos uno de sus trabajos publicados no podemos saber cuáles fueron los intercambios de ideas previas entre los individuos involucrados, y es porque sólo podemos ver el trabajo final.

El caso que aquí trataremos gira en torno de los primeros trabajos sobre teoría de los números de Leonhard Euler. Actualmente, cuando se estudian las aportaciones de Euler a la teoría de los números, se hace tomando como referencia escritos modernos, ya sea libros o artículos de revistas especializadas, y éstos generalmente son presentados como ejemplos de los estándares de rigor de lo que hoy entendemos como demostrar en matemáticas. Aquí, en el trabajo de tesis, lo que nos interesa es regresar a los artículos originales de Euler y a partir de ellos entender cómo se gestaron sus primeras aportaciones a la teoría de los números. Con este enofoque se podrá entrever cómo se desarrollaron los resultados que podemos encontrar en los libros actuales, pero expuestos de manera generalmente diferente a los trabajos originales.

Al recurrir a los artículos originales y a la correspondencia, es posible conocer las relaciones que mantuvo Euler con diversos personajes de su época,[2] así como los trabajos relevantes de la teoría de los números, y no

[2]Esto es relevante porque su relación con otros personajes se puede reconstruir a través de la correspondencia, y es ahí donde se puede encontrar parte de las claves para entender el génesis de diversas teorías. Y para el caso de la teoría de los números es fundamental la relación de intercambio matemático que se dio entre Euler y Christian Goldbach. Además del interés por tratar de entender los primeros trabajos de Euler nos parece importante mostrar en esta tesis que el intercambio matemático entre ellos no se puede restringir a pensar que prácticamente lo único que se dio es lo correspondiente al pasaje de lo que hoy conocemos como conjetura de Goldbach. Consideramos que es importante mostrar una parte de lo fructífero y trascendente que fue su intercambio de ideas matemáticas.

quedarse sólo con aquellos que son los más conocidos.

Sabemos del interés de Euler por la teoría de los números desde su llegada a San Petersburgo, invitado por Pedro el Grande y Catalina I. A las pocas semanas de llegar conoció a Christian Goldbach y la relación entre ellos fue duradera. Por la correspondencia que ha llegado a nuestros días, ahora nos podemos enterar que desde finales de 1729 ellos empezaron a tener una comunicación escrita muy fructífera desde el punto de vista matemático. Al revisar los inicios de la correspondencia se puede entender cuales fueron las inquietudes que llevaron a Euler a escribir el primer trabajo sobre teoría de los números,[3] y nos referimos al *Observationes de theoremate quodam Fermatiano aliisque ad numeros primos spectantibus*.[4] Este artículo es el punto de partida del trabajo de tesis, cuyo objetivo es estudiar los temas que ahí se desarrollan, y a partir de ellos investigar hasta donde es que Euler logró profundizar –a través de otros trabajos- sobre cada uno de ellos. Para alcanzar dicho objetivo la tesis se sustenta principalmente en los artículos originales en los que Euler trató de alguna manera los mismos temas que en E26.

A continuación se presenta una breve exposición del contenido de cada capítulo que contiene esta tesis.

[3]Es importante mencionar que toda la correspondencia conocida entre ellos cubre diversos temas, y que cada una de las cartas contiene varios puntos sobre cuestiones matemáticas.

[4]*Observaciones sobre teoremas que Fermat y otros sobre números primos.* A partir de aquí nos referiremos a los trabajos de Euler por la clasificación hecha por Gustav Eneström, que enlista todos los artículos escritos por Euler de 1 a 866. Para el caso del artículo mencionado es E-26. El archivo completo se puede consultar en: www.eulerarchive.org

- En el primer capítulo se hace un análisis de los tres temas centrales del primer artículo de Euler en teoría de números (E26), y son los siguientes: Primero se trata el argumento para deducir que el quinto número de Fermat ($2^{2^5}+1$) no es primo; después se describen ciertos resultados que Euler encontró acerca de números perfectos, además de la descripción que hace sobre el pequeño teorema de Fermat y, finalmente, se revisan los teoremas que presentó al final del artículo, pero que no demostró.

  En los siguientes capítulos se lleva a cabo el estudio de la trascendencia de las propuestas planteadas por él en E26.
- En el segundo capítulo se retoman los números de Fermat, tema que Euler trató en tres artículos, además de E26. Se hará un análisis de cada uno de ellos, pero sobre todo del segundo *Theoremata circa divisores numerorum*[5], que es en realidad el primero, en donde explica cómo es que encontró el divisor del quinto número de Fermat. Además se agregará una demostración moderna de este hecho.
- En el tercer capítulo se tratan los números perfectos, sobre todo la demostración de Euler donde exhibe que todo número perfecto par tiene que ser de la forma euclidiana. Al final se anexa un apéndice en el que se detalla la demostración de Euclides de este resultado.
- En el cuarto capítulo se estudian los trabajos de Euler sobre el pequeño teorema de Fermat, tema que trató principalmente en tres

[5] *Teoremas sobre divisores de números*, con la clasificación E134.

artículos, seleccionados para ser analizados porque cada uno de ellos proporcionó una demostración diferente. En los trabajos la prueba del pequeño teorema pareciera el objeto perfecto a través del que se pudieron mostrar avances en la construción de la teoría de números.

- Finalmente, en el quinto capítulo, se presenta un tema que está totalmente vinculado con el cuarto capítulo. Se trata de la generalización del pequeño teorema de Fermat (conocido actualmente como teorema de Euler-Fermat). Además del estudio de la demostración se hace una revisión de algunos teoremas que se encuentran en el artículo *Theoremata arithmetica nova methodo demonstrata* (E271) en el que Euler desarrolla la teoría de residuos. Y para terminar se agregan algunos resultados modernos sobre la función ϕ de Euler.[6]

[6] Esta función se refiere a que un entero positivo n tiene $\phi(n)$ enteros positivos menores o iguales a él, y que son primos relativos con n.

Capítulo I

El encuentro con Christian Goldbach

Ya se mencionó en la introducción que el interés de Euler por la teoría de los números surgió -por lo menos en un sentido- desde 1729 a partir de su cercanía con Christian Goldbach[7] que inició cuando llegó a San Petersburgo. En 1732 el producto de las primeras reflexiones que iniciaron con Goldbach se reflejó en las *Observaciones sobre teoremas que...* (E26). Como uno de los objetivos de la tesis es estudiar la trascendencia de sus primeras proposiciones, entonces es conveniente revisar las primeras comunicaciones con Goldbach para así entender cómo se originaron las ideas vertidas en el artículo arriba señalado.

La primera carta entre ellos fue del 13 de octubre de 1729 y la escribió Euler. La inició con un comentario sobre una de las ideas que había utilizado para el cálculo del factorial de valores fraccionarios o irracionales de la expresión convergente

$$\frac{1\cdot 2^m}{1+m}\cdot\frac{2^{1-m}\cdot 3^m}{2+m}\cdot\frac{3^{1-m}\cdot 4^m}{3+m}\cdot\frac{4^{1-m}\cdot 5^m}{4+m}\cdot\ldots=$$

$$\left[\left(\frac{2}{1}\right)^m\frac{1}{1+m}\right]\left[\left(\frac{3}{2}\right)^m\frac{2}{2+m}\right]\left[\left(\frac{4}{3}\right)^m\frac{3}{3+m}\right]\ldots,$$

[7] A la muerte de Catalina I de Rusia en 1727, el nuevo Zar Pedro II designó a Christian Goldbach (1690-1764) asesor de su prima Ana Ivanovna de Courland. A la muerte de Pedro II en 1730, Goldbach siguió al servicio de Ana —la sucesora al trono—, y en 1732 fue nombrado secretario de la *Academia de Ciencias de San Petersburgo*, posteriormente, en 1737 junto con Johann Schumacher, se hizo cargo de su administración.

misma que le generaba valores semejantes a los que obtenía Daniel Bernoulli con la serie hipergeométrica.

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 creada con métodos de integración, y así Euler consideró los trabajos de Newton y Wallis, y en especial usó la integral de Wallis $\int_0^1 x^{\frac{p}{q}}(1-x)^n dx$ como punto de partida para su estudio. También es importante mencionar que le recomendó consultar lo expuesto por Christian Wolff en su *Elementa Matheseos Universae*.

Después de que Goldbach terminó con sus comentarios a la fórmula antes expuesta, y casi para concluir la carta, escribió en el último párrafo lo siguiente:

> *¿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.*

A partir de este pequeño párrafo Euler dio inicio a toda una vida de extraordinarias aportaciones a la teoría de los números.

La respuesta de Euler sobre este particular llegó el 8 de enero de 1830, mencionando que aún no tenía una solución para los posibles primos de Fermat. Pero los dos años siguientes Euler mostró un gran interés ya no sólo en los posibles divisores de los números de la forma $2^{2^n}+1$, sino que además su visión del problema se dirigió al estudio general de los divisores

de los números con las representaciones $a^n \pm 1$ y $a^n \pm b^n$.

El primer artículo

Antes de adentrarnos en proporcionar un panorama general del artículo (E26) de 1832, es apropiado señalar algunas de las características de sus publicaciones. En la época de Euler el rigor de los editores y la forma en la que se exponía la matemática era diferente a lo que es ahora. Por un lado, no se exigía que todos los resultados fueran probados de manera tan rigurosa; por el otro, era posible publicar resultados matemáticos en los que sólo se daba a conocer el enunciado sin ninguna demostración; además, los artículos no eran siempre monotemáticos, y en el caso de Euler, uno de ellos podía contener diversas vertientes aunque estuvieran comprendidos en la misma disciplina.

Respecto a E26 pasa exactamente lo mencionado. Para los ojos de un lector actual, acostumbrado a un orden lógico de los resultados expuestos y con un resumen previo de lo que se le va a presentar, resulta que este artículo puede ser confuso, carente de un objetivo, ya que no concreta algo en particular, esto es, proporciona información importante pero no demuestra prácticamente nada. Lo que que nos muestra esta situación es que no se deben leer por separado los artículos, y es porque algunos pueden contener las primeras reflexiones, otros las justificaciones, o lo que llamamos demostraciones, y otros los nuevos resultados generados a partir de los primeros trabajos.

En este artículo de las *Observaciones...* podemos ver claramente el proceso señalado. En él presenta resultados que en su mayoría no son justifi-

cados; parece que son las primeras reflexiones a las preguntas que le había formulado Goldbach durante los tres años anteriores. Para poder entender el desarrollo de las teorías expuestas es necesario consultar los artículos relacionados que publicó en los años posteriores dado que en ellos se encuentran las justificaciones a sus primeras propuestas.

¿Qué contiene este artículo de 1832?

Resumen

El primer tema de Euler fue la respuesta a la pregunta de Goldbach sobre la posibilidad de que los números de Fermat fueran primos[8]. La respuesta que escribió no se limitó al estudio de los números de la forma $2^{2^n}+1$, sus ideas escalaron a ver cómo tenían que ser las sumas de potencias a^n+1 para que el número pudiera ser o no un primo de Fermat, es decir, tenía que ver cómo es n cuando a^n+1 es factorizable, y cómo cuando no lo es.

Después afirma que hasta el momento no se había encontrado algún caso en el que $2^{2^m}+1$ tuviera divisores, en el entendido que sólo se probó (hasta esos días) para *m* igual a 0,1, 2, 3 y 4,y por esta razón Euler cree que Fermat llegó a concluir que $2^{2^m}+1$ siempre podía ser primo.

El camino de su exposición en el artículo se dirigió después a los números de Mersenne, es decir, aquellos de la forma 2^n-1. Ahí señala que 2^n-1 es compuesto cuando n no es primo; también observa que lo mismo pasa con números de la forma a^n-1. Y de aquí llevó su atención hacia los

[8] Un número de Fermat es de la forma $2^{2^n}+1$ que puede ser o no un número primo.

números perfectos, aquellos de la forma $2^{n-1}(2^n - 1)$ donde $(2^n - 1)$ tenía que ser un primo de Mersenne.[9]

Euler terminó el artículo con la mención de que ha encontrado más problemas relacionados con lo anterior, y pensó que deberían de ser investigados. Así, finalizó con seis enunciados que él llama teoremas, de los que no proporcionó las demostraciones, y posiblemente no lo hizo porque parece ser que éstas dependían de otros resultados en proceso.

Sobre los *Teoremas de Fermat*

En esta sección exponemos el contenido del artículo y lo que añadiremos son las justificaciones de algunos de los resultados que Euler nos presenta, y en los capítulos posteriores de la tesis presentamos la trascendencia de los resultados que bosquejó en este artículo de 1832.

Inicia suponiendo que es conocido que la cantidad a^n tiene divisores diferentes de uno siempre que *n* sea un número impar, o que sea divisible por un número impar distinto de la unidad. Euler no da una demostración para este hecho por lo que aquí se presenta una en la que se intenta usar sólo elementos matemáticos de su época:

Demostración. Primero probaremos que $a^n + b^n$ con n impar o con n divisible por un impar diferente de la unidad, se puede factorizar como$(a + b)(a^{n-1} - a^{n-2}b + a^{n-3}b^2 - \ldots - ab^{n-2} + b^{n-1})$.

[9] Un primo de Mersenne es un número primo de la forma $2^n - 1$

Al desarrollar$(a+b)(a^{n-1}-a^{n-2}b+a^{n-3}b^2-\ldots-ab^{n-2}+b^{n-1})$ obtenemos $(a^n-a^{n-1}b+a^{n-2}b^2-\ldots-a^2b^{n-2}+ab^{n-1})+(ba^{n-1}-b^2a^{n-2}+b^3a^{n-3}-\ldots-ab^{n-1}+b^n)$. Por ser *n* impar tenemos un número par de sumandos repetidos entonces podemos reescribirlo así:

$$a^n+((ba^{n-1}-ba^{n-1})+(b^2a^{n-2}-b^2a^{n-2})+\ldots+(b^{n-1}a-b^{n-1}a)+b^n=a^n+b^n$$

por lo tanto $(a+b)|(a^n+b^n)$. Ahora, si *n* es divisible por un impar, es decir, $n=rs$ con s impar entonces podemos escribir a^n+b^n como $a^{rs}+b^{rs}=(a^r)^s+(b^r)^s$,y como s es impar podemos repetir el proceso anterior y así $(a+b)|(a^n+b^n)$. Por lo tanto, si tomamos $b=1$ y como *n* es impar, se sigue que $a+1|a^n+1$.

Euler continuó en esta dirección con el análisis de a^n+1, y vio que si n es par por lo tanto a^n+1 no se puede factorizar de la manera anterior, por ejemplo

$a^4+1\neq(a+1)(a^3-a^2+a-1)=a^4-a^3+a^2-a+a^3-a^2+a-1=a^4-1$. Y más aún, dice que estos números no siempre son factorizables, por ejemplo $2^4+1=17$ es primo. Euler concluyó sin demostrar que si existen primos de la forma a^n+1, éstos podrían ser de la forma $a^{2^m}+1$. Pero dice que $a^{2^m}+1$ no siempre da como resultado un número primo; por ejemplo, si tomamos a impar y distinta de la unidad, entonces a^{2^m}será unnúmero impar y por lo tanto $a^{2^m}+1$ será un número par mayor que 2. Pero aún si a es un número par se pueden encontrar varios casos en los que $a^{2^m}+1$ da como resultado un número compuesto, por ejemplo, a^2+1 es

divisible por 5 cuando $a = 5b \pm 3$, y es así porque $a^2 + 1 = 25b^2 \pm 30b + 10$, y como 5 divide a cada elemento de la suma, por lo tanto $5|a^2 + 1$.

Continúa el texto, y en él afirma que hasta el momento no se había encontrado algún número de la forma[10] $2^{2^m} + 1$ que tuviera divisores diferentes a él mismo y a la unidad, pero en esta parte aclara que la revisión se hizo con una tabla de números primos hasta 100000, y por estas razones menciona que posiblemente Fermat llegó a pensar que $2^{2^m} + 1$ siempre genera un primo, y esto lo hizo saber a Wallis y a otros matemáticos para que trataran de demostrarlo. Enseguida señaló que el teorema de Fermat es cierto sólo para valores de m iguales a 1, 2, 3 y 4 (actualmente agregamos al cero), que dan como resultado al 5, 7, 257 y 65537, todos ellos números primos. Finalmente concluye cuando dice que no sabe porqué para *n* = 5 el teorema falla, y es porque 641 divide a $2^{2^5} + 1$. Aunque se tiene que mencionar que en este artículo Euler no dice cómo es que llegó a dicha factorización (en el capítulo 2 de la tesis se expone cómo es que lo hace).

Como ya se dijo antes, su artículo tiene como propósito el estudio de ciertos divisores de los binomios $a^n \pm 1$,[11] y en este sentido, después de ocuparse de los números de Fermat dirigió su exposición a los números de

[10] Una razón probable por la que se eligió a $2^{2^m} + 1$, es que *si* $2^m + 1$ *es un primo impar entonces* m *es una potencia de 2.*

Demostración. Supongamos que *m* no es potencia de 2, entonces $m = rs$ y con s impar, y por la demostración anterior sabemos que si sustituimos $a = 2^r$, $b = 1$ y $n = s$ tenemos que $(2^r + 1)|(2^{rs} + 1)$ entonces $(2^r + 1)|(2^m + 1)$ entonces $2^m + 1$ no es primo, por lo tanto *m* debe ser una potencia de dos.

[11] Años después se podrá ver que esto era un inicio de lo que sería la gran teoría de los residuos de potencias, y en particular de los residuos cuadráticos.

Mersenne, aquellos de la forma $2^n - 1$.

Señala que $2^n - 1$ es compuesto cuando n no es primo; también observa que lo mismo pasa con números de la forma $a^n - 1$. Una vez más Euler no presenta una demostración para estos dos resultados. Cabe de cualquier manera, el siguiente comentario: para el caso general de a^n-1 resulta que éste puede ser compuesto directamente, casi para cualquier *a*, pues se tiene que

$$a^{n-1} + a^{n-2} + a^{n-3} + ... + a + 1 = \frac{a^n - 1}{a - 1}$$

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

Así, se ve que si *a* no tiene restricciones, entonces en la mayoría de los casos se puede concluir que $a^n - 1$ no es primo, por ello es que si $a = 2$ entonces se llega a que $2^n - 1 = 2^{n-1} + ... + 2 + 1$, y esta suma al menos a primera vista no tiene porqué ser un compuesto. De manera más detallada se tratará el caso de 2^n-1 en el capítulo 3.

Euler posteriormente consideró el caso cuando n es primo en la expresión $2^n - 1$, y mencionó que parecía que en este último caso podía ser primo, pero exhibe que $2^{11} - 1$ tiene a los divisores 23 y 89, así como $2^{23} - 1$ puede ser divido por 47. Euler mencionó que los ejemplos anteriores, junto con $2^9 - 1$, estaban incluidos en la lista de primos de Christian Wolff que aparecen en su libro *Elementa Matheseos Universae*, pero señala que Wolff ha cometido un error al señalar algunos números como primos sin que lo sean. El paso natural hacia donde se extendió su análisis de los núme-

ros de Mersenne fue el considerar a los números perfectos.

En este mismo tenor a Euler le llamó la atención que Wolff afirmara que $2^{n-1}(2^n-1)$ es un número primo siempre que 2^n-1 lo fuera, y en consecuencia propuso que n debe ser un primo (ya que cree que si 2^n-1 es un número primo entonces n también lo será). Euler al respecto escribió en su artículo que encontró que vale la pena el esfuerzo de examinar los casos en los que 2^n-1 no es primo, a la vez que n si lo es. Continuó con el análisis de los números de Mersenne,y dice que si $8m-1$ y $n=4m-1$ son dos números primos, entonces $8m-1|2^n-1$. Nuevamente Euler no proporcionó una prueba para este hecho(ésta se abordará en el capítulo 3). Con este resultado aclara que se deben excluir los siguientes números primos: 11, 23 , 83, 131, 179, 191, 239 etc., cuando se sustituyen por n, pues resulta que2^n-1 será un número compuesto, y lo mismo dice para las potencias de números primos en $2^{37}-1$ que es dividido por 233, $2^{43}-1$ por 431, $2^{29}-1$ por 1103 y $2^{73}-1$ por 439 (una vez más sin decir como encontró estos divisores). A pesar de esto no puede excluir al resto de los primos, pero con estos resultados se aventuró a aseverar que excluyendo los casos anteriores, el resto de los primos menores de 50, y hasta menores de 100, daban lugar a que $2^{n-1}(2^n-1)$ fuera un número perfecto; así es como se pueden obtener 11 números perfectos al tomar a n entre los primos: 1, 2, 3, 5, 7, 13, 17, 19, 31, 41 y 47. De esta lista sabemos que el 41 y 47 no generaban perfectos pares, y Euler lo rectificó hasta 1750 después que lo notó Christian Winsheim en 1749 [Sandifer, 2007, 76].

