UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE CIENCIAS

ESTUDIO SOBRE EL TRATADO DE LOS NÚMEROS DE LEONHARD EULER

T E S I S

QUE PARA OBTENER EL TÍTULO DE:

M A T E M Á T I C O

P R E S E N T A:

JORGE RENÉ LEDESMA GRANADOS

DIRECTOR DE TESIS:
MAT. JULIO CÉSAR GUEVARA BRAVO
2016

CIUDAD UNIVERSITARIA, CDMX

Estudio sobre el *Tratado de los Números* de Leonhard Euler

Jorge René Ledesma Granados
Director: César Guevara Bravo

Índice general

Introducción

Durante los años de estudio de las diversas áreas de la matemática en la Facultad de Ciencias los estudiantes nos adentramos en aprender el Cálculo, Geometría, Teoría de Números, entre muchas otras disciplinas. Es común que nuestra preparación tenga entre sus elementos fundamentales buscar y cuestionar el origen de las teorías, y en este contexto es que frecuentemente nos preguntamos sobre los autores y sus respectivas obras que son las bases de la matemática que actualmente estudiamos. Así, nos enteramos que la geometría está vinculada a los *Elementos* de Euclides o que la mecánica tratada con el cálculo y lo está con los *Principia Mathematica* de Newton.

Para el caso de la teoría de los números es frecuente encontrar que la primera obra ya formal que se escribió para esta área fue el *Tractatus de Numerorum* (Tratado de los Números) de Leonhard Euler, y resulta que sí es posible encontrar fragmentos de la obra pero sólo en trabajos especializados, sin embargo la obra completa no es de fácil acceso en otro idioma que no sea en el que se escribió, que es el latín. Así, después de haber realizado una búsqueda integral sobre estudios de la obra, los resultados obtenidos no fueron muy satisfactorios. En realidad, es difícil encontrar un texto dedicado específicamente al análisis del *Tractatus*. Derivado de lo anterior consideramos (el profesor César Guevara y el que presenta esta tesis) que era oportuno hacer un trabajo directamente a partir del *Tractatus* y estudiar su contenido. Cabe señalar que fue posible trabajar directamente con la obra de Euler gracias a que el pro-

fesor Guevara ya tenía desde el 2015 muy avanzada la traducción al español que realizó junto con el profesor de latín Ulises Bravo de la Facultad de Filosofía y Letras. Es importante mencionar que el análisis del *Tractatus* que se presenta en esta tesis no tiene el objetivo de comentar cada uno de los parágrafo que componen la obra, éstos son 587, lo que haremos es dar un panorama completo pero general del alcance de la teoría desarrollada hasta la muerte del autor.

La tesis se divide en 5 capítulos e incluye 2 apéndices donde se abordan los temas siguientes:

1. El capítulo 1 inicia poniendo en contexto el estado de la teoría de los números cuando Euler llegó a San Petersburgo y que a partir de esa época se le despertaría un gran interés por los temas aritméticos. Se muestran las posibles influencias que se pudieron dar entre los libros aritméticos de los *Elementos* de Euclides y el *Tractatus*. Se plantea una separación del contenido del *Tractatus* en cuatro secciones temáticas, que son los capítulos dos al cuatro de la tesis.

2. El capítulo 2 muestra el tema de primos y la controversia que se genera por la definición de número. Euler expone las propiedades de divisores y suma de ellos para poder llegar a los resultados sobre números perfectos pares e impares. Aquí se muestra la importancia que Euler le dio a las funciones aritméticas $\sigma(n), \tau(n)$ y $\phi(n)$ para desarrollar teoremas sobresalientes en el ámbito de funciones generadores y teoría de particiones.

3. El objetivo del capítulo 3 es estudiar los capítulos V al IX del *Tractatus*, aquí se aborda el temas de residuos. Esta manera de Euler de ver a los números enteros es novedosa, en el sentido de que anteriormente se estudiaba la divisibilidad solamente a través de divisiones que no dieran lugar a residuo. Ahora, el estudio se centra en los residuos que deja un número al ser dividido por otro, en particular los primos impares. En particular se estudian aquí los residuos de enteros

en progresiones aritméticas y geométricas, así como divisores de números de la forma $a^n \pm b^n$.

4. El capítulo 4 trata los resultados del *Tractatus* referentes a los residuos que dejan potencias cuadradas, cúbicas, cuartas y quintas cuando son divididas por un primo p. En esta sección del *Tractatus* aparece lo que conocemos como Criterios de Euler para los residuos de potencias.

5. El capítulo 5 abarca el estudio de los dos último capítulos del *Tractatus*, ahí se analizan las dos formas cuadráticas binarias $x^2 + y^2$ y $x^2 + 2y^2$. En esta parte de la obra encontramos resultados referentes a primos que dividen a alguna de estas formas binarias, o qué números pueden expresarse en alguna de estas formas.

Capítulo 1

Antecedentes

1.1. Introducción.

La teoría de los números es una de las áreas de la matemática más antiguas, pero, a la vez es de las que tenían menos desarrollo a principios del siglo XVIII, es decir, mientras que en los siglos XVI y XVII personajes como Descartes, Galileo, Cardano ya habían sentado las bases para el desarrollo del cálculo, álgebra, mecánica, geometría analítica, entre otras, la teoría de números atravesó por un periodo de rezago que llegó hasta las primeras décadas del siglo XVIII, y sólo hasta esos tiempos fue que pudo adquirir una ruta de creatividad que la hizo llegar a ser una de las disciplinas matemáticas más atractivas y fructíferas.

Podríamos datar sus inicios en la época de Euclides cuando escribió los tres libros aritméticos para sus *Elementos*[1], éstos son del VII al IX. Esta gran aportación de Euclides nos proporcionó las bases sobre las que construyó la teoría de la divisibilidad, los números primos y el manejo de los primeros algoritmos. Así, al igual que la geometría, se hubiera esperado que después del letargo matemático por el que se atravesó durante la edad media, la geometría y el estudio de los naturales se retomara para llegar al esplendor del renacimiento de las matemáticas, pero éste no llegó

[1] Euclides [1994, tomo II].

para ambas disciplinas, sí lo fue para la geometría, pero no de la misma manera para la teoría de los números. Durante los siglos XVI, XVII y parte del XVIII los textos euclidianos se publicaban generalmente sólo con los libros del I al VI, ya que se consideraba que para ser una persona culta bastaba con que se conociera esta parte de los *Elementos*, que era sólo geometría y la parte de números se excluía. Para especialistas de la matemática sí existían ediciones completas como las de Clavius o Tartaglia.

Fue hasta la década de los años treinta del siglo XVII que alguien fijó su atención de manera más profunda en los problemas de números, él fue Pierre de Fermat, y prácticamente nadie más abordó de manera sistemática los problemas de aritmética. Sus contemporáneos, por ejemplo Huygens, mostraron indiferencia ante los resultados planteados por Fermat. Así, a pesar de las relaciones que sostenía Fermat con Carcavi y Mersenne, no se logró una consolidación de la investigación de los temas aritméticos. Después de la muerte de Fermat fueron escasas las aportaciones así como los interesados en estos temas.

De esta manera se llegó a los días finales del siglo XVII nuevamente con un letargo casi como en el siglo X pero ahora sólo en los temas de la Aritmética. Por otro lado, áreas de la matemática y de la física-matemática ya en plena madurez habían proporcionado al mundo las ideas de lo que serían sus obras fundamentales sobre las que se seguiría construyendo su teoría; por ejemplo Copérnico, Newton, Galileo, Descartes, Pascal, Cavallieri, etc., ya habían publicado *Sobre las revoluciones, Principios Matemáticos, Dos nuevas ciencias*, la *Geometría*, entre otras, que fueron obras emblemáticas en sus áreas científicas, ellas recopilaban gran parte del conocimiento avanzado de la época y a la vez marcaban los caminos de la investigación para los que retomaran estas teorías.

De regreso a la teoría de los números, era claro que no existía una obra que marcara los caminos a seguir, es más, no existía una obra que recopilara los conocimientos aportados hasta el momento, el único referente era Euclides con los libros aritméticos.

1.2. La historia cambió.

En las primeras décadas del siglo XVIII se daría un cambio importante que marcaría para siempre la manera de percibir el estudio de los enteros. Esta historia inició con el proyecto del Zar de Rusia Pedro el Grande para crear la *Academia de Ciencias de San Petersburgo*. A partir de 1714 convocó a personajes como Johann Schumacher, Christian Wolff y Christian Goldbach para que se encargaran del proyecto de la Academia, la biblioteca e invitar a formar parte de ella a los mejores científicos de Europa [2].

Goldbach (1690-1764) fue un hombre de grandes relaciones públicas, conoció a Leibniz en 1711, Nicolaus Bernoulli, A. de Moivre en 1712 y a Daniel Bernoulli en 1724, entre otros. Goldbach a través de Nicolás y Daniel Bernoulli logró que el joven Euler –tenía veinte años– aceptara formar parte de la *Academia*[3], y así en 1727

[2] *La Academia de Ciencias de San Petersburgo* fue el proyecto de Pedro el Grande, Zar de Rusia entre 1682 y 1725. Pedro sabía que un cambio significativo en la vida intelectual rusa tenía que basarse en el desarrollo de la enseñanza. En 1701 fundó una escuela de matemáticas y navegación (escuela para navegantes, arquitectos, ingenieros e hidrógrafos). En 1715 se creó la escuela naval para promover el entrenamiento práctico y fundó escuelas en las provincias para enseñar las *cifras* (aritmética). Pedro quería que Rusia ascendiera a los primeros planos europeos en el trabajo científico, para lo que planeó personalmente la creación de la Academia de Ciencias, que entró en funciones algunos meses después de su muerte.

Para iniciar el proyecto de la *Academia*, en 1720 el zar solicitó a Christian Wolff, profesor alemán de filosofía y física en Halle, que le ayudara en la creación de la institución. Desde 1714 Pedro había llamado a Johann Schumacher para que se encargara de la biblioteca y en 1721 le asignó la tarea de establecer contacto con destacados profesores extranjeros de Europa, así como de traer los más avanzados instrumentos astronómicos y físicos.

[3]Después de ser rechazado para ingresar como docente en la universidad de Basilea en 1727, fue invitado por Nicolás y Daniel Bernoulli para ir a San Petersburgo y formar parte de la *Academia* que estaba bajo el mando y cuidado de Catalina I; pero cuando Euler llegó en mayo de 1727 ella murió. Pedro II, el nuevo zar no consideraba importante el estudio de las ciencias, y ante tal incertidumbre para la *Academia* Euler prefirió ingresar a la marina rusa. Con la muerte de Pedro II en febrero de 1730, Ana Ivanovna asume el trono y, su tolerancia con la ciencia hace que le ofrezca a Euler la cátedra de física con lo que él regresa a San Petersburgo en 1730 y permanecer en la *Academia* hasta

llegó a San Petersburgo y tuvo su primer contacto con Goldbach. La afinidad de intereses hizo que iniciaran una amistad y una relación profesional y, aunque Goldbach partió a Moscú en 1729 y Euler estaba temporalmente ocupado en la marina rusa, sostuvieron correspondencia desde 1729 hasta 1764. Ésta comprende cerca de doscientas cartas —las conocidas—, que abarcan temas tan variados e importantes como: teoría de los números, series, números complejos, teoría de funciones, cálculo, etc. Además, en esta correspondencia podemos encontrar el génesis de muchos de los resultados que posteriormente publicaría Euler. La primera carta del 13 de octubre de 1729 que le escribió Euler a Goldbach[4] contiene comentarios sobre una de las ideas que había trabajado para el cálculo de una función interpolante que permitía obtener el factorial de valores fraccionarios o irracionales. [5]

El primero de diciembre del mismo año Goldbach le respondió, y lo que predominó en la carta fueron los comentarios a la fórmula para el factorial antes mencionada.[6] Goldbach le señaló que sería

1741.

[4][Euler-Goldbach 1965, pág. 19].

[5]La motivación de Euler para escribir esta carta estuvo a cargo de Daniel Bernoulli, porque resulta que éste último había escrito una carta el 6 de octubre de 1729 a Goldbach donde le planteaba que para una x positiva y A que tiende a infinito, el producto

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

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

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

Cuando Daniel Bernoulli se percata que Euler se interesaba en este problema le sugiere que le escriba a Goldbach y que le de a conocer su propuesta de que

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

y así es como se generó la carta del 13 de octubre de 1729 entre Euler y Goldbach.

[6]Ver [Euler-Goldbach 1965 pag. 24].

conveniente explorar con una expresión equivalente pero que ésta ahora fuera de manera integral.[7]

Después de que Goldbach terminó con sus comentarios a la fórmula antes expuesta, y casi para concluir la carta, le 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.

Con este pequeño párrafo Euler dio inicio a una vida de extraordinarias aportaciones a la teoría de los números. La respuesta de Euler llegó el 8 de enero de 1830 y le mencionó que aún no tenía una solución para los posibles primos de Fermat. Pero los dos años siguientes Euler mostró un interés ya no sólo en los posibles divisores de los números de la forma $2^{2^n}+1$; su visión del problema se dirigió al estudio general de los divisores de los números con las representaciones $a^n \pm 1$ y $a^n \pm b^n$.

Con esta carta de Goldbach de 1729 se abrió una gran ventana de interés en la que Euler ya no dejó de mirar el resto de su vida, y así la teoría de los números fue una de sus principales áreas de interés. Actualmente podemos contabilizar en la obra de Euler más de 800 trabajos publicados entre artículos y libros, repartidos en aproximadamente 24 áreas de la física matemática[8], pero lo que queremos hacer notar es que aproximadamente la sexta parte de sus trabajos corresponde a teoría de números, y más todavía, de la correspondencia y documentos que se encuentran en archivos la misma proporción corresponde a tópicos de teoría de números.

Euler abordó temas, en el ámbito de la teoría de los números, que ahora podemos clasificar en:

1. Primos de Fermat

[7] Estas cartas tendrían gran repercusión en lo que hoy conocemos como las funciones gamma y beta.

[8] Una clasificación se puede ver en el portal «The Euler Archive» cuya dirección es `http://eulerarchive.maa.org`

2. Pequeño teorema de Fermat
3. Suma de cuadrados
4. Representación de primos a través de formas cuadráticas binarias
5. Ecuaciones diofantinas
6. Último teorema de Fermat
7. Reciprocidad cuadrática
8. Función Zeta
9. Producto de Euler
10. Distribución de primos
11. Pruebas de primalidad
12. Particiones de enteros, funciones generadoras
13. Fracciones continuas
14. Números algebraicos y trascendentes

Entre 1830 –cuando Euler respondió la carta a Goldbach respecto de su pregunta de los números de Fermat– y 1832, Euler parece que reflexionó sus ideas sobre aritmética y el mismo año publicó su primer artículo sobre teoría de los números, éste es *Observationes de theoremate quodam Fermatiano aliisque ad numeros primos spectantibus* [9]. Como lo señala el título, el artículo contiene el análisis de Euler de problemas de Fermat y entre ellos el que le

[9] *Observaciones sobre teoremas que Fermat y otros autores sobre números primos.* A partir de aquí nos referiremos a los trabajos de Euler por la clasificación hecha por Gustav Enestrom, que para el caso del artículo mencionado es E26. El archivo completo se puede consultar en: `http://eulerarchive.maa.org`.

propuso Goldbach en la carta de 1829.[10] Como se mencionó, éste fue el primer trabajo de muchos con los que ahora sí la teoría de los números se consolidaba como una disciplina, con vida propia, dentro de las matemáticas y proporcionaría grandes temas de investigación que posteriormente retomarían Legendre, Lagrange, Riemann, Gauss, Galois, entre otros.

A Euler le agradaba la idea de exponer los grandes temas para lectores novicios, por ejemplo, escribió la obra *Elementos de Álgebra*[11] cuyos primeros capítulos estaban pensados para un lector inexperto en los temas algebraicos. Por otro lado, de regreso a la teoría de los números, parece que la segunda mitad del siglo XVIII era el momento propicio para retomar la aritmética euclidiana, junto con todas las aportaciones de Euler –pasando por Fermat–, y así crear la primera obra sobre teoría de los números que recopilara los conocimientos sobresalientes de la época y que fuera la base formativa para cualquier lector interesado en hacer investigación en el tema de los enteros.

Euler trabajó entre 1848-1850 en lo que sería el primer tratado sobre los enteros, su título es *Tractatus de numerorum doctrina Capita XVI, quae supersunt*[12]. Desgraciadamente nunca terminó la obra, escribió 16 capítulos y éstos se publicaron póstumamente

[10]La respuesta que escribió no se quedó en el 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.

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

[11]Se puede consultar la edición de John Hewlett de 1972. En la bibliografía está la referencia.

[12]L. Euler (1849), *Tractatus de numerorum doctrina, Commentationes Arithmeticae Collectae II*, 504 575, Petropoli. [In *Opera omnia* I.5, 182–283, Genevae, 1944]. *Tratado sobre la Doctrina de los números, compuesto por XVI capítulos*, pero en toda la tesis nos referiremos a la obra como *Tractatus*.

en 1849. En la sección que sigue haremos una presentación de este trabajo.

1.3. *Tractatus de Numerorum Doctrina.*

Actualmente contamos con los dieciséis capítulos que dejó manuscritos y estamos casi seguros que la versión que conocemos no era la que Euler pensaría enviar a la imprenta para su publicación. Los dieciséis capítulos contienen lo siguiente:

I. Sobre la composición de los números.

II. Sobre los divisores de un número.

III. Sobre la suma de los divisores de cada número.

IV. Sobre los números que son primos y compuestos entre sí.

V. De los residuos que se originan a partir de una división.

VI. Sobre los residuos que surgen a partir de una división de los términos de una progresión aritmética.

VII. Sobre los residuos que surgen a partir de la división de una progresión geométrica.

VIII. De los residuos que al ser divididos por un número primo dejan a la unidad como residuo.

IX. Sobre los divisores de los números de la forma $a^n \pm b^n$.

X. De los residuos surgidos de la división de los cuadrados entre números primos.

XI. Sobre los residuos surgidos de la división de los cubos entre los números primos.

XII. De los residuos de la división de los bicuadráticos entre números primos.

XIII. Sobre los residuos surgidos de la división de un *sursólido* entre números primos.

XIV. De los residuos originados de la división de los cuadrados entre los números compuestos.

XV. De los divisores de los números de la forma $xx + yy$.

XVI. Sobre los divisores de un número de la forma $xx + 2yy$.

Consideramos que no es apropiado seguir inmediatamente con el estudio de los dieciséis capítulos enunciados, haremos una pausa para recordar qué es lo que Euclides expone en los libros aritméticos contenidos en su obra *Elementos*. Creemos que es importante recordar esto ya que al ser el *Tractatus* el primer proyectos de libro introductorio para la teoría de los números, seguramente Euler tenía en mente lo planteado por Euclides, ya que él era el único antecedente de un trabajo estructurado sobre los enteros.[13]

1.4. Los libros aritméticos (VII al IX) de los *Elementos*.

Los libros aritméticos dentro de los *Elementos* son:

VII. Proporciones, máximo común divisor, mínimo común múltiplo, primos relativos.

VIII. Progresiones, números cuadrados y cúbicos.

IX. Factorización de primos, infinitud de los primos, números perfectos.

[13] Euler seguramente 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 Tartaglia (1586), Mardele (1622), Henrion (1676), Zamberti (1537), Gregorii (1703), Commandino (1575), Clavius (1574) entre otras, que contenían los libros del VII al IX.

Los libros VII al IX de los *Elementos* tratan sobre lo que denominamos los números enteros positivos, pero, se hace desde un punto de vista «geométrico», donde el uso de las magnitudes de segmentos representan a los números enteros. Al tratarse de contenidos sobre teoría de números, esto parece inusual, pero el manejo de magnitudes no altera la esencia de los resultados a la manera como los concebimos actualmente. En el libro VII aparecen las primeras definiciones de unidad, divisor,[14] número primo, máximo común divisor y diversas proposiciones que nos muestran el interés de Euclides por exhibir propiedades de la divisibilidad, pero que en su momento las visualizaba más desde la teoría de proporciones. Además, en esta parte se encuentran –enunciados y demostrados– el algoritmo de la división y el importante algoritmo para encontrar el máximo común divisor de dos enteros.[15]

En el libro VIII encontramos proposiciones básicas de divisibilidad y sobre números cuadrados y cúbicos, así como propiedades de números que se encuentran en progresiones aritméticas. Algo interesante a resaltar es sobre las potencias que estudia. Una pregunta natural sería, ¿si estudió los números con potencias cuadradas y cúbicas, por qué no bicuadráticas, potencias quintas, y demás? Esta tarea estuvo a cargo de Euler, quien retomó la idea y sí la generalizó, pero no es una coincidencia que Euclides se haya detenido en la tercera potencia, debemos tener muy presente al leer esta obra que el enfoque es geométrico, y por lo tanto no tiene sentido pensar en cuartas o quintas potencias ya que éstas estarían vinculadas a la cuarta y quinta dimensión, cosa que para la matemática griega no tenía sentido.

En el libro IX hay resultados, definiciones y afirmaciones de gran importancia que son retomadas por Euler. En primer lugar, todo el manejo de los números primos que llegan a una pausa importante cuando demuestra la infinitud de ellos (la cual es pertinen-

[14] Durante toda la exposición Euclides se refiere a las «partes» de un número, como aquello a lo que actualmente reconocemos como divisores.

[15] Su importancia actualmente es indiscutible, y bajo ciertas modificaciones menores, es adaptable a generalizaciones en otros anillos, por ejemplo el de los polinomios.

te decir, que es la que todavía se encuentra en los textos modernos de teoría clásica de los números). Por otro lado, las discusiones sobre divisores y la suma de los divisores llevan naturalmente a caracterizar a los números perfectos pares.

Es inevitable no pensar en las similitudes de ambos trabajos aritméticos –*Tractatus* y *Elementos*–, porque sí las hay. Ambos libros empiezan con ideas similares sobre los números enteros. Ahora, sin tomar en cuenta la evolución del lenguaje o las respectivas traducciones, ambas obras definen lo que es un números de la misma forma: «una colección de unidades». De hecho, una referencia más directa puede ser mostrada: en el libro IX de los *Elementos* de Euclides, se enuncia y demuestra la proposición sobre la infinitud de los números primos, afirmación que es retomada y citada por Euler en el *Tractatus* en el parágrafo 134 del capítulo IV. Debemos notar, sin embargo, que ambas obras, a pesar de que una influye en la otra, son esencialmente diferentes. Por ejemplo, la obra de Euler no menciona ni demuestra el algoritmo de Euclides para encontrar el máximo común divisor de dos números; la lectura sugiere que el lector ya tiene conocimiento de éste.

Algunos conceptos centrales en la teoría de los números, como el de los números perfectos, encuentran su nacimiento en estas obras. En la obra de Euclides se define a un número perfecto como aquél que es igual a la suma de sus partes (o en el lenguaje moderno, de sus divisores). El concepto es retomado en el *Tractatus* pero con una modificación que hasta hoy se conserva: un número perfecto es aquél cuyo doble es igual a la suma de sus divisores. Como se discutirá más adelante, la diferencia radica en que ahora se considera a un número n como un divisor de sí mismo, y esto facilita la clasificación de los números perfectos pares.

En este mismo sentido podemos considerar la definición que establece Euclides de un número primo: es aquél que es dividido sólo por la unidad. De la modificación que se mencionó arriba se deriva lo siguiente: para Euler, siendo n divisor de sí mismo, un número que no sea la unidad tendrá al menos dos divisores distintos (él mismo y la unidad) y por lo tanto un número primo es aquél

que tiene exactamente dos divisores distintos.

1.5. Contenido general del *Tractatus*.

Mencionamos anteriormente que el *Tractatus* está estructurado en dieciséis capítulos, pero consideramos que ellos se pueden agrupar en cuatro grandes bloques temáticos que son:

1. Introducción y propiedades básicas;
2. Residuos y clases;
3. Residuos de potencias;
4. Representación de números como formas cuadráticas (dos casos)

Cada una de estas partes la estudiaremos con detalle en los capítulos siguientes, pero antes daremos una breve explicación de cada uno.

Introducción y propiedades básicas va de capítulo I al IV abarca nociones generales de la teoría clásica, tales como propiedades sobre divisibilidad, números primos, números perfectos, la introducción de la función ϕ (que representa a los enteros positivos y primos relativos con un número y que son menores que él), máximo común divisor, la función σ (que representa la suma de los divisores de un números) entre otras. Estos temas constituyen la primera parte de casi cualquier texto actual sobre teoría clásica de números, y es el pilar sobre el que se han construido teorías nuevas y que han motivado el estudio y la investigación sobre los números enteros. Además, es importante señalar que este bloque es de alguna manera equivalente a lo que Euclides expone en sus libros aritméticos, pero sin querer insinuar que las formas de presentar los resultados son semejantes, ya que ambas teorías matemáticas atienden a paradigmas diferentes y épocas muy distantes.

La segunda parte que va del V al IX corresponde al estudio de la aritmética de los residuos que dejan los enteros cuando son

divididos por un número primo, también muestra de qué manera se construye lo que hoy conocemos como las clases residuales (o clases de equivalencia) y sistemas de residuos[16]. Primero presenta un ordenamiento en clases de los números de acuerdo al residuo que dejan al ser dividido por un número fijo. Las propiedades que se exponen corresponden a lo que identificamos como aritmética de los residuos, que son: la suma de dos residuos, el producto de dos de ellos, el residuo de un producto, la cantidad de residuos en una progresión, etc. Enseguida, Euler dedica el capítulo VIII a caracterizar a los enteros que dejan residuo uno cuando son divididos por un entero d. Con estas herramientas, y como un preámbulo natural a la tercera parte aquí se estudian brevemente los residuos de los números de la forma $a^n \pm b^n$.