Concluyó esta parte del artículo con un teorema que no demostró y a partir del cual parece que dedujo algunas de las observaciones anteriores. El teorema referido es una versión del pequeño teorema de Fermat y lo enunció como sigue:

Teorema 1 *$a^n - b^n$ siempre es divisibles por $n+1$, si $n+1$ es un primo que no divida a o b.*

Dice que cree que la prueba es difícil pues el teorema no es cierto a menos que $n+1$ sea primo. A partir de este teorema llegó a las siguientes conclusiones: I) $2^n - 1$ podrá dividirse por $n+1$ siempre que $n+1$ sea un número primo, y siempre que $n+1$ no sea 2, pues si pasa que $a = 2$ entonces no puede ocurrir que $n+1 = 2$, ya que el teorema requiere que $n+1$ no divida a a; II) también se sigue del teorema que $2^{2m} - 1$ es divisible por $2m+1$ siempre que $2m+1$ sea un primo. Aquí regresa al punto de los divisores de los números de la forma $a^n \pm 1$, y dice que $2^m + 1$ ó $2^m - 1$, serán divididos por $2m+1$; esto es porque $2^{2m} - 1 = (2^m + 1)(2^m - 1)$, y por ser $2m+1$ primo y divisor de $2^{2m} - 1$, entonces debe dividir a alguno de los dos términos. Además, dice que $2^m + 1$ puede ser dividido si $m = 4p + 1$ ó $4p + 2$; mientras que $2^m - 1$ tendrá el divisor $2m+1$ si $m = 4p$ ó $4p - 1$.

Euler terminó el artículo con otros teoremas vinculados con lo anterior, y de ellos sólo proporciona los enunciados sin dar demostraciones, y menciona que estos resultados aún tienen que ser investigados.

Lo que resta de este capítulo de la tesis será dedicado a enunciar los

teoremas y proporcionaremos las demostraciones desarrolladas para esta tesis.

El primer teorema es una versión diferente del pequeño teorema de Fermat.

Teorema 2 *Si n es un número primo, todas las potencias que tengan el exponente n-1 dejarán residuo 1 ó 0 cuando son divididas por n.* (En notación moderna: *si n es primo entonces* $a^{n-1} \equiv 1(mod\ n)$ *ó* $a^{n-1} \equiv 0(mod\ n)$)[12]

Demostración. Suponga primero que $n|a$, entonces a deja residuo 0, y como $a|a^{n-1}$, por lo tanto $n|a^{n-1}$, y entonces a^{n-1} deja residuo 0.

Ahora suponga que $n \nmid a$ entonces los residuos más pequeños de los números $a, 2a, 3a, \ldots, a(n-1)$ módulo n son los mismo que los enteros 1,2,3,...,$(n-1)$ en algún orden, así que su producto es congruente módulo n, es decir, $1 \cdot 2 \cdot 3 \cdot \ldots \cdot (n-1) \equiv a \cdot 2a \cdot 3a \ldots \cdot a(n-1) (\mathrm{mod}\, n)$ entonces $(n-1)! \equiv (n-1)!\, a^{n-1}$, pero $((n-1)!,\ n) = 1$ y entonces $a^{n-1} \equiv 1(\mathrm{mod}\, n)$.

El siguiente teorema es un caso especial del teorema de Euler y, además, prefigura a la función φ de Euler, y es porque aparece el término $n^{m-1}(n-1)$, que es el mismo que $\varphi(n^m)$.

Teorema 3 *Si n es un número primo, cada potencia cuyo exponente sea*

[12]Para todas las demostraciones de los siguientes teoremas se emplean elementos matemáticos de la época de Euler, pero también posteriores a él. La idea es proporcionar demostraciones para el trabajo de tesis, aun cuando no correspondan a la herencia matemática de Euler.

$n^{m-1}(n-1)$ *deja residuo 0 ó 1 cuando es dividido por* n^m. (En notación moderna: *si n es primo y a es cualquier entero, entonces* $a^{n^{m-1}(n-1)} = a^{\varphi(n^m)} \equiv 1(mod\ n^m)$ *ó* $a^{\varphi(n^m)} \equiv 0(mod\ n^m)$)

Demostración. Si $n^m|a$ y como $a|a^{\varphi(n^m)}$, entonces, por transitividad, $n^m|a^{\varphi(n^m)}$ por lo tanto $a^{\varphi(n^m)} \equiv 0(\text{mod}\ n^m)$.

Por otro lado si $n^m \nmid a$ entonces los residuos de los números *a*, 2*a*, 3*a*, ..., (n^{m-1}(n – 1))*a* son los enteros 1, 2, 3, ..., n^{m-1}(n – 1), que aparecerán en algún orden. Y al igual que en el teorema anterior se obtiene la relación

$$a^{\varphi(n^m)} \equiv 1(mod\ n^m).$$

■

El tercer teorema es una generalización del teorema de Fermat.

Teorema 4 *Sean m, n, p, q, etc. números primos distintos, y sea A el mínimo común múltiplo de ellos reducidos por la unidad, piense en ellos como m-1,n-1,p-1,q-1,etc. Digo que cualquier potencia del exponente A, como por ejemplo* a^A*, si se divide por mnpq... dejará residuo 0 ó 1, a menos que a pueda ser dividida por alguno de los números m, n, p, q, etc.*

(En notación moderna: Sean *m, n, p, q, r*, ... primos y A = m. c. m. de (*m* – 1), (*n* – 1), (*p* – 1), (*q* – 1), ..., es decir, A = [(*m* – 1), (*n* – 1), (*p* – 1), (*q* – 1), ...]. Entonces, para cualquier entero *a* se tiene que:

$a^A \equiv 1(mod\ mnpq..)$ ó $a^A \equiv 0\ (mod\ mnpq..)$, a menos que *a* sea dividida por alguno de los enteros *m, n, p, q*, ...).

Demostración. Si tanto *mnpq* ...|*a*, como $a|a^A$ entonces por transitividad *mnpq* ...|a^A, y en consecuencia dejará residuo 0.

Ahora se tiene el caso en que $mnpq \ldots \nmid a$ y ninguno de los números $m, n, p, q \ldots$ divide a a. Por comodidad nombramos la lista de primos como $p_1, p_2, p_3 \ldots$, y por el pequeño teorema de Fermat resulta que $a^{p_i-1} \equiv 1 (\mathrm{mod}\, p_i)$. Si ambos lados de la congruencia se elevan a la potencia $\frac{A}{p_i-1}$ (que es un entero porque A es el m.c.m de $p_1 - 1, p_2 - 1, p_3 - 1, \ldots$) se obtiene:

$$(a^{p_i-1})^{\frac{A}{p_i-1}} \equiv 1^{\frac{A}{p_i-1}} (\mathrm{mod}\, p_\mathrm{i}) \Rightarrow a^\mathrm{A} \equiv 1 (mod\ p_i),$$

y como se puede hacer lo mismo con todos los primos $p_1,\ p_2,\ p_3, \ldots$entonces se llega a que

$$a^A \equiv 1 (\mathrm{mod}\ \ \mathrm{m.c.m}(p_1, p_2, p_3, \ldots))$$

Por lo tanto

$$a^A \equiv 1 (\mathrm{mod}\ \ p_1 p_2 p_3 \ldots)$$

Los últimos 3 teoremas tratan sobre problemas de divisores de los números de la forma $a^n \pm b^n$, y están relacionados con el pequeño teorema de Fermat, aunque Euler no lo menciona. Pero lo importante es que son parte del camino hacia el desarrollo de la teoría de los residuos cuadráticos.[13]

Los tres teoremas con los que termina el artículo nos proporcionan indicios para entender que ya tenía en mente lo que sería la teoría de los residuos cuadráticos. Los elementos matemáticos que emplearemos para las

[13] Sea m un entero positivo y a un entero tal que a y m sean primos relativos. Entonces sedice que a es un residuo cuadrático de m si la congruencia $x^2 \equiv a\ (mod\ m)$ tiene solución.

demostraciones fueron usados posteriormente por Euler a lo largo de otros trabajos.

Teorema 5 *Sea* $2n+1$ *un número primo, entonces* 3^n+1 *podrá ser dividido por* $2n+1$, *si* $n=6p+2$ *ó* $n=6p+3$, *mientras que* 3^n-1 *podra ser dividido por* $2n+1$ *si* $n=6p$ *ó* $n=6p-1$.

Demostración. Primero veamos que $2n+1$ es divisor de 3^n-1 o de 3^n+1.

Como $2n+1$ es primo entonces se puede usar el *pequeño teorema de Fermat* y obtener que $2n+1|3^{2n+1-1}-1$ y en consecuencia $2n+1|3^{2n}-1$; por otro lado como $3^{2n}-1=(3^n-1)(3^n+1)$ y $2n+1$ es primo, entonces[14] $2n+1|3^n-1$ ó $2n+1|3^n+1$

Renombremos a $2n+1=q$. Sabemos que si existe x tal que

$$x^2\equiv 3 \pmod{q}$$

entonces se dice que 3 es un residuo cuadrático módulo q, y esto sólo pasa si $q\equiv\pm1(\mathrm{mod}12)$, y si no es residuo cuadrático entonces $q\equiv\pm5(\mathrm{mod}12)$.[15] Ahora, 3 es un residuo cuadrático módulo q sólo cuando $n=6p$ ó $n=6p-1$, y con base en esto Euler propone que tiene que suceder que $3^n\equiv 1(\mathrm{mod}\ 2n+1)$, por lo tanto $2n+1|3^n-1$.

Para el otro caso, si no existe x tal que $x^2\equiv 3(\mathrm{mod}\ q)$, entonces se dice que 3 no es un residuo cuadrático módulo q, y esto sólo pasa si $q\equiv\pm5(\mathrm{mod}12)$. Así, cuando 3 no es residuo cuadrático módulo q sucede que

[14]No puede dividir a ambos porque se llegaría a que $2n+1|2$, lo que no es posible.

[15]Esto se deduce de las leyes de reciprocidad cuadrática y propiedades del simbolo de Legendre para mayores detalles vease [Koshy, 2002, 508].

$n = 6p + 2$ *ó* $n = 6p + 3$, y por esto Euler propone que tiene que suceder que $3^n \equiv -1 (\text{mod } 2n + 1)$, por lo tanto $2n + 1 | 3^n + 1$.

Teorema 6 $3^n + 2^n$ *puede ser dividido por* $2n + 1$ *si* $n = 12p + 3$, $12p + 5$, $12p + 6$ *ó* $12p + 8$, *y* $3^n - 2^n$ *puede ser dividio por* $2n + 1$ *si* $n = 12p$, $12p + 2$, $12p + 9$ *ó* $12p + 11$.

Demostración.Como $2n + 1$ es primo entonces, por la versión del *pequeño teorema de Fermat* que da Euler en este texto, se sigue que $2n + 1 | (3^{2n} - 2^{2n})$. Ahora, como $3^{2n} - 2^{2n} = (3^n - 2^n)(3^n + 2^n)$, y $2n + 1$ es primo, entonces $2n + 1 | (3^n - 2^n)$ ó $2n + 1 | (3^n + 2^n)$.

Se demostrará primero el caso cuando $2n + 1 | (3^n - 2^n)$.

- Si $n = 12p$, entones $2n + 1 = 2(12p) + 1 = 12r + 1$, y si esto lo llamamos q, entonces $q \equiv 1 (\text{mod } 12)$, y por ello 3 es residuo cuadrático módulo q, y en consecuencia, por el criterio de Euler, $3^n \equiv 1 (\text{mod } 2n + 1)$, y por lo tanto $2n + 1 | (3^n - 1)$.
- Nuevamente, si $n = 12p$, entones $2n + 1 = 2(12p) + 1 = 8r + 1$, a lo que llamamos nuevamente q, *y* entonces $q \equiv 1 (\text{mod } 8)$, y por lo tanto 2 es residuo cuadrático módulo q y en consecuencia por el criterio de Euler $2^n \equiv 1 (\text{mod } 2n + 1)$, por ende, $2n + 1 | (2^n - 1)$.

Es así como se llega a que $2n + 1 | 3^n - 1$ y $2n + 1 | 2^n - 1$ cuando $n = 12p$, y que entonces $2n + 1 | (3^n - 2^n)$, y con esto se tiene el primer caso.

De la misma manera si $n = 12p + 2$, entones $2n + 1 = 2(12p + 2) + 1 =$

$12r + 5$, a lo que llamamos q. Entonces $q \equiv 5(\text{mod } 12)$, y de aquí que 3 no es residuo cuadrático módulo q, y en consecuencia, por el criterio de Euler, $3^n \equiv -1(\text{mod } 2n + 1)$, y por lo tanto, $2n + 1|(3^n + 1)$. Por el otro lado, $2n + 1 = 2(12p + 2) + 1 = 8r - 3 = q$, y entonces $q \equiv 3(\text{mod } 8)$, por lo que 2 no es residuo cuadrático módulo q, y por el criterio de Euler $2^n \equiv -1(\text{mod } 2n + 1)$, por lo que $2n + 1|(2^n + 1)$.

Así, para este caso se concluye que $2n + 1|(3^n + 1)$ y $2n + 1|(2^n + 1)$ y en consecuencia $2n + 1|(3^n - 2^n)$.

Con un proceso semejante se llega a lo mismo para los casos $12p + 9$ ó $12p + 11$, e igualmente para $n = 12p + 3$, $12p + 5$,$12p + 6$ *ó* $12p + 8$ se llegaría a que $2n + 1|(3^n + 2^n)$.

El último teorema es una extensión del anterior, y la diferencia está en que los numeradores $(3^n \pm 1)$ y $(2^n \pm 1)$ ahora se multiplican. El teorema dice lo siguiente:

Teorema 7 *Bajo las mismas condiciones que se pedían para* $3^n + 2^n$, $6^n + 1$ *también será dividido por* $2n + 1$ *y* $6^n - 1$ *para aquellas que se pedían para* $3^n - 2^n$.

Si se reescribe el enunciado, dice lo siguiente:

$2n + 1$ divide a $6^n + 1$ si pasa que $n = 12p + 3$, $12p + 5$, $12p + 6$ *ó* $12p + 8$. O pasa que $2n + 1$ divide a $6^n - 1$ si sucede que $n = 12p$, $12p + 2$,$12p + 9$ *ó* $12p + 11$.

Demostración. La prueba tiene un camino semejante, por ejemplo, si $n = 12p + 2$, entonces $3^n \equiv -1(\text{mod } 2n + 1)$ y $2^n \equiv -1(\text{mod } 2n + 1)$, y de

esto se obtiene que $6^n \equiv 1(\text{mod } 2n+1)$, y entonces que $2n+1|(6^n-1)$.

Otro ejemplo, si $n = 12p+3$, entonces $3^n \equiv -1(\text{mod } 2n+1)$ y $2^n \equiv 1(\text{mod } 2n+1)$ y de esto se obtiene que $6^n \equiv -1(\text{mod } 2n+1)$, y entonces $2n+1|(6^n+1)$.

De la misma forma se demuestra para todos los casos.

Con esta exposición se puede apreciar que las primeras preguntas que le planteó Goldbach sobre algunos problemas de Fermat no quedaron en respuestas acotadas, esto es, lo que le preguntó Goldbach fue un detonador para que él se adentrara en estos temas, y el artículo de 1732 fue el primer reflejo que lo que se vendría en los siguientes años, y si bien en este primer trabajo no formalizó la mayoría de los resultados, sí nos deja ver por donde caminaban sus ideas. Y un ejemplo de esto es la función que ahora denotamos como ϕ; Euler ahí aún no menciona la necesidad de calcular los enteros menores, positivos y primos relativos a un entero *n*, pero por otro lado encontramos expresiones que corresponden a los valores de ϕ, y más aún, varias de las demostraciones que aquí se propusieron para los teoremas que él no demostró se conducen de manera natural usando la función ϕ. Así, da la impresión a partir de algunos enunciados, que Euler ya manejaba la idea de ϕ, aunque en ese trabajo de 1732 no dio los elementos que lo exhiban explícitamente.

Capítulo II

¿Serán primos los números de Fermat?

Por la información proporcionada en la introducción y en el Capítulo I se aprecia que la puerta de entrada para que Euler se interesara en la teoría de los números fue la de los números de Fermat. Además, se mencionaron en el Capítulo I las primeras respuestas que Euler le envió a Goldbach respecto a la primalidad de los números de la forma $2^{2^n}+1$, que son los números de Fermat.

En este capítulo se expone la manera en la que Euler continúo su interés por este tema y que dio a conocer por primera vez en el artículo de 1732. En ese trabajo dejó ver que la interrogante de Fermat acerca de si $2^{2^n}+1$ podía ser número primo, para cualquier *n*, estaba resuelta, y su respuesta fue que no, pues resultó que 641 divide a $2^{2^5}+1$. Pero en el artículo no dijo explícitamente cómo llegó a tal resultado. Fue hasta el artículo *Theoremata circa divisores numerorum*[16] (E134), escrito en 1747, que profundizó sobre la cuestión de cómo son los divisores de un número de Fermat. Pero su interés se extendió en el tiempo, y en 1760 escribió el artículo "Sobre números primos muy grandes", y también su obra inconclusa "Tratado de los números", donde aborda el tema en el capítulo nueve. Pero de ésta última no se sabe exactamente cuando la escribió.

En el resto de este capítulo de la tesis se analizan secciones de los

[16] *Teoremas sobre divisores de números.*

trabajos mencionados, que se ocupan de los números de Fermat.

Recuérdese que en el artículo de 1732 Euler hizo señalamientos respecto a los números de la forma a^n +1 y la posibilidad de que éstos sean primos. Primero se descartó el caso cuando *n* tiene un factor impar, es decir, que *n* fuera divisible por un impar diferente de la unidad. De esto concluyó que si a^n + 1 es un primo, entonces éste requiere ser de la forma a^{2m} + 1. Pero aún estos números no siempre resultan primos, pues si *a* es un número impar a^{2m} + 1 dará como resultado un número divisible entre 2, además, Euler da varios ejemplos en los cuales *a* es un número par y a^{2m} + 1 no es un primo. Así, con estos resultados como base, menciona que no se había encontrado ningún caso en el cual los números de la forma $2^{2^n}+1$ no resultaran un número primo, cuando eran comprobados en la lista de números primos (que no iban más allá del 100000 según el propio Euler).

El siguiente artículo donde Euler retomó a los números de Fermat es el *Theoremata…* (E134). En esta exposición Euler sí da una explicación acerca de porqué $2^{2^5}+1$ no es un primo y porqué 641 lo divide.[17]

Los temas centrales para Euler en este artículo fueron: I) encontrar los divisores de los números de la forma $a^m + b^m$, para lo que antes necesita presentar teoremas relacionados con el pequeño teorema de Fermat; II) en otra parte demuestra algunos resultados que corresponden a las diferencias de potencias y sus divisores.

[17] Además, es en este trabajo donde (como ya se mencionó en la Introducción) se encuentra la segunda demostración hecha por Euler del "pequeño teorema de Fermat".

Divisores de $a^m + b^m$

Euler usó un método muy parecido a lo que hoy conocemos como inducción, al que ya había recurrido en otros artículos de teoría de números. Se debe considerar que este método –a mediados del siglo XVIII- aún estaba en su etapa de gestación y por ello tiene algunas lagunas lógicas, y es la razón por la que no se le consideró como una demostración bien cimentada.

La demostración inicia con el caso m = 1, donde el problema se reduce a encontrar los divisores de $a^{2^1} + b^{2^1} = a^2 + b^2$; después continua para el caso m = 2, posteriormente para m = 3 y, finalmente, analiza el caso general. Además, es importante mencionar que en todas las demostraciones de estos casos, el pequeño teorema de Fermat jugó un papel fundamental, pues es necesario en cada uno porque a través de él se pueden eliminar los primos que no dividen a $a^{2^m} + b^{2^m}$.

Para proponer un resultado general Euler requirió los siguientes teoremas que enseguida se presentan.

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

Demostración. Sea $4n-1$ un número primo que no divide ni a a ni a b.

Por el pequeño teorema de Fermat se tiene que $(4n - 1) \mid (a^{4n-2} - 1)$, y de la misma forma $(4n - 1) \mid (b^{4n-2} - 1)$, y por lo tanto

$$(4n - 1) \mid (a^{4n-2} - 1) - (b^{4n-2} - 1),$$

pero $(a^{4n-2} - 1) - (b^{4n-2} - 1) = a^{4n-2} - b^{4n-2}$. Por otro lado, si suponemos que $a^{4n-2} + b^{4n-2}$ es divisible por 4n-1, entonces se tendría que

$$(4n - 1) \mid [(a^{4n-2} - b^{4n-2}) + (a^{4n-2} + b^{4n-2})],$$

pero de este resultado se infiere que $(4n - 1) \mid a$, lo que es una contradicción porque se supuso que (4n – 1) no divide a *a*.

Por lo anterior se llega a que 4n − 1 no puede dividir a $a^{4n-2} + b^{4n-2}$. Además, como 4n − 2 = 2(2n − 1), entonces se puede reescribir a $a^{4n-2} + b^{4n-2}$ como $(a^2)^{(2n-1)} + (b^2)^{(2n-1)}$, pero de esto se tiene que

$$(a^2)^{(2n-1)} + (b^2)^{(2n-1)} = (a^2 + b^2)((a^2)^{2n-2} - (a^2)^{2n-3}(b^2) + \ldots - (a^2)(b^2)^{2n-3} + (b^2)^{2n-2}),$$

y como 4n − 1 no divide a $a^{4n-2} + b^{4n-2}$ entonces tampoco divide a ninguno de los dos factores de la derecha en la igualdad anterior, y en particular no divide a $a^2 + b^2$. ■

Euler agrega que nadie más, a excepción de Fermat, había probado este resultado, pero que como Fermat no publicó la prueba, él recibiría el crédito por haberlo publicado por primera vez. Sin más continua con el siguiente teorema.

Teorema 2. Todos los divisores de la suma de dos números a la cuarta potencia $(a^4 + b^4)$ y que además son primos relativos, son el 2 o números de la forma 8n + 1.

Demostración. Sean a^4 y b^4 dos cuartas potencias con a y b primos relativos, entonces, o ambos son impares o uno es par y el otro impar. En el primer

caso, 2 es divisor de la suma $a^4 + b^4$; en el otro caso, los divisores impares, si es que existen, deben ser de la forma 4n+1, y es porque se puede ver a las cuartas potencias como cuadrados. Entonces podemos escribir la suma como $a^4 + b^4 = (a^2)^2 + (b^2)^2$, y por el teorema anterior resulta que sólo los números primos de la forma 4n + 1 dividen a la suma de dos cuadrados.

Ahora bien, los números de la forma 4n+1 también se pueden escribir de la forma[18] 8n + 1, o de la forma[19] 8n – 3. Pero ningún número de la forma 8n − 3 puede dividir a la suma de dos cuartas potencias, pues si se tiene un primo de dicha forma, éste tendría (por el pequeño teorema de Fermat) que dividir a $a^{8n-4} - b^{8n-4}$, por lo tanto no podría dividir a $a^{8n-4} + b^{8n-4}$, porque si lo hace entonces 8n – 3 dividiría a *a*, y esto pasaría sólo si a y b fueran divisibles entre 8n – 3, pero este caso se puede eliminar pues por hipótesis a y b son primos relativos. Por lo tanto ningún número primo de la forma 8n − 3 podrá dividir a $a^{8n-4} + b^{8n-4}$.

Y como en el teorema anterior, se tiene que $a^{8n-4} + b^{8n-4} = a^{4(2n-1)} + b^{4(2n-1)}$, y se puede escribir como $(a^4)^{2n-1} + (b^4)^{2n-1}$, y además

$$(a^4)^{(2n-1)} + (b^4)^{(2n-1)} = (a^4 + b^4)((a^4)^{2n-2} - (a^4)^{2n-3}(b^4) + \ldots - (a^4)(b^4)^{2n-3} + (b^4)^{2n-2}),$$

pero como 8n − 3 no divide a $(a^4)^{2n-1} + (b^4)^{2n-1}$, entonces tampoco lo hace para $a^4 + b^4$.

Ahora, para el caso en que un divisor de $a^{4(2n-1)} + b^{4(2n-1)}$ no sea pri-

[18] Si n=2k entonces 4n+1=4(2k)+1=8k+1, por lo tanto 4n+1 se puede escribir como 8n+1 si n es par.

[19] Si n=2k+1 entonces 4n+1=4(2k+1)+1=8k+4+1=8k+5, pero 5≡ -3 (mod 8), por lo tanto 4n+1 se puede escribir como 8n-3 si n es impar.

mo, entonces cualquier divisor primo de ese divisor no puede ser de la forma 8n – 3 porque entonces dividiría a $a^{4(2n-1)} + b^{4(2n-1)}$ y eso no es posible, entonces, cualquier factor primo del divisor tiene que ser de la forma 8n + 1, y para terminar se tiene que el producto de divisores de esta forma es de ésta misma, por lo tanto cualquier divisor es de la forma 8n + 1, y en consecuencia los divisores de $a^4 + b^4$, sólo son aquellos de la forma 8n + 1 ó 2.[20]

Así, Euler continua con el caso en el que m = 3, en el cual busca los divisores de $a^8 + b^8$.

Teorema 3. Todos los divisores de los números de la forma $a^8 + b^8$, dado que a y b son números primos relativos, son el 2 o son de la forma 16n + 1.

Demostración. Como a^8 y b^8 se pueden escribir como cuartas potencias, sólo los números de la forma 8n+1 pueden dividir a la suma $a^8 + b^8$.

Ahora 8n + 1 se puede escribir como[21] 16n + 1 o 16n –7.[22] Si es de la forma 16n − 7 entonces debe dividir a $a^{16n-8} - b^{16n-8}$, pero no a $a^{16n-8} + b^{16n-8}$, por lo anterior. Como $a^{16n-8} - b^{16n-8}$ es igual a

$$a^{8(2n-1)} + b^{8(2n-1)} = (a^8)^{2n-1} + (b^8)^{2n-1}$$

y de esto se tiene que

[20] Que cabría preguntarnos si un compuesto que sea divisor de $a^{8n-4} + b^{8n-4}$ puede ser de la forma 8n – 3 y lo que se tiene es que no puede ser generado por factores sólo de la forma 8n + 1.

[21] Si n=2k entonces 8n+1=8(2k)+1=16k+1 por lo tanto 8n+1 se puede escribir como 16n+1 si n es par.

[22] Si n=2k+1 entonces 8n+1=8(2k+1)+1=16k+8+1=8k+9 pero 9≡ -7 (mod 16), por lo tanto 8n+1 se puede escribir como 16n-7 si n es impar.

$$(a^8)^{(2n-1)} + (b^8)^{(2n-1)} = (a^8 + b^8)((a^8)^{2n-2} - (a^8)^{2n-3}(b^8) + \ldots - (a^8)(b^8)^{2n-3} + (b^8)^{2n-2}),$$

entonces 16n−7 tampoco dividirá a $a^8 + b^8$. Y de manera semejante a como se hizo antes los divisores de $a^8 + b^8$ son números de la forma $16n + 1 = 2^4n + 1$.

Así, Euler llegó al caso general, que es el teorema que utilizó para explicar cómo es que encontró los divisores del quinto número de Fermat. Pero antes proporciona la siguiente demostración.

Teorema 4. La suma de dos números $a^{2^m} + b^{2^m}$, para los que el exponente es una potencia de dos, no admite otros divisores que aquellos de la forma $2^{m+1}n + 1$.

Demostración. Por el teorema 1 se tiene que todos los divisores de $a^2 + b^2$ son de la forma 4n+1, y a partir de esto se mostró que los divisores de $a^4 + b^4$ son de la forma 2^3n+1; y aquellos divisores de $a^8 + b^8$ son de la forma $2^4n + 1$; de la misma manera se demuestra que $a^{16} + b^{16}$ sólo admite divisores de la forma 2^5n+1. De aquí en adelante se puede entender que $a^{32}+b^{32}$, $a^{64}+b^{64}$, sólo pueden tener divisores de la forma 2^6n+1, 2^7n+1, etc. Así, en general es evidente que $a^{2^m} + b^{2^m}$ sólo tiene divisores de la forma $2^{m+1}n + 1$.

No pasó mucho tiempo para que se observara que la demostración presentada por Euler no estaba completa. Como se puede ver, a través de tres casos particulares infirió que se podía generalizar para cualquier potencia de la forma 2^m. Pero también se tiene que decir que sí tenía razón en que los divisores tenían la forma $2^{m+1}n + 1$.

Si se trata de completar la demostración por el método de inducción –

el que conocemos actualmente- se trataría de hacer lo siguiente:

Demostración. Suponga que vale el caso para m = k – 1; ahora se tiene que ver que se cumple para m = k, es decir, que los divisores de $c^{2^k} + d^{2^k}$ son de la forma $2^{k+1}n + 1$.

Así, se tiene que $a^{2^k} = a^{2\times 2^{k-1}} = (a^2)^{2^{k-1}}$ y $b^{2^k} = b^{2\times 2^{k-1}} = (b^2)^{2^{k-1}}$. Por lo tanto $a^{2^k} + b^{2^k} = (a^2)^{2^{k-1}} + (b^2)^{2^{k-1}}$, pero esto último es de la forma $c^{2^{k-1}} + d^{2^{k-1}}$, y por tanto tiene divisores de la forma $2^k n + 1$, y en consecuencia estos también son divisores de $c^{2^k} + d^{2^k}$. Ahora, $2^k n + 1$ se puede escribir como $2^{k+1}n + 1$ ó $2^{k+1}n - (2^k - 1)$. Si $2^{k+1}n - (2^k - 1)$ es primo entonces, por el pequeño teorema de Fermat, divide a $a^{2^{k+1}n-2^k} - b^{2^{k+1}n-2^k}$ pero no a $a^{2^{k+1}n-2^k} + b^{2^{k+1}n-2^k}$. Ahora, como $a^{2^{k+1}n-2^k} + b^{2^{k+1}n-2^k} = (a^{2^k})^{2n-1} + (b^{2^k})^{2n-1}$, por lo tanto $2^{k+1}n - (2^k - 1)$ tampoco puede dividir a la suma de $(a^{2^k}) + (b^{2^k})$, por lo tanto sólo lo dividen los primos de la forma $2^{k+1}n + 1$. Por otro lado cualquier otro divisor sólo puede tener divisores de la misma forma, y como antes, un compuesto de la forma $2^{k+1}n - (2^k - 1)$ no puede ser producto de factores $2^{k+1}n + 1$. ■

De esta forma se puede ver que el resultado acerca de los divisores de los números de Fermat es correcto. Pero nos podemos preguntar ¿por qué no terminó la demostración? Una respuesta podría ser que como la exposición para exhibir a los divisores de $a^2 + b^2$, $a^4 + b^4$ y $a^8 + b^8$, acudía a una manera recursiva que usaba la forma de los divisores de las sumas de las potencias

del anterior, entonces, parece que decidió dejárselo al lector, y en verdad sólo se tenían que seguir las formas que uso en esos casos particulares, pero ahora suponiendo que se cumplía con m = k – 1, para llegar a m = k. Posiblemente, la carga de trabajo que Euler tenía por la gran cantidad de artículos que escribió en ese año, lo llevaron a confiar en que el lector entendería, en este caso, como se demostraba la generalización, y de esta forma ya no empleaba tiempo en escribir esta parte.

En 1878 Édouard A. Lucas [1878] demostró de manera general que los divisores primos *p* de un número de Fermat F_m (m > 1) son de la forma $p = 2^{m+2}k + 1$. El teorema es el siguiente.

Teorema (Lucas). Si *m* > 1 y *p* es un primo que divide a F_m, entonces *p* es de la forma $p = 2^{m+2}k + 1$, donde k pertenece a los naturales.

Demostración.

Sea $b = 2^{2^{m-2}}(2^{2^{m-1}} - 1)$. Por hipótesis $p \mid (2^{2^m} + 1)$.

Entonces $b^2 = (2^{2^{m-2}})^2(2^{2^{m-1}} - 1)^2 = 2^{2^{m-1}}(2^{2^m} - 2 \cdot 2^{2^{m-1}} + 1) =$

$$= 2^{2^{m-1}}(2^{2^m} + 1) - 2 \cdot 2^{2^m} \equiv -2 \cdot 2^{2^m} \equiv 2 \,(\textit{módulo } p),$$

entonces se obtiene que $b^2 \equiv 2 \pmod{p}$

$\Rightarrow\ b^{2^{m+1}} \equiv 2^{2^m} \equiv -1$ (mód *p*), pues $p \mid (2^{2^m} + 1) \Rightarrow 2^{2^m} \equiv -1 \pmod{p}$

$\Rightarrow b^{2^{m+2}} \equiv 1 \pmod{p}$

Como *b* y *p* son primos relativos entonces existe una potencia de *b* que es la

más pequeña de todas tal que $b^r \equiv 1\ (mod\ p)$, y ésta divide a cualquier otra potencia de b que sea congruente con 1 módulo p; por lo tanto la potencia más pequeña es de la forma 2^j (*i.e.* $Ord_p b = 2^j$), donde j $\leq m + 2$. Si se considera que j $< m + 2$ y e es la más pequeña de las potencias tal que $b^e \equiv 1 (\text{mod } p)$, entonces, $b^{e2^{m+1-j}} - 1 = b^{2^{m+1}} - 1 \equiv 2^{2^m} - 1 (\text{mod } p)$. Así, de la última congruencia se tiene que $2^{2^m} - 1 \equiv 0 (\text{mod } p)$, y de la hipótesis se tenía que $p | (2^{2^m} + 1)$, con lo que se llega a una contradicción, porque si esto sucede entonces $p | 2$, lo cual es imposible. Con lo anterior se tiene que la más pequeña de las potencias es 2^{m+2}, y por el pequeño teorema de Fermat se tiene que $b^{p-1} \equiv 1\ (mod\ p)$. Por otro lado, la más pequeña de las potencias, que es 2^{m+2}, divide a p-1, y entonces

p-1= k$2^{m+2} \Rightarrow p = k2^{m+2} + 1$.

Se puede notar que el resultado al que llegó Lucas es semejante al que propone Euler. Por un lado Euler dice que los divisores de F_m son de la forma $p = 2^{m+1}k + 1$, mientras que Lucas demuestra que son de la forma $p = 2^{m+2}k' + 1$,[23] con lo que se nota que parece que la k generalmente es par.

Pero el resultado original de Euler puede tener otra justificación sustentada en resultados más actuales, y son los siguientes:

Teorema 5. Sea $q = p^n$ una potencia de un número primo impar p, con $n \geq 1$. Entonces el número de Fermat F_m es divisible por q si y sólo si $Ord_q 2 =$

[23] Y aquí no se trata sólo de modificar la cota inferior de m en el teorema de Lucas, ya que si se trata de demostrar el teorema para m mayor o igual a uno el proceso se altera.

2^{m+1}.

Demostración. Supongamos que $q|F_m$. Entonces q divide a $\left(2^{2^m}+1\right)\left(2^{2^m}-1\right)=2^{2^{m+1}}-1$. Por lo tanto[24] $Ord_q 2 \leq 2^{m+1}$ y $2^{m+1}=kOrd_q 2$ para alguna $k \in \mathbb{N}$. Entonces, k tiene que ser una potencia de 2 y $e=Ord_q 2=2^j$. Sin embargo, si j fuera menor que m+1 entonces $2^{e2^{m-j}}-1=2^{2^m}-1$ sería divisible por el número impar $q>1$, lo cual contradice la suposición de que $q|F_m$, por lo tanto $Ord_q 2 \geq 2^{m+1}$, y por lo anterior, entonces $Ord_q 2 = 2^{m+1}$.

Ahora, supongamos que $Ord_q 2=2^{m+1}$. Entonces $q|2^{2^{m+1}}-1=\left(2^{2^m}+1\right)\left(2^{2^m}-1\right)$. Como p es impar, $p>1$ y q es una potencia de p entonces q debe dividir a $2^{2^m}+1$ o $2^{2^m}-1$. Pero q no puede dividir a $2^{2^m}-1$ pues $Ord_q 2$ que es 2^{m+1} tendría que dividir a 2^m, lo que no es posible, por lo tanto $q|2^{2^m}+1=F_m$. ■

Teorema 6. Si p es un primo y $p|F_m$, entonces p es de la forma $2^{m+1}k+1$, donde k es un número natural.

Demostración. Como $p|F_m$ entonces (por el teorema anterior) $Ord_p 2 = 2^{m+1}$, por lo tanto $p|(2^{2^{m+1}}-1)$. Por otro lado, como p es primo impar, entonces p divide a $(2^{p-1}-1)$, y como el orden de 2 módulo p es 2^{m+1} entonces 2^{m+1} divide a $p-1$. Por lo tanto $p-1 = k2^{m+1}$ entonces $p = k2^{m+1}+1$. ■

[24] Pues si $e=Ord_q 2$ entonces $q|2^n-1$ con $n=ek$ con $k \in \mathbb{N}$.

Con este teorema Euler puede concluir que el quinto número de Fermat no es primo, pues al ser los números de Fermat de la forma $2^{2^m}+1$, y de no ser primo, debe tener como divisores a los números de la forma $2^{m+1}n + 1$. De esta manera Euler dice que en lugar de buscar los divisores de $2^{2^5}+1 = 2^{32}+1$ entre la lista de primos puede reducir el problema a buscar entre los de la forma 64n + 1. También dice que le fue fácil encontrar que con n = 10 el primo 641 divide a $2^{32} + 1$, y que encontrar un número primo más grande que $2^{2^5}+1$ sigue siendo un problema abierto.

A continuación daremos una prueba de que un número de la forma $2^{m+1}n + 1$ divide al quinto número de Fermat

Como $641 = 2^6 \cdot 10 + 1$ entonces $2^{2^5} + 1 = 2^{32} + 1 = 2^4 \cdot 2^{28} + 1 = (641 - 625)2^{28} + 1 = (641 - 5^4)2^{28} + 1 = 641 \cdot 2^{28} - (5 \cdot 2^7)^4 + 1 = 641 \cdot 2^{28} - (10 \cdot 2^6) + 1 = 641 \cdot 2^{28} - (641 - 1)^4 + 1 = 641 \cdot 2^{28} - (641^4 - 4 \cdot 641^3 + 6 \cdot 641^2 - 4 \cdot 641 + 1) + 1 = 641(2^{28} - 641^3 + 4 \cdot 641^2 - 6 \cdot 641 - 4)$ por lo tanto $641|(2^{2^5} + 1)$

En el intercambio de ideas que se dio entre Euler y Goldbach, los números de Fermat ocuparon su atención más de lo que muestra la carta de 1729. Goldbach, por su parte, aportó algunos resultados que son parte de toda la gama de propiedades de estos números. Propuso por ejemplo, que dos números diferentes de la forma $2^{2^m}+1$ no podrían tener factores comunes diferentes de 1.

Teorema. Dos números de Fermat diferentes no pueden tener un máximo común divisor diferente que 1.

Demostración. Supongamos que

$$q|F_m \; y \; q|F_{m-k}$$

Para $m \geq k \geq 1$. Ahora como $q|F_{m-k} \; y \; F_s|(F_m - 2)$[25] para toda $s = 0, 1, \dots, m-1$ por lo tanto $q|(F_m - 2)$. Entonces como $q|F_m$, se tiene que $q|2$, pero como F_m es impar, se tiene que $q = 1$. ■

De este resultado se sigue que cada número de Fermat $(F_0, F_1, \dots, F_m)$ es divisible por un primo que no divide a ningún otro número de Fermat. Por lo tanto existen al menos *m+1* números primos que no dividen a F_m, de esto se puede concluir que existen una infinidad de números primos.

---

[25] Primero demostremos que $F_{m+1} = F_m + 2^{2^m} F_o F_1 \cdots F_{m-1}$ para toda $m \geq 1$.

Demostración. Se tiene que $F_{m+1} - F_m = 2^{2^{m+1}} + 1 - 2^{2^m} - 1 = 2^{2^m}(2^{2^m} - 1)$ pero $2^{2^m} - 1 = \left(2^{2^{m-1}} - 1\right)\left(2^{2^{m-1}} + 1\right) = (2^{2^{m-1}} - 1)F_{m-1}$ así, a su vez, $2^{2^{m-1}} - 1$ también se puede ver como una diferencia de *m-1* potencias con lo cual se obtiene que $2^{2^m} - 1 = (2^{2^{m-2}} - 1)F_{m-1}F_{m-2}$, de esta manera aplicando el procedimiento recursivamente se tiene que $2^{2^m} - 1 = (2^{2^{m-k}} - 1)F_{m-1}F_{m-2} \cdots F_{m-k+1}F_{m-k}$ para toda $k \in \{1, \dots, m\}$, en particular cuando $m = k$ se tiene que $2^{2^m} - 1 = F_{m-1} \cdots F_1 F_0$. Con esto se obtiene que $F_{m+1} - F_m = 2^{2^m} F_{m-1}F_{m-2} \cdots F_1 F_0$ por lo tanto $F_{m+1} = F_m + 2^{2^m} F_o F_1 \cdots F_{m-1}$.

Ahora demostraremos que $F_m = F_0 F_1 \cdots F_{m-1} + 2$

Demostración Por el teorema anterior se tiene que para toda $m \geq 1$ se tiene que $F_m - 2 = \left(2^{2^m} + 1\right) - 2 = 2^{2^m} - 1 = F_0 F_1 \cdots F_{m-1}$que es lo que se quería demostrar.

De esto se sigue que $F_k|F_m - 2$ para toda $k = 0, 1, \dots, m-1$.

Capítulo III

Los números perfectos

De regreso nuevamente al primer artículo de 1732, se puede apreciar que después de las ideas que vertió Euler acerca de los números de la forma $a^n + b^n$ -en particular los de Fermat-, no es de extrañarse que extendiera el estudio de los divisores de estas sumas de potencias ahora a los de la forma $a^n - b^n$. Y no es raro porque ya se mencionó que el estudio de los residuos de estos números está relacionado con los residuos de potencias, que fue uno de sus grandes temas en la teoría de los números.

La última expresión la dirigió principalmente, como caso particular, hacia los números de la forma $2^p - 1$, que son los que actualmente conocemos como primos de Mersenne. Euler señala que $2^p - 1$ es compuesto cuando *n* es compuesto, pero dejó claro, aunque no lo demuestra, que no se cumple para todos los casos; así, por ejemplo, si *n* es primo entonces $2^p - 1$ también lo es. Él sabía que si *P* no es un primo, entonces es un compuesto de la forma $P = a \cdot b$ donde $a > 1$ y $b > 1$. Ahora, si P se sustituye en $2^P - 1$ se tiene que: $2^P - 1 = 2^{a \cdot b} - 1 = \left(2^a\right)^b - 1$.

Por otro lado, como la diferencia $\left(2^a\right)^b - 1$ es igual a:

$$\left(2^a - 1\right)\left(\left(2^a\right)^{b-1} + \left(2^a\right)^{b-2} + \left(2^a\right)^{b-3} + \left(2^a\right)^{b-4} \cdots \left(2^a\right)^{b-(b-1)} + \left(2^a\right)^{b-b}\right)$$

Entonces,

$$2^P - 1 = \left(2^a - 1\right)\left(\left(2^a\right)^{b-1} + \left(2^a\right)^{b-2} + \left(2^a\right)^{b-3} + \cdots + 2^a + 1\right)$$

De esta manera, $2^P - 1$ tendrá como factor a $\left(2^a - 1\right) \geq 3$. Así, $2^P - 1$ no es un número primo, y cuando sí lo es, tiene que suceder que *P* también sea un primo.[26]

La atención que prestó a los números de Mersenne le marcó un camino para extender sus intereses hacia los números perfectos.