La tercera parte es un estudio sobre los residuos de potencias. Es claro que muchas ideas sobre la reciprocidad cuadrática debieron nacer en esta obra. Esencialmente se estudian los números con potencia n que al ser divididos por d dejan residuo uno, además para d casi siempre primo aunque algunas proposiciones son para un divisor d en general. La forma de estructurar la investigación de las propiedades pretende adaptar para los casos $n = 3, 4, 5$ lo hecho en el caso $n = 2$, que es donde son más numerosos los resultados profundos. Es precisamente este capítulo (el X) el más extenso de toda la obra.

Finalmente, la cuarta parte contiene una exposición breve sobre los residuos de los números que pueden ser representados por expresiones de la forma $x^2 + y^2$ y $x^2 + 2y^2$. Actualmente es sabido que las formas cuadráticas binarias poseen increíbles propiedades relacionadas con la teoría de los números. A partir de esto, se han desarrollado y estudiado otras ramas de las matemáticas que han contribuido al estudio de la teoría de los números; por ejemplo, el grupo modular $PSL(2;\mathbb{Z})$ es central en la geometría hiperbólica,

[16]En esta sección también se está gestando lo que hoy conocemos como teoría de congruencias, lo que se está exponiendo en estos cinco capítulos son la base de la teoría que posteriormente Gauss llevaría a la notación que actualmente usamos para las congruencias.

como lo es en la teoría de números, y que emana de manera natural del estudio de las formas cuadráticas binarias. El estudio de estos objetos en esta obra de Euler es el inicio, y sólo se concentra en los residuos que pueden ser obtenidos a partir de estos números. No obstante, dejó las bases para futura investigación y su legado sigue siendo estudiado actualmente. Más aún, dado que Euler no pudo ver publicada esta obra en vida, no queda claro si tenía planeado escribir sólo dos capítulos sobre este tema; tal vez pudieron haber sido más o cada uno con más información.

Capítulo 2

Primera parte del *Tractatus*

2.1. Divisibilidad, Primos y Perfectos

El análisis de esta parte del *Tractatus* que comprende los capítulos I al IV se presenta aquí a sabiendas que ésta –seguramente– no fue la versión que Euler consideraba como definitiva, y se desea hacer esta aclaración porque el trabajo presenta elementos que pudieran ser criticados, ya sea porque se omiten algunos conceptos; algunos son un tanto discordantes; posiblemente no queda definido totalmente el perfil que quiere mostrar Euler en los dieciséis capítulos, y pudiéramos mencionar otros puntos que darían lugar al debate, pero consideramos que sería injusto hacer una reseña crítica del *Tractatus* ya que éste no fue terminado.

La clase de análisis que presentamos –para este capítulo y los que siguen– estará más en la dirección de estudiar sus aportaciones y cómo éstas trascendieron, así como la manera en la que él retoma a sus antecesores, y nos alejaremos definitivamente de un estudio comparativo con textos actuales de teoría de los números.

Al iniciar la lectura del capítulo 1 del *Tractatus* no es posible abstenerse de recordar el libro VII de los *Elementos* de Euclides; éste inicia –sin una introducción previa, al igual que Euler– con las

definiciones:

Definición 1. Una unidad es aquello en virtud de la cual cada una de las cosas que hay, se llama *una*.

Definición 2. Un número es una pluralidad compuesta de unidades.

Por su lado, Euler inicia con esto[1]:

1. Número es una multitud de unidades.

2. Cualquier número que se elija, éste indica cuántas unidades están contenidas en él.

Desde el inicio de ambas obras podemos notar las diferencias. Mientras que en Euclides ya encontramos un orden constructivo que parte de definir qué es la unidad y a partir de ella se construyen los números; en Euler se ve una manera más directa. Él en primer lugar define cómo se estructura un número, es decir, que con cierta cantidad de unidades formamos un número, pero en el enunciado que sigue en el *Tractatus* parece que está en una clase de regreso que nos dice que si tenemos cualquier número entonces éste nos indica la cantidad de unidades que lo componen. Aquí podemos ver que no es muy clara la ruta que quiere seguir, incluso, parece que estuviera redundando. Pero no hay duda que nos está presentando el concepto de número.

No pretendemos comparar el *Tractatus* con los *Elementos*, cada uno atiende a su perfil. Euclides por su lado, parece que en el libro VII de su obra tiene como eje central la construcción del algoritmo que le proporcionará la existencia de divisores comunes de dos o más enteros, y a partir de ahí dará entrada a toda la teoría de primos relativos, proporciones irreducibles y la existencia de primos entre los divisores de un entero. Entonces, el algoritmo para encontrar divisores comunes, o dicho de otra forma, el algoritmo para saber si dos enteros son primos relativos es pieza principal del libro VII de Euclides.

[1]En el caso de Euler no insertamos la etiqueta de «definición» ya que él no lo hace, aunque intrínsecamente lo es, y con Euclides sí se encuentra así en los *Elementos*.

Por su lado Euler enuncia el mismo algoritmo euclidiano pero hasta el final de su capítulo IV y además lo hace en una nota a pie de página. Esto significa que definitivamente tienen diferentes maneras de construir la teoría que quieren exhibir, entonces consideramos que sólo en ciertos casos –necesarios– recurriremos a la comparación.

De regreso al capítulo I, Euler nos presenta a los enteros positivos, sin duda podemos encontrar en este capítulo de la obra algunos elementos que nos dan entrada a proponer que Euler ya estaba cerca de enunciar alguna estructura algebraica de los enteros, como la que hoy denominamos anillo. Esto es, en la exposición encontramos que su construcción de los enteros deja la posibilidad de trabajar con negativos cuando enuncia en el parágrafo 8 que es posible restarle unidades a un entero para encontrar al antecesor de cada número, y aunque no enuncia directamente la existencia de los negativos, sí deja de manera explícita que el proceso de restar unidades se puede hacer de manera continua, por lo que no niega que se pueda llegar al cero y en consecuencia, de seguir así a los negativos. Es más, el caso del cero es aparte, plantea su existencia desde el parágrafo 5.

Desde las primeras proposiciones encontramos las piezas que constituyen una estructura algebraica actual: con su definición de número como conjunto de unidades y la idea de múltiplo, se podría dar paso a la existencia de una cerradura en la suma y producto. A través de su planteamiento de un número precedente –como ya se mencionó– tendría a un elemento neutro. Posteriormente con su definición de índice y múltiplo plantea la conmutatividad. Podemos seguir de esta forma y llegaríamos a que sólo le faltó mencionar algo sobre la asociatividad para tener lo que es un anillo.

Pero aún podríamos llegar más lejos con este tipo de análisis. Como a partir del capítulo V empieza el estudio de los residuos y más adelante los sistemas completos de residuos (o también conocidas como clases de equivalencia), entonces podemos ver en el *Tractatus* a los enteros agrupados en conjuntos con características comunes –los residuos según el módulo– , y esta manera de agrupar

facilita la expansión de cada conjunto, agregando todos los elementos de una misma clase en ese conjunto, y con la cualidad de que basta sólo un elemento para representarlos. Así, tendríamos a partir del *Tractatus* esta construcción de los enteros que sólo depende de los elementos que representan a las clases del sistema completo de residuos, y de paso podemos decir que ya estaba la idea de lo que posteriormente se definió en el álgebra moderna como conjunto cociente.

Con lo mencionado en los últimos párrafos queremos hacer notar que el análisis del *Tractatus* se podría ir sólo por el camino de ver cómo encaja esta obra de Euler en el contexto del álgebra actual, y hacerlo así sería un perfil de estudio perfectamente válido. Para el caso de este trabajo de tesis lo haremos de manera combinada, es decir, analizaremos las partes desde la matemática del siglo XVIII y cuando consideremos que la trascendencia de las proposiciones llegó hasta la matemática actual, entonces usaremos la mirada del siglo XXI.

2.2. Los números primos

Consideramos que en los capítulos I y II están las partes que forman la base para los resultados principales del capítulo IV, y esta base son los números primos. En estos capítulos de inicio, ya mencionamos que Euler construye propiedades de los enteros, pero a partir del parágrafo 30 nos enuncia la primera definición de número primo, y nos referimos a la primera porque lo hará de varias formas en estos dos capítulos. Es interesante descubrir que la controversia de la definición de primo estaba presente en el pensamiento de Euler y el *Tractatus* lo refleja. Seguramente en una edición final de la obra no hubiéramos encontrado tantas variantes como sí las hay en esta edición, pero esto es una fortuna porque nos permite saber cómo se gestaban las ideas que posteriormente veríamos en las obras ya finales. La manera en la que aborda los primos es como la presentamos a continuación. En el parágrafo 31 nos enuncia lo siguiente:

> Si en la serie de números $1, 2, 3, 4, 5, 6, 7$, etc., se eliminaran todos los múltiplos, los números restantes no serán múltiplos de ningún número (puesto que hemos excluido a la unidad). Estos números se llaman simples o primos.

Se puede percibir que ésta es la presentación de la criba de Eratóstenes, y en el parágrafo 32 desarrolla el proceso para decir que lo que queda después de la eliminación es el conjunto

$$1, 2, 3, 5, 7, 11, 13, 17, 19, \ldots$$

Aquí se nos presenta la controversia del uno, en primer lugar, ¿por qué en el parágrafo 31 no lo usó para eliminar a sus múltiplos?. La respuesta es directa, pues si lo usa entonces elimina a todos los enteros, pero esto ya está atajado con el parágrafo 26, pues en él enuncia que se quitará de la denominación de los múltiplos a los de la unidad. Por otro lado dice que los que quedan son los primos que son aquellos que no son múltiplos de nadie. Pero, entonces qué pasa con el uno, resulta que no es de los que quedan porque nunca lo usó para eliminar a otros, y por otro lado sí está en la lista de los primos. ¿Pasa que el uno es el único que queda por definición de que no es múltiplo de nadie?

Tener al uno entre los primos no es una novedad en el *Tractatus*, en otros momentos matemáticos de Euler se presenta algo semejante. Un caso se puede ver en la carta que le mandó Goldbach a Euler el 7 de junio de 1742. Goldbach le escribe:

> «[...]; de este modo quiero aventurar una conjetura: que todo número que está compuesto [como suma] de dos números primos es a la vez un agregado de tantos números primos como queramos (incluyendo la unidad), hasta alcanzar puras unidades [que es lo más a lo que se puede extender].»

Inmediatamente agrega estos ejemplos:

$$4= \begin{cases} 1+1+1+1 \\ 1+1+2 \\ 1+3 \end{cases} \qquad 5= \begin{cases} 2+3 \\ 1+1+3 \\ 1+1+1+2 \\ 1+1+1+1 \end{cases} \qquad 6= \begin{cases} 1+5 \\ 1+2+3 \\ 1+1+1 \\ 1+1+1+1+2 \\ 1+1+1+1+1+1 \end{cases}$$

etc.

En la misma carta le añade a manera de nota margina lo siguiente:

> Después de leer esto otra vez, considero que pudiera ser demostrada con todo rigor para el caso $n + 1$, si sucede para el caso n, y si $n + 1$ puede ser dividido en dos primos. Entonces la demostración es muy fácil. Parece por lo menos que todo número mayor que dos es la suma de tres números primos.

Como se puede notar esto es de donde se partió para lo que hoy conocemos como Conjetura de Goldbach, pero lo que queremos hacer notar es el uso del uno entre los primos. Cuando Euler le responde a Goldbach en la carta del 30 de junio de 1742 le dice lo siguiente:

> «que todo número que es resoluble como [suma] de dos primos, puede [a su vez] ser representado como [suma] de tantos primos como se quiera, puede ser ilustrado y confirmado por una observación, misma que usted me comunicó formalmente, concretamente, que todos los números pares son suma de dos primos.»
>
> «Supongamos que el número propuesto n sea par, por lo tanto es una suma de dos números primos, y entonces $n-2$ también es una suma de dos números primos, por lo que n también es una de tres, y también 4 y así sucesivamente. Pero si n es un número impar, entonces es una suma de tres números primos, ya que $n - 1$ es la suma de dos, y se puede seguir resolviendo las demás sumas. Sin embargo, que todo número par sea la suma de dos números primos, lo que considero un teorema correcto, es algo que no puedo demostrar».

La respuesta de Euler nos marca dos rubros: el del primer párrafo, donde acepta que la conjetura de Goldbach puede ser verdadera y admite —sin demostración— que todos los números pares son suma de dos primos; el segundo párrafo, donde muestra que si suponemos verdadera la relación binaria entonces la terciaria es posible.

Pero lo que ahora nos interesa más no es la famosa conjetura, lo que queremos resaltar, en el contexto del *Tractatus*, es que ambos parece que estaban en sintonía con que el uno se hallara entre los primos.

De regreso al *Tractatus* y al asunto de los primos, en los parágrafos 33 y 34 encontramos la idea de que los primos no pueden ser producto de dos enteros, ambos diferentes de uno, y esto lo requiere porque enunciará en el parágrafo 34 que:

> Todos los números que no son primos se llaman compuestos; a partir de esto es evidente que todos los números compuestos son múltiplos de otros números menores; y éstos pueden ser primos o, nuevamente, múltiplos de otros números menores, y también éstos son múltiplos de cualquier producto que se quiera, y a la vez que son múltiplos de cada uno de sus factores. Se sigue así que todos los números compuestos son reducidos, finalmente, a ser los múltiplos de los números primos.

Este parágrafo nos proporciona el resultado fundamental de que todo número compuesto tiene un factor primo y esto será la base de lo que nos enuncia en el parágrafo 35 que es lo que conocemos como el *Teorema Fundamental de la Aritmética*, aquél que nos indica que todo entero se puede escribir como un producto de primos (entre diferentes y repetidos).

En los parágrafos 50 y 53 recapitula un conjunto de resultados previos sobre la clasificación de los enteros según su cantidad de factores primos que lo forman, pero a lo que vamos es que cuando presenta a los que sólo tienen un factor primo nuevamente el uno está entre ellos.

En el Capítulo 2 que tiene como tema principal a los divisores de un número nos presenta otra definición de número primo. En el parágrafo 61 enuncia que «[...] si p denota un número primo, sus divisores serán, 1 y p, y no tiene otro más que éstos». Pero lo que está en el parágrafo 62 nos muestra cómo se estaba ajustando la teoría de los primos, ahí define lo siguiente:

> Por lo tanto los números primos [...] tienen solamente

> dos divisores. Y se excluye [de entre ellos a] la unidad, ya que tiene un solo divisor, por eso es que a la unidad no suele considerársele entre los números primos.

Aquí ya tenemos una restricción para la unidad en cuanto a que se le permita ser un primo, y usamos el verbo permitir porque pensamos que eso está pasando, es decir, cuando Euler ya enuncia que la unidad no es primo lo hace sin un fundamento sólido, porque sí está diciendo en el parágrafo 61 que un primo p es aquel que sólo lo divide el uno y el mismo p, entonces al uno sí lo divide el uno y él mismo, aunque coincidan. Incluso, Euler en el parágrafo 62 dice «la unidad no suele considerársele entre los números primos», y la frase no es totalmente excluyente, parece que da lugar a que bajo ciertas circunstancias sí se le considere primo, como pasó en los intercambios con Goldbach.

Si en la matemática euclidiana no tomaban a la unidad como primo, entonces ¿qué pasó?, por qué se encuentra tanta duda en el *Tractatus* en cuanto a los primos, ¿por qué Euler no asumió el entorno euclidiano de la aritmética para no tener dudas con la unidad? A continuación trataremos de resolverlo.

Posiblemente el entorno axiomático de los *Elementos* –en la parte aritmética– no logró convencer a Euler de que tenía que asumirla tal como estaba planteada. Ya mencionamos que en Euclides un número[2] es «una pluralidad compuesta de unidades», y más adelante en la definición 12 enuncia que «Un número primo es el medido por la sola unidad», es decir, nos deja ver desde el inicio que un número no es dividido por sí mismo. En lo que corresponde al planteamiento de número nos señala que son una pluralidad de unidades, pero no menciona la posibilidad de que sólo la unidad pueda ser número, porque en la primera definición, cuando define unidad, parece que le da un estatus mayor, pues ella es como un generador, y que no necesariamente tiene que ser un segmento, puede ser algo de otra naturaleza. Entonces parece que en este contexto

[2]En el entorno Euclidiano existían diversas opiniones sobre qué es un número, pero una digna de ser recordad es la de Aristóteles que dice «la unidad no es un número (Metafísica 1008a6), sino solo el principio de un número»

de los *Elementos* la unidad no es un número, éstos empiezan a partir del dos. Y en cuanto a los primos, resultará que si los números inician a partir del dos, entonces no tiene sentido pensar que la unidad pudiera ser un primo, ésta ni siquiera es número. Y más aún, como dice que un primo «es el medido por la sola unidad», entonces si el uno es considerado primo se tiene que admitir que un número es dividido por sí mismo, y esto es inadmisible en los *Elementos*.

Así, se tiene que Euler se educó leyendo esta visión de los números y parece que no le fue completamente satisfactoria. Para el siglo XVIII la visión es otra y la justificación de por qué el uno podría ser primo atiende a otras causas. Podemos decir que los euclidianos siempre tuvieron la razón en cuanto a los primos, el problema fue no poder asumir siempre sus justificaciones, y parece que eso sucedió en el *Tractatus*.

2.3. ¿Quién divide a n?

Después de presentarnos de manera intercalada entre los capítulos I y II sus definiciones y propiedades de los enteros –y en particular de los primos– así como de la certeza de que se pueden representar como productos de números primos, ahora Euler se adentra desde el capítulo II a construir la teoría de los divisores. En primer lugar él ya sabe que un número se puede escribir como producto de otros números, incluso en el capítulo I exhibe lo que llama «clases», que son los números que son producto de ciertas cantidades de primos que pueden ser iguales o diferentes, y con esto entonces ya puede extender la idea de múltiplo de un número. En segundo lugar, aborda el tema de los divisores en el capítulo II, pero ahora lo hará con base en el concepto de múltiplo.

Lo que expone Euler respecto a la teoría de la divisibilidad podría considerarse dentro de lo convencional de la época, pero sucede que en la cuarta proposición del capítulo II –que es el parágrafo 58– enuncia que:

> Puesto que cualquier número es el número simple de sí

> mismo, entonces la unidad es un divisor de cada número. Así, cualquier número es el divisor de sí mismo, y el cociente existente es la unidad.

Aquí sí tenemos un verdadero cambio que no parece notorio, nos referimos a la parte que dice «cualquier número es el divisor de sí mismo», pues resulta que desde Euclides se había considerado que esto no podía ser, es decir, un número no se consideraba como divisor de sí mismo, o en términos euclidianos, un número no es parte de sí mismo. Entonces, ¿por qué en los *Elementos* no consideran a n un divisor de n?

En las nociones comunes contenidas en el libro I encontramos que

El todo es mayor que la parte.

En la definición 1 del libro V se dice que

Una magnitud es parte de una magnitud, la menor de la mayor, cuando mide a la mayor.

Recordemos que la definición 3 del libro VII de los *Elementos* enuncia lo siguiente:

Un número es parte de un número, el menor del mayor, cuando mide al mayor.

Se puede ver que desde las nociones comunes no se contempla la posibilidad de que una parte pueda ser igual al todo, porque de ser así entonces ya no es una parte. En el entorno de la época euclidiana se tiene que considerar que la opinión aristotélica contenida en la *Metafísica* [1023b12] señala que «se llama parte en un sentido aquello en que puede ser dividida una cantidad (pues siempre lo que se quita de una cantidad en cuanto cantidad se llama parte de ella [...]»

Lo que tenemos es que una parte –divisor en nuestra época– es algo que se puede extraer del número mayor, y por la noción común, tiene que ser menor que él, entonces todo parece indicar

que a una cantidad no se le puede extraer su misma cantidad; dicho de otra manera, un número no es divisor de sí mismo.

Donde se percibe la primera diferencia entre que si un número es divisor de sí mismo o no, es cuando se aborda el tema de los números perfecto. Por el lado de Euclides la definición 23 del libro VII describe que

> *Número perfecto es el que es igual a sus propias partes.*[3]

Y para confirmar que no considera al mismo número entre los divisores, cuando enuncia y demuestra la proposición 36 del libro IX, que trata sobre el conjunto de números de la forma $2^n(2^{n+1}-1)$, que demuestra que son perfectos, no está considerando entre la suma de sus divisores al mismo $2^n(2^{n+1}-1)$. Euler en el *Tractatus* (parágrafo 106) enuncia

> [...] si pasa que[4] $\int N = 2N$, el número N será un número perfecto.

Ahora, ¿esta diferencia es algo importante? o ¿sólo fue una actualización del concepto que se dio en el siglo XVIII? Para esto veamos cómo fue que ambos abordaron el teorema de los números perfectos, éste se enuncia de la siguiente manera:

> Un entero par es de la forma $n = 2^{p-1}(2^p - 1)$, donde $2^p - 1$ es primo, si y sólo si, n es un número perfecto par.

Euclides por su parte demostró que

> Si un entero par es de la forma $n = 2^{p-1}(2^p - 1)$ donde $2^p - 1$ es primo, entonces n es un número perfecto.

Pero el enunciado original en los *Elementos*, proposición 36 del Libro IX, dice:

> 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

[3] En términos actuales diríamos: M entero positivo es número perfecto si M es igual a la suma de sus divisores propios.

[4] El símbolo $\int x$ se refiere a la suma de divisores de un entero x, es notación propia de Euler.

último produce algún número, el producto será [un número] perfecto[5].

En notación moderna decimos que se tendría una sucesión de segmentos de magnitud $1, 2^1, 2^2, 2^3, 2^4, 2^5, \ldots, 2^{n-1}$ que se encuentran en proporción duplicada (es decir, la longitud de cada segmento es el doble del que le precede) y cuya suma resulte ser un primo M. Ahora, si M se multiplica por el último término de la sucesión que es 2^{n-1}, entonces, se obtiene el producto y aunque Euclides no lo menciona explícitamente sí deja ver que M es $2^n - 1$. Así, en notación y lenguaje actual se tiene que si un número es de la forma $2^{n-1}(2^n - 1)$ con $2^n - 1$ primo entonces es perfecto par.

Cabe señalar que en los *Elementos* sólo se llega a mencionar como ejemplos de números perfectos a $2^{2-1}(2^2 - 1) = 6$ y a $2^{3-1}(2^3 - 1) = 28$. Es Nicómaco quien proporciona los dos siguientes: $2^{5-1}(2^5 - 1) = 496$ y $(2^{7-1})(2^7 - 1) = 8128$.

Euclides en la anterior proposición 36 muestra una ley de construcción de los números perfectos, es decir:

$1 + 2^1 = 3$	3 es primo	entonces $2^1 \times 3 = 6$ es Perfecto
$1 + 2^1 + 2^2 = 7$	7 es primo	entonces $2^2 \times 7 = 28$ es Perfecto
$1 + 2^1 + 2^2 + 2^3 = 15$	15 no es primo	entonces $2^3 \times 15 = 120$ no es Perfecto
$1 + 2^1 + 2^2 + 2^3 + 2^4 = 31$	31 es primo	entonces $2^4 \times 31 = 496$ es Perfecto

Con este algoritmo queda establecida una condición suficiente, pero no necesaria, para hallar números perfectos pares.

Pero recordemos que todo esto fue para tratar de responder la interrogante sobre que n entero sea un divisor de sí mismo, y que si el cambio de concepto ¿sólo fue una actualización que se dio en el siglo XVIII?

Veamos qué pasa con la construcción euclidiana cuando n es divisor de sí mismo y cuando no lo es. Así, de la proposición euclidiana ya observamos que:

[5]Haciendo un breve paréntesis en el desarrollo de la exposición, aquí se recomienda leer la demostración de manera euclidiana de la proposición 36 que está en un Apéndice de la tesis, para recordar cómo los griegos trataban a los números desde una perspectiva de magnitudes.

Se toma una suma apropiada de potencias de dos $1+2+2^2+2^3+\ldots+2^k=p$, donde p es primo, y esta suma se multiplica por la última potencia para obtener que $p2^k=2^k(2^{k+1}-1)$. Ahora, veamos qué pasa con la suma de los divisores de este número. Éstos son los conjuntos $1,2,2^2,2^3,\ldots,2^k$ y $p,2p,2^2p,2^3p,\ldots,2^{k-1}p$, entonces si sumamos ambos conjuntos tenemos que uno es $(2^{k+1}-1)$ y el otro $p(2^k-1)=(2^{k+1}-1)(2^k-1)$, por lo tanto, la suma total es $(2^{k+1}-1)+(2^{k+1}-1)(2^k-1)=(2^{k+1}-1)(1+(2^k-1))=2^k(2^{k+1}-1)$. Por lo tanto, la suma de los divisores propios es igual al mismo número. Pero, ¿qué pasa si ahora sí consideramos a $p2^k$ como uno de los divisores? veamos.

Entre los divisores de $p2^k$ ahora sí consideraremos al mismo $p2^k$, por lo tanto sumaremos los conjuntos $1,2,2^2,2^3,\ldots,2^k$ y $p,2p,2^2p,2^3p,\ldots,2^{k-1}p,2^kp$, y obtenemos como resultado $(2^{k+1}-1)+(2^{k+1}-1)(2^{k+1}-1)=(2^{k+1}-1)(1+(2^{k+1}-1))=2^{k+1}(2^{k+1}-1)=2(2^k(2^{k+1}-1))$. En resumen, la suma de los divisores es dos veces $2^k(2^{k+1}-1)$, que es el doble del mismo resultado cuando no se consideraba al número como divisor de sí mismo.