Antes de ver cuál fue el que juegan estos números en el artículo, recordemos que Goldbach, desde la primera carta que le escribe a Euler en 1729, le sugirió consultar el *Elementa Matheseos Universae* de Christian Wolff. Además de que Euler tenía que conocer la obra por las cuestiones físicas y matemáticas ahí tratadas, sabemos –porque él lo menciona en su artículo- que la consultó para estar al tanto sobre qué escribió Wolff respecto a los números perfectos.

Wolff en su *Elementa Matheseos* menciona que los números perfectos son de la forma $y^n x$, donde *x* y *y* son primos. Así, la suma de los divisores de estos números es igual a $y^n x$, esto es,

---

[26]Fermat obtuvo tres resultados que fueron usados por Mersenne en su "*Cogitata Physica Mathematica*" para generar a los primos de la forma $2^P - 1$ que se hallan en el número perfecto $2^{P-1}\left(2^P - 1\right)$. Tales resultados son los siguientes:

a) "*Si P es compuesto, entonces,* $2^P - 1$ *es compuesto*".
b) "*Si P es primo, entonces,* $a^P - a = Pt$ *para algún* $t \in \mathbb{Z}$
(Es decir, $a^P - a$ es un múltiplo de P).
c) "*Si P es primo y m divide a* $2^P - 1$*, entonces,* $(m-1) = P \cdot q$ *para algún q*
que pertenece a los enteros".
(Es decir, $m-1$ es un múltiplo de P).

Con estos enunciados Mersenne logró establecer la propiedad: "*Si un número de la forma* $2^P - 1$ *es primo, entonces, P es primo*". De esta manera, la búsqueda de primos de Mersenne se redujo a los P primos. Fermat también estableció un test donde condiciona a estos P primos para obtener a $2^P - 1$ primo.

$1+y+y^2+y^3+...+y^n+x+xy+...+xy^{n-1}=xy^n$,[27]

Si se factoriza *x* se obtiene

$$1+y+y^2+y^3+...+y^n+x(1+y+...+y^{n-1})=xy^n$$

Entonces

$1+y+y^2+y^3+...+y^n+=xy^n-x(1+y+...+y^{n-1})$

Por lo tanto,

$$x=\frac{1+y+y^2+...+y^n}{y^n-1-y-y^2-...-y^{n-1}}$$

y como *x* es un número entero entonces se requiere que

$$y^n-1-y-y^2-...-y^{n-1}=1,$$

Wolff aquí comentó que esto sólo pasa cuando y = 2, pues $y^n-1-y-y^2-\cdots-y^{n-1}=y^n-(\frac{y^n-1}{y-1})$, y cuando y=2 se tiene que $y^n-\left(\frac{y^n-1}{y-1}\right)=1$.

Entonces, si y = 2 se tiene que

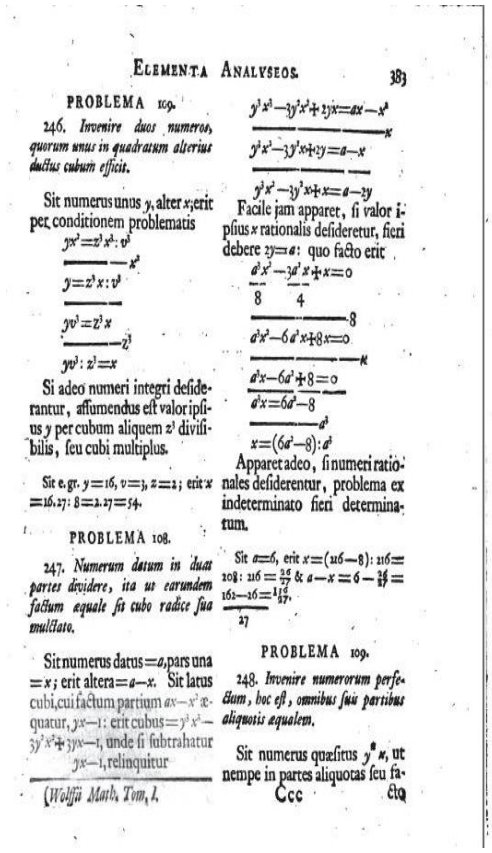
$$x=1+2+2^2+\cdots+2^n=2^{n+1}-1,$$

por lo tanto $xy^n=2^n(2^{n+1}-1)$, donde 2 y $2^{n+1}-1$ son primos por hipótesis. De esta manera Wolff llegó a la forma que propuso Euclides y la que más tarde conoció Euler.

Con ayuda del binomio $2^{n+1}-1$, Wolff generó los primos que darían lugar a los perfectos, y es aquí donde comete el error de decir que 2047 es primo, error que Euler señaló en E26. Además, Euler también dice que Wolff indica que 511 es primo, cosa que no es cierto como se puede ver

[27] Nótese que para Wolff el término xy^n no es uno de los divisores.

en el siguiente texto:



ELEMENTA ANALYSEOS. 383

PROBLEMA 107.

246. *Invenire duos numeros, quorum unus in quadratum alterius ductus cubum efficit.*

Sit numerus unus y, alter x; erit per conditionem problematis

$yx^2 = z^3$: v^3

$y = z^3 x : v^3$

$yv^3 = z^3 x$

$yv^3 : z^3 = x$

Si adeo numeri integri desiderantur, assumendus est valor ipsius y per cubum aliquem z^3 divisibilis, seu cubi multiplus.

Sit e. gr. $y = 16$, $v = 3$, $z = 2$; erit $x = 16.27 : 8 = 2.27 = 54$.

PROBLEMA 108.

247. *Numerum datum in duas partes dividere, ita ut earundem factum aequale sit cubo radicis suae multiplato.*

Sit numerus datus $= a$, pars una $= x$; erit altera $= a - x$. Sit latus cubi, cui factum partium $ax - x^2$ aequatur, $yx - 1$: erit cubus $= y^3x^3 - 3y^2x^2 + 3yx - 1$, unde si subtrahatur $yx - 1$, relinquitur

$y^3x^3 - 3y^2x^2 + 2yx = ax - x^2$

$y^3x^2 - 3y^2x + 2y = a - x$

$y^3x^2 - 3y^2x + x = a - 2y$

Facile jam apparet, si valor ipsius x rationalis desideretur, fieri debere $2y = a$: quo facto erit

$a^3x^2 - 3a^2x + x = 0$

$a^3x - 6a^2 + 8 = 0$

$a^3x = 6a^2 - 8$

$x = (6a^2 - 8) : a^3$

Apparet adeo, si numeri rationales desiderentur, problema ex indeterminato fieri determinatum.

Sit $a = 6$, erit $x = (216 - 8) : 216 = 208 : 216 = \frac{26}{27}$ & $a - x = 6 - \frac{26}{27} = 162 - 26 = \frac{136}{27}$.

PROBLEMA 109.

248. *Invenire numerorum perfectum, hoc est, omnibus suis partibus aliquotis aequalem.*

Sit numerus quaesitus $y^n x$, ut nempe in partes aliquotas seu fa-

ctores resolvi possit: erunt partes ejus aliquotae $1 + y + y^2 + y^3$ &c. donec exponens evadat $= n$, & $x + yx + y^2x + y^3x$ &c. donec exponens fiat $= n - 1$. Quamobrem ex natura numeri perfecti

$1 + y + y^2 + y^3$ &c. $+ x + yx + y^2x + y^3x$ &c. $= y^n x$

$1 + y + y^2 + y^3$ &c. $= y^n x - x - yx - y^2x - y^3x$ &c.

$1 + y + y^2 + y^3$ &c. $= x$

$y^n - 1 - y - y^2 - y^3$ &c.

Jam ut x sit numerus integer, nec in casu speciali, si y per numerum explicetur, numerus partium aliquotarum diversus sit a numero earundem in formula generali; necesse est ut $y^n - 1 - y - y^2 - y^3$ &c. $= 1$: quod cum non alio in casu contingat, nisi cum $y = 2$ (§. 124.); erit $x = 1 + 2 + 2^2 + 2^3$ &c. $= 1 + 2 + 4 + 8$ &c. & numerus perfectus $2^n x$. Quoniam vero x est numerus primus, necesse est ut $1 + 2 + 2^2 + 2^3$ &c. in omni casu sit merus primus, consequenter series terminetur prope terminum, qui unitate mulctatus est numerus primus (§. *cit.*) & n notat numerum terminorum, qui istiusmodi terminum praecedunt. Quare problema, quod speciem indeterminati mentiebatur, determinatum est.

Patet autem simul

Theorema 1. Si numerorum series in ratione dupla ab unitate continue proportionalium continuetur, donec eorum summa sit numerus primus; summa in maximum multiplicata faciet numerum perfectum.

Theorema 2. Si in numerorum serie in ratione dupla ab unitate continue proportionalium occurrat terminus, qui unitate mulctatus est numerus primus; numerus iste primus in proxime praecedentem ductus efficit numerum perfectum.

In serie numerorum ab unitate in ratione dupla continue proportionalium 1. 2. 4. 8. 16. 32. 64. 128. 256. 512. 1024. 2048. 4096.

$4 - 1 = 3$, $8 - 1 = 7$, $32 - 1 = 31$, $128 - 1 = 127$, $2048 - 1 = 2047$ &c. sunt numeri primi. Ergo $2.3 = 6$, $4.7 = 28$, $31.16 = 496$, $127.64 = 8128$, $2047.1024 = 2096128$ &c. &c. sunt numeri perfecti.

SCHOLION.

249. *Problemata indeterminata, qualia plurima solvit* Diophantus, *difficiliora sunt determinatis, nisi simplicia*

Aunado a lo que Euler encontró sobre números perfectos en la obra de Christian Wolff, seguramente también conoció lo que otros pensaban sobre este tema en la primera mitad del siglo XVII. La lista de personajes que se adentraron en el estudio de propiedades de estos números es amplia, pero sus aportaciones en general no son trascendentes. Sin embargo hay un personaje que no se puede dejar de mencionar: René Descartes. Él envió una carta el 15 de noviembre de 1638 al matemático francés Marin Mersenne en la que

afirmaba que tenía nuevos resultados sobre números perfectos de la forma euclidiana. Conociendo sus capacidades matemáticas, era de esperarse que presentara algún resultado interesante respecto a los perfectos pares, y con ello se podría ver algo trascendente para estos números, pues desde Euclides no se tenía algo verdaderamente sobresaliente. Lamentablemente nunca se dieron a conocer dichos resultados, y solamente Descartes sabe qué es lo que tenía entre manos.

Con Euler se llega a las condiciones necesarias y suficientes.

Euler conocía muy bien los libros aritméticos de los *Elementos* de Euclides. Se sabe que para inicios del siglo XVIII circulaban por Europa las ediciones – de los Elementos - de Tartaglia (1586), Mardele (1622), Henrion (1676), Zamberti (1537), Gregorii (1703), Commandino (1575), Clavius (1574), entre otras, que contenían los libros del siete al nueve. El resultado euclidiano de la proposición 36 del libro 9 dice lo siguiente:

> "*Todo número de la forma* $2^{P-1}\left(2^P-1\right)$ *con* 2^P-1 *primo, es número perfecto par*"[28].

Pero Euler sabía de la posibilidad de que pudieran existir otros perfectos pares que tuvieran una forma diferente a la de $2^{P-1}\left(2^P-1\right)$con 2^P-1 primo. Es decir, con este teorema se tenía la existía de un conjunto de números que sí

[28] Aquí se enuncia una versión moderna del resultado. Para conocer el enunciado original, así como la demostración, se puede ver un apéndice al final de este capítulo, y una demostración en términos actuales se proporciona más adelante.

eran perfectos pares, pero que dependían de la existencia de primos con la forma $(2^p - 1)$, y de éstos últimos, a la fecha no sabemos si es un conjunto infinito. Así, si la aparición de los primos de Mersenne es tan escasa,[29] y esto nos lleva a tanta incertidumbre sobre la existencia de perfectos pares de la forma euclidiana, entonces, ¿por qué no pensar en la existencia de perfectos pares con otra forma?

Por otro lado, si se piensa que la existencia de los perfectos pares se reduce a los de la forma euclidiana, entonces se requiere demostrar el inverso de la proposición 36 del libro 9 de los *Elementos*, y con ello se establecerían las condiciones necesarias y suficientes para que todo perfecto par sea sólo de la forma $2^{P-1}(2^P - 1)$ con $2^P - 1$ primo.

Durante el siglo XVII el resultado euclidiano no proporcionó los elementos adecuados para demostrar el recíproco. El inverso del teorema euclidiano tuvo que esperar alrededor de 2000 años, y la persona que enfrontó este pendiente fue Euler. La demostración del recíproco de la proposición 36 de Euclides se encuentra en dos de sus trabajos. Uno es el libro inconcluso de Teoría de los Números titulado "*Tractatus de Numerorum*" (E-792) que se conoció hasta 1849, sesenta y seis años después de su muerte[30]. El otro trabajo donde se encuentra la demostración es: "*De Numeris Amicabilis*" (E152).

[29] Actualmente se conocen menos de cincuenta.
[30] Se desconoce cuándo lo escribió; de hecho, hubiese sido el primer libro sobre Teoría de los Números, ya que fue posteriormente, en 1798, que apareció publicado el de Legendre.

Demostración de Euler[31]

En el apartado 106 del *Tractatus* Euler caracterizó lo que es un número perfecto N como: $\int N = 2N$.[32] Posteriormente, supone que si éste es par entonces puede tener la forma $N = 2^n \times A$, con A impar.

Así, $N = 2^n \times A \quad \Leftrightarrow \quad 2N = 2 \cdot 2^n \times A = 2^{n+1} \times A$

$$\Leftrightarrow \quad 2^{n+1} \times A = \int (2^n \times A),$$

lo último se puede hacer porque $2N = \int N$. Por otro lado como 2^n y A no tienen divisores comunes, entonces Euler factorizó a la función suma de divisores para obtener que $2^{n+1} \times A = \int 2^n \times \int A$.

Ahora, como la suma de los divisores de 2^n es

$$1 + 2 + 2^2 + 2^3 + \cdots + 2^n = 2^{n+1} - 1,$$

entonces,

$2^{n+1} \times A = (2^{n+1} - 1) \times \int A \quad \Leftrightarrow \quad \frac{\int A}{A} = \frac{2^{n+1}}{(2^{n+1} - 1)}$. El hecho de que $\frac{2^{n+1}}{(2^{n+1} - 1)}$ es un número muy cercano a uno le bastó a Euler para usar otro de sus resultados que dice lo siguiente:

---

[31] La demostración que aquí se presenta está totalmente apegada a la original que se encuentra en el *Tractatus*, pero hemos agregado algunos pasos adicionales en el proceso con del fin de que sea más comprensible.

[32] Euler denota a la función suma de los divisores de N como: $\int N$. Aquí es muy importante señalar que la enorme diferencia entre el trabajo de Euclides y el de Euler es que el primero consideró como divisores de N sólo a los divisores propios, es decir, no consideró al mismo N como uno de ellos, mientras que Euler sí lo hizo.

"Si $\frac{\int N}{N}=\frac{m}{n}$ *donde* $\frac{m}{n}$ *es un número pequeño y N es diferente de uno, entonces,* $m>n$ *y* $N=n$"

y con esto pudo concluir que $A=\left(2^{n+1}-1\right)$ y en consecuencia, como

$$2^{n+1}\times A=\left(2^{n+1}-1\right)\times\int A\Rightarrow\int A=2^{n+1}$$

y por la forma antes mencionada de A, se tiene que $\int A=A+1$.

De esta manera concluyó que A es primo. Finalmente, dado que $\mathrm{N}=2^{\mathrm{n}}\times\mathrm{A}$ es perfecto par y $\mathrm{A}=\left(2^{\mathrm{n}+1}-1\right)$ es primo, entonces $N=2^{n}\left(2^{n+1}-1\right)$.

Con este resultado por fin se llegaba a una demostración del recíproco de la proposición 36 de Euclides. Es claro que el paso donde concluyó que $A=\left(2^{n+1}-1\right)$ no está plenamente justificado, pero ya sabemos que en la vasta obra de Euler es frecuente encontrar situaciones de esta clase, y las soluciones a estas interrogantes se pueden encontrar en trabajos subsecuentes, en algunos casos, o de plano ya no los demuestra. Sin embargo, y con mucha frecuencia llegarían otros matemáticos, posteriores a él, para justificar estos resultados matemáticos que Euler dejó pendientes, y que en la mayoría de los casos si eran resultados válidos.

Es en este tenor que Euler nos proporciona su "*De Numeris Amicabilis*" (escrito en 1747), donde trabajó con la igualdad $\frac{\int \mathrm{A}}{\mathrm{A}}=\frac{2^{\mathrm{n}+1}}{\left(2^{\mathrm{n}+1}-1\right)}$. Ahí supone que existe una *c* tal que $\mathrm{A}=\mathrm{c}\left(2^{\mathrm{n}+1}-1\right)$ y $\int \mathrm{A}=\mathrm{c}\cdot 2^{\mathrm{n}+1}$, y de la que logra de-

ducir que $c \geq 1$. Pero aún con la lectura de este último artículo no quedaba plenamente justificado (desde nuestra perspectiva actual), que a partir de $\frac{\int A}{A} = \frac{2^{n+1}}{(2^{n+1}-1)}$ se pudiera concluir que $\int A = A + 1$.

Lo que haremos ahora es retomar el proceso euleriano y tratar de llegar al final de la demostración sin que existan tropiezos en el proceso, pero se aclara que los elementos matemáticos que se usarán ya no son necesariamente con los que contaba Euler.

Entonces, de $\frac{\int A}{A} = \frac{2^{n+1}}{(2^{n+1}-1)}$ se tiene que $2^{n+1} \times A = (2^{n+1}-1) \times \int A$ y entonces la suma de divisores de A se puede separar en aquellos que son propios y los que no lo son; en la notación de Euler sería $\int A = A + t$, donde $t = \sum_{\substack{d|A \\ d<A}} d$ con lo que se obtiene que $2^{n+1} \times A = (2^{n+1}-1) \times (A + t)$. Simplificando se llega a que $A = t(2^{n+1}-1)$, por lo que $t \mid A$, pero recuérdese que t es la suma de los divisores menores que A, y como t divide a A entonces t tendría que pertenecer al conjunto de los mismos sumandos de t, lo cual sucede sólo cuando $t = 1$ y, por consiguiente, $\int A = A + 1$ con lo que se concluye que A es un primo y además es tal que $A = (2^{n+1}-1)$. Por lo tanto, $N = 2^n \times A = 2^n (2^{n+1}-1)$ con $(2^{n+1}-1)$ primo.

Con estos ajustes queda completa la demostración, y la parte fundamental para que Euler pudiera avanzar en esta dirección es que él ya consideraba

que uno de los divisores de un entero dado es el mismo entero. Hay que resaltar que esto nunca lo consideró Euclides.

Para terminar esta exposición euleriana de los perfectos pares ahora presentamos las demostraciones modernas de las dos partes del teorema.

Teorema: *Sea n un entero de la forma* $2^{P-1}\left(2^P-1\right)$ *donde* 2^P-1 *es número primo, si y sólo si es un número perfecto par.*

DEMOSTRACIÓN.

Euclides $\Rightarrow$)

Sea *n* un número par de la forma $2^{P-1}\left(2^P-1\right)$ donde 2^P-1 es un primo. Como *n* es un producto de potencias de primos diferentes, y como la función suma de divisores es multiplicativa para factores que son primos relativos, entonces la función suma de divisores para *n* es:

$$\sigma(n)=\left(1+2^1+2^2+2^3+\cdots+2^{P-1}\right)\left(1+\left(2^P-1\right)\right).$$

Por inducción se sabe que

$$1+2^1+2^2+2^3+2^4+\cdots+2^{P-1}=2^P-1.$$

Entonces, $\sigma(n)=2^P\left(2^P-1\right)=2\left(2^{P-1}\left(2^P-1\right)\right)=2n$, y por la definición de número perfecto, entonces toda $n = 2^{P-1}\left(2^P-1\right)$ donde 2^P-1 es número primo, es un número perfecto par.

Euler $\Leftarrow$)

Sea n un número perfecto par, y sin pérdida de generalidad siempre puede

ser representado de la forma $n = 2^{p-1}(r)$, donde r es un impar y $P > 1$. Dado que $(2^{P-1}, r) = 1$ (primos relativos), entonces $\sigma(n) = \sigma(2^{P-1}) \cdot \sigma(r)$. Y como

$$1 + 2^1 + 2^2 + 2^3 + \cdots + 2^{P-1} = 2^P - 1 = \sigma(2^{P-1}),$$

entonces, $\sigma(n) = (2^P - 1) \cdot \sigma(r)$, y además $\sigma(n) = 2(2^{p-1}(r)) = 2^p \cdot r$ por ser n perfecto.

Por otro lado, podemos plantear que $\sigma(r) = r + s$, donde s representa a la suma de todos los divisores positivos de r menores que r. Así, sustituyendo:

$$\sigma(n) = \sigma(2^{P-1}) \cdot \sigma(r) = (2^P - 1)(r + s) = 2^P \cdot r \quad \Leftrightarrow$$

$$s(2^P - 1) = r(2^P) - r(2^P - 1) \quad \Leftrightarrow \quad r = s(2^P - 1)$$

de aquí se ve que $s \mid r$, pero s es la suma de todos los divisores positivos de r menores que r, por lo que, $s = 1$ y $r = (2^P - 1)$. De esto se tiene que $\sigma(r) = r + 1$, y en consecuencia r es un número primo. Por lo tanto, el número perfecto par *n* es de la forma $2^{p-1}(2^p - 1)$ con $2^p - 1$primo.

Con este resultado Euler finalmente cerró el círculo de un teorema que tenía aproximadamente 2 mil años en espera de ser demostrado. Pero él no se detuvo –respecto a números perfectos- con lo que ya habia empezado en el artículo de 1732; faltaba dar los primeros pasos para resolver el problema más complicado de esta clase de números, y nos referimos a encontrar los perfectos impares.

El Factor de Euler.

El primer resultado significativo para los números perfectos impares fue aportado por Euler, y lo pudo hacer a pesar de no conocer alguno. Tuvo el genio de dar un perfil de cómo tendrían que ser, en el caso de existir. Demostró que

Si n es un perfecto impar entonces $n = q^{\alpha} P_1^{2\beta_1} P_2^{2\beta_2} P_3^{2\beta_3} \cdots P_r^{2\beta_r}$, *donde* $q \equiv \alpha \equiv 1 \pmod 4$ *y* $q, P_1, P_2, \cdots P_r$ *son primos impares diferentes.*

Esta aportación inicial dio lugar a que al factor q^{α} se le conozca actualmente como el "Factor de Euler".

De esta manera, con números de la forma $n = q^{\alpha} P_1^{2\beta_1} P_2^{2\beta_2} P_3^{2\beta_3} \cdots P_r^{2\beta_r}$ se tuvo el punto de partida para construir un conjunto de propiedades que hasta ahora no ha dejado de crecer. Sin embargo, aunque ya se tenía la caracterización de Euler para los perfectos impares, fue necesario esperar hasta las primeras décadas del siglo XX para tener nuevamente resultados dignos de ser mencionados.

Ahora proporcionamos unos ejemplos de investigaciones recientes para ver que el camino que trazó Euler respecto a los perfectos impares fue el correcto. Estas aportaciones ayudan a descartar aquellos impares que no pueden ser perfectos, con la esperanza de que exista uno entre aquellos que quedan.

- De la forma euleriana de los perfectos impares

$$n = q^{\alpha} P_1^{2\beta_1} P_2^{2\beta_2} P_3^{2\beta_3} \cdots P_r^{2\beta_r}$$

ahora sabemos que estos *n* no pueden existir con la particularidad de que los factores β_i de los exponentes pertenezcan a la misma clase residual.

- Iannucci [2003] demostró que si $3|n$ y $n = q^{\alpha} P_1^{2\beta_1} P_2^{2\beta_2} P_3^{2\beta_3} \cdots P_r^{2\beta_r}$ donde $q \equiv \alpha \equiv 1 \pmod 4$ con α, β_i enteros positivos y tales que $\beta_1 \equiv \beta_2 \equiv \cdots \equiv \beta_r \equiv 2 \ (mod\ 5)$, entonces n no es un perfecto impar.
- Otro resultado semejante se da cuando $\beta_1 \equiv \beta_2 \equiv \cdots \equiv \beta_r \equiv 38 \pmod{77}$, también, Hagis y McDaniel [1975] lo probaron para $\beta_i \equiv 17 \pmod{35}$.
- McDaniel [1970] demostró que si todos los β_i cumplen que $\beta_i \equiv 1 \pmod 3$, entonces no puede existir un perfecto impar con las características eulerianas.
- Steuerwald [1937] demostró que n no es un número perfecto impar si $\beta_1 = \beta_2 = \beta_3 = \ldots = \beta_r = 1$. Hagis y McDaniel lo probaron para $\beta_1 = \beta_2 = \beta_3 = \ldots = \beta_r = 3$.

Con estos elementos como telón de fondo toca ahora revisar la demostración de Euler que se encuentra en el "*Tractatus de numerorum"*. El teorema enuncia lo siguiente:

Teorema. Si n es un número perfecto impar, entonces n es de la forma $n = q^{\alpha} P_1^{2\beta_1} P_2^{2\beta_2} P_3^{2\beta_3} \cdots P_r^{2\beta_r}$***, donde los*** $q, P_1, P_2, \cdots P_r$ ***son primos im-***

pares distintos y, además, $q \equiv \alpha \equiv 1 \pmod 4$.

DEMOSTRACIÓN.

Como n es un número perfecto impar entonces se tiene por definición que $\sigma(\mathrm{n}) = 2\mathrm{n}$ y sin pérdida de generalidad podemos decir que su factorización en primos es $n = q^{\alpha} P_1^m P_2^t P_3^u \cdots P_r^z$. Ahora, considerando que σ (función suma de divisores) es una función multiplicativa se tiene que:

$$2n = \sigma\left(q^{\alpha} P_1^m P_2^t P_3^u \cdots P_r^z\right) = \sigma\left(q^{\alpha}\right) \cdot \sigma\left(P_1^m\right) \cdot \sigma\left(P_2^t\right) \cdot \sigma\left(P_3^u\right) \cdots \sigma\left(P_r^z\right)$$

Además, dado que n es impar se sigue que $2\mathrm{n}$ es el doble de un impar; entonces, entre los factores $\sigma\left(q^{\alpha}\right) \cdot \sigma\left(P_1^m\right) \cdot \sigma\left(P_2^t\right) \cdot \sigma\left(P_3^u\right) \cdots \sigma\left(P_r^z\right)$ sólo hay uno que es "imparmente" par y los restantes son impares.

Ahora, sin pérdida de generalidad, se toma el factor $\sigma\left(P_1^m\right)$ como un impar y por lo tanto $\sigma\left(P_1^m\right) = \dfrac{P_1^{m+1} - 1}{P_1^m - 1} = P_1^m + P_1^{m-1} + \cdots + P_1^2 + P_1 + 1$.

Como el primo P_1 es impar y $P_1^m + P_1^{m-1} + \cdots + P_1^2 + P_1 + 1$ es una suma de m impares más uno, entonces se deduce que el exponente *m* tiene que ser par para que se cumpla que el factor $\sigma\left(P_1^m\right)$ sea impar. De esta manera, P_1^m es una potencia par de un número impar, por lo que P_1^m será un cuadrado perfecto de la forma $P_1^{2\beta_1}$. Así se concluye que todos los factores primos $P_1^m P_2^t P_3^u \cdots P_r^z$ de n, a excepción de q^{α}, serán cuadrados perfectos.

Por otro lado, sea $\sigma\left(q^{\alpha}\right)$ el factor imparmente par de $\sigma(\mathrm{n})$

$\left(\text{es decir, } \sigma\left(q^{\alpha}\right)=2(2\varphi+1)=4\varphi+2 \Rightarrow \sigma\left(q^{\alpha}\right)\equiv 2 \pmod 4\right)$, por lo que q es de la forma $4\mathrm{k}+1$ ó $4\mathrm{k}+3$. Se afirma que q es de la forma $4k+1,$ porque si $\mathrm{q}=4\mathrm{k}+3$ se tendría que $\sigma\left(q^{\alpha}\right)\not\equiv 2 \pmod 4$ lo que contradice el hecho de que $\sigma\left(q^{\alpha}\right)$ es imparmente par. Y esto se puede probar de la siguiente manera. A partir de la suma $\sigma\left(q^{\alpha}\right)=q^{\alpha}+q^{\alpha-1}+\cdots+q^{2}+q+1,$ veamos cómo son los sumandos para potencias pares o impares de cualquier número de la forma 4k+3.

i) $(4k+3)^{s}\equiv 1 \pmod 4$ si s es par. Esto se justifica al ver que si

$(4k+3)^{2}\equiv 1 \pmod 4$, entonces $\left((4k+3)^{2}\right)^{n}\equiv 1^{n} \pmod 4$

$\Rightarrow (4k+3)^{2n}\equiv 1 \pmod 4$, por lo tanto se cumple para la potencia par.

ii) $(4k+3)^{s}\equiv 3 \pmod 4$ si s es impar. Y se justifica a partir del resultado anterior para pares $(4k+3)^{2n}\equiv 1 \pmod 4$, al que se multiplica por (4k + 3), para obtener

$(4k+3)(4k+3)^{2n}\equiv 1(4k+3) \pmod 4$

$\Rightarrow (4k+3)^{2n+1}\equiv (4k+3) \pmod 4$, pero $4k+3\equiv 3 \pmod 4$.

Y se llega finalmente a que $(4k+3)^{2n+1}\equiv 3 \pmod 4$, y así se tiene el resultado para toda potencia impar.

Con i) y ii) se cubren todas las potencias $s=\alpha,\alpha-1,\ldots,2,1$ de

$$\sigma\left(q^{\alpha}\right)=q^{\alpha}+q^{\alpha-1}+\cdots+q^{2}+q+1,$$

y se concluye con las suma de las congruencias respectivas de i) y ii) que:

$\sigma\left(q^{\alpha}\right)\equiv 1\left(\mathrm{mod}\ 4\right)$ si α es par, o

$\sigma\left(q^{\alpha}\right)\equiv 0\ \left(mod 4\right)$ si α es impar.

De las dos congruencias se ve que no puede suceder que:

$\sigma\left(q^{\alpha}\right)\equiv 2\left(\mathrm{mod}\ 4\right)$, para $q = 4k + 3$.

Así, q tiene que ser de la forma $4\mathrm{k}+1$, y entonces

$$1,\ \mathrm{q},\ \mathrm{q}^{2},\ \cdots\ \mathrm{q}^{\alpha-1},\ \mathrm{q}^{\alpha}\ \equiv\ 1\ \ (\mathrm{mod}\ \ 4).$$

Ahora, dado que $\sigma\left(q^{\alpha}\right)=q^{\alpha}+q^{\alpha-1}+\cdots+q^{2}+q+1$ es una suma par cuya cantidad de sumandos es $\alpha+1$, entonces se deduce que α es impar, el cual podría ser de la forma $4\lambda+1$ ó $4\lambda+3$. Por la estructura de las potencias de q se tiene que cada una es de la forma:

$$4\mathrm{k}_{1}+1,\ \ 4\mathrm{k}_{2}+1,\ \ 4\mathrm{k}_{3}+1,\ \ 4\mathrm{k}_{4}+1,\ \ 4\mathrm{k}_{5}+1\ \ \ldots\ \ 4\mathrm{k}_{\alpha}+1\ \Rightarrow$$

$$1+\mathrm{q}+\mathrm{q}^{2}+\mathrm{q}^{3}+\cdots+\mathrm{q}^{\alpha}\ \ =\ \ 1+4\left(\mathrm{k}_{1}+\mathrm{k}_{2}+\mathrm{k}_{3}+\cdots+\mathrm{k}_{\alpha}\right)+\alpha\ \ \Leftrightarrow$$

$$4\left(\mathrm{k}_{1}+\mathrm{k}_{2}+\cdots+k_{\alpha}\right)+\left(\alpha+1\right)\ =\ 4K'+\left(\alpha+1\right)=2\Gamma=\sigma\left(q^{\alpha}\right)$$

Así, $\alpha=4\lambda+3$ implica que $\sigma\left(q^{\alpha}\right)=2\Gamma$ *con* Γ *par* es decir $\sigma\left(q^{\alpha}\right)=2\left(2\varphi\right)$ llegándose a una contradicción ya que por hipótesis $\sigma\left(q^{\alpha}\right)$

es imparmente par. Por lo tanto, $\alpha = 4\lambda + 1$ y por consiguiente $\alpha \equiv 1 \pmod 4$.

Por todo lo anterior, ha quedado demostrado que todo número perfecto impar *n* es de la forma $n = q^{\alpha} P_1^{2\beta_1} P_2^{2\beta_2} P_3^{2\beta_3} \cdots P_r^{2\beta_r}$ donde los q, P_1, P_2, $\cdots$ P_r son primos impares distintos y $q \equiv \alpha \equiv 1 \pmod 4$. ■

Para terminar esta sección de los números perfectos, regresamos al artículo de los teoremas de Fermat (E26) para señalar que Euler mencionó la siguiente propiedad que pareciera ser un simple resultado sobre los primos de Mersenne. Y es el siguiente:

Si (4q – 1) y (8q – 1) son primos, entonces $2^{4q-1} \equiv 1\ (mod\ (8q-1))$.

Por un lado este teorema proporciona elementos para descartar números de la forma $2^n - 1$ que no pueden ser primos, pues sucede que si n = (4q – 1), entonces otro primo divide a $2^n - 1$, y por consiguiente este tipo de números de Mersenne no pueden ser primos, y a la vez tampoco ser factor primo de un perfecto par. Pero si revisamos con más cuidado este teorema encontramos que para justificarlo ya intervienen elementos que Euler estaba usando para la construcción de la teoría de los residuos cuadráticos.

Si vemos un bosquejo de demostración[33] empleando los elementos matemáticos que tenía Euler, se tiene que como $(8q - 1)$ y 2 son primos relativos, y recurriendo al pequeño teorema de Fermat, entonces

$2^{8q-2} \equiv 1 \pmod{8q-1} \Rightarrow 2^{8q-2} - 1 = \left(2^{4q-1} - 1\right)\left(2^{4q-1} + 1\right)$ y de aquí se

[33] Euler no demuestra este resultado en el artículo de 1732 (E26); sólo lo menciona como algo que sucede en el contexto de los números perfectos.

tiene que $8q-1$ divide a $\left(2^{4q-1}+1\right)$ ó $8q-1$ divide a $\left(2^{4q-1}-1\right)$, pero no a ambos, porque pasaría que $8q-1$ divide a 2, lo cual no puede suceder pues $8q$ – 1 es impar. A partir de aquí se podría ver qué casos particulares de primos de la forma $8q-1$ no divide a $\left(2^{4q-1}+1\right)$, pero que sí dividen a los de la forma $\left(2^{4q-1}-1\right)$. Así, es posible que Euler haya inferido a partir de casos particulares que *"Si (4q – 1) y (8q – 1) son primos, entonces* $2^{4q-1}\equiv 1 \pmod{8q-1}$ *"*.

Pero también es posible que Euler ya estuviera intercalando diversas ideas que involucraban a los divisores primos de los números de la forma $a^n - b^n$. Ya sabemos que propuso que

> "Si *p* es un primo impar y *a* que pertenece a los enteros positivos es primo relativo con *p,* y cumple que $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$, entonces *a* es un residuo cuadrático módulo p.

Y de aquí se pasa al criterio de que *a* es un residuo cuadrático modulo *p*, siempre y cuando *p* sea de la forma $(8q – 1)$.

Con este resultado se puede apreciar que Euler tenía un cúmulo de ideas que involucraban diferentes implicaciones partiendo de las mismas premisas, es decir, los elementos que descartaban primos de Mersenne para los factores de perfectos pares, serían los mismos que nos indicarían criterios para conocer las posibilidades de que un número fuera residuo cuadrático módulo un determinado primo.

Apéndice

Demostración de la Proposición 36 del Libro IX de *"Los Elementos"* de Euclides.[34]

Proposición 36: *"Si tantos números como se quiera a partir de una unidad se disponen en proporción duplicada hasta que su* [suma] *total resulte* [un número] *primo, y el total multiplicado por el último produce algún número, el producto será [número] perfecto".*

Demostración.

Pues dispónganse tanto números como se quiera, A, B, Γ y Δ, a partir de una unidad en proporción duplicada hasta que su (suma) total resulte (un número) primo, y sea E igual al total y E, al multiplicar a D, haga ZH.

Digo que ZH es un (número) perfecto.

A__ B___ Γ _____ Δ _____

Pues cuantos números son en cantidad A, B, Γ y Δ, tómense tantos números E, ΘK, Λ, M, en proporción duplicada a partir de E; entonces, por igualdad, como A es a Δ, así es E a M [Libro VII, Prop. 14]. Así pues, el producto de E, Δ es igual al (producto) de A, M [Libro VII, prop. 19]. Ahora bien, el producto de E, Δ es ZH; entonces el (producto) de A, M es también ZH. Luego A, al multiplicar M, ha hecho ZH; por tanto, M mide ZH según las unidades de A. Pero A es una díada; luego ZH es el doble de M. Pero M, Λ,

[34] La siguiente traducción se tomó íntegra de la edición de editorial Gredos. La traducción fue realizada por María Luisa Puertas Castaños.

ΘK, E son sucesivamente el doble uno del otro; entonces E, ΘK, Λ, M, ZH son continuamente proporcionales en proporción duplicada.

E_____

Θ_____ N_____K

Λ_____

Z_____Ξ_____

M_____

O_____

Ahora del segundo ΘK y del último ZH quítense ΘN y ZΞ, respectivamente iguales a E. Entonces como el exceso del segundo número es al primero, así el exceso del último a todos los anteriores a él [Libro IX, Prop. 35]. Así pues, como NK es a E, así ΞH a M, Λ, KΘ, E. Y NK es igual a E; entonces ΞH también es igual a M, Λ, ΘK, E. Pero ZΞ también es igual a E y E a A, B, Γ, Δ y la unidad. Así pues, el total ZH también es igual a los (números) E, ΘK, Λ, M y a los (números) A, B, Γ, Δ y la unidad; y es medido por ellos.

Digo que ZH no será medido por ningún otro fuera de A, B, Γ, Δ, E, ΘK, Λ, M y la unidad. Pues, de ser posible mida un número O a ZH, y no sea O el mismo que ninguno de lo números A, B, Γ, Δ, E, ΘK, Λ, M. Y cuantas veces O mida a ZH, tantas unidades haya en Π; entonces Π, al multiplicar a O, ha hecho ZH. Pero, en efecto, E, al mutiplicar a Δ, ha hecho también ZH; entonces, como E es a Π, O es a Δ [Libro VII, Prop. 19]. Y puesto que A, B, Γ, Δ, son continuamente proporcionales a partir de la unidad, entonces Δ no será medido por ningún otro fuera de A, B, Γ [Libro IX Prop. 13]. Ahora

bien, se ha supuesto que O no es el mismo que ninguno de los (números) A, B, Γ; por tanto, O no medirá a Δ. Pero, como O es a Δ, E es a Π; entonces E tampoco mide a Π [Libro VII, Def. 21]. Y E es primo. Pero todo número primo es primo con respecto a todo aquel al que no mide [Libro VII, Prop. 29]. Asi pues, E, Π son primos entre sí. Pero los primos también son los menores [Libro VII, Prop. 21] y los menores miden a los que guardan la misma razón que ellos el mismo número de veces, el antecedente al antecedente y el consecuente al consecuente [Libro VII, Prop. 20]; ahora bien, como E es a Π, O es a Δ; entonces, E mide a O el mismo número de veces que Π a Δ. Pero Δ no es medido por ningún otro fuera de A, B, Γ; luego Π es uno de los (números) A, B, Γ. Sea el mismo que B y cuantos son B, Γ, Δ en cantidad tómense tantos E, ΘK, Λ a partir de E. Ahora bien, E, ΘK, Λ guardan la misma razón que B, Γ, Δ; entonces, por igualdad, como B es a Δ, E es a Λ [Libro VII, prop. 14]. Luego el (producto) de B, Λ es igual al (producto) de Δ, E [Libro VII, Prop 19]; pero, el (producto) de Λ, E es igual al (producto) de Π, O; entonces el (producto) de Π, O es igual al (producto) B, Λ. Luego como Π es a B, Λ es a O [Libro VII, Prop.19]. Pero Π es el mismo que B; entonces Λ es el mismo que O; lo cual es imposible, porque se ha supuesto que O no era el mismo que ninguno de los (números) puestos, luego ningún número medirá a ZH fuera de A, B, Γ, Δ, E, ΘK, Λ, M y la unidad. Y se ha demostrado que ZH es igual a A, B, Γ, Δ, E, ΘK, Λ, M y la unidad. Pero un número perfecto es igual a sus propias partes [Libro VII, Def. 23].

Por consiguiente, ZH es un (número) perfecto. Q.E.D.

Capítulo IV

Sobre el pequeño teorema de Fermat.

Antecedentes

Desde el inicio de este trabajo de tesis ha quedado de manifiesto que desde los primeros años en los que Euler se interesó por la teoría de los números los problemas de Fermat siempre estuvieron en su mente. De los problemas que el matemático francés planteó, muchos de ellos producto de su lectura de la *Aritmética* de Diofanto, Euler abordó prácticamente todos, y para cada uno tuvo comentarios importantes, e incluso les dio solución.

Entre los problemas pendientes que dejó Fermat existe uno que no podía haber dejado de llamar la atención de Euler, y esté apareció en su artículo de 1732. Se trata de un caso particular de los divisores de los números de la forma a^n-b^n, y que ahora conocemos como el *Pequeño Teorema de Fermat*.

Como se vio en el primer artículo (E26), Euler planteó entre otras cosas, que de existir números primos de la forma $a^n + 1$, éstos tendrían que ser como un número de Fermat, y mostró además que el quinto número no es primo (*i.e.* $2^{2^5} + 1$ no es primo). En una segunda parte hace un análisis acerca de los números perfectos, pero sobre todo de cuándo los números de la forma $2^n - 1$ no son primos, a pesar de que *n* sí lo es. Al final de esta sección Euler comentó que dedujo todas estas observaciones de cierto teorema para el cual no tenía una demostración, pero del que estaba seguro de su va-

lidez. Sin decir más enuncia el teorema, que es el siguiente:

> $a^n - b^n$ siempre será divisible por $n + 1$, si $n + 1$ es un número primo que no divida ni a a ni a b.