Hemos llegado a que no importa si se toma o no al número como divisor de sí mismo, porque a partir del enunciado euclidiano no existe problema para extender el resultado. Entonces, hasta esta parte parece que no considerar esta propiedad de la división, corresponde más a los fundamentos que a la misma operatividad de los enteros. Pero si queremos confirmar esto pasemos a ver si el resultado siguiente de Euler, el que dice: *si n es un número perfecto par entonces es de la forma $n=2^{p-1}(2^p-1)$ donde (2^p-1) es primo*, ¿también se puede demostrar sin que se considere que un entero n es divisor de sí mismo?

En los parágrafos 106, 107 y 108 Euler expone que

> 106. [...] si pasa que $\int N=2N$, el número N será un número perfecto. Si aquél es par, será de la forma 2^nA, con la existencia de un número A impar, que es primo o compuesto. Entonces, de cualquier modo $N=2^nA$, y pasará que $\int N=(2^{n+1}-1)\int A=2^{n+1}A$, dando lugar a que $\frac{\int A}{A}=\frac{2^{n+1}}{2^{n+1}-1}$.

107. Y puesto que el numerador de esta fracción $\frac{2^{n+1}}{2^{n+1}-1}$ tan sólo supera en una unidad al denominador, el denominador A no puede sobrepasar [el número A] a la suma de los divisores de A, así pues, éste será igual o menor. En el caso anterior no existe solución; en cambio en el primer caso, no puede existir, a no ser que $2^{n+1}-1$ sea un número primo. Por lo tanto siempre que $2^{n+1}-1$ sea un número primo, que a la vez es A, se obtendrá un número perfecto $= 2^n(2^{n+1}-1)$.

108. Así, todos los números perfectos pares tienen la forma $2^n(2^{n+1}-1)$ donde $2^{n+1}-1$ es un número primo, y esto no puede suceder, a no ser que $n+1$ sea un número primo; aún así no todos los números primos tomados en el lugar de $n+1$ generan un número primo con $2^{n+1}-1$. [...]

Ahora damos nuestra interpretación de este pasaje:

Define un número perfecto N como aquél que satisface $\int N = 2N$, después supone que el perfecto N es par y por tanto puede ser de la forma $N = 2^n \times A$ con A impar, $2N = 2 \cdot 2^n \times A = 2^{n+1} \times A$, pero $\int N = 2N$, entonces $2^{n+1} \times A = \int(2^n \times A)$, y como 2^n y A son primos relativos, se tiene que $2^{n+1} \times A = \int 2^n \times \int A$.

Ahora, la suma de los divisores de 2^n es $\int 2^n = 1+2+2^2+2^3+\cdots+2^n = 2^{n+1}-1$ entonces, $2^{n+1} \times A = (2^{n+1}-1) \times \int A \Rightarrow \frac{\int A}{A} = \frac{2^{n+1}}{2^{n+1}-1}$. Ya que $\frac{2^{n+1}}{2^{n+1}-1}$ es un número cercano a uno, entonces Euler para aplicar un Lema propio: *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* $N = n$. Así, con el lema pudo concluir que $A = 2^{n+1}-1$ y, en consecuencia, como $2^{n+1} \times A = (2^{n+1}-1) \times \int A \Rightarrow \int A = 2^{n+1}$ y por la forma mencionada de A, se tiene que $\int A = A + 1$. Por lo tanto se tiene que A es un número primo.

Finalmente, dado que $N = 2^n \times A$ es perfecto par y $A = 2^{n+1}-1$ es primo entonces $N = 2^n \times (2^{n+1}-1)$, obteniéndose por fin, el recíproco de la proposición 36 de Euclides.

En el artículo de *De Numeris Amicabilis*[6] (publicado en 1750 y escrito en 1747), Euler trabaja con la igualdad $\frac{\int A}{A} = \frac{2^{n+1}}{2^{n+1}-1}$

[6][Euler 1747].

suponiendo que existe una c tal que $A = c \cdot (2^{n+1} - 1)$ y $\int A = c \cdot 2^{n+1}$, y logra deducir que $c \geq 1$ Después, llegarían otros para demostrar que $c = 1$. En ambas demostraciones se nota la falta de una plena justificación (desde nuestra perspectiva actual y no en la época de Euler), desde que $\frac{\int A}{A} = \frac{2^{n+1}}{2^{n+1}-1}$ hasta la conclusión de $\int A = A + 1$.

Actualmente podríamos evitar la controversia que podría generar el uso de la igualdad $\frac{\int A}{A} = \frac{2^{n+1}}{2^{n+1}-1}$ y retomar la demostración de Euler desde la igualdad previa $2^{n+1} \times A = (2^{n+1} - 1) \times \int A$ y reescribir a la suma de los divisores de A como $\int A = A + t$ donde $t = \sum_{d|A, d<A} d$, para obtener: $2^{n+1} \times A = (2^{n+1} - 1)(A + t)$. 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, $N = 2^n \times A = 2^n \times (2^{n+1} - 1)$ con $2^{n+1} - 1$ primo. Entonces, con estos ajustes queda la demostración, pero es importante recordar que todo esto se hizo bajo la premisa de que un entero se considera como divisor de sí mismo y por ello la definición de perfecto cumple con que $\int N = 2N$ y se usa además la partición de los divisores de A en $\int A = A + t$, donde t es el conjunto de todos los divisores propios de A.

Por el lado de la definición euclidiana de divisor, donde un número no tiene entre sus divisores a él mismo pasa algo diferente. Retomando la demostración anterior tendríamos que $\int N = N$ y del mismo proceso se llegaría a que $2^n \times A = (2^n - 1) \times \int A \Rightarrow \frac{\int A}{A} = \frac{2^n}{2^n-1}$ y por lo tanto $N = 2^n \times A = 2^n \times (2^n - 1)$, que es diferente a $2^n \times (2^{n+1} - 1)$ que es a lo que se tiene que llegar.

Finalmente, tenemos un ejemplo de que sí es determinante considerar a un entero divisor de sí mismo o no, ya mostramos que bajo la definición euclidiana de perfecto no se puede llegar a que todo perfecto par es de la forma $2^n \times (2^{n+1} - 1)$. Con esto vemos

que el parágrafo 58 del *Tractatus* era más que un enunciado del tema de divisores, verdaderamente fue un cambio en la aritmética euclidiana.

2.4. Perfectos impares y el factor de Euler.

En cuanto a los perfectos pares Euler ya estaba cerrando el círculo –junto con Euclides– de las condiciones necesarias y suficientes para la existencia y forma de estos números. Pero, ya para terminar el capítulo III del *Tractatus* Euler menciona lo siguiente en los parágrafos 108 y 109:

> 108. [...] además de los números perfectos pares, existen también los impares, o no? Todavía nadie lo ha demostrado.
>
> 109. Si se diera un número perfecto impar, es necesario que todos sus factores sean impares. Sea por lo tanto $= ABCD$ etc., es necesario [a partir de la definición de número perfecto] que $\int A \int B \int C \int D = 2ABCD$ sea un número imparmente par. Por lo que entre las sumas de los divisores $\int A, \int B, \int C, \int D$ debe existir sólo un imparmente par, todos los otros serán impares. Así, todos los factores A, B, C, D, con excepción de uno, son números primos con potencias pares. Aquél que es la excepción, en cambio, será o un número primo de la forma $4\lambda + 1$, que tendrá una potencia también de la forma $4\delta + 1$. Entonces, tal número perfecto tendrá la forma $(4n+1)^{4\lambda+1}PP$, donde los números P son impar y un número primo es de la forma $4n + 1$.

Como podemos ver Euler ya se cuestionaba la existencia de los perfectos impares, y actualmente seguimos en lo mismo, es decir, no conocemos uno, pero tampoco podemos afirmar su inexistencia. Pero el primer resultado sobresaliente respecto a los perfectos impares lo aportó Euler en el parágrafo 109. Él tuvo la visión de poder caracterizarlos a pesar de no conocer a uno. En terminología moderna lo que enuncia en el parágrafo 109 es:

> 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 $q, p_1, p_2, \ldots, p_r$ son primos impares diferentes.

Actualmente identificamos al factor q^{α} como «Factor de Euler».

Como se ve en los parágrafos citados Euler sólo enunció el problema, ahora damos lugar a una demostración tratando de seguir los criterios del entorno de Euler.

Demostración.

Como n es un perfecto impar entonces se tiene por definición que[7] $\sigma(n) = 2n$ y por la factorización única en primos, $n = ABCD\cdots$ (estos divisores de n pueden verse como potencias de primos diferentes entre ellos e impares).

Ahora, considerando que σ es multiplicativa se tiene $2n = \sigma(ABCD\cdots) = \sigma(A)\sigma(B)\sigma(C)\sigma(D)\cdots$. Además, dado que n es impar se deduce que $2n$ es el doble de un impar y como diría Euclides es un número «imparmente par», es decir, $2n = 2(2\lambda+1) = 4\lambda+2$ por lo tanto $2n \equiv 2 \pmod 4$, pero, nótese que $4 \nmid 2n$ (porque si sucede que $4 \mid 2n$, entonces, $4 \mid n$ o $2 \mid n$ lo cual no es posible ya que n es impar). Así, es importante señalar que entre los factores $\sigma(A)\sigma(B)\sigma(C)\sigma(D)\cdots$ sólo hay uno que es imparmente par y los restantes son impares. Sin perdida de generalidad, tómese al factor $\sigma(B)$ como impar y supóngase que B es la potencia de un primo tal que: $B = P^m \Rightarrow \sigma(B) = \sigma(P^m) = P^m + P^{m-1} + \cdots + P^2 + P + 1$. Como el primo P es impar y $P^m + P^{m-1} + \cdots + P^2 + P + 1$ es una suma de m impares más uno se deduce que el exponente m debe ser forzosamente par para que se cumpla que el factor $\sigma(B)$ sea impar. De esta manera $B = P^m$ es una potencia par de un número impar, por lo que, B será un cuadrado perfecto. Concluyéndose por tanto que todos los factores primos $ABCD\cdots$ de n, a excepción de uno, serán cuadrados perfectos.

Por otro lado, sea $\sigma(A)$ el factor imparmente par de $\sigma(n)$, es decir, $\sigma(A) = 2(2\varphi+1) = 4\varphi+2$ entonces $\sigma(A) \equiv 2 \pmod 4$. Y sea $A = q^{\alpha}$ donde q es un primo impar, por lo que q es de la forma $4k+1$ o $4k+3$. Se afirma que q es de la forma $4k+1$ porque si $q = 4k+3$ se tendría que $\sigma(A) \not\equiv 2 \pmod 4$ lo cual contradice el hecho de que $\sigma(A)$ es imparmente par; esto se concluyó al aplicar a $\sigma(A) = \sigma(q^{\alpha}) = q^{\alpha} + q^{\alpha-1} + \cdots + q^3 + q^2 + q + 1$ las dos propiedades

[7] Función suma de divisores.

siguientes:

1. $(4k+3)^s \equiv 1 \pmod 4$ si s es par y $(4k+3)^s \equiv 3 \pmod 4$ si s es impar, para las respectivas $s = \alpha, \alpha-1, \ldots, 2, 1$.

2. $\sigma(q^\alpha) \equiv 1 \pmod 4$ si α es par y $\sigma(q^\alpha) \equiv 0 \pmod 4$ si α es impar donde $\sigma(q^\alpha) = q^\alpha + q^{\alpha-1} + \cdots + q^3 + q^2 + q + 1$.

Así, como q es de la forma $4k+1$ entonces $1, q, q^2, \ldots, q^{\alpha-1}, q^\alpha \equiv 1 \pmod 4$. Ahora, dado que $\sigma(A) = \sigma(q^\alpha) = q^\alpha + q^{\alpha-1} + \cdots + q^3 + q^2 + q + 1$ es una suma par cuya cantidad de sumandos es $\alpha+1$ se deduce que α es número impar, el cual, podría ser de la forma $4\lambda + 1$ o $4\lambda + 3$. Y por la estructura de las potencias de q se tiene que cada una es de la forma:

$4k_1 + 1, 4k_2 + 1, 4k_3 + 1, 4k_4 + 1, 4k_5 + 1 \cdots, 4k_\alpha + 1 \Rightarrow$

$1 + q + q^2 + q^3 + \cdots q^\alpha = 1 + 4(k_1 + k_2 + k_3 + \cdots + k_\alpha) + \alpha \Rightarrow$

$4(k_1 + k_2 + k_3 + \cdots + k_\alpha) + (\alpha + 1) = 4k + (\alpha + 1) = 2\Gamma = \sigma(A) = \sigma(q^\alpha)$.

Por lo que, si $\alpha = 4\lambda + 3$ implica que Γ es par, esto es, $\sigma(A) = 2(2\varphi)$ llegándose así a una contradicción ya que por hipótesis $\sigma(A)$ es imparmente par. Por 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 $q, p_1, p_2, \ldots, p_r$ son primos impares distintos y $q \equiv \alpha \equiv 1 \pmod 4$. □

Este resultado del *Tractatus* hasta nuestros días es usado con frecuencia por aquéllos que siguen investigando las propiedades que podrían tener o no los perfectos impares

2.5. Funciones aritméticas

En nuestro análisis de los números perfectos usamos sin mayor explicación la función aritmética suma de divisores de un entero n, denotada por $\sigma(n)$ (y en el original de Euler por $\int n$). Ahora dedicaremos esta sección de la tesis al estudio de las funciones aritméticas dentro del *Tractatus* y nos referimos a $\sigma(n)$; a la función

cantidad de divisores, denotada por $\tau(n)$; y la función cantidad de primos relativos positivos menores a n, denotada por $\phi(n)$. En los capítulos III y IV Euler construye las tres funciones aritméticas, el III está dedicado en su mayoría a la función $\sigma(n)$ y el IV a la función $\phi(n)$.

2.5.1. Funciones $\tau(n)$ y $\sigma(n)$

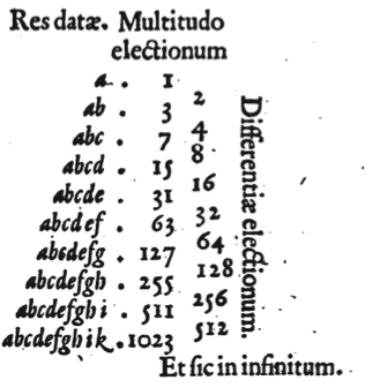
Si nos quedamos sólo con la exposición del *Tractatus* podríamos tener una interpretación muy restringida de la manera en que Euler usó estas funciones aritméticas, que parecería que sólo fue para los números perfectos. Pero, en realidad estas funciones las usó para desarrollar más resultados que presentaremos más adelante, ya que primero proporcionaremos los antecedentes de las funciones que seguramente Euler conocía.

De las primeras referencias que se tiene registro tenemos la de Girolamo Cardano con su obra de 1537 *Practica arithmetica et mensuran disingularis* (Aritmética práctica y las mediciones individuales)[8], ahí enuncia que para un número P que es producto de k primos diferentes, la cantidad de sus divisores menor que P es igual a

$$1 + 2 + 2^2 + \cdots + 2^{k-1} = 2^k - 1$$

En 1657 Francisci á Schooten publicó *Exercitationum mathematicarum. LiberV. Sectiones trigintamiscellaneas*, en las primeras cuatro secciones (páginas 373-390) encontramos la más extensa exposición sobre la cantidad de divisores de un entero formado con factores primos diferentes y si están repetidos se agrupan para presentarse como potencias. Es interesante notar que nuevamente no se considera al número como divisor de sí mismo, además expone la progresión geométrica de las diferencias de las clases de números que están formados con primos diferentes que crecen de manera consecutiva, véase el ejemplo directo del libro (pág. 375):

[8]Referencia tomada de [Dickson 2005, tomo II pág. 51].



La exposición es extensa y detallada y cualquier interesado en la función $\tau(n)$ que vivió a mediados del siglo XVIII debió de haber tenido entre sus manos la obra de Francisci á Schooten. Euler posiblemente conocía la obra, y entre la exposición del *Tractatus* y el *Exercitationum*, en lo que corresponde a la $\tau(n)$, se tienen claramente antecedentes de lo que se conocía a mediados del siglo XVII[9]. Citaremos un ejemplo, veamos los siguientes parágrafos del *Tractatus*:

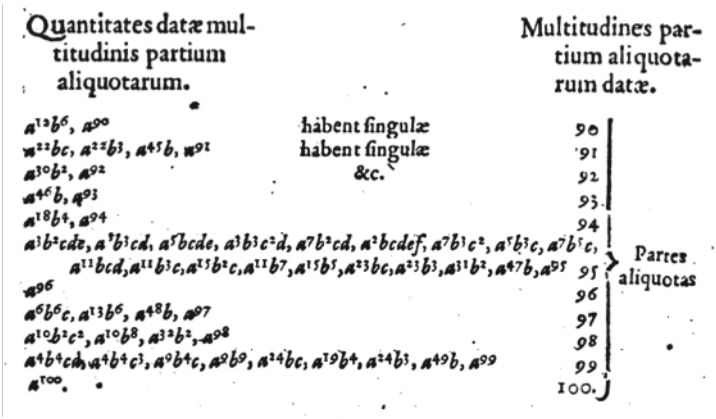
> 77. A partir de esto, parece que la regla para definir la cantidad de divisores de cualquier número es fácil. Sea $p^\lambda q^\mu r^\nu s^\xi$ la forma del número propuesto; puesto que la cantidad de divisores del número p^λ es $\lambda + 1$, entonces, la cantidad de divisores de $p^\lambda q^\mu$ será $(\lambda+1)(\mu+1)$; la del número $p^\lambda q^\mu r^\nu$ será $(\lambda+1)(\mu+1)(\nu+1)$, y la de este otro $p^\lambda q^\mu r^\nu s^\xi$ será $(\lambda + 1)(\mu + 1)(\nu + 1)(\xi + 1)$. Pero la clase hacia la cual debe referirse este número está indicada por el número $\lambda + \mu + \nu + \xi$, que es la suma de los exponentes.
>
> 78. Pueden presentarse una infinidad de números de los cuales se puede dar su cantidad de divisores. Si tal cantidad es a, y considerando la existencia del número primo p, entonces los números buscados serán en la forma p^{a-1}, siendo p cualquier número primo.
>
> 80. De allí, si la cantidad de divisores es igual a 2, es porque se tiene que sólo se satisface para los números primos

[9]No sabemos con certeza si Euler leyó la obra, pero pretendemos señalar el tipo de teoría que heredó Euler, ya sea de Francisci á Schooten o de otros autores.

o los números que están contenidos en la forma p. Entonces se tiene:

Cantidad de divisores	Forma de los números
3	p^2
4	p^3, pq
5	p^4
6	p^5, p^2q
7	p^6
8	p^7, p^3q, pqr
9	p^8, p^2q^2
10	p^9, p^4q
11	p^{10}
12	$p^{11}, p^5q, p^3q^2, p^2qr$

Ahora veamos uno del *Exercitationum*


Quantitates datæ multitudinis partium aliquotarum.

Multitudines partium aliquotarum datæ.

habent singulæ
habent singulæ
&c.

90 91 92 93 94 95 96 97 98 99 100.

Partes aliquotas

En ambos trabajos encontramos exposiciones semejantes y didácticamente bien presentadas, donde la idea de tener una infinidad de números que tienen la misma cantidad de divisores está presente, y considerando que en nuestro primer autor un número sí se divide a sí mismo y en el segundo no.

Antes de Euler la obra de Francisci á Schooten fue de las más completas, pero no la única que se adentró en el tema, y para terminar con los antecedentes históricos de $\tau(n)$ –que a la vez podrían ser del *Tractatus*– debemos de recordar lo siguiente. Newton en *Arithmetica Universalis* de 1732, en la parte *De inventione divisorom* (pág. 37) exhibe la manera de encontrar la cantidad de

divisores de un número, pero no intenta generalizar un resultado y plantea una función aritmética[10]. De forma semejante trataron el tema John Wallis en su *Treatise of Algebra* en 1685 (capítulo III) y Pierre Rémond de Montmort en su *Essay d'analyse sur les jeux de hazard*, en el corolario IV contenido en la primera parte (segunda edición 1713 pág. 55) aborda sólo lo necesario para poder trabajar sobre un asunto de combinaciones que es su verdadero objetivo.

En cuanto a la función $\tau(n)$ ya mostramos donde podrían encontrarse las posibles fuentes que Euler conoció para saber de ella, ahora pasamos al análisis de los antecedentes de la función $\sigma(n)$.

Nuestro primer personaje es Descartes, en sus *Œuvres de Descartes* volumen 10 y bajo el título de la sección *De Partibus Aliquotis Numerorum* (edición de Chales Adam y Paul Tannery 1908, páginas 300 y 301) menciona de manera breve que la suma de los divisores de la n-ésima potencia de un primo a es $\frac{a^n-1}{a-1}$, y aquí tenemos un resultado que ya no nos es ajeno en el *Tractatus*, pero sí es de señalar que nuevamente tenemos que para Descartes a^n no es en sí mismo un divisor y lo quita, lo dice explícitamente. También nos proporciona la fórmula del producto de un primo por un compuesto y dice: «*si b es la suma de los divisores de a, y x es un primo, entonces la suma de los divisores de ax es* $bx+a+b$»[11]. Después extiende su desarrollo para enunciar que la suma de los divisores ax^n con a y x primos relativos es $\frac{bx^{n+1}+ax^n-a-b}{x-1}$ .Y no está claro si tenía una regla general para el producto de números que son primos relativos, es decir, que

$$\sigma(nm) = \sigma(n)\sigma(m).$$

Pero en una carta que le manda a Marin Mersenne el 27 de mayo de 1638 le menciona que tiene una regla para encontrar el producto de dos números si ya conoce el producto que representa la suma de sus divisores.

[10]Y cabe señalar que parece que Newton al menos desde el ejemplo que muestra ya considera a un número como divisor de sí mismo.

[11]En el caso de que un número es divisor de sí mismo entonces la suma de los divisores sería $b(x+1)$.

Tenemos que hacer mención que estos resultados posiblemente no los conoció Euler, y menos la carta, pero lo exponemos ya que eran temas de interés en los inicios del siglo XVII.

De la misma manera encontramos en la obra *Algebra Tractatus*, 1693 (pág. 812), de John Wallis una carta que le envió a Kennet Gigby el 4 de marzo de 1658, en ella le exponen diversos problemas donde plantea que se puede cumplir la igualdad $\sigma(nm) = \sigma(n)\sigma(m)$. En este contexto podríamos mencionar a Fermat, G.W. Kraft, Frenicle pero ya sólo sería para decir que mostraban algunos casos particulares en sus obras o correspondencia.

Ahora podemos regresar a Euler y analizar que hizo con la función $\sigma(n)$, tanto en el *Tractatus* como en otros trabajos.

Ya mencionamos que se podría tener una mala interpretación de qué tanto aportó con la función $\sigma(n)$ si nos quedamos sólo con la visión del *Tractatus*, –es más, se podría decir que no expone algo que no se encuentre en lo hecho por Descartes, Wallis o Fermat–, pero consideramos, después de estudiar la obra en su totalidad, que el perfil de ésta –hasta los dieciséis capítulos que se conocen– estaba cimentado sobre la idea de estudiar la teoría de residuos, entonces, en este contexto no requería más de las funciones $\tau(n)$ y $\sigma(n)$. Pero lo que sí sabemos es que desde una perspectiva de la teoría de particiones, de la que Euler es esencialmente el creador, entonces la función $\sigma(n)$ sí está involucrada en resultados que son verdaderamente sobresalientes. Ahora, expondremos lo contenido en el *Tractatus* y posteriormente los resultados más sobresalientes que se encuentras en otras de sus publicaciones.

A partir del parágrafo 82 del capítulo III Euler construye desde lo más elemental los conceptos de la función suma de divisores, y como ya lo mencionamos antes cuando expusimos lo de números perfectos «tal notación $\int n$ represente la suma de los divisores del número n» (parafraseando a Euler).

Después, entre los parágrafos 83 al 89 construye los casos particulares de $\int n$ cuando:

I) n es la potencia de un primo,

$$\int p^1 = p + 1 = \frac{pp - 1}{p - 1},$$

$$\int p^2 = pp + p + 1 = \frac{p^3 - 1}{p - 1},$$

$$\int p^3 = p^3 + p^2 + p + 1 = \frac{p^4 - 1}{p - 1},$$

y en general,

$$\int p^n = p^n + p^{n-1} + p^{n-2} + \cdots + 1 = \frac{p^{n+1} - 1}{p - 1}.$$

II) Cuando n es un producto de primos pq (parágrafo 85).

> Los divisores son $1, p, q, pq$ entonces la suma de éstos será: $1 + p + q + pq = (1 + p)(1 + q)$ y por esto $\int pq = (p + 1)(q + 1)$. De igual modo será la suma de los números de la tercera clase: $\int p^2 q = (pp + p + 1)(q + 1)$ y $\int pqr = (p + 1)(q + 1)(r + 1)$.

III) n es producto de un entero (compuesto) por un primo o potencia de un primo (parágrafo 87).

> [...] si el número N se multiplica por el cuadrado del número primo p, que no es parte de éste contenido en este mismo, la suma de los divisores del producto Np^2 será: $(1 + p + p^2) \int N$, o $\int Np^2 = \int N \int p^2$; y del mismo modo sería: $\int Np^3 = \int N \int p^3$, y así sucesivamente.

IV) Da un producto de potencias de primos, e introduce la idea de sigma multiplicativa (parágrafo 90).

> Así, si se tiene un número N y es necesario encontrar la suma de sus divisores, entonces [la operación] se implementará en sus factores primos de esta manera: $N = p^l q^m r^v s^e$ y el resultado es $\int N = \int p^l \int q^m \int p^v \int s^e$.

Aquí tenemos que la función suma de divisores es multiplicativa, y aunque no está una demostración formal, podríamos decir que el proceso expuesto entre los parágrafos 82 y 89 nos llevaría a una inducción, pero no podemos esperar que la encontremos como actualmente la entendemos, tenemos que considerar que en esta época de la creación del *Tractatus*, lo que hoy conocemos como demostración por inducción apenas estaba en sus primeras etapas de gestación, y Euler fue el principal artífice de esta manera de demostrar y que hoy es tan común.

V) En los parágrafos 92 al 95 muestra una breve reflexión de que la función $\int N$ pueda ser par, impar y primo, dice que la potencia de un primo par puede tener la $\int$ prima, por ejemplo $\int 2^2 = 7, \int 3^2 = 13, \int 5^2 = 31, \int 4^2 = 31$. Para el caso de la potencia impar se tendrá que $\int$ es un compuesto, por ejemplo en el 95 escribe:

> Si $N = p^5$, y como $\int p^5 = 1 + p + pp + p^3 + p^4 + p^5$ es la suma de sus divisores entonces $\int p^5 = (1+p+pp)(1+p^3) = (1+p)(1+p+pp)(1-p+pp)$, y por lo tanto este número compuesto tiene en sus factores las sumas [de los divisores] de valores inferiores, de tal manera que sea $\int p^5 = (1-p+pp) \int p \cdot \int p^2$.

En este mismo contexto no profundiza más pero sería un estudio muy interesante conocer más sobre el contradominio de la función $\int$, y en particular cuando son primos, porque seguramente los respectivos enteros del domino guardarán características interesantes.

VI) El parágrafo 100 da una lista de $\int$ entre 1 y 60 y menciona que varios tienen el mismo valor, y en el parágrafo 103 parece que quiere ver cuales enteros N, junto con $\int N$ están en una misma proporción dada, es decir, la pregunta es: dada la proporción $\frac{m}{n}$, ¿para cuales valores de N se tiene que $\frac{N}{\int N} = \frac{m}{n}$? En particular parece que se dirige a la construcción de los perfectos, por lo tanto requerirá encontrar los N que cumplan con la razón dada $\frac{N}{\int N} = \frac{1}{2}$, que lo lleva a que $\int N = 2N$, que es la definición de perfecto.

Prácticamente aquí se termina lo que corresponde a la función

suma de divisores, nuestra actual función $\sigma(n)$, pero ya mencionamos que como consideramos que su objetivo es el tema de los residuos y por otro lado el *Tractatus* no pretende adentrarse en todos lo temas de la teoría de números, entonces parece que para Euler con esta exposición era suficiente. Pero no podemos pasar por alto que si hacemos una comparación con los texto actuales podemos notar que tampoco es tan insuficiente lo que Euler expone en el *Tractatus* sobre $\sigma(n)$, prácticamente proporciona lo fundamental para que los interesados ahonden más por su cuenta, porque otras de las aplicaciones, además de los perfectos será en teoría de particiones y funciones generadoras, pero esto tampoco es tan común en los textos actuales.

2.6. Particiones, funciones generadoras y $\sigma(n)$

Para terminar con $\sigma(n)$ expondremos algunos resultados de Euler, publicados en diversos años, porque consideramos que son muy importantes en la teoría de los números y aunque están al margen del *Tractatus*, Euler fue el creador y pensamos que tienen que ser mencionados en este trabajo para que no se quede una idea de que Euler tuvo aportaciones limitadas en el campo de $\sigma(n)$.

2.6.1. Función generadora de $\sigma(n)$

Definición. Dada una sucesión de enteros $a_0, a_1, a_2, \ldots$, a la función polinomial

$$G(x) = a_o + a_1 x + a_2 x^2 + \ldots$$

la llamaremos función generadora de la sucesión. Pero se puede tener el caso de una sucesión generada para una función $f(x)$ con dominio en los enteros no negativos, entonces la función generadora para $f(x)$ está dada por $G(x) = \sum_{n=0}^{\infty} f(n)x^n$.

Estas funciones las presenta Euler en varios trabajos, entre ellos podemos mencionar el *Introductio in analysin infinitorum* publicado en 1748. Podríamos extender el estudio de estas funciones pero sólo nos restringiremos a la que desarrolló para el caso de $\sigma(n)$.

En el artículo *Demonstratio theorematis circa ordinem in summis divisorum observatum*, escrito en 1754, pero publicado hasta 1760, desarrolla una función generadora para $\sigma(n)$, es de la siguiente forma

$$G(x) = \sum_{n=1}^{\infty} \sigma(n)x^n = \sum_{n=1}^{\infty} \frac{nx^n}{1-x^n}$$

En el artículo plantea que se tome la serie

$$Z = x\sigma(1) + x^2\sigma(2) + x^3\sigma(3) + x^4\sigma(4) + x^5\sigma(5) + \dots$$

que relaciona directamente a los exponentes con los valores de σ. Ahora dice que si se desarrollan las funciones $\sigma(n)$ de acuerdo a los sumandos que forman cada una y después se reagrupan los términos, se obtiene

$Z = 1(x + x^2 + x^3 + x^4 + x^5 + \dots) + 2(x^2 + x^4 + x^6 + x^8 + x^{10} + \dots) + 3(x^3 + x^6 + x^9 + x^{12} + x^{15} + \dots) + 4(x^4 + x^8 + x^{12} + x^{16} + x^{20} + \dots) + 5(x^5 + x^{10} + x^{15} + x^{20} + x^{25} + \dots) + 6(x^6 + x^{12} + x^{18} + x^{24} + x^{30} + \dots) + \dots$

Lo que se tiene es un conjunto de series geométricas y al sumar cada una se tiene lo siguiente

$$Z = \frac{1x^1}{1-x^1} + \frac{2x^2}{1-x^2} + \frac{3x^3}{1-x^3} + \frac{4x^4}{1-x^4} + \frac{5x^5}{1-x^5} + \frac{6x^6}{1-x^6} + \dots$$

Por lo tanto podemos ver que de

$$Z = \sum_{n=1}^{\infty} \sigma(n)x^n = \sum_{n=1}^{\infty} \frac{nx^n}{1-x^n}$$

se obtiene una función generadora para $\sigma(n)$. Sabemos que es común en Euler que queden partes que se tienen que justificar matemáticamente, y esta construcción no es la excepción, pero en esta parte del trabajo nuestro fin es mostrar algunas de sus aportaciones a las función $\sigma(n)$.

Otro gran resultado que no puede faltar en los estudios actuales sobre teoría de particiones, y que está en el mismo artículo de Euler, es el que sigue:

Si n es un entero positivo[12],

$$\sigma(n) = \sigma(n-1)+\sigma(n-2)+\sigma(n-5)+\sigma(n-7)+\sigma(n-12)+\sigma(n-15)+$$

$$\sigma(n-22)+\cdots+(-1)^{k+1}\left[\sigma\left(n-\frac{3k^2-k}{2}\right)+\sigma\left(n-\frac{3k^2+k}{2}\right)\right].$$

Lo que nos está presentando Euler es una relación para encontrar $\sigma(n)$ pero a través de las diferencias de n con los números de la forma $\frac{3k^2\pm k}{2}$, donde los que tienen el signo negativo $\frac{3k^2-k}{2}$ son los números pentagonales.

Antes de presentar la demostración de Euler necesitamos enunciar un teorema de teoría de particiones que no demostraremos aquí, este se enuncia así:

Teorema de los Números Pentagonales.

Para todo entero positivo n

$$\prod_{n=1}^{\infty}(1-x^n) = 1-x-x^2+x^5+x^7-x^{12}-x^{15}+x^{22}+\cdots =$$

$$1+\sum_{n=1}^{\infty}(-1)^n x^{\frac{n(3n+1)}{2}}+\sum_{n=1}^{\infty}(-1)^n x^{\frac{n(3n-1)}{2}} =$$

$$1+\sum_{n=1}^{\infty}[p_e(n)-p_0(n)]x^n$$

donde $p_e(n)$ es el número de particiones de n, con una cantidad par de sumandos cada una; $p_0(n)$ es el número de particiones de n, con una cantidad impar de sumandos cada una. Además, se tiene que considerar que en ambos grupos de particiones los sumandos son diferentes en cada una.

Este teorema de Euler es de una gran trascendencia para conocer más de la composición aditiva de los enteros que en términos menos teóricos nos enuncia que la diferencia de las cantidades del número de particiones de n con una cantidad par de sumandos,

[12]En la siguiente igualdad considérese $\sigma(k) = 0$ si $k < 0$ y $\sigma(0) = k$.

menos la cantidad de particiones de n, con una cantidad impar de sumandos, es igual a $1, -1$ ó 0, que son precisamente los coeficientes de

$$\prod_{n=1}^{\infty}(1-x^n) = 1 - x - x^2 + x^5 + x^7 - x^{12} - x^{15} + x^{22} + \cdots$$

Lo más sobresaliente es que los términos de la serie que tienen coeficiente ± 1, es decir, los diferentes de cero son los de la forma $\frac{3k^2 \pm k}{2}$ y entre ellos los de signo negativo son nuevamente los números pentagonales.

Este teorema lo desarrolló Euler en los artículos *Evolutio producti infiniti* $(1-x)(1-x^2)(1-x^3)(1-x^4)(1-x^5)\cdots$ *etc. in seriem simplicem* y *De mirabilibus proprietatibus numerorum pentagonalium*, ambos escritos en 1775.[13]

Ahora regresamos a la demostración de la igualdad

$$\sigma(n) = \sigma(n-1)+\sigma(n-2)+\sigma(n-5)+\sigma(n-7)+\sigma(n-12)+\sigma(n-15)+$$

$$\sigma(n-22) + \cdots + (-1)^{k+1}\left[\sigma\left(n - \frac{3k^2-k}{2}\right) + \sigma\left(n - \frac{3k^2+k}{2}\right)\right].$$

Demostración:

De la función generadora Z de $\sigma(n)$ que es: $Z = \sum_{n=1}^{\infty}\sigma(n)x^n = \sum_{n=1}^{\infty}\frac{nx^n}{1-x^n}$, dividimos ambos lados entre x e integramos para obtener

$$\int \frac{Z dx}{x} = \int \sum_{n=1}^{\infty} \frac{nx^{n-1}}{1-x^n} dx = -\sum_{n=1}^{\infty} \log(1-x^n) =$$

$$-\log\left(\prod_{n=1}^{\infty}(1-x^n)\right),$$

[13] La clasificación Eneström es E541 y E542, respectivamente. Ver bibliografía de la tesis.

y por el teorema de los números pentagonales aplicado en la igualdad de la derecha

$$\int \frac{Zdx}{x} = -\log(1 - x - x^2 + x^5 + x^7 - x^{12} - x^{15} + \dots)$$

derivando ambos lados de la igualdad

$$\frac{Z}{x} = \frac{-1 - 2x + 5x^4 + 7x^6 + 12x^{11} + 15x^{14} - \dots}{1 - x - x^2 + x^5 + x^7 - x^{12} - x^{15} + \dots}$$

entonces

$$Z = \frac{-x - 2x^2 + 5x^5 + 7x^7 + 12x^{12} + 15x^{15} - \dots}{1 - x - x^2 + x^5 + x^7 - x^{12} - x^{15} + \dots}.$$

Al inicio Euler propuso que $Z = x\sigma(1)+x^2\sigma(2)+x^3\sigma(3)+x^4\sigma(4)+x^5\sigma(5)+\dots$, entonces multiplicando la última igualdad con el denominador de la anterior e igualando con $-x - 2x^2 + 5x^5 + 7x^7 + 12x^{12} + 15x^{15}$ se llega a una igualdad entre polinomios cuyos coeficientes son iguales para cada x^n, por lo tanto cada coeficiente cumple con

$$\sigma(n) = \sigma(n-1) + \sigma(n-2) + \sigma(n-5) + \sigma(n-7)+$$

$$\sigma(n-12) + \sigma(n-15) + \sigma(n-22) + \cdots +$$

$$(-1)^{k+1}\left[\sigma\left(n - \frac{3k^2-k}{2}\right) + \sigma\left(n - \frac{3k^2+k}{2}\right)\right]$$

que es lo que Euler quería demostrar.□

Aquí terminamos una muestra de las aportaciones de Euler con respecto a $\sigma(n)$, y podemos constatar que la lectura del *Tractatus* si bien no se adentra en el estudio de $\sigma(n)$, sí proporciona lo necesario para llegar a una lectura de los otros trabajos mencionados arriba, donde expone los resultados más especializados. Con esto terminamos el análisis de las funciones aritméticas $\tau(n)$ y $\sigma(n)$, y para terminar esta parte de las funciones aritméticas en el *Tractatus* damos lugar a la función $\phi(n)$.

2.7. Función aritmética $\phi(n)$

El capítulo IV está dedicado en su mayoría al estudio de los números que son primos relativos positivos y menores a un número dado, nos referiremos a la cardinalidad de este conjunto como la función $\phi(n)$, pero tenemos que mencionar que Euler no la definió así, el que la usa por primera vez de esa manera es Gauss en sus *Disquisitiones Arithmeticae*[14].

La exposición de Euler sobre $\phi(n)$ sí es nueva, no podemos mencionar antecedentes como fue en el caso de las otras funciones aritméticas expuestas antes, y tampoco mencionaremos otros de sus trabajos donde se aplica, porque su uso es tan extenso, incluso dentro del mismo *Tractatus*, que preferimos ahora limitarnos a lo que él expuso en el capítulo IV. El capítulo tiene el título «Sobre los números que son primos y compuestos entre sí» y desde el primer parágrafo (que es el 111) desarrolla los conceptos necesarios para adentrarse en el estudio de los números que son primos entre sí, así como compuestos entre sí. Entre los parágrafos 117 al 124 desarrolla las formas para obtener la cardinalidad de los conjuntos de primos relativos con un primo p; con un múltiplo de p; con el producto de dos primos diferentes pq; con las potencias de un primo como p^2, p^3, p^n; el producto de la potencia de un primo por otro primo diferente como p^2q.

En todos los casos la metodología es la de extraer de la cantidad total aquellos que son números compuestos para que sólo queden los primos con el número. Por ejemplo en el parágrafo 120 enuncia

> [...] si $a = 5p$, los números que poseen un divisor común con a, primero, son todos los divisibles por 5, que son una cantidad igual a p; además son los divisibles por p, es decir, $p, 2p, 3p, 4p$,y el mismo número $5p$, ya antes señalado. La cantidad de números compuestos con respecto a a es $p + 4$, y la cantidad de los números primos con a es $= 4p - 4 = 4(p - 1)$, es decir, aquellos que no son mayores al mismo a.

Se puede percibir que al número $a = 5p$ le restará los múltiplos

[14] Ver [Gauss, 1801].

de 5 y de p y por esa razón llega a que $\phi(5p) = 4(p-1)$. Para el caso general del producto de dos primos se tiene lo siguiente del parágrafo 121

> [...] sea $a = pq$ donde ambos factores p y q son primos, desde la unidad hasta a se dan p números primos divisibles por q, es decir, $q, 2q, 3q, \ldots pq$, después, hay q números que son divisibles por p, es decir, $p, 2p, 3p, \ldots, qp$, cuyo último número qp ya fue contado. Por lo tanto, la cantidad de los números que no superan a a, y que son compuestos con respecto a a, son $p+q-1$, y los restantes, cuya cantidad es $= qp - p - q + 1 = (p-1)(q-1)$, serán primos con a.

y podemos ver que está planteando en el caso anterior, que se tiene que quitar a pq los múltiplo de p y de q, pero, es muy importante regresarle una vez el producto pq, porque de lo contrario se lo estaría quitando dos veces. Por lo tanto llega a que $\phi(pq) = (p-1)(q-1)$.

Con el mismo proceso para el caso $a = p^2q$ llega en el parágrafo 125 a que $\phi(p^2q) = p(p-1)(q-1)$. En los tres casos últimos Euler ya está preparando el camino para enunciar que si a y b son primos entre sí entonces $\phi(ab) = \phi(a)\phi(b)$, veamos los tres casos anteriores: el primero, $\phi(5p) = 4(p-1)$ pero es igual a decir que $\phi(5p) = \phi(5)\phi(p)$; en el segundo $\phi(pq) = (p-1)(q-1)$, que es igual a $\phi(pq) = \phi(p)\phi(q)$; el tercero $\phi(p^2q) = p(p-1)(q-1) = \phi(p^2)\phi(q)$.

En el parágrafo 127 nos presenta una lista de once productos cuyos factores son primos y potencias de primos, y en cada caso se percibe de manera general que

$$\phi(p^a q^b r^c s^d) = \phi(p^a)\phi(q^b)\phi(r^c)\phi(s^d).$$

Es importante notar que en todos los casos se construye aumentando un factor al número al que ya se le había calculado la función ϕ, y aún así se cumple la igualdad anterior. De esta manera Euler ya dejaba el camino trazado para demostrar de manera general que

$$\phi(p_1^{\alpha_1} p_2^{\alpha_2} p_3^{\alpha_3} \ldots p_k^{\alpha_k}) = \phi(p_1^{\alpha_1})\phi(p_2^{\alpha_2})\phi(p_3^{\alpha_3}) \ldots \phi(p_k^{\alpha_k}),$$

y aquí es donde se expone la parte más sobresaliente del capítulo IV que es una demostración por inducción de esta igualdad. Sabemos que demostrar por inducción aún era una técnica en gestación a mediados del siglo XVIII, de hecho Euler fue de los que desarrolló esta forma de darle sustento a ciertos resultados matemáticos, entonces, bajo una lectura actual no esperemos encontrar un proceso de inducción impecable, como sí lo exigiríamos actualmente.
Demostración por inducción:

La inducción se hace aumentando factores primos para que así crezca un entero. Entonces, por los parágrafos 117 a 127 ya sabemos que para un primo p se cumple que $\phi(p) = p - 1$, y como ya se dijo antes se cumplirá para más factores primos. Ahora, con el parágrafo 128 podemos dar lugar al segundo paso de inducción, esto sobre el hecho de que supondremos que se sabe cómo es ϕ para algún M entero positivo –ya no tiene que ser un primo o potencia de él–, entonces asumamos que $\phi(M) = \mu$, y veremos que se cumple para un primo más que multiplica a M. Esto es, para $M = p_1^{\alpha_1} p_2^{\alpha_2} p_3^{\alpha_3} \cdots p_s^{\alpha_s}$ se tiene que[15]

$$\phi(M) = p_1^{\alpha_1 - 1}(p_1 - 1)p_2^{\alpha_2 - 1}(p_2 - 1)\ldots p_k^{\alpha_k - 1}(p_k - 1) = \mu.$$

Ahora se considera el número $a = Mp$, con p primo que no es factor de M. Ya sabemos que desde 1 hasta M se tiene que $\phi(M) = \mu$, o como lo menciona Euler, la cantidad de compuestos es $(M - \mu)$, por lo tanto los compuestos desde 1 hasta Mp son $p(M-\mu)$, pero estos son respecto a M, porque falta considerar a los múltiplos de p que son: $p, 2p, 3p, \ldots, Mp$. Pero de estos múltiplos de p se tienen que quitar los que ya son compuestos con M, (porque de no hacerlo los estaríamos quitando dos veces), y esto se hace a través de ver que en los factores de p que son de 1 a M hay $(M - \mu)$ compuestos con M, por lo tanto $(M - (M - \mu)) = \mu$ son los múltiplos de p y que no tienen factores comunes con M. Entonces, el total de compuestos que se le tienen que quitar a Mp

[15] Actualmente reconocemos esta igualdad como
$\phi(M) = \left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_k}\right) = \phi(p_1^{\alpha_1})\phi(p_2^{\alpha_2})\ldots\phi(p_k^{\alpha_k})$.

son: $Mp - p(M - \mu) - \mu = \mu(p - 1)$, que es el total de primos con Mp, así se llega a que

$$\phi(Mp) = \phi(M)\phi(p).$$

Si se considera que

$$\phi(M) = p_1^{\alpha_1 - 1}(p_1 - 1)p_2^{\alpha_2 - 1}(p_2 - 1)\dots p_k^{\alpha_k - 1}(p_k - 1) = \mu,$$

entonces

$$\phi(p_1^{\alpha_1}p_2^{\alpha_2}p_3^{\alpha_3}\dots p_s^{\alpha_s}p) = \phi(p_1^{\alpha_1})\phi(p_2^{\alpha_2})\phi(p_3^{\alpha_3})\dots\phi(p_s^{\alpha_s})\phi(p).$$

Aquí podríamos terminar y decir que el proceso se puede extender aumentando factores primos para crear un nuevo número, y repetimos el proceso considerando que conocemos ϕ para el caso anterior. Pero Euler extendió más el análisis de los casos, y en los parágrafos 130 y 131 consideró la posibilidad de que se multiplicara el número ya conocido M por un factor p^n, y ahora lo que quiere conocer el la cantidad de números menores y primos con Mp^n, es decir, $\phi(Mp^n)$. El procedimiento es semejante al anterior, ya se tiene que los compuestos desde 1 hasta M son $(M - \mu)$ y de 1 hasta Mp^n son $p^n(M - \mu)$. Por otro lado los compuestos respecto a p son

$$p, 2p, 3p, \dots, (Mp^{n-1})p,$$

pero de estos debemos de quitar a los que son compuestos con M, y esto depende nuevamente de los coeficientes de p (para no tener que quitarlos dos veces), por lo tanto la cantidad que se le quita es $p^{n-1}(M - \mu)$, entonces $Mp^{n-1} - p^{n-1}(M - \mu) = Mp^{n-1} - p^{n-1}M - p^{n-1}\mu = p^{n-1}\mu$ y esta es la cantidad de compuestos múltiplos de p que ahora sí se quitan a los enteros entre 1 y Mp^n. Entonces, quitando los compuesto quedan los primos con Mp^n que son:

$$Mp^n - p^n(M - \mu) - p^{n-1}\mu = \mu p^{n-1}(p - 1) = \mu(p^n - p^{n-1})$$

y la última igualdad es la cantidad de primos con Mp^n, entonces se obtiene

$$\phi(Mp^n) = \phi(M)\phi(p^n). \ \square$$

Con esto se puede ver un proceso de inducción que está dentro de los niveles de exigencia de la matemática actual. Lo que Euler demostró entre los parágrafos 117 a 131 lo podemos identificar con una redacción actual de la siguiente manera:

Teorema
Si $n = \prod_{i=1}^{k} p_i^{\alpha_i}$ es un entero positivo representado como producto de potencias de primos, entonces

$$\phi(n) = \prod_{i=1}^{k} (p_i^{\alpha_i} - p_i^{\alpha_i - 1}) = n \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right).$$

Euler tenía claro que una cosa era construir $\phi(n)$ para cualquier n y otra era aclarar que $\phi(mn) = \phi(m)\phi(n)$ para cualesquiera m y n primos entre si, y precisamente en los parágrafos 132 y 133 escribe lo siguiente:

> 132. Como la cantidad de números que son primos con p^n y menores que éste es $p^{n-1}(p-1)$, entonces a partir de la proposición precedente podemos concluir con absoluto rigor que: si el número propuesto es $= p^{\lambda} q^{\mu} r^{\nu} s^{\xi}$ etc., entonces, la cantidad de los números primos y menores a éste será: $p^{\lambda-1}(p-1)q^{\mu-1}(q-1)r^{\nu-1}(r-1)s^{\xi-1}(s-1)$
>
> 133. Así pues, si los números M y N fueran primos entre sí, y si la cantidad de números entre 1 y M, que son primos con M, es m; y si la cantidad de los números entre 1 y N, y que son primos con N es n, entonces la cantidad de números primos con el producto MN, y no mayores a éste, será $= mn$.

Con esto finalmente muestra la claridad de sus ideas en cuanto que ϕ es una función multiplicativa y terminamos el análisis de las funciones aritméticas que Euler plantea en los capítulos III y IV del *Tractatus*.

Capítulo 3

Residuos de potencias, clases y función $\phi(n)$

En las secciones I a IV del *Tractatus* mostramos que ahí se encuentra la teoría necesaria para iniciarse en el estudio de los números enteros, así como en aportaciones importantes de Euler dentro del campo de los números perfectos, los primos, la función $\sigma(n)$, particiones y funciones generadoras y la función aritmética $\phi(n)$. Parte del trabajo ahí presentado atiende a las interrogantes que se le plantearon en su primera llegada a San Petersburgo, y sin duda resolvió problemas que estaban pendientes desde la aritmética de Euclides, Fermat, Leibniz, Descartes, Mersenne, y mostró la existencia de una nueva ruta para el estudio de otras propiedades de los enteros, nos referimos al tema de las funciones generadoras y particiones. Pero sí se tiene que decir que todos esto temas no daban lugar a la creación de lo que ahora llamaríamos una plataforma innovadora para la creación de una teoría que diera lugar a desarrollar una herramienta totalmente nueva con la que se pudiera construir una rama diferente de la teoría de los números.[1]

[1]Es importante recordar que no debemos esperar que todos los resultados sean innovadores en el *Tractatus*, ya que esta obra estaba pensada para ser una clase de compendio para aquellos interesados en los temas de la aritmética avanzada. Esta obra permitiría consultar lo temas más sobresalientes de la

Con lo mencionado en el párrafo anterior no pretendemos minimizar el trabajo de Euler en esos capítulos, nuestro interés fue preparar la entrada para decir que en este Capítulo III de la tesis, en el que abordamos los Capítulos V al IX del *Tractatus*, expondremos lo que conocemos como la teoría de los residuos, y esta sí fue una plataforma innovadora que sirvió de base a Legendre, Lagrange y Gauss, por mencionar algunos, para crear resultados importantes en la matemática.

Gauss en su obra *Disquisitiones Arithmeticae* publicada en 1801, en el prefacio escribe lo siguiente para justificar porque su libro inicia en determinado tema:

> Para que nadie se sorprenda porque comienzo así desde el principio [...][2] , debo explicar que cuando primero me encaminé a este tipo de investigaciones, a principios de 1795, no estaba al tanto de los modernos descubrimientos en el campo y no tenía los medios para descubrirlos. En efecto, ocupado en otro trabajo, me encontré con un extraordinario resultado aritmético (artículo 108) [...]; puesto que lo consideré bellísimo en sí mismo y en vista de que sospeché su conexión con resultados aún más profundos, concentré en él todos mis esfuerzos, con el fin de entender los principios de los que dependía y para obtener una prueba rigurosa. Cuando tuve éxito en esto, me atrajeron tanto estos asuntos que no pude dejarlos.