Este teorema lleva al pequeño teorema de Fermat para un caso particular de b. Posteriormente Euler presentó en el mismo artículo (E26) algunas proposiciones relacionadas con este teorema, pero en ninguna concretó algo que pudiera parecer una demostración del *pequeño teorema*.

Este teorema de Fermat fue uno de los problemas recurrentes a lo largo de la vida matemática de Euler, reapareciendo una y otra vez mientras se ocupaba de diversos temas y a lo largo de su periplo geográfico. No se puede dejar de mencionar que además de los artículos donde publicó las demostraciones del teorema, también su correspondencia tuvo un rol fundamental para darnos a conocer la evolución de las ideas matemáticas que le llevaban de regreso a esta temática. En este contexto la comunicación con Christian Goldbach proporciona partes importantes de la evolución de las demostraciones del pequeño teorema.

San Petersburgo

En 1736 Euler presentó el trabajo *Theorematum quorundam ad numeros primos spectantium demonstratio* (*Una prueba de ciertos teoremas respecto a números primos*, E54). Aquí incluyó la primera demostración del pequeño teorema, y como se indicó antes, el objetivo del trabajo no era sólo este resultado, sino que fue la consecuencia de una serie de implicaciones que enseguida se comentarán.

En *Theorematum quorundam* introduce el método que ahora conocemos como inducción. Sobre éste menciona que aún le parecía insuficiente y poco eficaz para demostrar algunas proposiciones. Euler, con esto en mente, recuerda nuevamente los números de la forma $2^{2^n}+1$. Posteriormente comenta que encontró algunos teoremas relacionados con números de Fermat y otros que conciernen a números perfectos, y que estos podrían ser demostrados por el método de inducción que era algo novedoso, y que estaba poniendo en práctica. Así, se dirigió a probar algunos teoremas y entre ellos se encontraba la primera de sus demostraciones del pequeño teorema de Fermat. Cabe recordar que el pequeño teorema no era el principal objetivo de este artículo de 1736. Más bien todo apunta a que existía un interés compartido entre abordar ciertos puntos arriba mencionados y experimentar con las nuevas herramientas de la inducción. El teorema se enuncia así:

> **Teorema 1** *Si p denota un número primo, el término* $a^{p-1}-1$ *siempre puede ser dividido por p, a menos que a pueda ser dividida por p.*

Para establecer su modalidad de inducción Euler primero demostró un par de teoremas que son casos particulares del pequeño teorema. Finalmente propuso un teorema que nos recuerda el método actual de inducción, en el supone que si se cumple que $p|(a^p-a)$ entonces se puede llegar a que $p|((a+1)^p-(a+1))$.

Antes de exponer los teoremas y sus respectivas demostraciones, recordemos nuevamente que la inducción que empleó Euler estaba en proceso de consolidación. Es más, recordemos que los primeros procesos de un

método de inducción empezaron con F. Maurolico en la segunda mitad del siglo XVI, y prácticamente fue para construir los términos generales de ciertas sucesiones. Cuando Euler usó un proceso inductivo en *Teoremas sobre divisores de números*, escrito en 1747, se notó que aún no había consistencia en el uso del método, esto es, no usó claramente los pasos para validar que determinado resultado se cumple de manera sucesiva para el valor actual y para el que le sigue. Pero es importante decir que para el proceso que sigue sí está aplicando los pasos que actualmente se esperarían para un proceso de inducción.

Ahora se presentan los teoremas y sus respectivas demostraciones.

Teorema 2 *Si p es un número primo impar, entonces el término $2^{p-1}-1$ siempre será dividido por p.*

Demostración. Si en lugar de 2 se toma la partición $1+1$, entonces por la fórmula del binomio de Newton se tiene que:

$$(1+1)^{p-1} = 1 + \frac{p-1}{1} + \frac{p-1}{1}\frac{p-2}{2} + \frac{p-1}{1}\frac{p-2}{2}\frac{p-3}{3} + \frac{p-1}{1}\frac{p-2}{2}\frac{p-3}{3}\frac{p-4}{4}\ldots$$

De esta manera se obtiene una cantidad *p* de sumandos que además es impar. Ahora, como cada uno de los sumandos es un coeficiente binomial, todos serán números enteros positivos. Si a la igualdad anterior se le resta uno, entonces se tiene:

$$\begin{aligned}(1+1)^{p-1} - 1 \\ &= \frac{p-1}{1} + \frac{p-1}{1}\frac{p-2}{2} + \frac{p-1}{1}\frac{p-2}{2}\frac{p-3}{3} \\ &+ \frac{p-1}{1}\frac{p-2}{2}\frac{p-3}{3}\frac{p-4}{4}\ldots\end{aligned}$$

donde el lado derecho de la igualdad tiene p-1 términos y es una cantidad par.

A continuación se suman por parejas los términos del lado derecho, es decir,

$$\frac{p-1}{1}+\frac{p-1}{1}\frac{p-2}{2},\quad \frac{p-1}{1}\frac{p-2}{2}\frac{p-3}{3}$$
$$+\frac{p-1}{1}\frac{p-2}{2}\frac{p-3}{3}\frac{p-4}{4},\quad \frac{p-1}{1}\frac{p-2}{2}\frac{p-3}{3}\frac{p-4}{4}\frac{p-5}{5}$$
$$+\frac{p-1}{1}\ldots\ldots\frac{p-6}{6},\ldots.$$

y así la suma original se reduce a la mitad de términos, con lo que se obtiene: $2^{p-1}-1=\frac{p}{1}\frac{p-1}{2}+\frac{p}{1}\frac{p-1}{2}\frac{p-2}{3}\frac{p-3}{4}+\frac{p}{1}\frac{p-1}{2}\frac{p-2}{3}\frac{p-3}{4}\frac{p-4}{5}\frac{p-5}{6}+\ldots\ldots$[35], el último término de esta nueva suma es p, pues[36] $\frac{(p-1)(p-2)(p-3)(p-4)\ldots.(p-(p-1))}{1\cdot2\cdot3\cdot4\cdot\ldots\cdot p-1}+1=\frac{(p-1)(p-2)(p-3)(p-4)\ldots.1+1}{1\cdot2\cdot3\cdot4\cdot\ldots\cdot p-1}=p.$ Y como cada término de la suma que representa a $2^{p-1}-1$ es un entero, entonces en la simplificación de cada uno de ellos queda el factor p primo, y en consecuencia se llega a que p divide a $2^{p-1}-1$.

El siguiente paso es demostrar bajo las mismas directrices que p divide a $3^{p-1}-1$, y después que p divide a $4^{p-1}-1$, y así hasta un caso general donde p divide a $a^{p-1}-1$. Pero sucede que con este método no se puede generalizar el **teorema 2**. Por ejemplo, para ver si p divide a $3^{p-1}-1$ se

[35]Euler usó la fórmula que con nuestra notación moderna conocemos así: $C_{p-1}^{k-1}+C_{p-1}^{k}=C_{p}^{k}$, es decir, que $\frac{(p-1)!}{(k-1)!(p-k)!}+\frac{(p-1)!}{k!(p-k-1)!}=\frac{p!}{k!(p-k)!}$.

[36] Se refiere a que $C_{p-1}^{p-2}+C_{p-1}^{p-1}=p$.

tiene que:

$$(1+2)^{p-1}-1=2\frac{p-1}{1}+2^2\frac{p-1}{1}\frac{p-2}{2}+2^3\frac{p-1}{1}\frac{p-2}{2}\frac{p-3}{3}+2^4\frac{p-1}{1}\frac{p-2}{2}\frac{p-3}{3}\frac{p-4}{4}\ldots$$

y por tanto

$$(1+2)^{p-1}-1=2\frac{p-1}{1}\left(1+2\frac{p-2}{2}\right)+2^3\frac{p-1}{1}\frac{p-2}{2}\frac{p-3}{3}\left(1+2\frac{p-4}{4}\right)+2^5\frac{p-1}{1}\frac{p-2}{2}\frac{p-3}{3}\frac{p-4}{4}\frac{p-5}{5}\left(1+2\frac{p-6}{6}\right)+\cdots$$

Pero de esta última igualdad se observa que en los sumandos del lado derecho no es claro que se pueda factorizar una *p*, y por ello no es posible llegar directamente a que p divide a $3^{p-1}-1$, y lo mismo pasa para los casos siguientes.

Pero a pesar de que Euler mencionó que este procedimiento no era el apropiado para la generalización, sí cabe preguntarnos para cuáles enteros sí era factible que se aplicara este método. Si se toma un entero de la forma 1 + *a*, entonces se tiene nuevamente que

$$(1+a)^{p-1}-1=a\frac{p-1}{1}+a^2\frac{p-1}{1}\frac{p-2}{2}+a^3\frac{p-1}{1}\frac{p-2}{2}\frac{p-3}{3}+a^4\frac{p-1}{1}\frac{p-2}{2}\frac{p-3}{3}\frac{p-4}{4}\ldots$$

y agrupando los sumandos de la derecha se tiene que

$$(1+a)^{p-1}-1=a\frac{p-1}{1}\left(1+a\frac{p-2}{2}\right)+a^3\frac{p-1}{1}\frac{p-2}{2}\frac{p-3}{3}\left(1+a\frac{p-4}{4}\right)+a^5\frac{p-1}{1}\frac{p-2}{2}\frac{p-3}{3}\frac{p-4}{4}\frac{p-5}{5}\left(1+a\frac{p-6}{6}\right)+\cdots$$

y de esto último resulta que si en los factores $\left(1+a\frac{p-2}{2}\right)$, $\left(1+a\frac{p-4}{4}\right)$, $\left(1+\right.$

$a\frac{p-6}{6}\Big)$, ...se considera que a es de la forma (1 - λp), con λ entero, entonces se llega a que p sí divide a $(1+a)^{p-1}-1$. Entonces podemos proponer que para los números enteros de la forma 1 + a = 1 + 1 - λp = 2 - λp, sí se puede usar el primer método de Euler. Y más aún, podemos decir que son enteros de la forma N = 2 - λp, que pertenecen a la clase de congruencias N ≡ 2 (mod p).

Segundo método

La segunda via que Euler propuso como una generalización tenía como base un resultado que dice (enunciado en términos modernos): $2^{p-1}-1$ es divisible por un primo p, si sólo si 2^p-2 el divisible por p (con p diferente de 2).

Para el caso particular de los intereses de Euler se tiene que

$$2^p=(1+1)^p=1+p+\frac{p(p-1)}{1\cdot 2}+\ldots+p+1$$

$$\Rightarrow \qquad 2^p-2=p+\frac{p(p-1)}{1\cdot 2}+\ldots+p,$$

Y es claro que si cada uno de los términos de la serie es divisible por p entonces 2^p-2 también lo será. Así que $2^{p-1}-1$ también es divisible entre p pues $2^p-2=2(2^{p-1}-1)$, y a menos que $p=2$, p sólo dividirá a $2^{p-1}-1$. De esta manera Euler siguió con su generalización del pequeño teorema.

Bajo el mismo esquema pasó a otro teorema que es el caso particular del pequeño teorema para $a=3$.

Teorema 3 *Si p es cualquier número primo excepto 3, entonces* $3^{p-1}-1$

siempre puede dividirse entre p

Demostración. Euler propuso que si $3^{p-1}-1$ puede dividirse por cualquier primo diferente de 3 entonces 3^p-3 podrá ser dividido por cualquier primo, y esto último es lo primero que demostró Euler para concluir finalmente lo primero.

Así, sea $3^p=(1+2)^p=1+2p+2^2\frac{p(p-1)}{2}+\ldots+2^{p-1}p+2^p$, entonces p divide a cada uno de los términos de la serie a excepción del primero y el último, por lo tanto p divide a 3^p-2^p-1, pero

$$3^p-2^p-1=3^p-3-2^p+2=3^p-3-(2^p-2),$$

y del **Teorema 2,** 2^p-2 siempre es divisible por un número primo, por lo tanto p divide a 3^p-3 y por ende si p es un primo distinto de 3 entonces divide a $3^{p-1}-1$, pues $3^p-3=3(3^{p-1}-1)$.

Después menciona que ya puede pasar de un valor de a al de $a+1$, y la forma de tratarlo será mediante el siguiente teorema.

Teorema 4 *Si* p *es un número primo que divide a* a^p-a *entonces* $(a+1)^p-(a+1)$ *también será dividido por* p.

Demostración. Si se expande $(1+a)^p=1+ap+a^2\frac{p(p-1)}{2}+\cdots+pa^{p-1}+a^p$, entonces nuevamente se tiene que cada término de la sucesión es divisible por p excepto el primero y el último, entonces $(1+a)^p-1-a^p$ será divisible entre p, pero

$$(1+a)^p-1-a^p=(1+a)^p-a-1-a^p+a=[(1+a)^p-(a+1)]-(a^p-a),$$

y de la hipótesis de que $(a^p - a)$ es divisible por p, entonces $(1 + a)^p - (a + 1)$ también lo será.

Así, como p divide a $(a + 1)^p - a - 1 = (a + 1)^p - (a + 1)$ entonces p divide a $(a + 1)^{p-1} - 1$, siempre y cuando p no divida a $(a + 1)$ y con esto se llega al final de la primera demostración del Pequeño Teorema de Fermat.

Desde Prusia

En 1747, cuando Euler ya estaba en Prusia contratado para trabajar en la Academia de Ciencias de Berlín, publicó el trabajo *Theoremata circa divisores numerorum* (Teoremas sobre divisores de números, E-134), y ahí se encuentra la segunda demostración del *Pequeño Teorema de Fermat*. En esta publicación —una vez más— su objetivo principal no fue sólo este teorema de Fermat. El trabajo tiene dos vertientes: por un lado primero se enfoca en la elaboración del aparato teórico necesario para demostrar que los números $a^{2^m} + b^{2^m}$ sólo tienen divisores de la forma $2^{m+1}n + 1$; por otra parte, demuestra algunos resultados acerca de diferencias de potencias y sus divisores. Más precisiones al respecto se presentan en los párrafos que siguen.

En la primera parte del artículo Euler enuncia un teorema acerca de diferencias de potencias y de las posibilidades de que sean divisibles entre números primos, y es a partir de este teorema que se deriva nuevamente el Pequeño Teorema de Fermat, mismo que resultó fundamental para demostrar algunos resultados posteriores. Después se dirige a teoremas sobre casos

particulares cuando los números de la forma $a^{2^m} + b^{2^m}$ son divisibles por primos. En este punto se tiene que mencionar que la demostración actualmente se consideraría una inducción incompleta, pues la prueba que da para el último teorema no está completa.

De regreso a los teoremas, Euler inició con el caso en el que $m = 1$, y demuestra que cuando a y b son primos relativos, entonces $a^2 + b^2$ es dividido por cualquier primo de la forma $2(2)n - 1$, es decir $4n - 1$. El siguiente resultado es para el caso $m = 2$ y concluyó que los divisores para $a^{2^2} + b^{2^2} = a^4 + b^4$ deben ser 2 o los primos de la forma $2^{m+1}n + 1 = 2^3 n + 1 = 8n + 1$. De esta manera, y como ya se hizo en el capítulo II, concluyó que los divisores de los números $a^{2^m} + b^{2^m}$ son aquellos de la forma $2^{m+1}n + 1$.

Para la segunda mitad del artículo, Euler dirigió su atención a las diferencias de potencias y sus divisores, principalmente para aquellos de los números de la forma $a^m - 1$, es decir, exploraba los números a que resuelven la congruencia $a^m \equiv 1 (\mathrm{mod} n)$.

El primer resultado importante de esta sección proporciona una manera de encontrar las a tales que un primo de la forma $2m + 1$ divida a $a^m - 1$, y que además a debe ser igual a $f^2 \pm (2m + 1)$. Prosigue con el caso en el que el número primo debe ser de la forma $3m + 1$ y por lo tanto que $a = f^3 \pm (3m + 1)$. Finalmente presenta una generalización en la que si $a = f^n \pm (nm + 1)$ y $nm + 1$ es un primo, entonces $nm + 1$ debe dividir a $a^m - 1$. Para terminar, enuncia algunos teoremas acerca de números de la

forma $a^n - b^n$ y sus divisores. Con esto concluye el artículo de Euler, pero en nuestro estudio ahora presentamos la demostración —la segunda— que Euler escribió para el *Pequeño Teorema de Fermat*.

En esta ocasión Euler presentó una demostración donde nuevamente usa un proceso de inducción, pero éste es incompleto ya que infiere que el resultado final se cumple si se siguen los pasos anteriores.

Así, la secuencia en la que presentó los teoremas es la siguiente:

Teorema 1 *Sea p un número primo, entonces cada número de la forma*

$$(a+b)^p - (a^p + b^p)$$

es dividido por p.[37]

Inmediatamente da el siguiente corolario que es un caso particular del teorema y que a la vez es el *Teorema de Fermat* para esos valores de *a* y *b*.

Corolario 1 *Sean* $a = 1$ *y* $b = 1$, *entonces* $2^p - 2$ *siempre será dividido por* p, *si* p *es un primo. Además, como* $2^p - 2 = 2(2^{p-1} - 1)$, *el segundo factor también es divisible entre* p. *A menos que* $p = 2$, *el primer factor no es divisible entre* p, *y de esto se sigue que* $2^{p-1} - 1$ *siempre será divisible entre* p, *mientras* p *sea un número primo diferente de 2.*

El teorema que sigue será fundamental para sus propósitos ya que por el corolario 1 y como *p* divide a $1^p - 1$, entonces lo que quiere dar a entender

[37] La justificación de este teorema puede ser a través del desarrollar $(a+b)^p$ de la forma $(a+b)^p = a^p + C_p^1 a^{p-1}b + C_p^2 a^{p-2}b^2 + ... + C_p^{p-1} ab^{p-1} + b^p$

$\Rightarrow (a+b)^p - (a^p + b^p) = C_p^1 a^{p-1}b + C_p^2 a^{p-2}b^2 + ... + C_p^{p-1} ab^{p-1}$, pero ya se sabe que si cada coeficiente del desarrollo de la derecha es divisible por *p*, entonces *p* divide a $(a+b)^p - (a^p + b^p)$.

en el corolario 2 es que si aplica reiteradamente esto dos resultados en el teorema 2, entonces puede generalizar el resultado.

Teorema 2 *Si $a^p - a$ y $b^p - b$ son divisibles por un primo p entonces*

$$(a+b)^p - (a+b)$$

también será divisible por el mismo primo p.[38]

Así, el siguiente corolario pretende ser la base de inducción:

Corolario 2 *Si $a^p - a$ es divisible por p, $(a+1)^p - a - 1$ también lo será de la misma manera y con la misma hipótesis, $(a+2)^p - 1 - 2$ y más aún $(a+3)^p - a - 3$, etc, en general $c^p - c$ es divisible por p.*

Dicho en nuestras palabras: Sean $p \mid 1^p - 1$ y $p \mid 2^p - 2$, entonces del teorema 2, $p \mid (2+1)^p - (2-1) \Rightarrow p \mid 3^p - 3$

Y como $p \mid 3^p - 3$ y $p \mid 1^p - 1 \Rightarrow p \mid (3+1)^p - (3-1) \Rightarrow p \mid 4^p - 4$, y de esta manera supongamos que $p \mid c^p - c$. Entonces se tiene que ver que $p \mid (c+1)^p - (c+1)$. Pero del paso anterior $p \mid c^p - c$ y como $p \mid 1^p - 1 \Rightarrow$ $p \mid (c+1)^p - (c+1)$. Y así se completa el proceso de inducción.

Con estos teoremas como precedente, Euler presenta lo siguiente:

Teorema 3. *Si p en un número primo entonces todo número de la forma $c^p - c$ es divisible por p.*

La prueba que da es la siguiente:

---

[38] Una justificación de este resultado se encuentra en que $p \mid (a+b)^p - (a^p + b^p)$ y de la hipótesis del teorema 2 se tiene que $p \mid (a^p + b^p) - (a+b) \Rightarrow$ p divide a la suma de ambos numeradores $\Rightarrow p \mid (a+b)^p - (a+b)$.

Demostración. Sea $a = 1$ como en el corolario anterior, entonces como $a^p - a = 0$ es divisible por p, de aquí se sigue que $2^p - 2$, $3^p - 3$, $4^p - 4$, etc, y en general $c^p - c$, son divisibles por p.

Corolario 3 *Si p es un número primo, entonces cada número de la forma $a^{p-1} - 1$ es divisible entre p, excepto en los casos en los que el número a sea divisible por p.*

Aunque Euler no da demostración para este corolario, ésta se deriva del teorema anterior, pues sabemos que si p es primo entonces éste divide a $a^p - a = a(a^{p-1} - 1)$ y por lo tanto p divide a a ó divide a $a^{p-1} - 1$. Así termina la segunda demostración.