El problema al que se refiere que lo publicó en el artículo 108 de las *Disquisitiones* enuncia lo que sigue:

> Teorema. -1 es un residuo cuadrático de todos los números primos de la forma $4n + 1$, pero es un no residuo de todos los números primos de la forma $4n + 3$.

La interpretación es que si existe una x tal que si al dividir x^2 entre un primo p el residuo es -1, entonces p siempre será de la

aritmética y el lector posteriormente se podría remitir a los artículos del mismo Euler que profundizaban más en cada tema y encontrar todas su aportaciones.

[2]Cuando se refiere a «desde el principio» lo hace para indicar que el primer tema del capítulo I es el de congruencias, pero abordadas desde una visión de los residuos.

forma $4n+1$. Si -1 no es el residuo entonces pasa que el primo p es de la forma $4n+3$.

Lo que queremos que resalte es que para Gauss el tema de los residuos de números cuadráticos obtenidos de la división de un primo le pareció sorprendente, y fue el estudio de los residuos con lo que precisamente inició su estudio de los enteros en las *Disquisitiones*. Gauss deja al lector el estudio de la teoría antigua correspondiente a enteros, él considera que la teoría de los números debe de iniciar con el estudio de las clases residuales, ya que esto es lo nuevo y una base fundamental para los temas de aritmética avanzada.

Deseamos que este preámbulo gaussiano de los residuos sirva de entrada a nuestra exposición de los capítulos V al IX del *Tractatus* porque ahí es donde Euler inicia con sus resultados sobre residuos, y esta teoría nueva en el siglo XVIII sí construiría las bases para grandes resultados matemáticos que posteriormente se conocerían.

3.1. Residuos y progresiones

El los capítulos V y VI Euler expone el tema de los residuos pensando en un lector sin antecedentes en el tema. En los parágrafos 140 y 141 enuncia lo que sigue:

> 140. Si el número a no es múltiplo del número b, sucede que la división de éste $[a]$ por aquél $[b]$ no se puede realizar. Al sobrante que se genera al dividir el número a sobre un múltiplo de b se llama residuo nacido de una división. Así, si $a = mb+r$, r será el residuo originado a partir de la división del número a entre b.
>
> 141. De aquí es evidente que el residuo r siempre es menor que el número b, que es el divisor; si pasa que fueran iguales $r = b$, entonces una vez aumentado el índice del múltiplo m con la unidad, éste sería el verdadero múltiplo del mismo b, es decir, $a = (m+1)b$; y si fuera $r > b$, entonces se hace crecer el índice m, y así se reduciría r hasta que sea menor que b.[3]

[3]Es decir, si $r > b$ entonces $r = bt+\alpha$, con esto $a = mb$ y $r = mb+bt+\alpha =$

Lo que se plantea es que si se tienen dos enteros a y b, donde $a > b$, entonces al dividir a entre b se tiene un residuo mínimo r, es decir, si a a se le extrae r entonces el resultado es un múltiplo de b, es decir, $(a - r) = mb$.[4] Pero también se puede ver, como en el parágrafo 140, que $a = mb + r$.

Euler nos hace ver que el residuo r tiene que ser uno de los enteros del conjunto $\{0, 1, 2, 3, \ldots, (b-1)\}$, y en el parágrafo 143 plantea una clasificación de los enteros según el divisor que se elija, si éste es b entonces nos dice que «para cualquier divisor b, todos los números pueden distribuirse en tantas clases, cuantas unidades contiene b» , es decir, como el divisor es b, y el posible residuo puede ser uno de los enteros contenido en $\{0, 1, 2, 3, \ldots, (b-1)\}$ entonces todo entero adquiere una de las formas $bk, bk + 1, bk + 2, \ldots, bk + (b - 1)$. Esas son las clases que mencionó Euler en el parágrafo 143, y que actualmente identificamos como clases residuales o de equivalencia.

Esta clasificación que llamó clases fue un paso importante para el estudio de los enteros, de esto se desprendieron múltiples conceptos y resultados, que de no existir no podríamos entender lo que actualmente es el álgebra moderna.

En todo el capítulo V se exponen las bases fundamentales de esta teoría de residuos y clases. Euler lleva al lector como en un paseo recorriendo las clases y escudriñando qué puede contener cada una de ellas y como la cantidad de clases depende del divisor[5] entonces la cantidad de ellas puede varias de maneras infinitas. Así Euler nos dice en el parágrafo 148 que

> En consecuencia, cualquier número que esté en lugar de cualquier divisor se puede identificar con determinada clase, o está expresado por una de estas formas, lo cual puede

$(m + 1)b + \alpha$, con $\alpha < b$.

[4] A partir de Gauss esto es lo que conocemos como la relación de congruencia, esto es, que como m divide a $(a - r)$ entonces se dice que a es congruente con r módulo m, se denota como $a \equiv r \pmod{b}$.

[5] Evitaremos, en la medida de lo posible, la tentación de usar el término módulo que es lo que directamente nos sugiere el contenido, y lo hacemos para tratar de hacer una lectura lo más apegada posible al contexto del *Tractatus*.

> suceder de maneras infinitas, puesto que el número de los divisores puede crecer infinitamente.

Lo que enuncia es que un entero puede pertenecer a diferentes clases según el divisor que se esté usando, y como podemos elegir una cantidad infinita de divisores, entonces se infiere que un entero puede pertenecer a una infinidad de clases.

Con Euler el uso de los enteros negativos ya no daba lugar a complicaciones, incluso ya forman parte de las nuevas clasificaciones, y nos referimos a que ya contempla a los negativos como parte de los residuos. Además, como ya se exhibió el uso de un representante por cada clase, entonces le da lugar al uso de lo que actualmente conocemos como un sistema completo de residuos, y dentro de ellos ya contemplaba el uso de negativo, por ejemplo para el divisor 9 se tiene el conjunto de residuos $\{0, 1, 2, 3, 4, 5, 6, 7, 8\}$ que corresponden a la clasificación de los enteros que serían de alguna de las formas:

$$9k, 9k+1, 9k+2, 9k+3, 9k+4, 9k+5, 9k+6, 9k+7, 9k+8,$$

pero Euler nos plantea que la clasificación también podría ser de la forma

$$9k-4, 9k-3, 9k-2, 9k-1, 9k, 9k+1, 9k+2, 9k+3, 9k+4,$$

o de esta otra:

$$9k+5, 9k+6, 9k+7, 9k+8, 9k+9, 9k+10, 9k+11, 9k+12.$$

Lo que se nos indica es que la clasificación de los enteros bajo el divisor 9 puede ser de una de las tres formas listadas, las tres son equivalentes, pero más aún, se pueden tener una infinidad de clasificaciones donde los residuos no tengan que estar expuestos necesariamente en un orden consecutivo.

De lo anterior entonces se puede extraer a los residuos que representan a las clases, y los sistemas completos de residuos son: $\{0, 1, 2, 3, 4, 5, 6, 7, 8\}, \{-4, -3, -2, -1, 0, 1, 2, 3, 4\}$,

$\{5, 6, 7, 8, 9, 10, 11, 12\}$, respectivamente. Pero también podría ser el conjunto $\{18, 46, -25, 12, -4, 33, 7, -10\}$, el cual ya no está representado en los listados anteriores. De lo anterior se puede percibir que la idea es tomar a un elemento de cada clase y con ellos se forma el sistema de residuos, y aquí ya quedó explícito que se pueden tomar residuos positivos y negativos, y además es posible formar una infinidad de sistemas de residuos, o clases de equivalencia.

El uso de los sistemas de residuos sí fue una estructura matemática que dio lugar a plantear resultados de gran trascendencia en el álgebra, y estos conjuntos no fueron planteados antes que Euler. Más adelante se podrá ver su uso dentro de algunas demostraciones.

A partir del parágrafo 157 y hasta el final del capítulo que es el 166 se exponen propiedades aritméticas de los residuos, lo que actualmente abordamos con las propiedades de congruencias. Enseguida enunciamos algunas de las propiedades ahí contenidas:

> 157. Si el número A al ser dividido por d, origina un residuo α, entonces también los números $A+d$, $A+2d$, $A+3d$, etc., dejarán el mismo residuo α al ser dividido por d. Pero el número $A + 1$, al ser dividido por el mismo número d, dará el residuo $\alpha + 1$, y en general el número $A + n$ tendrá un residuo $\alpha + n$, y si éste excede al divisor d, entonces se extrae éste cuantas veces sea posible hasta reducirlo a la forma mínima.
>
> 159. Tomado el divisor d, si el residuo α corresponde al número A; el residuo β, en cambio, con el número B; la suma de los números $A + B$ tendrá asociado un residuo $\alpha + \beta$; el cual es equivalente con $\alpha + \beta - d$, si acaso fuera $\alpha + \beta > d$.[6]
>
> 161. Si el número A es dividido por d y origina un residuo α, entonces el doble $2A$ dará lugar al residuo 2α, o al residuo $2\alpha - d$; en cambio el triple $3A$ dará el residuo 3α, cuya mínima expresión será $3\alpha - d$, o $3\alpha - 2d$, si éste es mayor

[6]Desde el lenguaje de las congruencias podemos ver que si $A \equiv \alpha \pmod{d}$, $B \equiv \beta \pmod{d}$, entonces $A + B \equiv \alpha + \beta \pmod{d}$. Si $\alpha + \beta > d$, entonces $\alpha + \beta = d + r$, entonces $\alpha + \beta - d = r$. Por lo tanto $\alpha + \beta \equiv \alpha + \beta - d \pmod{d}$, entonces $\alpha + \beta$ es equivalente con $(\alpha + \beta - d)$.

que d. Así, en general, el residuo de cualquier múltiplo nA será $n\alpha$, o $n\alpha - md$.

162. Sea d el divisor de A y α el residuo correspondiente; si se divide a B y arroja residuo β, el residuo $\alpha\beta$ corresponde al producto AB, pero si el residuo $\alpha\beta$ es mayor que el divisor d, este se puede recalcular a $\alpha\beta - d$, o $\alpha\beta - md$.

A partir del producto se puede pasar a los residuos de potencias en el 164:

164. A partir de esto entendemos que, si el número A dividido entre d deja un residuo α, entonces el residuo $\alpha\alpha$ corresponde a su cuadrado A^2; el residuo α^3 corresponde a su cubo A^3 y al número A^n le corresponde el residuo a^n, el cual, al ser dividido entre d se puede reducir a su forma mínima.

Con estos resultados termina el capítulo V y ellos nos permiten visualizar que el *Tractatus* tenía el propósito de acercarse a un lector aún inexperto en esta disciplina, y esto se percibe en que la mayoría de lo que se expuso en este capítulo es lo más elemental de la teoría de residuos, ya que lo expuesto en los capítulos VI y VII que tiene que ver con residuos de progresiones y potencias sí se puede encontrar en sus artículos como E271, E134 y E262, cuyos títulos son *Theoremata arithmetica nova methodo demonstrata; Theoremata circa divisores numerorum; Theoremata circa residua ex divisione potestatum relicta* respectivamente.

Por los teoremas que se presentan en estos artículos se supone que el lector ya tiene los conocimientos básico de la teoría de residuos, por ejemplo el E262 inicia directamente con el teorema:

Si p es un número primo y a es primo con p, entonces ningún término de la progresión geométrica $1, a, a^2, a^3, a^4, a^5, a^6$, etc. es divisible por el número p.

y en el caso de E134:

Si p es un primo, entonces todo número de la forma $(a+b)^p - a^p - b^p$ es divisible por p.

En ambos artículos es necesario tener los conocimientos previos sobre residuos, pero en el *Tractatus* sí los expone previamente antes de llegar a los mismos resultados señalados en los artículos. Y es importante adentrarse en la comprensión de los sistemas de residuos y sus respectivas clases de equivalencia, tópicos que también omite en los artículos, pero que consideramos que son importantes para tener una base teórica más firme. Se tiene que señalar que en el caso de los tres artículos mencionados se exponen la mayoría de las demostraciones de los teoremas que enuncia, y se presentan con buena precisión, por otro lado, en el *Tractatus* se presentan los resultados de una manera más didáctica, de tal manera que parte de lo más elemental para construir toda la teoría, y en conjunto todo queda muy autocontenido, pero la cantidad de los resultados que demuestra son pocos en comparación con los que enuncia, es decir, Euler nos presenta hasta el capítulo V del *Tractatus* un tipo de compendio donde cubrirá la mayoría de los resultados sobre divisibilidad y residuos, trabajo que no presentó en los artículos con toda su amplitud, pero lo que sí presentó en ellos lo hace con mayor profundidad en las demostraciones. Lo que podemos concluir hasta el capítulo V es que el *Tractatus* y los artículos son complementarios, el primero nos presenta una visión más panorámica de los temas y los otros complementan las partes formales.

3.2. Progresiones Aritméticas del Capítulo VI

Con base en lo presentado en el capítulo V ya entra directamente al estudio del conjunto de residuos que se obtienen de una progresión aritmética, en el parágrafo 168 enuncia lo que sigue:

> Se propone ahora cualquier progresión aritmética
>
> $$a, a+b, a+2b, a+3b, a+4b, a+5b, \text{etc.},$$
>
> donde cada término se divide entre el divisor d. Del primero se origina el residuo a, el cual no se repite antes de que se llegue al término $a+nb$, cuya parte nb es divisible entre d.

> Después de este término los residuos seguirán en el mismo orden como en el inicio.

El interés de Euler para trabajar en particular con progresiones aritméticas no es algo fuera de contexto, ya que este tipo de progresiones intrínsecamente habían estado presentes desde la matemática de Diofanto. Recordemos la manera en la que se definen a los números poligonales diofantinos:

Los números poligonales son enteros no negativos construidos geométricamente a partir de polígonos regulares. Los números triangulares son aquellos que cuentan los puntos de un arreglo triangular


La sucesión de los triangulares es $0, 1, 3, 6, 10, 15, \ldots$


De manera similar para los cuadrados es $0, 1, 4, 9, 16, 25, \ldots$


Para el caso de los pentagonales resultan ser $0, 1, 5, 12, 22, \ldots$

De manera semejante se pueden construir los números n-gonales correspondientes para cada polígono regular de $(m+2)$ lados, donde m es igual a $1, 2, 3, 4, \ldots$.

Algebraicamente, y que ya era una manera de abordarlos desde el siglo XVI, se puede observar que para $m \geq 1$, el k-ésimo número poligonal de orden $m+2$ denotado por $P_m(k)$ es la suma de los primeros k términos de la progresión aritmética que inicia en 1 y tiene diferencia m, así la progresión aritmética es $1, (m+1), (2m+1), (3m+1), \ldots, ((k-1)m+1)$. Por lo tanto $P_m(k)$ es

$$P_m(k) = 1+(m+1)+(2m+1)+\cdots+((k-1)m+1) = \frac{mk(k-1)}{2}+k.$$

Así, se llega a un polinomio cuadrático en k, y con esto para $m = 1, 2, 3, \ldots$ se tiene que $P_1(k) = \frac{k(k+1)}{2}, P_2(k) = k^2, P_3(k) =$

$\frac{k(3k-1)}{2}$, corresponden a los triangulares, cuadrados y pentagonales, respectivamente.

Esta breve exposición de los poligonales nos lleva a recordar que Euler se involucró a un alto nivel con ellos, en el capítulo anterior presentamos el teorema de los números pentagonales, y como éstos están definidos a partir de progresiones aritméticas entonces no debe de ser extraño que él las abordara en el capítulo VI para estudiar sus residuos al ser divididas por un número d.

A partir de esto nos podríamos preguntar cómo es el residuo del k-ésimo número poligonal de orden $m+2$, es decir, el residuo de $P_m(k)$ al ser dividido por d. Aunque Euler no trató este problema en el *Tractatus* sí podemos ver que está totalmente en el contexto de las progresiones aritméticas, el estudio de los residuos y su interés por los números poligonales. Entonces podemos pensar que seguramente Euler contemplo la idea de que los términos de una progresión aritmética y sus residuos r_i cuando se dividen entre d se vinculan así

$$1 = 1$$

$$(1 + m) = dq_1 + r_1$$

$$(1 + 2m) = dq_2 + r_2$$

$$\vdots$$

$$(1 + (k - 1)m) = dq_{k-1} + r_{k-1}$$

Por lo tanto, al sumar las igualdades se obtiene

$$P_m(k) = dQ + \sum_{i=1}^{k-1} r_i$$

y es interesante ver que el residuo del k-ésimo poligonal de orden $m + 2$ al ser dividido entre d dejará un residuo $\sum_{i=1}^{k-1} r_i$ el cual se tendría que estudiar para ver a cual es equivalente dentro del sistema de residuos del número d. Con esto podemos notar que

para Euler tenía mucho sentido el estudio de los residuos de los elementos de una progresión aritmética.

De regreso al *Tractatus*, Euler plantea que en una progresión aritmética

$$a, a+b, a+2b, a+3b, a+4b, a+5b, \ldots, a+kb, \ldots$$

al ser dividido cada término entre d generará un residuo que es menor que d. Se tendrán dos casos, cuando $(b,d)=1$ y cuando no, es decir, $(b,d)=g$ diferente de la unidad. Si $(b,d)=1$ entonces la progresión tendrá a lo más d residuos y éstos se repetirán a partir de que d divida a k. Euler escribió lo siguiente en el parágrafo 168:

> Del primero [de los términos de la sucesión] se origina el residuo a, el cual no se repite antes de que se llegue al término $a+kb$, cuya parte kb es divisible entre d. Después de este término los residuos seguirán en el mismo orden como en el inicio.

con esto entonces ya podemos sugerir que la progresión queda repartida en d clases residuales.

En los parágrafos 174 y 175 demuestra que en efecto si $(b,d)=1$ entonces los residuos son exactamente una cantidad d, y ellos son $0, 1, 2, \ldots, (d-1)$, que no necesariamente aparecen en este orden. Con esto entonces nos enuncia en el 176 que «si r fuera cualquier número menor que el divisor d, entonces existe un término de la progresión $a+kb$, donde $k<d$, el cual dividido entre d arroja el residuo r», esto es, las d clases son diferentes del vacío.

Para el caso de $(b,d)=g\neq 1$ entonces se tiene que $b=Bg$ y $d=Dg$, donde $(B,D)=1$, y la cantidad de residuos diferentes son D, Euler en el parágrafo 170 menciona esto:

> Si la diferencia de la progresión, que es b, fuera un factor del divisor d, o si al menos b y d tuvieran un factor común g, de manera que $b=Bg$ y $d=Dg$, entonces antes que se llegue al término $a+db$, aparecerá el primer residuo a; esto puede suceder en el término $a+Db$, cuyo índice es $D+1$, puesto que $Db=BD\varphi=Bd$ es divisible entre d.

Es interesante que todos los términos de la progresión quedan repartidos sólo en d clases de residuos. Por ejemplo para la progresión $5 + 7k$ y un divisor igual a 28, se tiene que $(7, 28) = 7$, y $28 = (4)(7)$, por lo tanto el conjunto de residuos de la progresión son cuatro, ellos son $5, 12, 19$ y 26.

De regreso al caso $(b, d) = 1$ con los d residuos, Euler plantea que se encuentre un elemento de la progresión aritmética $a + kb$, si se toma un residuo determinado, es decir, pensémoslo como una ecuación, que dado el residuo r y el divisor d, encontremos x en la progresión de tal manera que $x = r + dq$, o de manera equivalente $(a + kb) = r + dq$. Para este caso sí usaremos la notación actual de congruencias, ya que ésta nos permite visualizar de manera directa que es lo que quiere exhibir Euler, entonces, nuevamente planteamos que Euler quiere encontrar a x en la progresión tal que

$$x \equiv r \pmod{d}$$

si no contempláramos que x tiene que ser de la forma $a+kb$, entonces se podría tener una solución rápidamente, pero como se requiere que sea de una progresión aritmética entonces Euler enuncia en el parágrafo 181 lo que sigue:

> [...] los términos que dejan los residuos dados pueden definirse fácilmente, mientras se haya distinguido el producto pb, que dividido entre d deje una unidad. Como sucede con el primer término a que arroja α, el término $a+npb$ arrojará $\alpha + n$.

Lo que nos presenta es que para encontrar el término $a + kb$ que deje un residuo dado r se tiene que encontrar p tal que $bp \equiv 1 \pmod{d}$, donde $(b, d) = 1$. Esto es lo que actualmente reconocemos como una congruencia lineal en p, o en otras palabras, encontrar a p que es el inverso de b módulo d.

Así, se quiere encontrar a $x = a + kb$ tal que $x \equiv r \pmod{d}$. Para esto considera al residuo α módulo d del término positivo más pequeño de la progresión, este es a, y por lo tanto $a \equiv \alpha \pmod{d}$.

Enseguida plantea encontrar p en la relación $bp \equiv 1 \pmod{d}$[7], y con la congruencia anterior se llega a que $a + bp \equiv \alpha + 1 \pmod{d}$, si $r \neq \alpha$ entonces se puede considerar la congruencia $b(np) \equiv n \pmod{d}$, para cualquier n en los enteros. De lo indicado ahora se puede tener la congruencia $a + b(np) \equiv \alpha + n \pmod{d}$, y para la n adecuada se tendrá que $\alpha + n = r$, y por lo tanto se obtiene el término $a + b(np)$ de la progresión tal que

$$a + b(np) \equiv r \pmod{d}.$$

Consideramos que es importante mencionar que su planteamiento de usar un inverso modular fue importante, no sólo para este problema, el uso del inverso fue fundamental para muchos resultados que construyó dentro de la teoría de los números.

3.3. Residuos de potencias

El capítulo VII está centrado en la presentación de la teoría de los residuos de potencias, en los parágrafos 192 y 193 escribe lo que sigue:

> 192. Generalmente representamos una progresión geométrica como: $a, ab, ab^2, ab^3, ab^4, ab^5$, etc., cuyos términos si se dividen entre cualquier número d darán siempre los residuos que fácilmente pueden obtenerse a partir de los residuos de la progresión $1, b, b^2, b^3$, etc., y que posteriormente cada uno es multiplicado por a.
>
> 193. Entonces, esta cuestión de los residuos se refiere principalmente para las potencias, de manera que el residuo debe definirse como aquello que queda cuando cualquier potencia b^n es dividida por cualquier número d. Además conviene distinguir los casos en los que los números b y d son o primos entre sí o compuestos.

[7]Encontrar p en $bp \equiv 1 \pmod{d}$, no le sería difícil, ya que al usar su propio resultado de $b^{\phi(d)} \equiv 1 \pmod{d}$, entonces $b(b^{\phi(d)-1}) \equiv 1 \pmod{d}$ y por lo tanto se puede considerar p igual a $b^{\phi(d)-1}$.

Podemos ver que la presentación de los residuos de potencias es tan vigente como las que hoy encontramos en los libros, con la única variante que actualmente la encontraríamos en términos de congruencias.

A lo largo de este capítulo VII se encontrarán las propiedades aritméticas de potencias y residuos, algunas de ellas son el producto de potencias y de sus respectivos residuos; para el caso en que b y d son primos entre sí Euler exhibirá que el conjunto $1, b, b^2, b^3, \ldots,$ etc. sólo tendrá residuos que también son primos con d; se verá que este conjunto de residuos primos con d formas un conjunto de cardinalidad menor o igual que d y es lo que ahora conocemos como *sistema reducido de residuos*; plantea que los residuos existen en la progresión $1, b, b^2, b^3, \ldots$ etc., de manera cíclica. En el parágrafo 200 nos menciona esto:

> [...] como los mismos residuos se repitan progresivamente a partir de la potencia b^n y también desde el inicio, entonces todas las potencias $b^0, b^n, b^{2n}, b^{3n}, b^{4n}, \ldots$ etc. generan el mismo residuo r. Pero no sólo aquellas potencias dejan el mismo residuo, también éstas [potencias] $b^1, b^{n+1}, b^{2n+1}, b^{3n+1}, \ldots$ etc., tendrán residuo igual, y de esta manera también las [potencias] $bm, b^{n+m}, b^{2n+m}, b^{3n+m}$ etc., divididas entre d arrojarán residuos iguales.

Después de mencionar algunas de las propiedades que se encuentran en este capítulo VII, podemos percibir que el contenido tendrá más adelante como resultado aglutinador de las propiedades a lo que hoy conocemos como el **Teorema de Euler**, enseguida lo enunciaremos usando la notación de congruencias

Teorema: **Si N y x son primos relativos entonces**

$$x^{\phi(N)} \equiv 1 \ (\textbf{mód } N).$$

$\phi(N)$ es la función aritmética que cuenta a los primos relativos positivos menores que N.

Ya mencionamos que el *Tractatus* es un obra con perfil de compendio y por tal razón no proporciona todas las demostraciones, y

para el caso de los residuos de potencias Euler escribió en 1755 el artículo ya mencionado *Theoremata circa residua ex divisione potestatum relicta* (Teoremas sobre residuos obtenidos por la división de potecias) (E262). Para una lectura panorámica de la teoría de residuos hasta llegar al teorema de Euler lo más apropiado sería consultar el *Tractatus*, pero si lo que se quiere es adentrarse en menos resultados pero acompañados de más demostraciones, entonces es apropiado consultar el trabajo mencionado (E262). Lo que presentaremos a continuación son los principales resultados que proporcionó Euler para los residuos de potencias y que se encuentran entre el *Tractatus* y el E262, los resultados son muchos más, y aquí sólo abordamos los más representativos del tema.

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

Demostración. Supongamos que λ es la menor potencia de a que deja residuo unitario 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. Sean $1, a^2, a^3, a^4, \ldots, a^{\lambda-1}$ las potencias que dan λ residuos diferentes cuando son divididos entre p. Además sea k un no residuo, entonces $ak, a^2k, a^3k, a^4k, \ldots, a^{(\lambda-1)}k$ tampoco serán residuos, y además serán diferentes entre sí. Entonces se tiene que $ak, a^2k, a^3k, a^4k, \ldots, a^{(\lambda-1)}k$ que son λ no residuos. Así existen al menos λ no residuos que no se encuentran entre los residuos, suponiendo que $\lambda < p-1$. $\square$

Corolario 1. En consecuencia se tienen λ números que son residuos diferentes, y son tantos como números diferentes menores que p. Entonces, el número total de 2λ no podrá ser mayor que $p-1$, porque no hay más números menores que p.

Corolario 2. Si a^λ es la mínima potencia que deja residuo uno cuando es dividida por p, entonces se tendría que $\lambda < p-1$, y por lo tanto no se tendría que $\lambda > \frac{p-1}{2}$, por lo tanto se tendría que $\lambda = \frac{p-1}{2}$ o $\lambda < \frac{p-1}{2}$.

Corolario 3. Sea λ la mínima potencia, ésta es menor que p; entonces será o bien $\lambda = p-1$ o $\lambda < p-1$; si $\lambda < p-1$, sabemos que será $\lambda = \frac{p-1}{2}$ o $\lambda < \frac{p-1}{2}$. Entonces λ no podrá ser ningún número contenido más allá de los límites $p-1$ y $\frac{p-1}{2}$.

Teorema 2. Sea p un número primo, y a^λ la mínima potencia 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 residuo uno cuando es dividida por p, sean $1, a^2, a^3, a^4, \ldots, a^{\lambda-1}$ las potencias que al ser divididas entre p dejan λ residuos diferentes. Como $\lambda < p-1$ entonces hay $p-1-\lambda$ números que no son residuos. Si r es uno de ellos, $r, ar, a^2r, a^3r, a^4r, \ldots, a^{(\lambda-1)}r$ 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 un número que no es un no residuo pero que tampoco es un residuo. Entonces los números $s, a^s, a^2s, a^3s, a^4s, \ldots, a^{(\lambda-1)}s$ serán no residuos y diferentes entre ellos. Además, ninguno de éstos será igual a algún número de la primera serie de no residuos. Así, 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. Si no se tiene que $\lambda < \frac{p-1}{3}$ se tendrá 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 que $\lambda = \frac{p-1}{3}$ o $\lambda = \frac{p-1}{2}$ o $\lambda = p-1$.

Corolario 5. Si $\lambda = \frac{p-1}{3}$ o $\lambda = \frac{p-1}{2}$, entonces a^{p-1} dividida por p dejaría como residuo la unidad. Pues como a^λ deja a la unidad como residuo, entonces también lo harán $a^{2\lambda}$ y $a^{3\lambda}$.

Teorema 3. Si a^λ es la mínima potencia de a que deja la unidad cuando es dividida por un primo p, y si fuera $\lambda < \frac{p-1}{3}$, entonces no pasa que $\lambda > \frac{p-1}{4}$, por lo tanto será $\lambda = \frac{p-1}{4}$ 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, $1, a^2, a^3, a^4, \ldots, a^{\lambda-1}$ entonces,

como $\lambda < \frac{p-1}{3}$, se originan el doble de números que no son residuos de las siguientes dos progresiones $r, a^r, a^2r, a^3r, a^4r, \ldots, a^{(\lambda-1)}r$ y $s, a^s, a^2s, \ldots a^3s, a^4s, \ldots, a^{(\lambda-1)}s$. 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 $t, a^1t, a^2t, a^3t, a^4t, \ldots, a^{(\lambda-1)}t$, cuyo número es igual a λ, que también serán no residuos. Además estos números no sólo son diferentes entre sí, sino que además serán diferentes a los de las primeras series, entonces el número de residuos y no residuos será igual a 4λ. Como ellos son menores que p, no se puede tener que $4\lambda > p-1$. 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 demuestra, 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 $\lambda = \frac{p-1}{n+1}$ o $\lambda < \frac{p-1}{n+1}$.

Corolario 8. De esto es claro que la cantidad de todos los números que no son residuos tiene que ser 0 o λ o 2λ, o cualquier otro múltiplo de λ, pues si hubiera más números de este tipo que $n\lambda$, entonces como otros λ siguen se tiene que el número de no residuos serían $(n+1)\lambda$; y si éstos no fueran los únicos números 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 residuos 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 $p-1-\lambda = n\lambda$ 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 $p-1$. □

Con esta serie de teoremas y corolarios Euler llega al 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 primo y a es primo con p entonces la potencia a^{p-1} dejará a la unidad como residuo cuando es 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 esta demostración es sobre el pequeño teorema de Fermat y cabe mencionar que cuando Euler la escribió no fue la primera, esta fue la tercera demostración, pero sí la primera en la que usa residuos, y ahí radicó su diferencia con las otras dos. Así, el pequeño teorema es una consecuencia del hecho de que los números menores que p que no son residuos módulo p son $p-1-\lambda = n\lambda$, donde λ es el orden de a módulo p. Euler no dejó pasar esta observación en el artículo, él compara su demostración con la que dio en 1736, y dice que difieren en que la primera que empieza por la expansión del binomio $(a+b)^n$, y que esto hace que el razonamiento parezca remoto a la proposición; pero en cambio esta nueva demostración se basa sólo en resultados concernientes a potencias, que hacen parecer la prueba más natural.

Como ya mencionamos, el capítulo VII del *Tractatus* tiene entre sus objetivos principales llegar al teorema que involucra a la potencia $\phi(N)$. En el *Tractatus* sólo encontramos un bosquejo de demostración, enseguida demostramos el teorema usando sólo los elementos que Euler construyó en el *Tractatus* y en otros trabajos.

Teorema: **Si N y x son primos relativos entonces**

$$x^{\phi(N)} \equiv 1 \ (\textbf{mód } N).$$

Demostración. Sea $\{r_1, r_2, \ldots r_{\phi(N)}\}$ un sistema reducido de residuos módulo N,[8] y como $(N, x) = 1$, entonces se tiene que $\{xr_1, xr_2, \ldots, xr_{\phi(N)}\}$ 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 primero, entonces sin pérdida de generalidad podemos afirmar que

$$xr_i \equiv r_j \pmod{N},$$

entonces si se multiplican todas las congruencias se obtiene

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

y cuando se reagrupan los factores se llega a:

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

y como $(r_i, N) = 1$, entonces $(r_1 r_2 r_3 \ldots r_{\phi(N)}, N) = 1$, 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

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

y este es el resultado al que se quería llegar[9]. □

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 demostrar que **si N y x son primos relativos entonces $x^{\phi(N)} \equiv 1$ (mód N).** Tratar de probar este teorema con

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

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

sistemas completos de residuos nos llevaría a la inmovilidad cuando estuviéramos en un punto de la demostración como el de

$$xr_1xr_2xr_3 \dots xr_N \equiv r_1r_2r_3 \dots r_N \pmod{N},$$

y es porque no se tendría la certidumbre de poder eliminar todas las 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 pertenezcan a un sistema reducido de residuos, pues recordemos que bajo esa situación cada r_i es primo relativo con N.

Veamos la demostración de Euler pero ahora se considerarán los elementos que aparecen en E271.

Para demostrar que $x^{\phi(N)} \equiv 1 \pmod{N}$ cuando x y N son primos relativos Euler construirá un sistema reducido de residuos módulo N con base en que el orden de x módulo N es un entero h. Así, se parte del hecho que existe h, que es el menor entero positivo tal que al ser divido x^h por N deja resto uno, es decir, se cumple que $x^h \equiv 1 \pmod{N}$. Ahora veamos que $h \leq \phi(N)$. Considérese el conjunto $\{1, x, x^2, \dots, x^{h-1}\}$, como x y N son primos relativos, entonces todas las potencias de x del conjunto también lo son, y además cualesquiera dos elementos del conjunto no son congruentes módulo N. [10]

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

[10] Para estar seguros de esto, supongamos que no es así, entonces pensemos que existen x_i y x_j del conjunto (diferentes entre ellos y que $i > j$) tal que $x^i \equiv x^j \pmod{N}$, y de aquí se obtiene que $x^{i-j} \equiv 1 \pmod{N}$. De la última congruencia se tiene que $(i-j) < h$, pero h es el menor entero positivo tal que $x^h \equiv 1 \pmod{N}$, por lo tanto se genera una contradicción. Así concluye que no pueden existir x_i y x_j elementos diferentes que sean congruentes o, dicho de otro modo, que dejen el mismo residuo al ser divididos entre N.

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

Nuevamente, si $2h = \phi(N)$ entonces ya se terminó la demostración porque $x^{\phi(N)} \equiv 1 \pmod{N}$, pero si $2h < \phi(N)$ entonces existe otro entero k menor que N y también primo relativo tal que el conjunto $\{k, kx, kx^2, \ldots, kx^{h-1}\}$ 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 $x^h \equiv 1 \pmod{N}$ y como ahora ya sabemos que $wh = \phi(N)$, entonces se llega a que $x^{wh} \equiv 1 \pmod{N}$ y por lo tanto $x^{\phi(N)} \equiv 1 \pmod{N}$, que es lo que Euler quería demostrar, y para el caso en que 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.

3.4. Criterio para residuos cuadráticos

En el capítulo VIII del *Tractatus* se encuentran resultados centrados en que el residuo de la potencia sea sólo la unidad, entonces se adentrará aún más en las propiedades de lo que conocemos como orden, y además considerará que el divisor es un primo impar, entonces podemos notar que hay una inclinación hacia los resultados

que corresponden a residuos cuadráticos y posteriormente ley de reciprocidad.

De los parágrafos 243 a 252 expone propiedades de la potencia que deja residuo uno cuando es dividida por un primo d de la forma $d = 2p + 1$. Siempre estarán presentes el teorema de Euler que involucra a la función $\phi(N)$ y las propiedades de orden, es decir, la mínima de las potencias que deja residuo uno cuando es dividida, en este caso por el primo $d = 2p + 1$.

Uno de lo resultados más relevantes que se encontrará en este capítulo es el que hoy conocemos como criterio de Euler para residuos cuadráticos. En el parágrafo 254 del *Tractatus* encontramos lo que sigue

> Como $a^{2p} - 1$ siempre es divisible por el número primo $2p+1$, entonces esta fórmula tendrá los factores a^{p-1} y a^{p+1}, entonces necesariamente uno de ellos es divisible por $2p+1$. Pero vemos que si $a = ee \pm \lambda(2p + 1)$ entonces $a^p - 1$ será divisible. Así que en estos casos $a^p + 1$ no será divisible por $2p + 1$.

Lo que nos está trasmitiendo[11] es que como $a^{2p} \equiv 1 \pmod{2p+1}$ entonces $(a^p + 1)(a^p - 1) \equiv 0 \pmod{2p+1}$, por lo tanto $2p+1$ divide sólo a uno de los dos factores $(a^p + 1)$ y $(a^p - 1)$, no puede ser a ambos ya que entonces tendría que dividir a la diferencia que es 2, y esto no es posible porque $2p + 1$ es impar. Ahora Euler señala «Pero vemos que si $a = ee \pm \lambda(2p + 1)$ entonces $a^p - 1$ será divisible [por $2p + 1$]», lo que nos está diciendo es que si existe una solución x para $x^2 \equiv 1 \pmod{2p + 1}$, y ésta es e, entonces $e^2 \equiv a \pmod{2p+1}$, por lo tanto $a^p \equiv e^{2p} \pmod{2p+1}$, y como se supone que e y $2p+1$ son primos relativos, entonces, por el teorema de Euler $e^{2p} \equiv 1 \pmod{2p+1}$ y por lo tanto $a^p \equiv 1 \pmod{2p+1}$, es decir, $2p + 1$ divide a $(a^p - 1)$.

En términos más actuales -pero que conservan totalmente la idea de Euler diríamos que:

[11] Nuevamente usaremos la notación de congruencias para facilitar la interpretación.

Dado un primo impar $2p+1$. Un entero positivo a que es primo con $2p+1$ es un residuo cuadrático de $2p+1$ si y sólo si $a^p \equiv 1$ (mód $2p+1$).

Euler nos menciona al final de la cita que en estos casos entonces (a^p+1) no será divisible por $2p+1$, y esto es lo que ahora retomaríamos para concluir que a no es un residuo cuadrático módulo $2p+1$, que en términos actuales lo tendríamos como un corolario que nos llevaría a la congruencia $a^p \equiv -1$ (mód $2p+1$).[12]

Casi para terminar el capítulo VIII, en el parágrafo 261 se enuncia lo que sigue:

> Sea $6p+1$ un número primo y puesto que la fórmula $a^{6p}-1$ es divisible por él, a no ser que a sea su múltiplo, se tendrán los casos en los que también $a^{2p}-1$ podrá ser dividido por este, es decir, teniendo $a = e^3 \pm \lambda(6p+1)$. Pero también se dan los casos en los que la fórmula $a^{2p}-1$ no será divisible por el número $6p+1$, como es evidente a partir de la demostración expresada.

Aquí lo que parece es que Euler nos presenta lo que sería el criterio para residuos cúbicos, esto parece que es así: sea $a^{6p} \equiv 1$ (mód $6p+1$), y de manera semejante al caso cuadrático, entonces $(a^{2p}+1)(a^{2p}-1) \equiv 0$ (mód $6p+1$) entonces $2p+1$ divide sólo a uno de los dos factores $(a^{2p}+1)$ y $(a^{2p}-1)$. Si existe e tal que $e^3 \equiv 1$ (mód $6p+1$) entonces se obtendrá que $(a^{2p}-1) \equiv 0$ (mód $6p+1$), es decir, $6p+1$ divide a $(a^{2p}-1)$.

Y nuevamente desde una visión actual diríamos que

Dado un primo impar $6p+1$. Un entero positivo a que es primo con $6p+1$ es un residuo cúbico de $6p+1$ si y sólo si $a^{2p} \equiv 1$ (mód $6p+1$).

Euler terminó el capítulo con el parágrafo 263 y en él sólo enuncia lo que sería como la extensión de todo lo anterior para residuos bicuadrático y ya no profundizó más en estos puntos.

Pareciera que sólo quería mencionar estos resultados de residuos cúbicos y bicuadráticos, sin profundizar más, pensando que

[12] Las demostraciones actuales de estos resultados del Criterio de Euler se pueden consultar en [Koshy 2007, pág. 499].

el entorno compendioso del *Tractatus* se lo permitiría. Pero tampoco podemos pasar por alto que Euler estaba creando esta teoría, entonces cabe considerar que en el tiempo que escribió estas partes del capítulo VIII aún no se tenía totalmente desarrollada la teoría.

3.5. Los divisores de $a^n \pm b^n$.

Este capítulo, el IX, contiene resultados que podemos decir que reflejan los intereses de juventud de Euler en lo que atañe a teoría de los números. Recordemos su interés por los números de Fermat que son de la forma $2^{2^n} + 1$; su cercanía al teorema del mismo francés que trata sobre los primos p que dividen a $a^{p-1} - 1$, donde a y p son primos entre si; o los primos de la forma $(a^m - 1)$ con m también primo, que son parte de los perfectos. Los tres problemas mencionados tienen que ver con números de la forma $a^n \pm b^n$, por tal razón en el *Tractatus* ya lo está presentando de manera general. Para entender más sobre los números $a^n \pm b^n$ en el contexto del *Tractatus* veamos primero que hizo años antes.

Sabemos que el 13 de octubre de 1729 Goldbach escribió a Euler una carta y al final de ésta le mencionó que si «¿Ha advertido usted la observación de Fermat de que todos los números de la forma, es decir, 3, 5, 17, etc. son números primos?». Mencionamos que los dos años siguientes Euler mostró un interés ya no sólo en los posibles divisores de los números de la forma 2^{2^n+1}, sino que estudió de forma general los divisores de los números con las representaciones $a^n \pm 1$ y $a^n \pm b^n$.

En 1732 el producto de las primeras reflexiones que iniciaron con Goldbach se reflejó en las *Observationes de theoremate quodam Fermatiano aliisque ad numeros primos spectantibus* (E26)[13], éste es el primer artículo de Euler sobre teoría de los números. Los temas que trata son:

1. La respuesta a la pregunta de Goldbach sobre la posibilidad

[13] *Observaciones sobre teoremas de Fermat y otros autores sobre números primos.*

de que los números de Fermat fueran primos, este problema lo trabaja con el estudio de cómo es n cuando $a^n + 1$ es factorizable, y cómo cuando no lo es.

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

3. Euler terminó el artículo con la mención de que había encontrado más problemas relacionados con lo anterior, y pensó que deberían de ser investigados.

Finalizó con seis teoremas de los que no proporcionó las demostraciones, y posiblemente no lo hizo porque parece que en este año aún dependía de otros resultados en proceso.

Ahora nos centraremos en los últimos tres teoremas con los que finalizó el artículo mencionado, y que ellos se vinculan directamente con los enunciados que posteriormente se encuentran en el *Tractatus*.

Los 3 teoremas de las *Observationes de theoremate quodam Fermatiano aliisque ad numeros primos spectantibus* tratan sobre problemas de divisores de los números de la forma $a^n \pm b^n$, y todo parece indicar que tenía en mente el pequeño teorema de Fermat, aunque él no lo menciona. Pero lo más importante es que son parte del camino hacia el desarrollo de la teoría de los residuos cuadráticos.

Enseguida presentamos los teoremas mencionados, y aunque las demostraciones no se encuentran en el artículo nosotros las hacemos tratando de usar sólo elementos matemáticos que el mismo Euler usaría posteriormente a lo largo de otros de sus trabajos entre ellos el *Tractatus*.

Teorema 4. 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 $3^n - 1$ podrá 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 $2n + 1 \mid 3^{2n+1-1} - 1$ y en consecuencia $2n + 1 \mid 3^{2n} - 1$, por otro lado como $3^{2n} - 1 =$

$(3^n - 1)(3^n + 1)$ y $2n + 1$ es primo, entonces[14] $2n + 1 \mid 3^n - 1$ ó $2n + 1 \mid 3^n + 1$. 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 $q \equiv \pm 1 \pmod{12}$, y si no es residuo cuadrático pasa que $q \equiv \pm 5 \pmod{12}$. Ahora, 3 es un residuo cuadrático módulo q sólo cuando $n = 6p$ ó $n = 6p - 1$, y de esto Euler propone que tiene que suceder que $3^n \equiv 1 \pmod{2n+1}$, por lo tanto $2n + 1 \mid 3^n - 1$. Para el otro caso, si no existe x tal que $x^2 \equiv 3 \pmod{q}$, entonces se dice que 3 no es un residuo cuadrático módulo q, y esto sólo pasa si $q \equiv \pm 5 \pmod{12}$. Así, cuando 3 no es residuo cuadrático módulo q pasa que $n = 6p + 2$ ó $n = 6p + 3$, y de esto ahora Euler propone que tiene que suceder que $3^n \equiv -1 \pmod{2n + 1}$, por lo tanto $2n + 1 \mid 3^n + 1$. □

Teorema 5. $3^n + 2^n$ puede ser dividido por $2n + 1$ si $n = 12p + 3, 12p + 5, 12p + 6$ ó $12p + 8$, y $3^n - 2^n$ puede ser dividido 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 $2n + 1 \mid (3^{2n} - 2^{2n})$. Ahora como $3^{2n} - 2^{2n} = (3^n - 2^n)(3^n + 2^n)$ y $2n + 1$ es primo, entonces $2n + 1 \mid (3^n - 2^n)$ ó $2n + 1 \mid (3^n + 2^n)$. Se demostrará primero el caso cuando $2n + 1 \mid (3^n - 2^n)$.

- Si $n = 12p$ entones $2n + 1 = 2(12p) + 1 = 12r + 1$, a lo que llamamos q, entonces $q \equiv 1 \pmod{12}$, y por ello 3 es residuo cuadrático módulo q, y en consecuencia por el criterio de Euler $3^n \equiv 1 \pmod{2n+1}$, y por lo tanto, $2n + 1 \mid (3^n - 1)$.

- Nuevamente, si $n = 12p$, entones $2n+1 = 2(12p)+1 = 8r+1$, a lo que llamamos nuevamente q entonces $q \equiv 1 \pmod{8}$, entonces 2 es residuo cuadrático módulo q y en consecuencia

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

por el criterio de Euler $2^n \equiv 1 \pmod{2n+1}$, por lo tanto, $2n+1 \mid (2^n - 1)$.

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

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

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 $2n+1 \mid (3^n + 2^n)$. □

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 6. 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 si $n = 12p+3, 12p+5, 12p+6$ 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 $3^n \equiv -1 \pmod{2n+1}$ y $2^n \equiv -1 \pmod{2n+1}$ y de esto se obtiene que $6^n \equiv 1 \pmod{2n+1}$, entonces $2n+1 \mid (6^n - 1)$. Otro ejemplo, si $n = 12p+3$, entonces $3^n \equiv -1 \pmod{2n+1}$ y $2^n \equiv 1 \pmod{2n+1}$ y de esto se obtiene que $6^n \equiv -1 \pmod{2n+1}$, entonces $2n+1 \mid (6^n+1)$. De la misma forma se demuestra para todos los casos. □

Los tres teoremas y sus demostraciones nos ponen en contexto con lo que Euler escribe en el capítulo IX del *Tractatus*. En los

parágrafos 266 al 278 expone resultados sobre divisores de $a^n - b^n$ que son de la forma $\lambda n+1$. En los parágrafos 271 y 272 encontramos lo siguiente

> 271. De donde, si n es un número primo, entonces para encontrar los divisores de $a^n - b^n$, adicionales a los que contiene $a - b$ debemos buscar entre los primos de la forma $\lambda n + 1$. Puesto que a y b son primos entre si, es evidente que tal condición debe añadirse.
>
> 272. Por lo tanto, para diversos valores del mismo n, los divisores primos de la fórmula $a^n - b^n$, además de $a - b$, deben hacerse como sigue:

Fórmula	Los divisores deben estar entre estos números primos
$a^2 - b^2$	$2\lambda + 1 \ldots 3, 5, 7, 11, 13, 17, 19,$ (ninguno excluido)
$a^3 - b^3$	$2\lambda + 1 \ldots 7, 13, 19, 31, 37, 43, 61, 67, 73, 79, 95,$ etc.
$a^5 - b^5$	$2\lambda + 1 \ldots 11, 31, 41, 61, 71, 101,$ etc.
$a^7 - b^7$	$2\lambda + 1 \ldots 29, 43, 71, 113, 127,$ etc.
$a^{11} - b^{11}$	$2\lambda + 1 \ldots 23, 67, 89, 199, 331,$ etc.
	etc.

Estos enunciados nos muestran que una lectura conjunta del *Tractatus* y de los teoremas del E26 es lo más recomendable para comprender cual es el origen de esta teoría. Para profundizar y formalizar en estos tópicos está su artículo del año 1742 *Theoremata circa Divisores Numerorum* (E134)[15], en este se encuentra una exposición más estructurada sobre los divisores de $a^n \pm b^n$. Los dos trabajos abordados –E134 y E26– son útiles para complementar este tema del capítulo IX, pero no implica que sean un tipo de remplazo unos del otro, Euler los escribió en épocas diferentes y en contextos diferentes, por esta razón los tres se complementan para formar una sola visión de este tema de divisores de potencias.

[15] Teoremas sobre divisores de números.

Capítulo 4

Residuos de potencias

4.1. Residuos cuadráticos, cúbicos, bicuadráticos y sursólidos

En el capítulo anterior se percibió que los residuos de potencia se abordaron principalmente para crear conjuntos de enteros que tuvieran las características de ser subconjuntos de un sistema reducido de residuos. Se construyeron –por mencionar algunos resultados– las definiciones de orden, raíz primitiva, residuos cuadráticos y el actualmente conocido Teorema de Euler que usa la función $\phi(N)$ para demostrar que $x^{\phi(n)} \equiv 1$ (mód N). En algunos casos se requerían los residuos de potencias para poder generar uniones de conjuntos ajenos que tuvieran cardinalidad igual a un múltiplo del orden y que a la vez fuera igual a $\phi(N)$, como sucedió en el caso de los conjuntos $\{1, x, x^2, \ldots, x^{h-1}\}$ y $\{g, gx, gx^2, \ldots, gx^{h-1}\}$ que sirvieron para demostrar el teorema de Euler. Así, la manera de usar los residuos de potencias funcionó como un puente para poder construir algunos de los resultados anteriores, pero aún Euler no consideraba el estudio de los residuos de potencias en sí mismos. En los libros X al XIV del *Tractatus* ya encontramos una manera diferente de plantear el estudio de los residuos.