Podemos notar similitudes entre la demostración de 1736 y la de 1747 en cuanto a que las dos se sustentan en una demostración por inducción. Pero la diferencia radica en que mientras la demostración de 1736 desarrolla la inducción para demostrar que $2^p - 2$ es divisible por p, y lo hace a través del desarrollo del binomio $(1 + 1)^{p-1}$, concluyendo que si p divide a $2^p - 2$ entonces divide a $2(2^{p-1} - 1)$, y por lo tanto a $2^{p-1} - 1$ a menos que p sea igual a 2. A partir de esto puede terminar la inducción demostrando que p divide a $a^p - a$, y con esto deduce el pequeño teorema de Fermat. En cambio, para la demostración de 1747, Euler utiliza dos hechos para la inducción el primero es que p divide a $1^p - 1$, y el segundo es que si $a^p - a$ y $b^p - b$ son divisibles por p entonces tambien lo será $(a + b)^p - (a + b)$. Así, la base de la inducción está en que p divide a $1^p - 1$, y por la segunda hipótesis p divide a $(1 + 1)^p - (1 + 1)$, y por lo tanto p divide a $2^p - 2$, de lo que

se concluye que divide a $2^{p-1}-1$ siempre que p no sea 2. Finalmente se puede demostrar que si p divide a $c^p - c$, y como divide a $1^p - 1$, entonces divide a $(c+1)^p - (c+1)$.

Llegó la teoría de residuos

La tercera demostración que nos proporciona Euler del pequeño teorema de Fermat está incluida en el artículo *Theoremata circa residua ex divisione potestatum relicta* (E262) (Teoremas sobre residuos obtenidos por divisiones de potencias) publicado en 1761.

En este trabajo aportó una exposición del origen de su teoría de los residuos, que sin duda es una de las herramientas fundamentales para la teoría de los números. Innumerables procesos matemáticos desarrollados por Lagrange, Legendre y Gauss, entre otros, pudieron ser concretados gracias a esta grandiosa aportación de la aritmética residual, que dio lugar a los sistemas completos y reducidos de residuos, que a su vez proporcionaron una clasificación de los enteros según el módulo que se requiera usar.

Euler inspeccionó los residuos que dejan cada una de las potencias de un número (se pueden ver en la progresión geométrica $1, a^2, a^4, ...$) al ser divididas por un primo. En el inicio del artículo Euler presenta algunas proposiciones básicas acerca de residuos, mismos que actualmente forman parte de los teoremas básicos de las relaciones de congruencia. Euler utilizó todo esto para mostrar algunos teoremas que los llevaron a desarrollar el concepto actual de orden de un número módulo *n* (es decir, la mínima potencia *m* de a tal que $a^m \equiv 1\ (mod\ n)$). Y es esta dirección por la que concluyó 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 esto se derivan lo que se mencionó antes como las clases residuales módulo p.

Continúa su artículo con teoremas referentes al orden de a módulo p, que finalmente lo llevan al pequeño teorema de Fermat, que es necesario para demostrar los teoremas 17 y 18 del (E262). Así, Euler llega a los teoremas sobre divisores de los números de la forma $ax^n - y^n$, y estos resultados fueron la base para que Lagrange encontrara irreducibles en los enteros de cuerpos cuadráticos; por otro lado Gauss pudo demostrar las actualmente conocidas *leyes de reciprocidad cuadrática*, las cuales, cabe mencionar, Euler ya había planteado, pero no con la precisión requerida.

De lo anterior ya es evidente que el trabajo de Euler no pretendía presentar y demostrar el teorema de Fermat, y queda de manifiesto que su interés estaba centrado en el comportamiento de los residuos de potencias y que el pequeño teorema de Fermat sólo fue una consecuencia de otros resultados que consideraba centrales en su artículo.

Como en esta parte del trabajo de tesis estamos interesados en el contexto en que se presentaron las demostraciones del pequeño teorema de Fermat, entonces, en lo que resta de la sección, se presenta la tercera prueba presentada por Euler del pequeño teorema de Fermat. En esta ocasión Euler aporta una demostración directa con ayuda de los siguientes teoremas y co-

rolarios[39]:

Teorema 1. Si el número de los diferentes residuos resultantes de dividir las potencias $1, a^2, a^4, a^5$ ...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.

Demostración. Supongamos que λ es la menor potencia de *a* que deja la unidad como residuo cuando a^λ es dividida por p. Además, si $\lambda < p-1$ entonces hay λ residuos diferentes, y como hay $p-1$ números menores que p, debe haber al menos λ no residuos. Ahora sean $1,\ a^2,\ a^3,\ a^4, \dots,\ a^{\lambda-1}$ las potencias que al ser divididas entre p dan λ residuos diferentes. Además sea k un no residuo, entonces los números $ak,\ a^2k,\ a^3k,\ a^4k, \dots,\ a^{\lambda-1}k$ tampoco serán residuos, y además todos estos serán diferentes entre sí. Por lo tanto se tiene que los números $k, ak,\ a^2k,\ a^3k,\ a^4k, \dots,\ a^{\lambda-1}k$ son λ no residuos. Por lo tanto existen al menos λ no residuos que no se encuentran entre los residuos, suponiendo que $\lambda < p-1$.

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

[39] En los siguientes teoremas y corolarios se presentan demostraciones parciales, y se debe a que el interés de presentar estos resultados se dirige a mostrar lo relevante de la teoría de residuos, que es donde se sitúa el pequeño teorema, y por esta razón se pone más énfasis en las partes que mejor representan su teoría de los residuos, utilizada en la demostración del pequeño teorema de Fermat. Para los interesados en ver las demostraciones completas pueden consultar el artículo original o la edición de Struik [1969].

Corolario 2. 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 3. 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. 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 $\lambda < \frac{p-1}{3}$.

Demostración. Supongamos que a^{λ} es la menor potencia que deja la unidad como residuo cuando es dividida por p. Sean $1,\ a^2,\ a^3,\ a^4, \dots,\ a^{\lambda-1}$ las potencias que al ser divididas entre p dan λ residuos diferentes. Como $\lambda < p-1$ entonces hay exactamente p-1-λ números que no son residuos. Si r es uno de ellos, entonces los números $r, ar,\ a^2r,\ a^3r,\ a^4r, \dots,\ a^{\lambda-1}r$ no serán residuos. Pero si $\lambda < \frac{p-1}{2}$, entonces $\lambda < p-1-\lambda$, y por lo tanto existen más números que no son residuos. Sea s el número que no se encuentra entre los no residuos pero que tampoco es un residuo. Entonces los números $s, as,\ a^2s,\ a^3s,\ a^4s, \dots,\ a^{\lambda-1}s$ serán no residuos y diferentes entre ellos.

Además, ninguno de estos será igual a algún número de la primera serie de no residuos. Por lo tanto cuando $\lambda < \frac{p-1}{2}$ se tienen λ residuos y 2λ no residuos y estos números son menores que p. Entonces no puede pasar que $\lambda > \frac{p-1}{3}$. En consecuencia $\lambda < \frac{p-1}{3}$ o $\lambda = \frac{p-1}{3}$, si $\lambda < \frac{p-1}{2}$ y p es primo.

Corolario 4. 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 5. 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 3. 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 sucede que $\lambda = \frac{p-1}{4}$ o $\lambda < \frac{p-1}{4}$.

Demostración. Como el número de todos los diferentes residuos resultantes de la división de las potencias de a entre p es λ, y se originan de los siguientes términos, $1,\ a^2,\ a^3,\ a^4, \dots,\ a^{\lambda-1}$, entonces, como $\lambda < \frac{p-1}{3}$, se originan el doble de números que no son residuos de las siguientes dos progresiones $r, ar,\ a^2r,\ a^3r,\ a^4r, \dots,\ a^{\lambda-1}r$ y $s, as,\ a^2s,\ a^3s,\ a^4s, \dots,\ a^{\lambda-1}s$. El número en total de residuos y no residuos es igual a 3λ y menor que $p - 1$,

por lo tanto existen más números que no son residuos. Sea t uno de ellos, por tanto todos los números $t, at,\ a^2t,\ a^3t,\ a^4t, \dots,\ a^{\lambda-1}t$, cuyo número es igual a λ, también serán no residuos. Además estos números no sólo son diferentes entre sí, sino que además serán diferentes a los de las primeras series, por lo tanto el número de residuos y no residuos será igual a 4λ. Como todos ellos son menores que p, no se puede tener que 4λ> p-1. Por lo tanto $\lambda < \frac{p-1}{4}$ o $\lambda = \frac{p-1}{4}$, suponiendo que $\lambda < \frac{p-1}{3}$ y que p sea un número primo.

Corolario 6. 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 7. 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 8. 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 hubieran más números de este tipo que $n\lambda$, entonces como otros siguen λ se tiene que el número de no residuos sería $(n+1)\lambda$; y si estos no fueran los únicos número contenidos en los no residuos, entonces de nuevo se tendrían otros λ no residuos.

Teorema 4. 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 $p-1$.

Demostración. Como a^λ es la mínima potencia entonces el número de resi-

duos de los divisores es λ, por lo que los números restantes menores que p que no sean residuos serán $p-1-\lambda$; pero por el corolario anterior $p-1-\lambda$ es múltiplo de λ. Así, sea p-1-λ = $n\lambda$ por lo que $\lambda = \frac{p-1}{n+1}$, por lo tanto λ es un divisor de $p-1$. Si $\lambda \neq p-1$ entonces λ será un factor de de $p-1$.

Con esta serie de teoremas y corolarios Euler llega al pequeño teorema de Fermat. Para la demostración sólo utiliza el teorema anterior como un lema, pero se puede notar que cada uno de los corolarios y teoremas es consecuencia del que lo precede.

Teorema 5. 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 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.

Como se puede ver la tercera demostración es totalmente diferente a las otras dos. Ésta se inscribe totalmente en el contexto de los residuos, pero también en los no residuos de potencias según un módulo primo. Así, el pequeño

teorema es una consecuencia del hecho de que los números menores que p que no son residuos módulo p son p-1-λ = $n\lambda$, donde λ es el orden de a módulo p. Euler no dejó pasar esta observación en el artículo, y compara su demostración con la que dio en 1736, y dice que difieren en que la primera que dio empieza con la expansión del binomio $(a+b)^n$, y que esto hace que el razonamiento parezca un tanto ajeno a la proposición; pero en cambio en esta nueva demostración se basa sólo en resultados concernientes a potencias, que hacen parecer la prueba más natural.

Para terminar, Euler escribe los siguientes corolarios que se pueden visualizar en la línea de propiedades de divisibilidad y no tanto como extensiones de las propiedades de los residuos.

Corolario 9. Como la potencia a^{p-1} deja la unidad cuando es dividida por el número primo p, la fórmula $a^{p-1}-1$ será divisible por el número primo p, suponiendo que p sea primo con a, es decir que a no sea divisible por p.

Corolario 10. Por lo tanto si p fuera un número primo, todas la potencias del exponente $p-1$, así como n^{p-1}, cuando sean divididas por p, dejarán como residuo la unidad o nada. Lo primero pasa si n es un número primo con p, lo segundo pasa si n es un número divisible por p.

Corolario 11. Si p fuera un número primo, y a y b fueran números primos con p, la diferencia de las potencias $a^{p-1}-b^{p-1}$ será divisible por p. Puesto que $a^{p-1}-1$ y $b^{p-1}-1$ son divisibles por p, por lo tanto la diferencia de estas fórmulas, es decir $a^{p-1}-b^{p-1}$, será divisible por p.

Capítulo V
La función ϕ(n) y el teorema de Fermat

Entre las grandes aportaciones de Euler a la teoría de números se encuentra la función $\phi(a)$ que denota la cantidad de enteros positivos menores que un entero positivo a y primos relativos con él. La notación de $\phi(a)$ para esta función fue de Carl Friederich Gauss, que dedicó tiempo para plantear y demostrar resultados sobre esta función, y hasta nuestros días es un tema que aún ofrece oportunidades para la investigación y tiene aplicaciones importantes.

A continuación presentamos algunos resultados de Euler así como algunas versiones modernas de sus teoremas que pueden ser de utilidad.

Desde su primer artículo de 1732, el (E26), en los últimos teoremas que enunció, se puede ver que las potencias de algunos primos son precisamente el desarrollo de la función ϕ para ciertos enteros. Pero fue hasta 1763 que Euler presentó la función ϕ en el trabajo *Theoremata arithmetica nova methodo demonstrata* (Demostración sobre un nuevo método en la teoría de la aritmética E271).

Euler inició el estudio de ϕ con la definición y después demostró algunas propiedades de ella para los casos de potencias de un primo, y posteriormente para el producto de dos primos. Además demostró que la función ϕ es multiplicativa,[40] y esto le permitiría encontrar la cantidad de números

[40] Si a y b son primos relativos entonces $\varphi(ab) = \varphi(a)\varphi(b)$

primos relativos para cualquier número compuesto.

La función ϕ tenía como principal destinatario a las potencias que dejan residuo uno cuando son divididas por determinados enteros. Así, lo que se tiene detrás de todo esto es que Euler necesitaba poner en correspondencia sistemas de residuos, pero sujeto a que cada elemento de los conjuntos fuera primo relativo con el módulo. Para entender el uso de la función ϕ en la generalización del pequeño teorema de Fermat consideramos que ahora es recomendable analizar primero la demostración moderna del teorema. El teorema de Euler es el siguiente:

Teorema: **Si *N* y *x* son primos relativos entonces $x^{\phi(N)} \equiv 1 \ (mod\ N)$.**

Demostración.

Sea $\{r_1, r_2, \ldots r_{\phi(N)}\}$ un sistema reducido de residuos módulo *N*,[41] y como (***N***, ***x***) = 1, entonces se tiene que $\{xr_1, x\ r_2, \ldots, xr_{\phi(N)}\}$ también es un sistema reducido de residuos módulo ***N***. Ahora podemos considerar que cada elemento del segundo conjunto es congruente a uno y sólo uno del segundo, entonces sin pérdida de generalidad podemos afirmar que

$$xr_i \equiv r_j \ (mod\ N),$$

Entonces si se multiplican todas las congruencias se obtiene

$$xr_1 xr_2 xr_3 \ldots xr_{\phi(N)} \equiv r_1 r_2 r_3 \ldots r_{\phi(N)} \ (mod\ N)$$

y cuando se reagrupan los factores se llega a

$$x^{\phi(N)} r_1 r_2 r_3 \ldots r_{\phi(N)} \equiv r_1 r_2 r_3 \ldots r_{\phi(N)} \ (mod\ N),$$

[41] Cada elemento de un sistema reducido de residuos tiene que ser primo relativo con el módulo, que en este caso es ***N***.

y como $(\boldsymbol{r_i},\ \boldsymbol{N}) = \boldsymbol{1}$, entonces $(\boldsymbol{r_1 r_2 r_3 \ldots r_{\phi(N)}},\ \boldsymbol{N}) = \boldsymbol{1}$, y con estas propiedades ahora se pueden eliminar los términos comunes de la congruencia, sin que se modifique el módulo N, y así se tiene que

$$\boldsymbol{x^{\phi(N)} \equiv 1\ (mod\ N).}$$

Y éste es el resultado al que se quería llegar.[42]

Nótese que la demostración está sustentada en la correspondencia entre dos sistemas reducidos de residuos. En el trabajo de Euler ya no era una novedad encontrar sistemas completos de residuos, que son aquellos que no ponen condiciones de divisibilidad respecto al módulo, pero trabajar con ellos no era la vía adecuada para demostrar propiedades de los residuos de potencias, y en particular para demostrar que ***si N y x son primos relativos entonces*** $\boldsymbol{x^{\phi(N)} \equiv 1\ (mod\ N)}$**.** Tratar de probar este teorema con sistemas completos de residuos nos llevaría a la inmovilidad cuando estuviéramos en un punto de la demostración como el de

$$\boldsymbol{xr_1 xr_2 xr_3 \ldots xr_N \equiv r_1 r_2 r_3 \ldots r_N\ (mod\ N),}$$

y esto porque no se tendría la certidumbre de poder eliminar todas las $\boldsymbol{r_i}$ de cada lado de la congruencia sin tener que alterar al módulo ***N***, situación que sí podría suceder en el caso de que éstas pertenecieran a un sistema reducido de residuos, pues recordemos que bajo esa situación cada $\boldsymbol{r_i}$ es primo relativo con ***N***.

Veamos la demostración de Euler pero ahora considerando los ele-

[42] Véase que en el caso de que ***N*** sea primo entonces $\phi(\boldsymbol{N}) = \boldsymbol{N} - 1$, y el teorema de Euler pasa a ser el pequeño teorema de Fermat.

mentos que aparecen en E271.

Para demostrar que $\boldsymbol{x^{\phi(N)} \equiv 1\ (mod\ N)}$ cuando $\boldsymbol{x}$ y $\boldsymbol{N}$ son primos relativos Euler construirá un sistema reducido de residuos módulo $\boldsymbol{N}$ con base en que el orden de $\boldsymbol{x}$ módulo $\boldsymbol{N}$ es un entero $\boldsymbol{h}$. Así, se parte del hecho de que existe $\boldsymbol{h}$, que es el menor entero positivo tal que al ser divido $\boldsymbol{x}^h$ por $\boldsymbol{N}$ deja resto uno, es decir, se cumple que $\boldsymbol{x^h \equiv 1\ (mod\ N)}$**.** Ahora veamos que $h \leq \phi(N)$. Considérese el conjunto $\{1, \boldsymbol{x}, \boldsymbol{x}^2, \ldots, \boldsymbol{x}^{h-1}\}$. Como $\boldsymbol{x}$ y $\boldsymbol{N}$ son primos relativos, entonces todas las potencias de $\boldsymbol{x}$ del conjunto también lo son, y además cualesquiera dos elementos del conjunto no son congruentes módulo $\boldsymbol{N}$; para estar seguros de esto, supongamos que no es así, entonces pensemos que existen $\boldsymbol{x}^i$ y $\boldsymbol{x}^j$ del conjunto (diferentes entre ellos y que $i > j$) tal que $\boldsymbol{x^i \equiv x^j\ (mod\ N)}$, y de aquí se obtiene que $\boldsymbol{x^{i-j} \equiv 1\ (mod\ N)}$**.** De la última congruencia se tiene que $(i - j) < \boldsymbol{h}$, pero $\boldsymbol{h}$ es el menor entero positivo tal que $\boldsymbol{x^h \equiv 1\ (mod\ N)}$**,** por lo tanto se genera una contradicción. Así concluye que no pueden existir $\boldsymbol{x}^i$ y $\boldsymbol{x}^j$ elementos diferentes que sean congruentes o, dicho de otro modo, y en consecuencia que dejen el mismo residuo al ser divididos entre $\boldsymbol{N}$.

Ahora, si $h = \varphi(n)$, entonces $\boldsymbol{x^{\phi(N)} \equiv 1\ (mod\ N)}$, y ya se terminó la demostración, pero si $h < \phi(N)$ entonces tiene que existir al menos otro entero g menor que $\boldsymbol{N}$ y también primo relativo, tal que en el conjunto $\{g, g\boldsymbol{x}, g\boldsymbol{x}^2, \ldots, g\boldsymbol{x}^{h-1}\}$ todos los elementos sean primos relativos con $\boldsymbol{N}$, y además que cualesquiera dos de ellos no sean congruentes módulo $\boldsymbol{N}$. La demostración de lo último es semejante a la justificación que ya se hizo para

el conjunto $\{1, \boldsymbol{x}, \boldsymbol{x}^2, \ldots, \boldsymbol{x}^{h-1}\}$. Pero es importante notar que un elemento de $\{1, \boldsymbol{x}, \boldsymbol{x}^2, \ldots, \boldsymbol{x}^{h-1}\}$ no puede ser congruente con uno de $\{g, g\boldsymbol{x}, g\boldsymbol{x}^2, \ldots, g\boldsymbol{x}^{h-1}\}$ módulo $\boldsymbol{N}$. Veamos porqué. Supongamos que $\boldsymbol{g}\boldsymbol{x}^{\boldsymbol{s}} \equiv \boldsymbol{x}^{\boldsymbol{t}}$ $(\boldsymbol{mod}\ \boldsymbol{N})$, con $t > s$; entonces $\boldsymbol{x}^{\boldsymbol{s}}(\boldsymbol{x}^{\boldsymbol{t}-\boldsymbol{s}} - \boldsymbol{g}) \equiv \boldsymbol{0}$ $(\boldsymbol{mod}\ \boldsymbol{N})$, pero $\boldsymbol{x}^{\boldsymbol{s}}$ y $\boldsymbol{N}$ son primos relativos, entonces $\boldsymbol{x}^{\boldsymbol{t}-\boldsymbol{s}} \equiv \boldsymbol{g}$ $(\boldsymbol{mod}\ \boldsymbol{N})$. Pero la última relación nos indica que $\boldsymbol{g}$ tiene que ser uno de los residuos de las potencias del conjunto $\{1, \boldsymbol{x}, \boldsymbol{x}^2, \ldots, \boldsymbol{x}^{h-1}\}$, y eso no es posible. Con esto Euler llegó a que los dos conjuntos suman $2\boldsymbol{h}$ elementos, y como cada uno es primo relativo con $\boldsymbol{N}$ y todos son diferentes módulo $\boldsymbol{h}$, entonces $2h \leq \phi(N)$.

Nuevamente, si $2h = \phi(N)$, entonces ya se terminó la demostración porque $\boldsymbol{x}^{\boldsymbol{\phi}(\boldsymbol{N})} \equiv \boldsymbol{1}$ $(\boldsymbol{mod}\ \boldsymbol{N})$, pero si $2h < \phi(N)$ entonces existe otro entero k menor que $\boldsymbol{N}$ y también primo relativo tal que el conjunto $\{k, k\boldsymbol{x}, k\boldsymbol{x}^2, \ldots, k\boldsymbol{x}^{h-1}\}$ satisface lo anterior para g, entonces se tendrá que $3h \leq \phi(N)$. De la misma manera se repite el proceso, tantas veces como sea necesario, hasta llegar a que la cantidad total de todos los elementos de los conjuntos sea $\phi(N)$, y entonces así se llegaría a que existe un entero w tal que $wh = \phi(N)$.