Empieza por retomar los residuos cuadráticos y señala que el residuo que deja a^2 al ser divido por el divisor d es el mismo que

el de $(nd \pm a)^2$:

> El residuo que queda si un cuadrado a^2 es dividido por cualquier número d es el mismo que queda con la infinidad de residuos $(nd \pm a)^2$ cuando se divide entre el mismo número d. (parágrafo 284)

Este resultado lo podrá extender para los residuos cúbicos, bicuadráticos y sursólidos[1]. Además, el siguiente parágrafo (285) indica cuantos y cuales números hace falta estudiar para obtener información sobre los residuos cuadráticos, a saber $1, 4, 9, \ldots, (d-1)^2$:

> Por lo que, si queremos examinar los residuos que se generan por la división de los números cuadrados entre el número dado d, será suficiente considerar los cuadrados cuya raíz cuadrada es menor que el divisor d, es decir, son
>
> $$1, 4, 9, 16, \ldots, (d-4)^2, (d-3)^2, (d-2)^2, (d-1)^2.$$

No hacen falta más, por la observación anterior. Como se mencionó arriba, este resultado es importante no solo para la teoría que se desarrolla en el capítulo X del *Tractatus*, también lo es para los que siguen hasta el capítulo XV. Estos capítulos toman como base este resultado y su análogo correspondiente para empezar a desarrollar la teoría. Por ejemplo, en el capítulo XI tenemos que:

> 371. Dado el divisor primo $d = 2p+1$, el residuo que deja el cubo a^3 [al ser dividido por d], es el mismo que dejan los cubos $(a+d)^3, (a+2d)^3$, etc. y en general $(a+nd)^3$. A partir de esto bastará considerar solamente a los cubos cuyas raíces son menores que d, estos son: $1, 8, 27, 64, \ldots, (d-4)^3, (d-3)^3, (d-2)^3, (d-1)^3$.
>
> 372. Sea r un residuo que deja cualquiera de los cubos a^3, y es manifiesto que el cubo $(d-a)^3$ dejará como residuo a $-r$ o $d-r$. Por lo que si entre los residuos cúbicos aparece cualquier número r, allí también estará su negativo $-r$ o $(d-r)$, al que llamaremos su complemento.

y en el XII y XIII encontramos, respectivamente en los parágrafos 412 y 413:

[1] Un sursólido es una potencia quinta.

412. Si el divisor primo es d, el residuo que deja el bicuadrático a^4 es el mismo no solo para los bicuadráticos $(d+a)^4, (2d+a)^4$, etc. sino también para $(d-a)^4$, de donde si $d = 2p+1$, entonces no pueden resultar más residuos diferentes que p.

464. Si el divisor es d y a^5 deja [residuo] α, entonces $(d-a)^5$ deja [residuo] $-\alpha$, y así todos los residuos surgirán de las potencias $1, 2^5, 3^5, 4^5, \ldots (d-1)^5$ y si todos fueran diferentes, su cantidad es igual a $d-1$.

Estos resultados son la base para adentrarnos en las clases de residuos que se estudian hoy en Teoría de Números, y sobra decirlo, son la base para la generalización de las clases como elementos de un cociente (de módulos, anillos, grupos, etc...)

El siguiente resultado también es fundamental y muy interesante, éste se desprende de las mismas observaciones que antes:

287. Ahora, sea d un número primo y como el resultado para el [único] par no tiene dificultad, entonces supongamos que $d = 2p+1$. Se tiene que todos los residuos son el resultados de los siguientes cuadrados $1, 4, 9 \ldots, (p-2)^2, (p-1)^2, p^2$, la cantidad de estos no puede ser mayor que p. De esto, es manifiesto que no todos los números menores que $d = 2p+1$, que son $2p$, se encuentran entre los residuos, por lo menos la mitad de estos se excluyen;

es decir, la observación se centra en que 1 y $(d-1)^2$ dejan el mismo residuo cuando son divididos por d. En general, los extremos de la lista anterior dejan el mismo residuos al ser divididos por d, por lo cual, si d es impar (que es el caso interesante y por tanto estudiado, puesto que, según el mismo Euler, «el caso par no presenta dificultad») entonces $d-1$ será par y por lo tanto habrá tantos residuos como no residuos, y serán exactamente $\frac{1}{2}(d-1)$. Más aún, dado que estamos considerado al divisor d como un número primo, y además se excluye del estudio al divisor par, entonces podemos escribir $d = 2p+1$, de donde es inmediato que la cantidad de residuos es exactamente igual a p. Como observamos, la adaptación de este resultado a todos los capítulos que siguen—hasta el XV—es constante, incluso se presenta en el mismo orden.

Del análisis anterior puede surgir una pregunta natural: ¿son exactamente p? La pregunta es totalmente válida puesto que *a priori* no se sabe que los p residuos que se están encontrando sean todos distintos, podría ser que haya algunos repetidos y entonces se tendría una cantidad menor a p (pero como ya vimos, nunca mayor) de residuos. El parágrafo 288 resuelve esta pregunta, y afirma que son exactamente p, como lo vemos a la letra:

> En primer lugar digo que todos los residuos surgidos de los cuadrados $1, 4, 9, \ldots, p^2$ son diferentes entre ellos. En efecto, sean dos cuadrados no mayores que p^2. Por ejemplo, supongamos que m^2 y n^2 dejan el mismo residuo, y que la diferencia entre ellos es $m^2 - n^2$, se llega a que $m-n$ o $m+n$ serán divisibles por el divisor primo $d = 2p + 1$, pero esto no puede suceder, puesto que $m + n$ es menor que d, ya que $m < \frac{1}{2}d$ y $n < \frac{1}{2}d$.

El mismo resultado se adapta en los siguientes capítulos: ya no será la mitad, pero hay una cota máxima, y de igual modo se demuestra que tal cota se alcanza y por tanto, independientemente del módulo, se sabe qué cantidad de residuos hay. Refiramos al resultado para residuos cúbicos: el primer cuestionamiento es similar al correspondiente para el capítulo sobre residuos cuadráticos, pues dice:

> 374. Investigaremos, ¿es posible que el mismo número r aparezca dos veces entre los residuos ? Supongamos que el mismo residuo r es el que se obtiene de los cubos a^3 y b^3 cuyas raíces a y b son menores y diferentes al mismo divisor d. Y su diferencia $b^3 - a^3 = (b-a)(aa+ab+bb)$ será divisible por d, pero d es primo con $b - a$, entonces es necesario que el otro factor sea divisible por d.

Después de las observaciones que siguen, se llega en el parágrafo 383 a la conclusión correspondiente al capítulo:

> Como todos los números primos excepto 2 y 3 son una de las formas $6q+1$ y $6q-1$, pasará que si el divisor primo es $6q-1$, entonces todos los números menores que este serán de los residuos, y no se da ningún no-residuo. Por el contrario,

si el divisor es $6q + 1$, puede suceder que la cantidad de residuos sea solo $2q$, y así serán $4q$ no-residuos.

Posteriormente, Euler se interesa a partir del parágrafo 395, en retomar a los residuos de los cuadrados. En capítulos anteriores del *Tractatus* ya había abordado el tema de los residuos cuadráticos, y recordemos que en esta tesis usamos la notación de congruencia para entender de mejor manera lo que nos exponía Euler.

En los parágrafos 293 al 306 expone lo que ahora vemos como una aritmética de residuos, y nos preguntamos en este contexto del *Tractatus* ¿el producto de dos números en alguna de las clases, a cuál de las clases pertenece? Más aún, ¿si mn y m son (o no son) residuos, n lo es o no? Estos resultados dependen de d? Es importante mencionar que, actualmente estos resultados se enfrentan usando el símbolo de Legendre, pero Euler fue el primero en proponerlos y demostrarlos, y por tanto su demostración es más extensa, pero el valor del resultado no está en haber encontrado la mejor prueba, sino en proponer esta ruta de estudio de los residuos y escribirla y demostrarla con las herramientas aritméticas disponibles en su época. Acto seguido se tiene para potencias de un residuo, o de un no residuo (pues se trata de un producto de un número por otro (a saber, él mismo)). El parágrafo 289 da un resultado muy valioso en este sentido:

> Por lo tanto, como todos los residuos que se generan a partir de la división de los cuadrados $1, 4, 9, \ldots, p^2$ entre el número primo $d = 2p + 1$ son diferentes, representémoslos de la siguiente manera
>
> | | | | | | | | | |
> |---|---|---|---|---|---|---|---|---|
> | raíces | 1 | 2 | 3 | 4 | 5 | 6 | ... | p |
> | cuadrados | 1 | 4 | 9 | 16 | 25 | 36 | ... | p^2 |
> | residuos | 1 | α | β | γ | δ | ε | ... | π |

Esto es consecuencia directa del Pequeño Teorema de Fermat, y la posibilidad de que una potencia inferior cumpla con lo mismo es lo que hoy llamaríamos, el orden del grupo. De esto nace la teoría de las raíces primitivas, el Teorema de Euler, y posteriormente los Teoremas de la Teoría de grupos sobre el orden de un grupo, como por ejemplo el de Lagrange. La parte central de esto queda resumida en el parágrafo 307. El análisis se «generaliza» para productos

de residuos de potencias y también se resumen en el parágrafo 320, el cual insertamos a la letra:

> Así, los residuos, así como los no-residuos de los cuadrados, están dispuestos de tal manera que:
>
> 1. Se inicia con la unidad;
> 2. Los productos de dos residuos también son un residuo
> 3. Los productos de un residuo y de un no-residuo dan un no-residuo, de esto es posible concluir que los productos de dos no-residuos dan lugar a estar en la clase de los residuos.

Esta forma de pensar y estructurar las ideas del capítulo X funcionaron suficientemente bien para dar, a los siguientes capítulos, el mismo perfil. Este resultado es necesario en todo el capítulo X, y en consecuencia, influye en los correspondientes capítulos del XI al XIV. Revisemos y comparemos la influencia de éste en los parágrafos 399 y 401 del capítulo siguiente:

> 399. Entonces, a partir del único no-residuo A se obtienen dos no-residuos, el primero $A, A\alpha, A\beta, A\gamma, A\delta$, etc. y el segundo $A^2, A^2\alpha, A^2\beta, A^2\gamma, A^2\delta$, etc., cada uno contiene tanto términos como los que contiene el orden de los residuos, los productos [surgidos] de uno de los órdenes se encontrarán en el otro orden, y los productos de ambos órdenes se volverán residuos.
>
> 401. Si AB no es un residuo, podemos representar los dos órdenes de los no-residuos de la siguiente manera:

Primer orden	$A, A\alpha, A\beta, A\gamma$, etc.	$B, B\alpha, B\beta, B\gamma$, etc.
Segundo orden	$A^2, A^2\alpha, A^2\beta, A^2\gamma$, etc.	$B^2, B^2\alpha, B^2\beta, B^2\gamma$, etc.

> y cualquier número del primer orden, multiplicado por cualquiera del segundo dará un residuo diferente a cualquier otro; a partir de esto resultarán más residuos de los que en verdad son, lo cual sería absurdo.

Más aún, en el capítulo XII, el resultado también se presenta, en el parágrafo 423:

> Si x^2 no está en los residuos de los bicuadráticos, entonces tampoco estarán allí mismo $\alpha x^2, \beta x^2, \gamma x^2, \delta x^2$, como ellos son residuos de los cuadrados, y es evidente que entre los residuos de los cuadrados, cuya cantidad es $2q$, hay tantos no-residuos bicuadráticos como los residuos bicuadráticos; de esto es evidente que la cantidad de los residuos bicuadráticos, es igual a q o menor, más que esto no puede ser.

Aunado a lo anterior, en el resumen en forma de tabla del capítulo X se encuentran datos semejantes a los del capítulo de bicuadráticos:

> Podemos construir estas tres clases de la siguiente manera: los cuadrados no están en los residuos; xx es un cuadrado; es verdad que ni x ni x^3 pueden encontrarse entre los residuos. Si los residuos son $1, \alpha, \beta, \gamma, \delta, \varepsilon$, etc. habrá tres clases de residuos:
>
> I. $x, \alpha x, \beta x, \gamma x, \delta x$, etc.
> II. $x^2, \alpha x^2, \beta x^2, \gamma x^2, \delta x^2$, etc.
> III. $x^3, \alpha x^3, \beta x^3, \gamma x^3, \delta x^3$, etc.

Hay que mencionar, sin embargo, que esta investigación en el capítulo XII no concluye con este punto; la influencia del capítulo X está presente pero el análisis es aquí mucho más extenso.

De una importancia especial es el parágrafo 321, ahí retoma lo que ya había planteado en los capítulos XVIII y XIX respecto al Criterio de Euler para residuos cuadráticos. Pero es de notar que este parágrafo (321) está escrito al margen. Los resultados, por ejemplo de parágrafo 325 sientan las bases para estudios posteriores. Como ya hemos mencionado antes, estos resultados son fundamentales para la Teoría de Grupos. Ahí se considera la progresión geométrica (como ya se había hecho antes) $1, a, a^2, \ldots$. Se demuestra que no todos los residuos producto de la división de elementos de esta progresión por el divisor d son distintos; como ya se notó antes alguno de ellos (además del 1) dejará residuo igual a 1; sabemos que esa lista es el grupo generado por a (habitual abuso de notación, pues en realidad es el grupo generado por el conjunto

que contiene al elemento a). Este resultado es importante también para los siguientes capítulos del XII al XIV, pues el análisis que aquí se presenta también se encuentra en lo siguiente. Basta leer los parágrafos 390 y 393:

> 390. Dado el divisor primo $d = 6q + 1$, entonces entre los residuos cúbicos existe α de tal manera que $\alpha^{2q} - 1$ es dividido por d. A partir de esto los residuos generados de la división de la progresión geométrica $1, \alpha, \alpha^2, \ldots, \alpha^{2q}$ por el mismo divisor [serán equivalentes] con los residuos de los cubos.
>
> 393. Pero, como los residuos de las potencias $1, a, a^2, a^3$, etc. diferentes son un número $2q$, igual que los residuos de los cubos, y también el orden de ambos iniciará a partir de la unidad y tendrán los términos comunes a^3, a^6, a^9, etc. entonces las propiedades restantes serán comunes entre ellas. Así, el orden de las potencias no puede contener ningún término diferente que los de las potencias.

Mas atrás, en el parágrafo 333 empezaron las «generalizaciones». De estas, la primera es clásica en cualquier libro actual de la teoría de números (clásica): si el divisor es de la forma $4p + 1$ entonces, si α es residuo cuadrático, $-\alpha$ también lo es.

> Entonces, sea $p = 2n$ y sea $4p + 1$ el número primo que es el divisor propuesto, entonces los complementos de cada uno están contenidos entre los residuos de los cuadrados, esto es, si los residuos fueran $1, \alpha, \beta, \gamma$, etc. también serán residuos $-1, -\alpha, -\beta, -\gamma$, etc.

Recordemos que $x^2 \equiv -1 \pmod{p}$ tiene solución si y solo si

$$p \equiv 1 \pmod{4} \ldots (1),$$

observación sumamente útil, (aunque con notación y actual). El «complemento» de este resultado, está en el parágrafo 337. Por la forma en la que se llegó a esta conclusión (considerar a p de alguna forma especial (por ejemplo par) en $d = 2p+1$) se puede decir más y avanzar en la generalización: si el divisor es $4p + 1$ y p es par, ¿por qué no pensar en el divisor de la forma $8q + 1$?¿y $8q + 3$, etc? Más aún, se pueden estudiar, variando la forma de p los residuos

de la forma $12q + r, 20q + r, 60q + r, \ldots$. Esto lo hace Euler en los siguientes puntos, y resume en una tabla que se presenta en el punto 343:

Entre los residuos estará el número	si el divisor primo fuera
1	$4q + (1, 3)$
-1	$4q + 1$
2	$8q + (1, 7)$
-2	$8q + (1, 3)$
3	$12q + (1, 11)$
-3	$12q + (1, 7)$
5	$20q + (1, 9, 11, 19)$
-5	$20q + (1, 3, 7, 9)$
6	$24q + (1, 5, 19, 23)$
-6	$24q + (1, 5, 7, 11)$
7	$28q + (1, 3, 9, 19, 25, 27)$
-7	$28q + (1, 9, 11, 15, 23, 25)$
10	$40q + (1, 3, 9, 13, 27, 31, 37, 39)$
-10	$40q + (1, 7, 9, 11, 13, 19, 23, 37)$
11	$44q + (1, 9, 25, 5, 7, 37, 39, 19, 35, 43)$
-11	$44q + (1, 9, 25, 5, 37, 3, 15, 23, 27, 31)$
12	$48q + (1, 11, 13, 23, 25, 35, 37, 47)$
-12	$48q + (1, 13, 25, 37, 7, 19, 31, 43)$
14	$56q + (1, 5, 9, 13, 25, 45, 11, 31, 43, 47, 51, 55)$
-14	$56q + (1, 5, 9, 13, 25, 45, 3, 15, 19, 23, 27, 39)$
15	$60q + (1, 7, 11, 17, 43, 49, 53, 59)$
-15	$60q + (1, 17, 49, , 53, 19, 23, 31, , 47)$

De cierto modo, puede presentarse y sostenerse una argumento para establecer que el análisis del capítulo X se estaciona, filosóficamente, en este punto. Parece ser que una vez que Euler notó que, al variar la forma de la p en $d = 2p + 1$ se puede generalizar la forma del divisor tanto como se quiera. En este sentido, una vez que se estudió el caso $4p + 1$, se pregunta, ¿qué pasa si en vez de considerar $4p$ pensamos en $4np$? ¿y en vez de $1, 3, 5, \ldots$ (como se hizo cuando los divisores eran de la forma $8q + 7, 20q + 3$, etc.) fuera reemplazado por algún número impar?[2]. Por ejemplo, en el

[2]Y es fundamental notar que es necesario que el término que acompaña al número $4np$ sea impar, pues de lo contrario d no sería primo, y en el presente

parágrafo 353 considera al primo de la forma $d = 4nq \pm ii$ donde i es un número impar; en este caso los residuos son n y $-n$ (como en el caso de $4p + 1$ el 1 y -1 eran ambos residuos cuadráticos) e igualmente los son naa y $-naa$, así que siempre hay un cuadrado xx tal que $xx - aa$ sea divisible por d (es decir la congruencia sí tiene solución bajo ese módulo), y de la misma forma hay un cuadrado yy para que $yy + naa$ sea divisible por d:

> 353. Dadas estas proposiciones, sin embargo la demostración aun no es evidente. Suponiendo i un número impar y $4nq \pm ii$ un primo, para el divisor primo $4nq + ii$, donde los residuos son n y $-n$ igualmente naa y $-naa$; siempre se dará un cuadrado del modo xx, para que $xx - aa$ sea divisible por $4nq + ii$, así también un cuadrado de la forma yy, para que $yy + naa$ sea divisible por $4nq + ii$.

El siguiente parágrafo trata sobre la misma situación pero con el divisor $d = 4nq - ii$.[3] Análogamente, los resultados para suma de cuadrados también se generalizan (y se mantienen, obviamente) cuando se hace lo mismo para la forma del divisor: en el parágrafo 357, así como los posteriores inmediatos: 358, 359, 360 se plantea cuando la suma de dos cuadrados será divisible o no por elementos primos de la forma $4nq \pm ii$.

> 358. Si el divisor primo es $d = 4nq + ii$, debido a que se dan tales fórmulas $xx - naa$, y también $qxx - nyy$ divisibles por éste [divisor]; también la forma $qxx - nyy$ será divisible por d. Sin embargo, si la forma del tipo $yy + qaa$ no es divisible por d, entonces tampoco ninguna forma del tipo $qxx + nyy$ será divisible por d.
>
> 359. Incluso, aunque estas proposiciones puedan demostrarse, las restantes que hemos visto arriba aun no son resueltas. Si de 345 se diera un cuadrado que dividido por d deje un residuo positivo n, también se dará uno que arroje naa; no obstante, existe un número $4nq \pm d$, y dado un cuadrado xx que dividido entre $4nq \pm d$ deje el mismo residuo o $xx - naa$ será divisible por $4nq + d$.

capítulo y los siguientes 3 todos los resultados se hacen con la hipótesis de que el divisor d es primo (como ya habíamos mencionado antes).

[3] Aquí no hay solución...recordemos que esto es generalización directa del resultado (1), el cual es una implicación en ambos sentidos.

> 360. A saber, si $bb - naa$ fuera divisible por d, entonces el número $xx - naa$ siempre será divisible por el número primo $4nq \pm d$. Por otra parte, sea i que denota un número impar, entonces se puede exhibir que la forma $xx - naa$ es divisible por el número primo $4nq \pm dii$.

Como es de esperarse (de nuevo, dado que es generalización directa y meramente aritmética del caso $4p \pm 1$), la divisibilidad se da cuando el divisor conserva el signo $+$, y no cuando conserva el signo $-$.

La última parte de esta sección de resultados generalizados es cuando el módulo cambia y es posible preguntarnos: ¿qué pasa si el número es ahora de la forma $bb - ncc$? Pensar que el divisor puede tomar esta forma no sería algo no-natural, puesto que los divisores eran, en un inicio, de la forma $4q + 1$, los cuales sabemos dividen a la suma de dos cuadrados (de hecho, cualquier primo de esa forma es suma de dos cuadrados), así que por qué no pensar que el divisor podría tomar una forma así?

Finalmente, Euler considera la posibilidad de que n (o el número naa esté entre los residuos). Hasta ese momento se había considerado qué residuos y qué no residuos se tienen, dada la hipótesis de que algún número de cierta forma lo era o no. Ahora se dice explícitamente que no lo es, a menos que d sea de la forma $d = 4nq + \alpha$. Este es el objeto del parágafo 364, y en el siguiente, se sigue la misma línea de antes: el resultado es idéntico (y la demostración también) si se considera, en vez de α a αii, con i un número impar. De hecho, los siguientes dos puntos a tratar son las demostración de estas afirmaciones.

Así, en el parágrafo 368, se resumen estas observaciones en un solo caso general: los números de la forma $xx \pm pyy$ serán divisibles por números de la forma $4fffp + ii$, donde i es impar, y se deducen como antes: se sabe ya que tanto $aa + bb$ como $aa - bb$ son divisibles por $4fffp + ii$, así que también lo son $iiaa + iibb$ y $iiaa - iibb$.

> Se tiene el divisor primo $4fffp + ii$ e i denota un número impar, y puesto que tanto la forma $aa + bb$ como $aa - bb$ pueden ser divisibles por éste [divisor], por lo tanto también $iiaa + iibb$ y $iiaa - iibb$; de esto si se extrae de una y se suma a

la otra $(4ffp+ii)bb$, se obtendrán las fórmulas $iiaa-4ffpbb$ y $iiaa+4ffpbb$, que son divisibles por $4ffp+ii$; entre los residuos de los cuadrados estará $\pm 4ffpbb$, lo mismo que $\pm p$. Por lo tanto, los números de la forma $xx+pyy$ así como los de la forma $xx-pyy$ serán divisibles por $4ffp+ii$.

Con estas observaciones se concluye que los divisores primos tendrá la forma $4rq+\alpha$ donde α es primo con $4r$ (y menores que él), y de estos residuos solo se considera la mitad (¡como el primer parágrafo de este capítulo!) y para ellos r estará entre los residuos. Para el resultado $-r$ se tiene el resultado análogo con los divisores correspondientes.

4.2. Series de residuos

Retomemos ahora el parágrafo 285. En él se enuncian cuáles son los números cuadrados que hay que dividir por el divisor d para obtener a los residuos cuadráticos; solo con considerar a los números $1, 4, 9, \ldots, (d-2)^2, (d-1)^2$ (cuya cantidad es $d-1$) se rescata toda la información necesaria para estudiar a los residuos cuadráticos. Haciendo referencia al capítulo 6 (en donde se estudian los residuos que surgen a partir de una división de los términos de una progresión aritmética), Euler propone la siguiente progresión aritmética a considerar:

$$a, a+b, a+2b, a+3b, \ldots$$

Si en vez de considerar a la serie $1, 4, 9, \ldots, (d-2)^2, (d-1)^2$ para estudiar a los residuos cuadráticos, estudiáramos a la serie $-\frac{1}{2}(d-1)^2, \ldots, 0, 1, 4, \ldots, \frac{1}{2}(d-1)^2$, los resultados serían idénticos (cabe notar que esto se puede hacer sin ajustar el caso donde d es un número par pues ese es descartado inmediatamente), y de esta forma se tendría una notación completamente simétrica. Sin embargo Euler en el *Tractatus* decide mantener la misma estructura en la series que mantuvo en el capítulo 6. Más aún, en el capítulo 7 (*Sobre los residuos que surgen a partir de la división de los*

términos de una progresión aritmética) la serie que se considera es

$$a, ab, ab^2, ab^3, \ldots$$

Debemos resaltar dos cosas importantes sobre la serie que considera Euler: en primer lugar, la serie de residuos en cuestión empieza en 0 termina en $(d-1)^2$. Es inmediato que el 0 es un residuo cuadrático y esto es independiente del divisor d, y también que d^2 deje el mismo residuo que 0. Esto se debe a que, por hipótesis, d es un número primo, y no hay ningún múltiplo de d entre 1 y $d-1$, así que estos quedan excluidos automáticamente, y por tanto, de la serie de números enteros que hay que considerar, al menos todos los múltiplos de d quedan fuera. En segundo lugar, en los capítulos antes citados (VI y VII) las progresiones aritméticas y geométricas se extienden indefinidamente, mientras que la correspondiente para residuos cuadráticos se estaciona en $d-1$. Esto, como ya hemos explicado, se justifica por el parágrafo anterior a este, el 284.

Desde el punto de vista del autor, hay dos razones más por las que prefiere desarrollar la exposición con la serie que da y no con alguna equivalente: recordemos que este trabajo fue el primero de su clase y no fue terminado ni publicado por Euler en vida, de modo que la versión que se tiene es la más básica (en cuestión de edición) que se tiene. Por ello no sabemos si Euler consideró la serie $-\frac{1}{2}(d-1)^2, \ldots, 0, 1, 4, \ldots, \frac{1}{2}(d-1)^2$ o no. Más aún, cuando contamos siempre lo hacemos empezando desde el 1 o el 0, nunca empezamos a contar empezando con un número negativo, y al pensar lo hacemos de la misma manera, por lo cual es natural que en una primera versión la serie empiece desde el 1, y no desde $-\frac{1}{2}(d-1)^2$.

Finalmente, y como se ha mencionado antes, el capítulo X sirve como base para los capítulos siguientes del mismo bloque. Dado que este capítulo respeta la exposición de los capítulos V y VI, además de mantener dichos números como los elegidos para estudiar a los residuos cuadráticos, en los capítulos siguientes sobre residuos cúbicos, bicuadráticos y sursólido siguen la misma lógica, los números que se consideran son los mismos respetando la potencia

correspondiente, tanto para respetar el formato del estudio de los residuos y las series, así como por los argumentos anteriores.

Capítulo 5

Formas binarias

5.1. El estudio de dos formas cuadráticas binarias

La última parte por estudiar del *Tractatus* se compone de dos capítulos: El capítulo XV «Sobre los divisores de los números de la forma $xx + yy$» y el XVI «Sobre los divisores de los números de la forma $xx + 2yy$». Estos son los capítulos mas cortos de la obra, y son ambos precursores del estudio de las formas cuadráticas binarias en la Teoría de los Números.

El primer capítulo de esta parte empieza con una pregunta conocida desde 1632 (planteada por Albert Girard y demostrada por primera vez por Fermat en 1654): ¿cuándo es $xx+yy$ un número primo? Es claro que el caso cuando dicha suma sea igual a 2 siempre es posible, y este caso es por lo tanto descartado inmediatamente por Euler (del mismo modo que durante la sección anterior de la tesis, todos los casos estudiados cuando el divisor es un primo, el cual será impar, pues el 2 no presenta mayor dificultad). Es interesante notar que Euler no demuestra este problema, sino que explica que todos los números primos $xx + yy$ son de la forma $4n + 1$, y ninguno de la forma $4n - 1$ puede ser suma de dos cuadrados. Sin embargo, hay que decir que esta implicación si es inmediata, pues los cuadrados son solo de la forma $4n$ o $4n + 1$,

así que al sumar dos de ellos solo se obtendrán números de la forma $4n, 4n+1$ o $4n+2$, pero no $4n-1$. El caso $4n+2$ es descartado pues, recordemos, Euler se concentra específicamente en estudiar los casos para los primos impares. La implicación recíproca se contesta en los siguientes puntos y se cita expresamente en el parágrafo 562.

A continuación en el capítulo XV se estudian las propiedades conocidas dentro de la escaleta general de trabajo del *Tractatus*: la aritmética entre los objetos. En primer lugar, obtenemos el siguiente resultado sobre el producto de dos números que son suma de dos cuadrados:

> 545. Si la suma de dos cuadrados se multiplica por la suma de otros dos cuadrados, el producto $(aa+bb)(cc+dd)$ será también la suma de dos cuadrados, que es iguala a $(ac \pm bd)^2 + (ad \mp bc)^2$, lo cual puede suceder solo con la alternancia del signo doble.

Y enseguida la proposición inversa:

> 546. Ahora se enuncia una proposición inversa: si la suma de dos cuadrados $pp+qq$ es divisible entre la suma de otros dos cuadrados $aa+bb$, entonces [esta] también sería la suma de dos cuadrados. La veracidad de la [afirmación] no se puede alcanzar solo de esto, se requiere una demostración especial.

Más aún, las cuestiones de divisibilidad quedan expuestas y son estudiadas en los siguientes parágrafos:

> 547. [...] primero enuncio que la forma $pp+qq$ es divisible por $aa+bb$. Cualesquiera que sean los números p y q, siempre pueden ser reducidos a números menores que $aa+bb$, para ser como $\frac{1}{2}(aa+bb)$, puesto que si $pp+qq$ es divisible entre $aa+bb$, también
>
> $$(\pm\alpha(aa+bb) \pm p)^2 + (\pm\beta(aa \pm q)^2$$
>
> se vuelve divisible.

Este es el resultado más amplio de este capítulo, y su demostración termina en el parágafo 556. En el siguiente Euler continúa con la investigación preguntando si los divisores de los números de la forma $pp + qq$ son todos suma de dos cuadrados. Es claro que para este momento, el número $pp + qq$ no es supuesto un número primo. Por medio de esta investigación se obtiene la verificación de la implicación recíproca sobre el resultado citado anteriormente de Albert Girard. Con la investigación de estas preguntas se conoce la forma del cociente resultado de la división, como lo observamos en los siguientes extractos del *Tractatus* en los parágrafos 562 y 564:

> 562. Así, propuesto cualquier número primo de la forma $4n + 1$, que entre sus residuo cuadráticos esté -1 o $4n$, siempre podrá ser exhibido como suma de dos cuadrados divisible por él; de aquí se sigue que todos los números de la forma $4n + 1$ son la suma de dos cuadrados.

> 564. Sin embargo, se requiere una demostración más breve, con la cual se pruebe que si la suma de dos cuadrados $pp + qq$ fuera divisible por la suma de otros dos cuadrados $aa + bb$, el cociente también necesariamente será la suma de dos cuadrados. Con el razonamiento siguiente intentaremos determinar esto.

El último resultado del capítulo XV responde a una pregunta natural sobre la posibilidad de escribir a un número (primo o no) como la suma de dos cuadrados: ¿Es esta representación única? Es claro que $2 = 1^2 + 1^2$ y que esta es la única forma de poder escribir a 2 como suma de dos cuadrados, pero como se mencionó desde el principio, este caso es omitido pues no presenta dificultad. El parágrafo 570 demuestra que la forma de escribir a un número como suma de dos cuadrados es única si el número en cuestión es un primo, y la demostración es absolutamente algebraica:

> 570. Si cualquier número N que tenga dos maneras de ser representado como suma de dos cuadrados, es decir
>
> $$N = aa + bb = cc + dd,$$

entonces no es primo. Puesto que $aa-cc=dd-bb$, se tendrá que $d+b=\frac{m(a+c)}{n}$ y $d-b=\frac{n(a-c)}{m}$, y por lo tanto $b=\frac{m(a+c)}{2n}-\frac{n(a-c)}{2m}$; entonces $N=aa+bb=\frac{(mm+nn)}{4mmnn}(nn(a-c)^2+mm((a+c)^2)=\frac{(mm+nn)}{4mm}((a-c)^2+(b+d)^2)$, en donde no puede eliminarse el factor del denominador.

En el capítulo XVI del *Tractatus* encontramos la relación correspondiente para el caso $xx+2yy$. Como sucedió en los capítulos X al XIV, los resultados que se obtenían con números primos de la forma $4n+1$ corresponden a aquellos de la forma $8n+1, 8n+3$, y los que son excluidos son los que son de la forma $8n+5, 8n+7$ y todos los números pares, como observamos a continuación:

> 574. Así, todos los números de la forma $xx+2yy$, donde x y y son primos entre sí; entonces ambos no son pares, y si fueran impares, pertenecerán a la forma $8n+1$, o a la [forma] $8n+3$; pero si estos números son pares, entonces o son de la forma $2(8n+1)$, o de $2(8n+3)$, y en el caso posterior sus mitades, es decir, $2zz+yy$ son también números de la forma $xx+2yy$.

Además de esto, encontramos en el capítulo XVI la proposición relacionada con aquella sobre el producto de dos números suma de dos cuadrados, y la demostración análoga para este caso, con el mismo formato:

> 576. El producto de dos números de esta forma está contenido en la misma forma, esto es $(aa+2bb)(cc+2dd)=(ac\pm 2bd)^2+2(ad\mp bc)^2$, de aquí es evidente que tal producto está de dos maneras en la forma [señalada].

El siguiente resultado es también el más largo, el más importante y el centro del capítulo XVI. La demostración de este resultado abarca la mayor parte del capítulo.

> 584. Por lo cual, si $pp+2qq$ puede dividirse entre el número $\mathfrak{U}$, que queda excluido de la forma $xx+2yy$. Entonces, el cociente, si es primo no será de esta forma; o si es compuesto, entonces tendrá un factor que no será de esta forma.

y finalmente concluye:

> 587. Veremos también si $pp+2qq$ puede dividirse entre un número $\mathfrak{U}$ que no es de la forma $xx+2yy$. Si esto es posible pasaría que $p < \frac{1}{2}\mathfrak{U}$ y $q < \frac{1}{2}\mathfrak{U}$, de donde $pp+2qq < \frac{3}{4}\mathfrak{UU}$, y el cociente $< \frac{3}{4}\mathfrak{U}$, el cual, él mismo no es un número de la forma $xx+2yy$, o tendría un factor $\mathfrak{B}$, el cual como también sería factor de $pp+2qq$; así, el más pequeño de tales números $\mathfrak{B}$ podría ser asignado como el divisor de cualquier forma $xx+2yy$, lo cual como no es posible, entonces los números $pp+2qq$ no poseen ningún divisor primo que no sea de la forma $xx+2yy$.

Finalmente tenemos la caracterización de Euler de los divisores primos de los divisores de los números de la forma p^2+2q^2, y este es el inicio de un estudio muy amplio, pero en el *Tractatus* ya no lo encontramos.

5.2. Hacia la forma general

Como se observa, ambos capítulos son muy parecidos entre ellos, tanto en los resultados que se estudian, como en la forma de presentarlos. En general, en ambos se estudia en gran medida que números pueden ser representados por alguna de las formas $xx+yy$ o $xx+2yy$, qué forma tiene el producto de éstas, cuándo un número primo impar puede ser representado por alguna de ellas y cómo son los divisores y los cocientes resultados de la división de estos números.

Ambos capítulos son casos particulares del estudio de las formas cuadráticas binarias; es decir, expresiones de la forma x^2+ny^2. Estas expresiones en forma más general eran conocidas por Euler, lo cual se deduce de la correspondencia que tuvo con Goldbach en el año 1742.[1] Incluso, Euler reunió estos resultados en un artículo que publicó en 1751 con el nombre *Theoremata circa divisores numerorum in hac forma paa* $\pm$ *qbb*. Los teoremas que se incluyen

[1] Ver [Euler-Goldbach 1965, pág. 116-118].

en el artículo son parecidos y hasta podemos argumentar que inductivos: así como sucedió con los últimos capítulos, y fuertemente con los capítulos del X al XIV, el método que usó para un caso fue adaptado para los siguientes hasta donde fue posible. Para muestra, algunas de las conjeturas y teoremas que Euler enuncia en el citado artículo son (expresadas en notación de Legendre):

$$\left(\frac{-3}{p}\right) = 1 \Leftrightarrow p \equiv 1, 7 \pmod{12}$$

$$\left(\frac{3}{p}\right) = 1 \Leftrightarrow p \equiv \pm 1 \pmod{12}$$

$$\left(\frac{-5}{p}\right) = 1 \Leftrightarrow p \equiv 1, 3, 7, 9 \pmod{20}$$

$$\left(\frac{5}{p}\right) = 1 \Leftrightarrow p \equiv \pm 1, \pm 11 \pmod{20}$$

$$\left(\frac{-7}{p}\right) = 1 \Leftrightarrow p \equiv 1, 9, 11, 15, 23, 25 \pmod{28}$$

$$\left(\frac{7}{p}\right) = 1 \Leftrightarrow p \equiv \pm 1, \pm 3, \pm 5 \pmod{28}$$

donde p es un primo impar tal que $p \nmid n$.

Como mencionamos anteriormente, los residuos que dejan los números al ser divididos por otro pueden ser positivos o negativos según el estudio de Euler en esta obra, pero la teoría de congruencias nos permite avanzar más rápido entre el 11 y el -9 módulo 20, ya que podemos ver que $11 \equiv -9 \pmod{20}, 3 \equiv -25 \pmod{28}$ y obtenemos

$$\left(\frac{3}{p}\right) = 1 \Leftrightarrow p \equiv \pm 1, \pmod{12}$$

$$\left(\frac{5}{p}\right) = 1 \Leftrightarrow p \equiv \pm 1, \pm 9 \pmod{20}$$

$$\left(\frac{7}{p}\right) = 1 \Leftrightarrow p \equiv \pm 1, \pm 25, \pm 9 \pmod{28},$$

donde todos los números son cuadrados. Es aventurado, pero no descabellado, pensar que si Euler hubiera tenido esta notación entonces hubiera llegado al estudio de la Reciprocidad Cuadrátrica mucho más rápido y de manera más formal.

Estos estudios fueron la base de la que Gauss, Lagrange y Legendre (entre otros muchos grandes matemáticos) partieron para el estudio profundo de estos resultados. Las aplicaciones a las que nos conduce el desarrollo y estudio íntegro de esta rama de la Teoría de los Números son muy diversas y muy profundas; por ejemplo la reciprocidad cuadrática. Recordemos brevemente la discusión de la divisibilidad de estas expresiones:

$$\forall\ (x,y)=1, \exists\ p \text{ primo tal que } p \mid x^2+y^2 \Leftrightarrow p \equiv 1 \pmod 4$$

$$\forall\ (x,y)=1, \exists\ p \text{ primo tal que } p \mid x^2+2y^2 \Leftrightarrow p \equiv 1,3 \pmod 8$$

Recordemos la notación del símbolo de Lagrange:

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

y 0 si $p \mid a$.

Con esta notación esto es equivalente a

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

y

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$$

respectivamente, por lo que concluimos lo que mencionabamos párrafos arriba: que Euler estaba trabajando, en el *Tractatus* con dos casos especiales de la reciprocidad cuadrática. Un caso general de esta observación se puede presentar en el siguiente

Teorema. Sea n un entero distinto de 0 y sea p un primo impar que no divide a n. Entonces se tiene

$$p \mid x^2 + ny^2, (x, y) = 1 \Leftrightarrow \left(\frac{-n}{p}\right) = 1$$

Demostración: Presentaremos la demostración del teorema con técnicas modernas, en primer lugar porque hacen la tarea mucho más sencilla y más corta, y en segundo lugar, porque el teorema anterior no se enceutra en el *Tractatus*, por lo que es imposible anexar una demostración fiel. Si $x^2+ny^2 \equiv 0 \pmod{p}$ y $(x, y) = 1$ entonces $(y, p) = 1$ y por tanto tiene un inverso multiplicativo módulo p, sea este s. Entonces, $(xs)^2 \equiv x^2s^2 \equiv -ny^2s^2 \equiv -n \pmod{p}$, que es lo que se busca. El regreso es completamente análogo. □

La demostración anterior es bastante elemental en sí misma, pues solo considera el inverso de un número módulo p (todo elemento no nulo en $\mathbb{Z}_p$ tiene uno al ser este un campo, el punto es mostrar que y es no nulo en este campo, lo cual se logra mostrando que no es múltiplo de p). Sin embargo, la facilidad de esta demostración es consecuencia de la notación de Lagrange y la notación de las congruencias, además de los resultados del símbolo de Legendre y el criterio de Euler. Debemos tomar en cuenta, sin embargo, que esta demostración y esta técnica no era fácil ni elemental para Euler; fue él quien empezó a desarrollar toda la teoría, y estudiar a los residuos cuadráticos como el objeto central que contenía la información fundamental.

Tomando en cuenta este método, esto se extiende hacia la reciprocidad cúbica (en $\mathbb{Z}[\omega]$)) y bicuadrática ($\mathbb{Z}[i)]$); más aún, haciendo uso de matemáticas modernas, el estudio de los primos y las expresiones de la forma $x^2 + ny^2$ y la teoría de campos, funciones elípticas, curvas elípticas y la Reciprocidad de Shimura, entre otras, se complementan una a otra. Esto, sin embargo, queda fuera del objetivo del presente trabajo, por lo que solo lo mencionamos como referencia de la importancia y trascendencia del trabajo y de las ideas en él.

Como ha sido mencionado repetidamente durante este texto, los resultados que aquí se juntan fueron novedosos en su mayoría, y dado que esta es una obra póstuma, y sabiendo que hubo más

resultados que Euler desarrolló pero que no fueron publicados en ésta obra, podemos conjeturar que él no tuvo suficiente tiempo de vida para incorporar al *Tractatus* los resultados que desarrolló sobre esta área, los cuales comunicó a Goldbach en la antes citada correspondencia.

Apéndice A

Demostración de la Proposición 36 del Libro IX de «Los *Elementos*» de Euclides.

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.

Sean los números $1, A, B, G$ y D en proporción duplicada siendo su conjunto E un número primo y sea ZH el producto de E por DW. Digo que ZH es un número perfecto.

A_____ B_____ G_____ D_____ E_____

Z_____H

Tómense tantos números E, TK, L, M como A, B, G, D en proporción duplicada empezando por E y entonces será A a D como E a M y por tanto el producto de E por D será igual al de A por M, pero, el producto de E por D es ZH; luego el de A por M será también ZH y por consiguiente M mide a ZH según A y como

A es la díada, ZH es doble de M y por estar M, L, TK y E en proporción duplicada, también, lo estarán E, TK, L, M y ZH.

E_____

T_____K

L_____

M_____

Z_____H

Ahora bien, si del segundo número TK y del último ZH quitamos los números TN y ZO, ambos iguales a E, el exceso del segundo (TK) será al primero (E) como el exceso del último (ZH) al conjunto de los anteriores (M, L, TK, E) y por tanto NK es a E como OH al conjunto M, L, TK, E y como NK es igual a E será OH igual al conjunto M, L, TK, E; y por ser ZO igual a E y E igual a $1, A, B, G, D$ el conjunto ZH es igual a $1, E, TK, L, M$ y está medido por ellos.

T_____N_____K

Z_____

O_____H

Digo además que ZH no puede estar medido por ningún otro número excepto estos, porque si fuera posible que algún número P midiera a ZH según Q no siendo P ninguno de los números A, B, G, D, E, TK, L, M el producto de Q por P sería ZH.

Z_____H

P_____

Q_____

Pero el producto de E por D es también ZH; luego E es a Q como P a D y puesto que $1, A, B, G, D$ están en proporción continua, D no puede ser medido por ningún número excepto A, B, G, ninguno de los cuales es P por hipótesis, luego P no mide a D y por ser P a D como E a Q tampoco E mide a Q pero E es primo y un número primo es primo con cualquier número que no sea múltiplo suyo, luego E y Q son primos entres sí y son los menores y E es a Q como P a D; luego E mide a P el mismo número de veces que Q a D y como D no esta medido por ningún número excepto A, B, G tiene que ser Q uno de estos. Sea B y como B, G, D son

tantos como E, TK, L empezando por E y estos E, TK, L tienen la misma razón con B, G, D será B a D como E a L y, por tanto, el producto de B por L es igual al de D por E, pero este producto de D por E es igual al de Q por P; luego el producto de Q por P es igual al de B por L y por consiguiente Q es a B como L a P y por ser Q igual a B, es L igual a P, lo cual es imposible porque por hipótesis P no es ninguno de esos números; luego ningún número mide a ZH excepto $1, A, B, G, D, E, TK, L, M$ y como ZH es igual al conjunto de estos números, ZH es un número perfecto.

Apéndice B

Extracto de la carta de Euler a Goldbach del 28 de agosto de 1742.

1. Si x y y son primos entre sí, la fórmula $x^2 + y^2$ no tiene divisores primos distintos de los de la forma $4n+1$, y además estos números primos son todos de la forma $u^2 + v^2$.

2. Si x y y son primos entre sí, la fórmula $2x^2 + y^2$ no tiene divisores primos impares distintos a los de la forma $8n + 1$ o bien $8n + 3$, y además estos factores primos también son de la forma $2u^2 + v^2$.

3. La fórmula $3x^2 + y^2$ en donde x y y son primos entre sí, no tiene divisores primos distintos a los del tipo $12n + 1$ y $12n + 7$, es decir de la forma $6n + 1$, y además estos primos también son de la forma $3u^2 + v^2$.

4. La fórmula $5x^2 + y^2$ en donde x y y son primos entre sí, no tiene divisores primos distintos a los del tipo $20n + 1, 20n + 3, 20n + 9$ y $20n + 7$; y cualquier número primo que se pueda expresar en alguna de estas formas, es también del tipo $5u^2 + v^2$.

5. La fórmula $6x^2 + y^2$ no tiene divisores primos impares distintos a los del tipo $24n + 1, 24n + 5, 24n + 7$ y $24n + 11$, y cualquier número primo que se pueda escribir de cualquiera de estas maneras, es también de la forma $6u^2 + v^2$.

6. La fórmula $7x^2 + y^2$, no tiene divisores primos distintos a los del tipo $28n + 1, 28n + 9, 28n + 11, 28n + 15, 28n + 23$ y $28n + 25$. Es decir, de la forma $14n + 1, 14n + 9$ y $14n + 11$, y cualquier número primo que se pueda escribir en una de estas formas también es un número del tipo $7u^2 + v^2$.

7. Si un número primo de la forma $4Pn + s$, es un divisor de la fórmula $Px^2 + y^2$, entonces los otros primos que dividen a $Px^2 + y^2$ son de la forma $4Pn + s^k$ y además estos divisores son de la forma $Pu^2 + v^2$.

8. Si dos números primos de los tipo $4Pn + s$ y $4Pn + t$, respectivamente, son divisores de la fórmula $Px^2 + y^2$, entonces cualquier número primo de la forma $4Pn + s^k t^j$, es también un número de la forma $Pu^2 + v^2$.

9. Todos los factores primos de la fórmula $x^2 - y^2$ (con x y y primos relativos) son de la forma $4n \mp 1$.

10. Todos los divisores primos de la fórmula $2x^2 - y^2$, son del tipo $8n \mp 1$.

11. Todos los divisores primos de la fórmula $3x^2 - y^2$ son del tipo $12n \mp 1$.

12. Todos los divisores primos de la fórmula $5x^2 - y^2$ son del tipo de la forma $20n \mp 1$ o de la forma $20n \mp 9$.

*Traducción de Iván Castro Chadid.

Bibliografía

[1] Aristóteles. 2000. *Metafísica*. Barcelona: Ed. Gredos.

[2] Descartes, Rene. 1908. Œuvres. volumen 10, sección: «De Partibus Aliquotis Numerorum». (edición de Chales Adam y Paul Tannery) páginas 300 y 301.

[3] Dickson, L.E. (1919). *History of the theory of numbers*, Vol. II. Carnegie Institution of Washington.

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

[5] Euler, Leonhard. 1738. (E26). *Observationes de theoremate quodam Fermatiano aliisque ad numeros primos spectantibus* (Observations on a theorem of Fermat and others on looking at prime numbers). Commentarii academiae scientiarum Petropolitanae 6: 103-107. (Traducción de Jordan Bell).

[6] Euler, Leonhard. 1750. (E100). *De numeris amicabilibus* (On Amicable Numbers). Opuscula varii argumenti 2: 23-107. (Traducción de Jordan Bell).

[7] Euler, Leonhard. 1750. (E134). *Theoremata circa Divisores Numerorum* (Theorems on Divisors of Numbers). Commentarii academiae scientiarum Petropolitanae 1. pp. 20–48.

[8] Euler, Leonhard. 1751 (E164). *Theoremata circa divisores numerorum in hac forma paa±qbb contentorum* (Theorems about

the divisors of numbers contained in the form $paa \pm qbb$), Commentarii academiae scientiarum Petropolitanae 14 (1751), 151–181, (Traducción de Jordan Bell).

[9] Euler, Leonhard. 1760 (E244). *Demonstratio theorematis circa ordinem in summis divisorum observatum* (A demonstration of a theorem on the order observed in the sums of divisors). Novi Commentarii Academiae scientiarum Imperialis Petropolitanae 5, 75–83.

[10] Euler, Leonhard. 1761. (E262). *Theoremata circa residua ex divisione potestatum relicta* (Theorems on residues obtained by the division of powers). Novi Commentarii academiae scientiarum Petropolitanae 7: 49-82. (Traducción de Jordan Bell).

[11] Euler, Leonhard. 1763. (E271). *Theoremata arithmetica nova methodo demonstrata.* Novi Commentarii academiae scientiarum Petropolitanae 8: 74-104.

[12] Euler, Leonhard. (1783) (E541). *Evolutio producti infiniti* $(1-x)(1-xx)(1-x^3)(1-x^4)(1-x^5)(1-x^6)$ *etc. in seriem simplicem* (The expansion of the infinite product $(1-x)(1-xx)(1-x^3)(1-x^4)(1-x^5)(1-x^6)$ etc. into a single series). Acta Academiae Scientarum Imperialis Petropolitinae, no. I, 47–55. (Traducción de Jordan Bell).

[13] Euler, Leonhard. 1783 (E542). *De mirabilis proprietatibus numerorum pentagonalium* (On the remarkable properties of the pentagonal numbers). Acta Academiae Scientarum Imperialis Petropolitinae 4 (1783), no. 1, 56–75. (Traducción de Jordan Bell).

[14] Euler, Leonhard. 1849. (E792). *Tractatus de numerorum doctrina capita sedecim, quae supersunt.* Commentationes arithmeticae 2: 503-575.

[15] Euler, L.,& Goldbach, 1965. *C. Leonhard Eulerund Christian Goldbach: Briefwechsel 1729-1764.* Berlin: Akademie-Verlag.

[16] Euler, Leonhard, 1972. *Elements of algebra*. Traducción de John Hewlett. New York: Springer Verlag.

[17] Euler, Leonhard. 1988. *Introduction in analysin infinitorum* (Introduction to analysis of the infinite). Traducción de John D. Blanton. New York: Springer Verlag.

[18] Gauss, Carl Friedrich. 1995. [1801] (versión en español). *Disquisitiones arithmeticae*, traducido por Hugo Barrantes, Michael Joseph y Ángel Ruiz, San José, Costa Rica: Centro de Investigaciones Matemáticas y Meta-Matemáticas (CIMM), Universidad de Costa Rica.

[19] Gauss, Carl Friedrich (1986) [1801] (versión en inglés). *Disquisitiones arithmeticae*, traducido por Arthur A. Clarke, Springer-Verlag.

[20] Koshy, Thomas, 2007. *Elementary Number Theory with Applications*. Estados Unidos de América: Academic Press, Segunda Edición.

[21] Niven, Ivan, Herbert S. Zuckerman y Hugh L. Montgomery. *An Introduction to the Theory of Numbers*, New Delhi: Wiley, Quinta Edición, 1991.

[22] Schooten, Francisci. 1657. *Exercitationum mathematicarum*. Lugd Batau. Ex officina Johannis Elsevirii.