De regreso a $\boldsymbol{x}^{\boldsymbol{h}} \equiv \boldsymbol{1}$ $(\boldsymbol{mod}\ \boldsymbol{N})$, y como ahora ya sabemos que $wh = \phi(N)$, entonces se llega a que $\boldsymbol{x}^{\boldsymbol{wh}} \equiv \boldsymbol{1}$ $(\boldsymbol{mod}\ \boldsymbol{N})$, y por lo tanto $\boldsymbol{x}^{\boldsymbol{\phi}(\boldsymbol{N})} \equiv \boldsymbol{1}$ $(\boldsymbol{mod}\ \boldsymbol{N})$**,** que es lo que Euler quería demostrar, y para el caso en que $\boldsymbol{N}$ es primo entonces se tiene el pequeño teorema de Fermat.

En las demostraciones que se presentaron es explícito el desarrollo de la teoría de las clases residuales y en particular el de los sistemas reducidos de residuos, y no se puede dejar de mencionar el uso del orden de un entero

módulo ***N***.

Para llegar a la generalización del pequeño teorema de Fermat se necesitó dar una base teórica a la función $\phi(N)$, porque ***N*** ya no tiene que ser sólo primo como en el caso particular de Fermat.

Algunos de los teoremas que se presentan también en E271 son los siguientes.[43]

Teorema 1. *Si n es una potencia de cualquier número primo p, es decir, $n = p^m$, entonces la cantidad de números menores y primos a n será igual a $p^m - p^{m-1} = p^{m-1}(p-1)$.*

Aquí presenta la manera de calcular la función $\phi(P^m)$ que actualmente conocemos como $\phi(P^m) = p^m(1 - \frac{1}{p})$.

Teorema 2. *Si el número n es un producto de dos números primos p y q, esto es, $n = pq$, entonces la cantidad de todos los números menores que n y primos a él es igual a $(p-1)(q-1)$.*

Teorema 3. *Si A y B son números primos entre si, y el número de partes primas a A es igual a r, y el número de partes primas a B es igual a s, entonces el número de partes primas al producto AB será rs.*

Enuncia también que la función es multiplicativa, es decir, que para cualesquiera dos enteros positivos A y B y que sean primos relativos se tiene que $\varphi(AB) = \varphi(A)\varphi(B)$.

Corolario 1. *Sean $p, q.r, s, \cdots$ números primos. Para todos los números N de la forma $N = p^\lambda q^\mu r^\gamma s^\zeta$, la cantidad de números primos a N será:*

$$p^{\lambda-1}(p-1)q^{\mu-1}(q-1)r^{\gamma-1}(r-1)s^{\zeta-1}(s-1).$$

Este corolario es lo que actualmente conocemos como el desarrollo

[43] Las demostraciones de Euler de los tres teoremas que siguen se encuentran al final del capítulo en un apéndice.

general de la función ϕ, y es así:

$$\varphi(N) = \prod_{p_i \; primo \; de \; N} N\left(1 - \frac{1}{p_i}\right)$$

donde $N = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_t^{\alpha_t}$.

Con la demostración de que la función ϕ es multiplicativa Euler terminó el análisis de ésta, y dio lugar a la segunda parte del artículo que tenía como objetivo exponer la teoría de los residuos de potencias, y como ya se vio ésta era la base para generalizar el pequeño teorema de Fermat. A continuación se presentan dichos teoremas.

Teorema 4. *Si* ***x*** *y* ***N*** *son primos relativos y cada elemento de la serie* $x^0, x^1, x^3, x^4, \ldots$ *fuera dividido por N, entonces existe una potencia [que es la más pequeña] que deja residuo uno.*

A esta potencia que es la más pequeña ahora la conocemos como el ***orden*** de ***x*** módulo ***N***.

Teorema 5. *Si* ***x*** *y* ***N*** *son primos relativos y cada término de la serie* $x^0, x^1, x^3, x^4, \ldots$ *fuera dividido por* ***N,*** *y los residuos resultantes fueran* $1, a, b, c, \ldots$ *entonces los mismos residuos se obtendrán cuando las potencias son elevadas al cuadrado, o al cubo, o tanto como se desee en su multiplicación.*

Teorema 6. *En los residuos resultantes a partir de la división de las potencias de cualquier número por un divisor primo a éste, o todas las partes primas al divisor ocurren, o el número de partes que no se encuentran serán igual, o tendrá una razón múltiple con relación al número de las partes, las cuales constituyen los residuos.*

Este teorema es donde plantea la idea de que la cantidad de elementos de un sistema reducido de residuos módulo ***N*** (es decir, $\phi(N)$) pueda ser representada como un múltiplo del orden de un número. Pero esto lo con-

cretó en el siguiente teorema:

Teorema. *Si x y N son primos relativos y x^v es la mínima potencia que al ser dividida entre N deja como residuo la unidad, entonces v es igual al número de números menores que N y primos relativos con N, o bien un divisor de éste.*

Estos fueron los elementos que Euler construyó para sustentar la teoría de los residuos de potencias y que fueron la base para la demostrar el resultado que actualmente conoce como teorema de Euler-Fermat.

Más reflexiones para la función $\phi(n)$

En *Speculationes circa quasdam insignes proprietates numerorum*[44] (E-564), Euler retomó el estudio de la función ϕ, pero en este artículo la búsqueda de los primos relativos menores a n y positivos estuvo inicialmente relacionada con encontrar racionales irreducibles en el intervalo $(0,1)$, y para tal objetivo presentó nuevamente las formas de construir la función $\varphi(n)$ para cualquier entero fuera primo o compuesto, así como su característica de ser multiplicativa.

Lo que sí es innovador en este artículo, es que ahí mostró las ideas que tenía de que los valores de la función $\varphi(n)$ pudieran estar vinculados con una función generadora. Pero antes de explicar que sucedió con esto en el artículo, revisemos brevemente qué fueron para Euler las funciones generadoras.

[44] *Especulaciones sobre algunas propiedades particulares de los números*. Cabe mencionar que en este artículo Euler usa el símbolo πa para denotar a la cantidad de números menores que a y primos relativos con a.

La idea es que dado un conjunto de enteros $a_0, a_1, a_2, \cdots$ se pueda obtener un polinomio $P(x) = a_0 + a_1x + a_2x^2 + a_3x^3 \cdots$ al cual se le llama polinomio generador del conjunto $a_0, a_1, a_2, \cdots$. Pero si estos enteros son el resultado de una función $f(n)$ entonces se tiene que $P(x) = \sum_{n=0}^{\infty} f\,(x)x^n$, y aquí lo que más interesa es ver si la serie infinita converge, y entonces los valores *f*(*n*) quedan como "empaquetados" dentro de la función a la que converge la serie. Por ejemplo, la sucesión de los enteros 1, 2, 3, 4, ⋯ está generada por:

$$P(x) = \frac{1}{(1-x)^2} = 1 + x + 2x^2 + 3x^3 + 4x^4 + \cdots$$

La de los números triangulares 1, 3, 6, 10, 15, 21,⋯, $\frac{k(k+1)}{2}$,⋯ está generada por:

$$P(x) = \frac{1}{(1-x)^3} = 1 + 3x + 6x^2 + 10x^3 + 15x^4 + \cdots$$

La de los números de Fibonacci 1, 1, 2, 3, 5, 8, 13, 21,⋯ está generada por:

$$P(x) = \frac{1}{(1-x-x^2)} = 1 + 1x + 2x^2 + 3x^3 + 5x^4 + \cdots$$

En este artículo Euler menciona la intención de tener una función generadora para la $\varphi(n)$, es decir, que dados

$$\begin{array}{ll} \varphi(1) = 1 & \varphi(7) = 6 \\ \varphi(2) = 1 & \varphi(8) = 4 \\ \varphi(3) = 2 & \varphi(9) = 6 \\ \varphi(4) = 2 & \varphi(10) = 4 \\ \varphi(5) = 4 & \varphi(11) = 10 \\ \varphi(6) = 2 & \vdots \end{array}$$

fuera posible encontrar a $P(x) = \sum_{n=2}^{\infty} \varphi\,(n)x^n = 1 + 1x + 1x^2 + 2x^3 + 2x^4 + 4x^5 + 2x^6 + \cdots$, y lo importante era que $P(x)$ no quedara sólo en términos de una serie infinita sino que fuera el resultado de la convergencia

de $1 + 1x + 1x^2 + 2x^3 + 2x^4 + 4x^5 + 2x^6 + \cdots$. Pero en su E564 Euler menciona que aún no es posible llegar a esa expresión en el sentido de los ejemplos previos que hemos presentado.

Con Euler no fue posible llegar a este resultado, pero tenemos que recordar que él estaba inaugurando la forma de ver ciertos conjuntos como coeficientes de polinomios, y por esto es demasiado pedir que resolviera todos los problemas al respecto.

Pero la solución llegó eventualmete y para ello se usaron las series de Dirichlet y la función zeta de Riemann ($\zeta(s)$) para llegar a que:

$$P(x) = \sum_{n=1}^{\infty} \frac{\varphi(n)}{n^s} = \frac{\zeta(s-1)}{\zeta(s)}$$

El *Tractatus de numerorum doctrina capita sedecim, quae supersunt* es el último texto en donde Euler trabajó con la función ϕ. Es en el cuarto capítulo donde Euler se enfoca sobre resultados sobre primos relativos y, sobretodo, en la cantidad de primos relativos a un número entero. Al ser el *Tractatus de numerorum doctrina capita sedecim, quae supersunt* un libro sobre teoría de números Euler repite en gran medida teoremas que desarrolló en otros artículos, y este capítulo no es la excepción por lo cual retoma los teoremas de *Theoremata arithmetica nova methodo demonstrata* y *Speculationes circa quasdam insignes proprietates numerorum* y sólo agrega una demostración diferente del siguiente teorema:

Teorema 1. Sea $a = pqr$ con p, q, r primos distintos, entonces la cantidad de primos menores a a es igual a $(p-1)(q-1)(r-1)$.

Difusión de sus resultados

Todos las aportaciones de Euler correspondientes a los temas abordados en este capítulo serían retomadas por Gauss en *Disquisitiones Arithmeticae*, libro sobre teoría de números publicado en 1801. En esta obra demuestra propiedades de la función ϕ ya antes demostradas por Euler, pero también añade propiedades innovadoras, como es el caso del siguiente teorema:

Teorema. Si $a, a', a'',$ etc. son todos los divisores de A (incluyendo a 1 y a A mismo), entonces se tendrá que

$$\varphi(a) + \varphi(a') + \varphi(a'') + \text{ etc.} = A,$$

es decir,

$$\sum_{d|A} \varphi\,(d) = A$$

No podemos dejar de mencionar que otro gran personaje que siguió reflexionando sobre la función ϕ fue Ivan Vinogradov, entre otra cosas aportó una manera de vincular a ϕ con la función aritmética de Möbius para demostrar que ϕ es multiplicativa.

Sin duda, la función ϕ y el manejo de las clases residuales son de los grandes elementos matemáticos que Euler nos proporcionó en los artículos que mencionamos en este capítulo. Y no es porque estos elementos se vinculen nuevamente con uno de los problemas de Fermat (el pequeño teorema), lo más importante radica en que fundamentó la clasificación de los enteros según sus residuos. Y este manejo de las clases residuales sería retomado por otros matemáticos, entre ellos Gauss, quien así pudo plantear sus grandes resultados sobre residuos cuadráticos o la ley de reciprocidad, entre otras

grandes aportaciones.

Apéndice

Teorema 1. Si n es una potencia de cualquier número primo p, es decir, $n = p^m$, entonces la cantidad de números menores y primos a n será igual a $p^m - p^{m-1} = p^{m-1}(p-1)$.

Demostración. La cantidad de números menores que la potencia $n = p^m$ que no son primos con *n* son todos los múltiplos de *p* menores que n, por lo tanto los números no primos con n serán:

$$p, 2p, 3p, 4p, \cdots, p^{m-1}p$$

cuyo número es p^{m-1}, que es un número menor a $n = p^m$; por lo tanto la cantidad de números menores que n y primos relativos con él es $p^m - p^{m-1} = p^{m-1}(p-1)$. ■

Teorema 2. Si el número *n* es un producto de dos números primos p y q, sea $n = pq$, la cantidad de todos los números menores que n y primos con él es igual a $(p-1)(q-1)$.

Demostración. Como el número menor al producto pq es $pq - 1$, por lo tanto de los primos con él se deben excluir los que son divisibles por p, y también los que son divisibles por q, y con esto se eliminará la cantidad deseada. Cabe señalar, por lo tanto, que los números desde la unidad hasta pq, que son primos relativos con p, se pueden ordenar de la siguiente manera

$$\begin{array}{ccccccc}
1, & 2, & 3, & 4, & \cdots & p-1 \\
p+1, & p+2, & p+3, & p+4, & \cdots & 2p-1 \\
2p+1, & 2p+2, & 2p+3, & 2p+4, & \cdots & 3p-1 \\
3p+1, & 3p+2, & 3p+3, & 3p+4, & \cdots & 4p-1 \\
\vdots & \vdots & \vdots & \vdots & & \vdots \\
(q-1)p+1, & (q-1)p+2, & (q-1)p+3, & (q-1)p+4, & \cdots & qp-1
\end{array}$$

y ahora, de entre estos sólo deben ser elegidos, los que son primos relativos con q. Considérese entonces las series verticales, cuyo número es $p-1$; ahora cada uno de los q términos en la progresión aritmética creciente, diferentes a los p existentes, son primos relativos con los q terminos. En cada serie vertical, por lo tanto, todos los términos menos uno serán primos con q; por consiguiente cada una de las series verticales contiene $q-1$ números primos relativos a q. Así, como el número de series verticales es $p-1$, en todas a la vez se encuentran $(p-1)(q-1)$ números primos con q, asimismo serán primos con el producto pq; por ende entre todos los números menores a pq se encuentran $(p-1)(q-1)$ números primos con pq.

Teorema 3. Si A y B son números primos entre sí, y el número de partes primas a A es igual a a, el número de partes primas con B es igual a b; entonces el número de partes primas con el producto AB será ab.

Demostración. Sean $1, \alpha, \beta, \gamma, \cdots \omega$ los números menores que A y primos relativos con él, entonces, por hipótesis, la cantidad es igual a a. Así, mientras se tenga la misma cantidad de números A, de igual manera se tendrá igual número de primos entre A y $2A$, igual entre $2A$ y $3A$, y así sucesivamente. De este modo se pueden mostrar todos los números primos con A desde la unidad hasta AB, como se muestra en el siguiente esquema:

$$
\begin{array}{ccccc}
1, & \alpha, & \beta, & \cdots & \omega \\
A+1, & A+\alpha, & A+\beta, & \cdots & A+\omega \\
2A+1, & 2A+\alpha, & 2A+\beta, & \cdots & 2A+\omega \\
3A+1, & 3A+\alpha, & 3A+\beta, & \cdots & 3A+\omega \\
\vdots & \vdots & \vdots & & \vdots \\
(B-1)A+1, & (B-1)A+\alpha, & (B-1)A+\beta, & \cdots & (B-1)A+\omega
\end{array}
$$

Así, cada serie horizontal tiene a términos, y el número de series horizontales es igual a B; de esta manera todas las series juntas contienen aB términos, todos primos con A. Por lo tanto, aún deben ser excluidos todos aquellos que no son primos con B, de esta manera se tiene no sólo los que son primos con A, sino también los que lo son con B, y por lo tanto al producto AB, y de éstos sólo falta encontrar aquéllos que son primos con B. Consideremos ahora las series verticales, y como el número de series verticales es igual a a, cualquier serie vertical contiene B términos en progresión aritmética, cuya diferencia es igual a A, y por lo tanto el número de primos con B, entonces cualquier serie vertical contiene tantos términos primos con B como la cantidad de números que se tiene de primos con B y por lo tanto ese número por hipotesis es igual a b. Se sigue entonces que con cada serie vertical conteniendo b términos primos con B, que también son primos con el producto AB, el número total de términos primos con AB es igual a ab. ■

Conclusión

Recordemos que el objetivo planteado para este trabajo era mostrar cómo fue que Euler desarrolló los diferentes temas tratados en su primer artículo. Analicemos brevemente los resultados obtenidos sobre este aspecto.

De la investigación realizada durante esta tesis se observó que aunque en apariencia los trabajos de Euler parecen haber sido producidos de manera un tanto desorganizada y con falta de rigor matemático, no deben de ser juzgados así. Aunque los artículos trataran diversos temas por lo general servian de introducción para trabajos posteriores en los cuales trataría con mayor profundidad dichos temas y en algunas ocaciones eran el preludio al desarrollo de nuevas teorías. Lo anterior nos ha llevado a pensar que Euler en muchas ocaciones a pesar de que no tuviera claro el desarrollo de sus ideas, o no pudiera precisarlas, sabía de antemano cual era su importancia y su posible uso como herramienta para el desarrollo de una teoría mas globalizante. Por otra parte no se debe juzgar las demostraciones como poco rigurosas, pues como ya se dijo, Euler iniciaba ciertas ideas en un artículo para posteriormente extender su desarrollo en alguno subsecuente, lo cual hacía difícil que pudiera concluir o dar en muchas ocaciones demostraciones para los teoremas que proponía. Además le exigencia que se pedía para presentar un trabajo no era la misma que hoy en día.

Al transcurrir la investigación encontramos información que nos

permite ahora mostrar datos que se apartaban del objetivo principal.

Uno de los más importantes es el hecho de que se puede observar la importancia que tuvo Goldbach, no solo en el desarrollo de las ideas matemáticas de Euler, sino también en el de la teoría de números, que era menospreciada en esa época. Fue gracias a Goldbach y ese pequeño párrafo en el que describe los números de Fermat a Euler, que este último se interesó en la teoría de números. Así, mediante el estudio de los números de Fermat, Euler encontró el pequeño teorema de Fermat, el cual sirvió para que pudiera iniciar, entre otras cosas, la tan importante teoría de residuos, así como la generalización del teorema de Fermat y, con esto, la función phi, temas todos ellos aún en uso y en desarrollo en nuestro tiempo.

Referencias

Euler, Leonhard. 1738, E-26. *Observationes de theoremate quodam Fermatiano aliisque ad numeros primos spectantibus*. Commentarii academiae scientiarum Petropolitanae 6: 103-107. (Traducción de Jordan Bell).

Euler, Leonhard. 1741, E-54. *Theorematum quorundam ad numeros primos spectantium demonstratio*. Commentarii academiae scientiarum Petropolitanae 8: 141-146. (Traducción de David Zhao)

Euler, Leonhard. 1750, E-134. *Theoremata circa divisores numerorum*. Novi Commentarii academiae scientiarum Petropolitanae 1: 20-48. (Traducción de David Zhao)

Euler, Leonhard. 1750, E-100. *De numeris amicabilibus*. Opuscula varii argumenti 2: 23-107. (Traducción de Jordan Bell)

Euler, Leonhard. 1761, E-262. *Theoremata circa residua ex divisione potestatum relicta*. Novi Commentarii academiae scientiarum Petropolitanae 7: 49-82. (Traducción de Jordan Bell).

Euler, Leonhard. 1763, E-271. *Theoremata arithmetica nova methodo demonstrata*. Novi Commentarii academiae scientiarum Petropolitanae 8: 74-104. (Traducción de Ulises Bravo con colaboración de Pedro Sobrevilla)

Euler, Leonhard. 1784, E-564. *Speculationes circa quasdam insignes proprietates numerorum*. Acta Academiae Scientarum Imperialis Petropolitinae 4: 18-30. (Traducción de Jordan Bell).

Euler, Leonhard. 1849, E-792. *Tractatus de numerorum doctrina capita sedecim, quae supersunt*. Commentationes arithmeticae 2: 503-575.

Wolff, Christian. 1742. *Elementa Matheseos Universae*. Tomo I. Prostat in oficina libraría Rengeriana.

Sandifer, Edward. 2007. *The Early Mathematics of Leonhard Euler*. The Mathematical Association of America.

Lucas, E. 1878. *Théorèmes d'arithmétique* . Atti della Reale Accademia della Scienze di Torino. Vol 13 (1878), 271-284. Este trabajo fue tomado de: Luca, Florian *et al*. 2001. *17 Lectures on Fermat Numbers*. Canadian Mathematical Society.

Euclides. 1994. *Elementos*. Libros V-IX. Traducción y notas: M. Luisa Puerta. No. de colección: 191. Madrid: Gredos.

Iannucci D. E. y Sorli R. M. 2003. *"On the total number of prime factors of an odd perfect number"*. Math. Comp. No. 224. 72: 2078-2084.

Hagis Peter Jr. y McDaniel W. L. 1975. *"Some results concerning nonexistence of odd perfect numbers of form* $p^{\alpha} \cdot m^{2B}$ *"*. The J. Fibonnacci Quart. No. 1. 13: 25-28.

McDaniel W. L. 1970. *"The non-existence of odd perfect number of a certain form"*. Arch. Math. 21: 52-53.

Steuerwald R. 1937. *"Verscharfung einer notwendigen Bedingung für die Existenz einer ungeraden vollkommenen Zahl"*. S.-B. Math.-Nat. Abt. Bayer, Akad. Wiss. 68-72.

Struik, J (Ed.). 1969. *A Source Book in Mathematics, 1200-1800*. Harvard University Press.

Koshy, Thomas. 2002. *Elementary Number with Applications*. Harcourt/Academic Press.